如何让尖刺球屈服以及更快的最近向量问题算法

Divesh Aggarwal AdityaMorolia 新加坡国立大学量子技术中心，新加坡
dcsdiva@nus.edu.sg morolia@u.nus.edu

arXiv:2611.32605v1 [cs.DS] 24 Nov 2026

2026年11月25日

摘要

我们给出了首个在 ℓ_p 范数下求解精确最近向量问题（CVP）的单指数时间算法，适用于 $1 < p < 2$。此前，这类算法仅在欧几里得范数下已知，即 ℓ_2；或者需要额外保证目标向量接近格。运用类似技术，我们还找到了一个在 ℓ_p 范数下求最短非零向量的算法，其运行时间为 $2^{O(n)}$，适用于每个 $p \in [1, 2)$，且指数中的常数不依赖于 p；该算法改进了 ℓ_p 范数下最短向量问题的当前最佳算法。

自 2010 年 Micciancio 和 Voulgaris 为欧几里得范数解决了这一问题以来，在 $p \neq 2$ 的 ℓ_p 范数下寻找一种用于最近向量问题的单指数时间算法一直悬而未决。

我们的一个关键思路是，对于 $0 < p \leq 2$，函数 $z \mapsto e^{-|z|^p}$ 是高斯分布的混合，因此格平移上的 ℓ_p 离散高斯分布是具有随机对角宽度的欧几里得离散高斯分布的混合。我们的算法利用这一点，将 ℓ_p 问题归约为随机缩放格上的欧几里得最近向量问题。

目录

1 引言 **1**

1.1 我们的结果 .3 1.2 技术概述 .5 1.3 更多相关工作 .9

2 预备知识 **10**

2.1 记号与计算模型 .10 2.2 稳定分布 .12 2.3 格 .14 2.4 计算问题与算法。 .15

3 离散高斯混合 **16**

4 $2^{O(n)}$ **最近向量问题算法**最近向量问题$_p$ **18**

A $2^{O(k)}$ **最短向量问题算法**最短向量问题$_p$ **35**

1 引言

格 $\mathcal{L} \subseteq \mathbb{R}^n$ 是由 k 个线性无关向量 $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k \in \mathbb{R}^n$ 的所有整数线性组合构成的集合。我们记作

$$\mathcal{L}(B) := \left\{ B\boldsymbol{z} : \boldsymbol{z} \in \mathbb{Z}^k \right\}$$

对于由基 B 生成的格，其中 $\boldsymbol{b}_i$ 是矩阵的第 i 列。我们称 k 为 $\mathcal{L}$ 的秩，称 n 为其维数；如果 $k = n$，则称 $\mathcal{L}$ 具有满秩。给定一个基和一个范数，最短向量问题 （SVP）要求求出 $\mathcal{L}$ 中的最短非零向量；而最近向量问题（CVP）则在另外给定一个目标向量 $\boldsymbol{t} \in \mathbb{R}^n$ 的情况下，要求求出 $\mathcal{L}$ 中距离 $\boldsymbol{t}$ 最近的向量。在本文中，我们研究 ℓ_p 范数下求解这些问题的算法。对于 $1 \le p \le \infty$ 和 $\boldsymbol{x} \in \mathbb{R}^n$， $\boldsymbol{x}$ 的 ℓ_p 范数为

$$\|\boldsymbol{x}\|_p = \left(\sum_j |x_j|^p \right)^{1/p},$$

当向量的长度在 ℓ_p 范数下度量时，我们记作 SVP$_p$ 和 CVP$_p$ 。

这些问题是数的算法几何中的基础问题 [MG02、Reg04b、Eis10、Ben23]。求解这些问题的精确算法和近似算法被用于多项式因式分解和基约化[LLL82、Bab86、Sch87、GN08、ALNS20、AEPS25] ，以及通信系统中的最近点译码[AEVZ02]。整数规划是一类尤为重要的离散优化问题，也可以作为格问题进行研究 [Len83、Kan83、Kan87、FT87、Dad12、RR23]。在 ℓ_2 范数下，它们在现代密码学中极为重要。其被猜想的困难性是基于格的密码学的基础，这依托于 Ajtai 和 Regev 提出的最坏情况到平均情况归约及其后续工作 [Ajt96、AD97、Mic04、MR07、Reg09、Pei09、GPV08、MP12、BLP+13、LPR13]；参见综述 [MR09、Pei16]。基于格的密钥封装如今已成为美国国家标准与技术研究院（NIST）标准 [Nat24], ，而最佳精确算法的运行时间决定了其实用参数。

困难性结果。对于每个 ℓ_p 范数 [vEB81]，精确最近向量问题都是 NP-困难的；近似在常数因子下是困难的 [ABSS97] ，在 $n^{c/\log\log n}$ [DKRS03], 因子下也是困难的，并且在允许预处理的情况下仍然困难 [Mic01a, FM04, Reg04a, AKKV11, KPV12]；关于最短向量问题，参见 [Ajt98, CN99, Mic01b, Kho05, HR12, Mic12, BP23]；而对于 ℓ_∞，参见 [Din02]。一份近期的工业界手稿宣布了一种确定性归约：对于每个固定的有理 $n^{1/(200p)}$困难性， $p \ge 1$ [Ope26] 均成立。另一方面，欧几里得间隙最近向量问题在因子 $O(\sqrt{n}/\log n)$ [GG00] 下属于 coAM，在因子 $O(\sqrt{n})$ [AR05], 下属于 NP，并且 Peikert 将此类限制扩展到了 ℓ_p 范数 [Pei08]。精细化下界明确体现了维数的作用。对于任意 $\rho > 0$ 以及任意有限的 $p \notin 2\mathbb{Z}$，在强指数时间假设（SETH）下，精确最近向量问题$_p$ 需要 $2^{(1-\rho)n}$ 时间；在间隙强指数时间假设（Gap-SETH）下，还存在常数因子对应结果 [BGS17, ABGS21]；对于任意有限的 p [，在指数时间假设（ETH）下，常数因子最近向量问题$_p$ 需要 $2^{\Omega(n)}$ 时间 26], AGMZ [另见 26]HKW$_p$ 。对于最短向量问题，Aggarwal 和 Stephens-Davidowitz 证明，在间隙指数时间假设（Gap-ETH）下，SVP$_p$ 不存在 $2^{o(n)}$-时间算法（适用于 $p > 2$ ），并给出了针对大p的基于 SETH 的下界；而对于 $1 \le p \le 2$ ，其下界还需要关于具有指数接吻数的格的额外假设 [AS18a]；关于后续改进，参见 [BPT22, AGMZ26] ，关于相关的精细化结果，参见 [AC21, ABB+23]。对于带有 $1 \le p \le 2$ 的 SVP$_p$ ，指数下界的证据因此仍然是有条件的。

欧几里得范数下的算法。这些问题在欧几里得（ℓ_2）范数下研究得最为充分。LLL 的多项式时间基约化算法 [LLL82]可将这两个问题的近似因子控制在

指数级或略低于指数级（见 [Bab86, Sch87, GN08, ALNS20, AEPS25]）。这些问题的精确版本算法可分为四类。由 Pohst、Kannan 和 Fincke 提出的枚举法 [Poh81, Kan83, FP85, Kan87], , 经 Helfrich [Hel85]改进，并由 Hanrot 和 Stephens-Davidowitz 作出精确分析 ´HS07], , 可在多项式空间内以 $n^{n/(2e)+o(n)}$ 的时间求解 SVP，以 $n^{n/2+o(n)}$ 的时间求解最近向量问题；Micciancio 和 Walter 对其进行了更精细的分析 [MW15]。Ajtai、Kumar 和 Sivakumar 提出的格筛法 [AKS01, AKS02], , 首次给出了用于 SVP 和近似CVP 的随机 $2^{O(n)}$时间算法；其指数中的常数（可证明正确）经过分析并得到改进 [NV08, MV10, PS09]。Micciancio 和 Voulgaris [MV13]通过计算 Voronoi 胞，给出了用于精确最近向量问题、进而用于大多数其他格问题的确定性 $2^{2n+o(n)}$时间算法；关于 Voronoi 单元的后续研究，参见 [BD15, HRS20]。Aggarwal、Dadush、Regev 和 Stephens-Davidowitz [ADRS15] 通过对离散高斯分布进行采样，以 $2^{n+o(n)}$ 的时间求解 SVP；Aggarwal、Dadush 和 Stephens-Davidowitz [ADS15] 则在欧几里得范数下，以相同的时间复杂度求解精确最近向量问题；Aggarwal 和 Stephens-Davidowitz 简化了这两种算法[AS18b]。近期研究进一步改进了欧几里得最短向量问题和离散高斯采样[GFH26b, GFH26a, Hha26b, Hha26a, Kim26]。我们的算法将[ADRS15, ADS15, MV13] 中的精确欧几里得算法作为黑盒使用。

其他范数的算法 ℓ_p 。历史上，发现适用于欧几里得范数的算法要容易得多，这或许并非巧合。ℓ_2 范数可以嵌入 ℓ_p 范数中，且畸变任意接近 1，因此最近向量问题$_2$ 和最短向量问题$_2$ 可归约为相应的 ℓ_p 类似问题，近似因子只需付出 $1+\varepsilon$ [RR06]倍的代价；而上述精细化下界恰恰在 $p \notin 2\mathbb{Z}$[BGS17、ABGS21], 中最强，这一范围包含了 $1 < p < 2$ 本文研究的区间。ℓ_1 范数尤其值得关注，因为整数规划可归约为精确最近向量问题$_1$ （见第 1.3 节）。

对于最短向量问题，单指数障碍早已被突破。Ajtai、Kumar 和 Sivakumar 提出的筛法可推广至任意 ℓ_p 范数，Bl¨omer 和 Naewe [BN09] 以及 Arvind 和 Joglekar [AJ08],证明了这一点；Mukhopadhyay [Muk21] 改进了常数，对于 ℓ_∞，相关结果见 [EHN11、AM18]。Dadush、Peikert 和 Vempala [DPV11]给出了用于求解任意范数下精确最短向量问题的 $2^{O(n)}$ 时间算法：通过以单位球的 M 椭球覆盖来枚举格点；对于任意凸体，他们可在期望 $2^{O(n)}$ 时间内计算该椭球，而对于 ℓ_p 球，则可在确定性多项式时间内计算。Dadush 和 Vempala 将这一通用构造改进为确定性算法 [DV12、DV13、Dad12]。在 ℓ_p 范数下，最短向量问题和最近向量问题的常数因子近似可在 $2^{(0.802+\xi)n}$ 时间内求解 [EV22] ；在任意范数下也可在 [时间内求解22]RV。

对于最近向量问题，情况则有所不同：除 ℓ_2 范数之外，所有单指数算法要么是近似算法，要么需要对目标向量作出承诺。Dadush、Peikert 和 Vempala 提出的方法，仅当目标向量距格不超过 γ 倍的 $\lambda_1(\mathcal{L})$ 时，才能在单指数时间内求解精确最近向量问题；其代价会随 γ [增长 DPV11, DV12]；这类承诺版本与有界距离译码密切相关 [LLM06, DRSD14]。Arvind 和 Joglekar 通过筛法获得了此类承诺结果，并证明：若给定达到连续最小值的格向量，则可由此推出无约束的精确最近向量问题结果 [AJ08]。已知有近似算法，且近似因子与时间复杂度之间存在权衡（见表 2）。常数近似因子可在 $2^{O(n)}$ [BN09, DK16] 和 $2^{(0.802+\xi)n}$ [EV22, RV22] 的时间内实现。对于 $(1+\varepsilon)$-近似，筛法可在 $2+1/\varepsilon)^{O(n)}$ 时间内处理 ℓ_p 范数 [BN09]；格点稀疏化可对任意范数确定性地在 $2^{O(n)}(1+1/\varepsilon)^n$ 时间内处理 [DK16]；覆盖法可在 $2^{O(n)}\varepsilon^{-n/\min\{2,p\}}$ 时间内处理 ℓ_p 范数 [NV22]；而对于 ℓ_∞ [EHN11] , 以及具有 $O(n)$ 个面的多面体范数，时间为 $2^{O(n)}(\log(1/\varepsilon))^{O(n)}$ NV22]。在所有情况下，对 ε 的依赖所对应的指数都随维数线性增长。

非欧几里得范数下求解最近向量问题的精确算法具有超指数复杂度。为了解释这一点，考虑一个格

基 B 和目标向量 $\boldsymbol{t}$。对于阈值 $R > 0$，考虑凸体

$$K_R := \left\{ \boldsymbol{z} \in \mathbb{R}^n : \|B\boldsymbol{z} - \boldsymbol{t}\|_p \leq R \right\}.$$

K_R 包含一个整数点，当且仅当存在一个格向量，其到 $\boldsymbol{t}$的距离不超过 R （在 ℓ_p 范数下）。这就是众所周知的带 n个变量的整数规划问题。Lenstra 算法 [Len83], ，结合 Kannan 的改进 [Kan83, Kan87] 以及后续改进 [FT87, HK13, Dad12, DER25], ，为该问题提供了一种 $n^{O(n)}$ 时间算法。Reis 和 Rothvoss 的近期工作[RR23] 给出了一种$(\log 2n)^{O(n)}$ 时间算法，目前这是已知的最佳算法。Bl¨omer 和 Naewe [BN11]通过将 Lenstra 算法推广到格成员问题，给出了一个确定性、多项式空间的精确最近向量问题算法$_p$ ，适用于每一种 ℓ_p 范数且满足 $1 < p < \infty$；对于 n维格以及位于其张成空间中的目标向量，该算法的运行时间为 $n^{(2+o(1))n}$ 乘以一个多项式。

因此，能否在 ℓ_2 以外的某种范数下，以单指数时间求解精确最近向量问题，至今仍是一个开放问题。Micciancio 和 Voulgaris 曾提出，他们的技术能否扩展到欧几里得范数之外 [MV13]；Dadush、Peikert 和 Vempala 则提出，他们的枚举方法能否扩展到承诺条件之外 [DPV11, DV12]。Bl¨omer 和 Kohn [BK18] 将“在非 ℓ_2 范数下以单指数时间求解精确最近向量问题”称为“该领域的主要开放问题”。他们证明，现有形式的 Voronoi 胞方法无法用于其他 ℓ_p 范数，因为在 $\mathbb{R}^3$ 中，格的 ℓ_3-Voronoi 相关向量的数量已经可能无界 [BK18]。其他欧几里得方法也无法直接迁移。人们还可以尝试推广 [ADS15, AS18b]中的离散高斯采样方法。离散高斯分布的 ℓ_p对应形式中，向量 $\boldsymbol{x} \in \mathcal{L} - \boldsymbol{t}$ 的概率 $e^{-\|\boldsymbol{x}\|_p^p / r^p}$与 r成正比；当参数足够小时，对该分布进行采样便能揭示最近向量。事实上，从该分布采样等价于求解最近向量问题$_p$ [Ste16，第 5], 节，因此无法先从中采样，再执行类似于欧几里得范数下算法的思路。范数之间的直接归约 [RR06, ACK+21] 会损失近似因子，无法得到精确解。

本文。我们首次获得了一个用于非欧几里得 ℓ_p 范数下精确最近向量问题的单指数算法，适用于 $1 < p < 2$，且不要求目标向量满足任何承诺条件。为此，我们建立了离散高斯分布与格平移上的“离散超高斯”分布之间的新联系。同一技术还给出了一个用于精确最短向量问题的简短算法$_p$ ，适用于每个满足 $1 \leq p < 2$ 的 p；与先前工作相比，该算法的指数常数有所改进。

1.1 我们的结果

我们用 $|I|$ 表示输入的位长度，用 dist$_p(\mathcal{L}, \boldsymbol{t})$ 表示 $\boldsymbol{t}$ 到 $\mathcal{L}$的 ℓ_p 距离，并用 $\lambda_1^{(p)}(\mathcal{L})$ 表示 $\mathcal{L}$中最短非零向量的ℓ_p 长度。

定理 1.1 （精确 最近向量问题$_p$）。 设定 $p \in$ （1、2）。存在一种随机化算法，给定一个秩为 n 的格 $\mathcal{L} \subseteq \mathbb{Q}^n$ 的基、一个目标向量 $\boldsymbol{t} \in \mathbb{Q}^n$ 和 $\delta \in$ （0、1/2], 以至少 $1 - \delta$ 的概率输出一个在 ℓ_p 范数下距 $\boldsymbol{t}$ 最近的 $\mathcal{L}$ 向量，期望时间为 $2^{O_p(n)} \cdot$多项式（$|I|$）$\cdot$对数（$1/\delta$）。

定理 1.1 在 第 4 节 (定理 4.1中得到证明。结合欧几里得情形 [MV13、ADS15], 可知，对于任意 最近向量问题$_p$ ，精确求解都可以在单指数时间内完成 $p \in (1, 2]$。据我们所知，这是首个能够在单指数时间内求解非欧几里得 最近向量问题 范数下精确 ℓ_p 最近向量问题的算法[1]

[1]我们注意到，实际上可以改进 CVP 和 SVP 的指数中的常数。我们选择当前的证明，是因为它们最能阐述我们的新技术。

且对目标向量的距离没有任何承诺。此前关于精确求解最近向量问题$_p$ 且 $1 < p < 2$的界 $n^{(2+o(1))n}$ 针对目标向量位于张成空间 [BN11]，并通过凸整数规划 [RR23] 结合标准的根分离界，得到 $(\log 2n)^{O(n)} \cdot 2^{O_p(n)}$。

定理 1.2 (精确 最短向量问题$_p$)。 对于每个 $p \in [1, 2)$，都存在一种随机化算法，给定秩为 n 的格 $\mathcal{L} \subseteq \mathbb{Q}^n$ 的一组基后，以至少 $1 - e^{-n}$ 的概率输出 $\mathcal{L}$ 在 ℓ_p 范数下的最短非零向量，运行时间至多为 $2^{2.4368n+o(n)} \cdot$ 多项式$(|I|)$。

对于 $p = 2$，相应的结论是 [ADRS15], 的定理，因此精确 最短向量问题$_p$ 对每个 $1 \le p \le 2$ 都是单指数的。

为简便起见，我们假设输入是一个满秩格。对于秩为 $k < n$、位于 $\mathbb{Q}^n$ 中的格，同一个最短向量问题算法的运行时间为 $2^{O_p(k)}$ poly$(|I|)$，而 CVP算法的运行时间为 $2^{O_p(n)}$ poly$(|I|)$。

Work	问题与设定	指数因子
Kannan；Hanrot–Stehl´e [Kan87，HS07]	精确最短向量问题$_2$,最近向量问题$_2$；确定性、多项式空间	$n^{n/(2e)+o(n)}$，$n^{n/2+o(n)}$
Micciancio–Voulgaris [MV13]	精确最近向量问题$_2$, 最短向量问题$_2$；确定性	$2^{2n+o(n)}$
Aggarwal、Dadush、（Regev、） Stephens-Davidowitz [ADRS15, ADS15]	精确最短向量问题$_2$, 最近向量问题$_2$	$2^{n+o(n)}$
Bl¨omer–Naewe；Arvind–Joglekar；Mukhopadhyay [BN09，AJ08，Muk21]	精确最短向量问题$_p$ 通过筛法	$2^{O(n)}$；$2^{2.751n+o(n)}$ 在 [Muk21]
Dadush–Peikert–Vempala [DPV11, DV12, DV13]	任意范数下的精确最短向量问题；如果 dist$(\boldsymbol{t}, \mathcal{L}) \le \gamma\lambda_1(\mathcal{L})$	$2^{O(n)}$；随 γ增长
Blömer–Naewe [BN11]	精确最近向量问题$_p$，$1 < p < \infty$；确定性；$\boldsymbol{t} \in$张成空间$(\mathcal{L})$	$n^{(2+o(1))n}$
Reis–Rothvoss [RR23]	n 变量的凸整数可行性；其中根分离、精确最近向量问题$_p$	$(\log 2n)^{O(n)}$
本文	精确最近向量问题$_p$, $1 < p < 2$	$2^{O_p(n)}$
本文	精确最短向量问题$_p$, $1 \le p < 2$	$2^{O(n)}$，在 p 中均匀分布的常数

表 1：维数为 n 时的精确算法。省略了输入长度中的多项式因子。

Work	问题与设定	指数与精度依赖
Blömer–Naewe [BN09]	$(1+\varepsilon)$-最近向量问题，ℓ_p 范数	$(2+1/\varepsilon)^{O(n)}$
Dadush–Kun [DK16]	$(1+\varepsilon)$-最近向量问题，任意范数；确定性	$2^{O(n)}(1+1/\varepsilon)^n$
Naszódi–Venzin [NV22]	$(1+\varepsilon)$-最近向量问题，ℓ_p 范数	$2^{O(n)}\varepsilon^{-n/\min\{2,p\}}$
Arya–da Fonseca–Mount [AdFM24]	$(1+\varepsilon)$-最近向量问题，良中心凸规范	$2^{O(n)}\varepsilon^{-(n-1)/2}$
Eisenbrand–H¨ahnle–尼迈耶 [EHN11]; Naszódi–Venzin [NV22]	$(1+\varepsilon)$-最近向量问题，ℓ_∞；具有以下多面体范数：$O(n)$个面	$2^{O(n)}$(对数$(1/\varepsilon))^{O(n)}$
Eisenbrand–Venzin [EV22]	$O_\xi(1)$-最近向量问题，ℓ_p 范数	$2^{(0.802+\xi)n}$
Rothvoss–Venzin [RV22]	$O_\xi(1)$-最近向量问题和最短向量问题，任意范数；秩 k 中任意维度	$2^{(0.802+\xi)k}$

表 2：非欧几里得范数下最近向量问题的近似算法，按其指数因子及其对精度的依赖关系进行比较。

的取值范围 p。对于 $0 < p \leq 2$ 函数 $e^{-|s|^p}$ 是中心高斯分布的混合，其混合由一个正的（$p/2$）稳定分布定义 [Fel71、Wes87、Nol20]；这使我们能够在随机的“对角度量”下将问题约化为欧几里得问题。对于 $p > 2$，不存在这样的表示 [Sch38]。该CVP 算法还需要 $p > 1$：将分析从未知的最近向量转移到算法当前持有的向量这一步，利用了 $s \mapsto |s|^p$的一致凸性，而其常数会随着 $p \to 1$而无限增长。

1.2 技术概述

令 $1 \leq p < 2$。给定一个满秩格 $\mathcal{L} \subset \mathbb{R}^n$ 和一个目标向量 $\boldsymbol{t} \in \mathbb{R}^n$，我们的目标是找到 a

$$\boldsymbol{v}^* \in \arg\min_{\boldsymbol{x} \in \mathcal{L}-\boldsymbol{t}} \|\boldsymbol{x}\|_p^p .$$

我们已经知道如何在欧几里得度量（最近向量问题（ℓ_2）上以单指数时间 [MV13、ADS15]求解该问题。 [ADS15] 算法中的一个关键子程序是针对某个概率分布的（近似）采样器 D_2（$\mathcal{L}-\boldsymbol{t}$，$r$）定义在 $\mathcal{L}-\boldsymbol{t}$ 上，使得

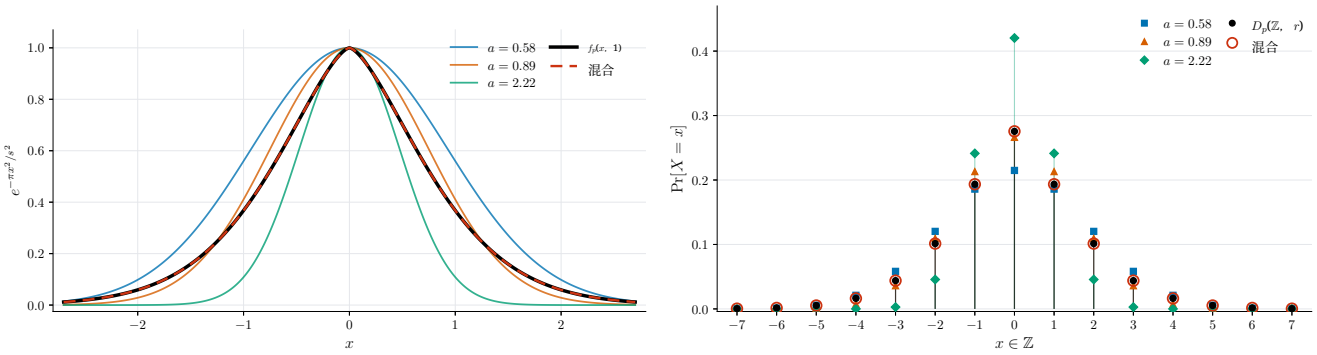
$$\Pr_{X \sim D_2(\mathcal{L}-\boldsymbol{t},r)}[X = \boldsymbol{x}] \propto \rho(\boldsymbol{x}, r) \coloneqq \exp\left(-\pi \frac{\|x\|_2^2}{r^2}\right).$$

因此，一个自然的方法是考虑 ℓ_p 度量中的类似分布： $D_p(\mathcal{L}-\boldsymbol{t}, r)$，其定义在$\mathcal{L}-\boldsymbol{t}$ 上，使得

$$\Pr_{X \sim D_p(\mathcal{L}-\boldsymbol{t},r)}[X = \boldsymbol{x}] \propto f_p(\boldsymbol{x}, r) \coloneqq \exp\left(-\frac{\|x\|_p^p}{r^p}\right),$$

并从中进行采样，其中 r足够小。该分布族称为超高斯分布，此前已在格问题之间的归约中得到研究 [Ste17、ACK+21]。

为此，我们从以下恒等式出发。对于 $x \in \mathbb{R}$ 和 $r > 0$，有



(a) (b)

图1：**用高斯函数的方差混合逼近超高斯分布**。其中 $p = 1.5$和 $a = \pi r^2/s^2$。**(a)** 对于 $r = 1$，黑色曲线为 $f_p(x,\ 1) = e^{-|x|^p}$；细彩色曲线为高斯函数 e^{-ax^2}，其 a 如图例所示。红色虚线曲线对 $N = 120,000$ 个具有独立 $a \sim g_{p/2}$ 的此类函数取平均，展示了恒等式 $f_p(x,\ 1) = \int_0^\infty e^{-\pi x^2/s^2} h_p(s,\ 1)\, ds$。**(b)**在具有 $r = 2$ 的 $\mathbb{Z}$ 上，归一化离散高斯通过按比例于 $h_p(s,\ r)\rho(\mathbb{Z},\ s)$ 的尺度权重混合，得到 $D_p(\mathbb{Z},\ r)$。

$$\exp\left(-\frac{|x|^p}{r^p}\right) = \int_0^\infty \exp\left(-\pi\frac{x^2}{s^2}\right) g_{p/2}\left(\frac{\pi r^2}{s^2}\right)\frac{2\pi r^2}{s^3} ds, \tag{1.1}$$

其中$g_{p/2}(\cdot)$ 是 $p/2$ 稳定分布 [AM74、Wes87、Nol20]的密度。关于这一恒等式的简短证明，请参见第 2.2 节；示意图见图 1。逐坐标应用这一恒等式，超高斯分布可以写成高斯分布的方差混合的边缘分布：

$$f_p(\boldsymbol{x}, r) = \int_{\mathbb{R}^n_{>0}} \rho(\boldsymbol{x}, \boldsymbol{s}) h_p(\boldsymbol{s}, r) d\boldsymbol{s},$$

其中

$$\rho(\boldsymbol{x}, \boldsymbol{s}) \coloneqq \exp\left(-\pi \sum_j \frac{x_j^2}{s_j^2}\right); \qquad h_p(\boldsymbol{s}, r) \coloneqq \prod_{j=1}^n g_{p/2}\left(\frac{\pi r^2}{s_j^2}\right)\frac{2\pi r^2}{s_j^3}.$$

利用这一结果，在 $\mathcal{L} - \boldsymbol{t} \times \mathbb{R}^n_{>0}$ 上对联合分布进行采样，已经足以让我们在 $2^{O(n)}$ 时间内求解 $p \in [1, 2)$ 的精确最短向量问题 $_p$ 和常数近似 CVP$_p$。然而，我们无法将这一方法扩展到精确最近向量问题。定义

$$F_p(\boldsymbol{x}) \coloneqq \sum_j |x_j|^p .$$

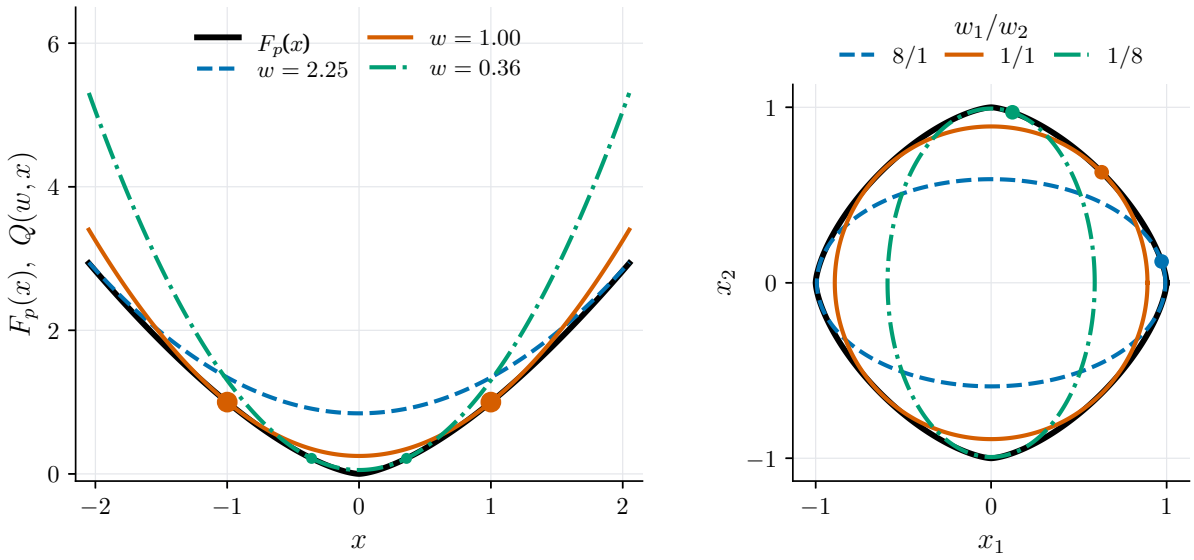
我们面临的一个几何障碍是，在 ℓ_2 度量下，海森矩阵为

$$\nabla^2 F_2(\boldsymbol{x}) = 2I,$$

而对于 $1 < p < 2$，对于非零坐标，

$$\nabla^2 F_p(\boldsymbol{x}) = p(p-1)\,\mathrm{diag}(|x_j|^{p-2}).$$

因此，目标函数的曲率取决于我们在何处对其进行求值。关键的是，当我们逐渐靠近那些“尖锐”的角时，它的表现会变得异常。



(a) (b)

图2：使用加权 ℓ_2 目标逼近 $\ell_{1.5}$ 目标。我们考虑 $p = 1.5$。**(a)** 黑色曲线为 $F_p(x) = |x|^p$；彩色曲线为 $Q(w, x) = \frac{p}{2}|w|^{p-2}x^2 + (1-\frac{p}{2})|w|^p$，对应图例中的不同 w 值。每个二次函数都位于 F_p 之上，并在 $x = \pm w$处与其相切。**(b)** 黑色曲线界定单位 ℓ_p 球。彩色椭圆为 $Q(\boldsymbol{w}, \boldsymbol{x}) = 1$，其中 $F_p(\boldsymbol{w}) = 1$，比值 w_1/w_2 如图所示。由于 $F_p(\boldsymbol{x}) \le Q(\boldsymbol{w}, \boldsymbol{x})$，每个椭球都位于 ℓ_p 球内，并且在 $\boldsymbol{w}$的每个坐标反射处相切。其边界为 $\sum_{j=1}^2 |w_j|^{p-2}x_j^2 = 1$。等价地，令 $s_j^2 = 2\pi|w_j|^{2-p}/p$（其中 $r = 1$）可得 $\pi\sum_{j=1}^2 x_j^2/s_j^2 = p/2$：改变尺度会改变欧几里得几何。

用 ℓ_p 几何来近似 ℓ_2。 我们将证明，公式（1.1）实际上可以用来定义一种自然分布，从而得到一组加权的 ℓ_2 球，这些球近似于一个目标向量 ℓ_p 球。因此，我们可以将 ℓ_p 目标函数 $F_p(\cdot)$ 替换为多个加权 ℓ_2 目标函数的混合。参见图2。此前也有人采用过类似的方法[2]，例如，在迭代加权最小二乘相关文献中，参见 [Gen24，第 5.7 节。1]。

对于任意满足 $\boldsymbol{w}, \boldsymbol{x} \in \mathbb{R}^n$ 且 $\forall j,\ w_j \neq 0$ 的对象，我们定义

$$Q(\boldsymbol{w}, \boldsymbol{x}) := \frac{p}{2}\sum_j |w_j|^p \left(\frac{x_j}{w_j}\right)^2 + \left(1 - \frac{p}{2}\right) F_p(\boldsymbol{w}).$$

由 $z \mapsto z^{p/2},\ z \ge 0$ 的凹性可知

$$F_p(\boldsymbol{x}) \le Q(\boldsymbol{w}, \boldsymbol{x}),$$

当且仅当 $\forall j:\ |w_j| = |x_j|$ 时取等号。重要的观察是，对于任意固定的 $\boldsymbol{w}$, $Q(\boldsymbol{w}, \cdot)$ 是一个二次函数。因此，在格平移上最小化 $Q(\boldsymbol{w}, \cdot)$，就是一个欧几里得最近向量问题$_2$, 的实例，我们可以使用 2^n 时间通过 [ADS15] 求解。

给定一个 $\boldsymbol{x} \in \mathcal{L} - \boldsymbol{t}$，高斯混合恒等式自然地定义了一个关于权重的后验分布，其正比于

$$P_{\boldsymbol{x},r}(\boldsymbol{s}) := \frac{\rho(\boldsymbol{x}, \boldsymbol{s})\, h_p(\boldsymbol{s}, r)}{f_p(\boldsymbol{x}, r)}.$$

[2]事实上，在这项工作中，人工智能工具发挥的一个重要作用是引导我们发现这条优美的研究脉络 .

设 $\boldsymbol{s}$ 是从该分布中抽取的样本，并令

$$w_j = \left(\frac{ps_j^2}{2\pi r^p}\right)^{1/(2-p)}.$$

这一选择的关键性质是，对于

$$E(\boldsymbol{v}^*, \boldsymbol{w}) \coloneqq Q(\boldsymbol{w}, \boldsymbol{v}^*) - F_p(\boldsymbol{v}^*),$$

我们有

$$\mathbb{E}_{\boldsymbol{s}\sim P_{\boldsymbol{v}^*,r}}\left[E(\boldsymbol{v}^*, \boldsymbol{w})\right] \le 2\ln 2\, nr^p.$$

如果 $\boldsymbol{y}$ 在包含 $\boldsymbol{v}^*$的陪集中使 $Q(\boldsymbol{w}, \cdot)$ 取得最小值，那么

$$F_p(\boldsymbol{y}) \le Q(\boldsymbol{w}, \boldsymbol{y}) \le Q(\boldsymbol{w}, \boldsymbol{v}^*) = F_p(\boldsymbol{v}^*) + E(\boldsymbol{v}^*, \boldsymbol{w}).$$

因此，

$$\mathbb{E}_{\boldsymbol{s}\sim P_{\boldsymbol{v}^*,r}}\left[F_p(\boldsymbol{y}) - F_p(\boldsymbol{v}^*)\right] \le 2\ln 2\, nr^p.$$

我们在引理 4.2中证明了一个类似的结果。暂且假设我们能够利用近似最短向量 $\boldsymbol{x} \in 2\mathcal{L} + \boldsymbol{v}^*$作为提示，从一个接近 $P_{\boldsymbol{v}^*,\, r}$ 的分布中采样“良好的二次目标函数” $Q(\boldsymbol{w}, \cdot)$。那么，我们就可以采用一种迭代方法：从 $\boldsymbol{x}$开始，对于 $\boldsymbol{w}$的许多种选择，我们反复寻找一个使 $Q(\boldsymbol{w}, \cdot)$ 最小的后继向量 $\boldsymbol{y}$，并保留其中最短的向量。最后，我们可以（相对容易地）证明，一旦 $\boldsymbol{y}$ 足够短（且位于正确的陪集中），我们就完成了。当然，我们不知道 $\boldsymbol{v}^*$ 属于哪个陪集，因此我们会尝试它们全部 2^n 。

我们证明，事实上，从 $P_{\boldsymbol{x},\, r}$中获取足够多的样本（其中 $\boldsymbol{x} \in 2\mathcal{L} + \boldsymbol{v}^*$ 足够短），就足以找到我们的“良好权重”。对于 $0 < \tau \le 1/2$，考虑重叠

$$I_\tau(P_{v^*,r}, P_{x,r}) = \int P_{\boldsymbol{v}^*,r}(\boldsymbol{a})^{1-\tau} P_{\boldsymbol{x},r}(\boldsymbol{a})^{\tau}\, d\boldsymbol{a}.$$

写作

$$J_\tau(a,b) = \left((1-\tau)a^2 + \tau b^2\right)^{p/2} - (1-\tau)|a|^p - \tau|b|^p,$$

我们在引理 4.4 中证明了

$$I_\tau(P_{u,r}, P_{x,r}) = \exp\left(-\frac{1}{r^p}\sum_j J_\tau(u_j, x_j)\right).$$

在最近向量问题 算法 [ADS15] 中的一个关键观察是，平行四边形恒等式将同一陪集中的两个格向量到目标向量的距离，与它们的中点到目标向量的距离联系起来。[3] 对于 $p \ne 2$，我们不再拥有这样的恒等式。然而，凸性仍然保证

$$F_p\left(\frac{\boldsymbol{x}+\boldsymbol{y}}{2}\right) \le \frac{F_p(\boldsymbol{x}) + F_p(\boldsymbol{y})}{2}. \tag{1.2}$$

[3]事实上，对于 $F_2(\boldsymbol{x}) = \|\boldsymbol{x}\|_2^2$，平行四边形恒等式给出

$$\frac{F_2(\boldsymbol{x}) + F_2(\boldsymbol{y})}{2} = F_2\left(\frac{\boldsymbol{x}+\boldsymbol{y}}{2}\right) + F_2\left(\frac{\boldsymbol{x}-\boldsymbol{y}}{2}\right).$$

特别地，如果 $\boldsymbol{x}$、$\boldsymbol{y} \in \mathcal{L} - \boldsymbol{t}$ 属于模 $2\mathcal{L}$的同一个陪集 $\mathcal{L} - \boldsymbol{t}$，那么它们的中点也属于 $\boldsymbol{y}$。因此，如果 $F_2(\boldsymbol{x}) \le F_2(\boldsymbol{y}) + \Delta$ 是最优的，那么 $F_2(\boldsymbol{x} - \boldsymbol{y}) \le 2\Delta$，因此它们彼此接近。这就是其聚类论证背后的几何观察（见 [ADS15，引理 5。1]）。

利用这一事实，我们能够证明，当 $\|\boldsymbol{x}\|_p^p$ 足够接近 $\|\boldsymbol{v}^*\|_p^p$ 时， J 有界，即[4]

$$\sum_j J_\tau(v_j^*, x_j) \le O_p(\tau^{p/2}) \left[\frac{F_p(\boldsymbol{v}^*) + F_p(\boldsymbol{x})}{2} - F_p\left(\frac{\boldsymbol{v}^* + \boldsymbol{x}}{2}\right) \right] \le O_p(\tau^{p/2}) \left[F_p(\boldsymbol{x}) - F_p(\boldsymbol{v}^*) \right].$$

因此，

$$I_\tau(P_{\boldsymbol{v}^*,r}, P_{\boldsymbol{x},r}) \ge 2^{-\mathcal{O}(n)},$$

我们在引理 4.5 中证明，可以使用上述技术找到距离逐步更近的格点。

1.3 进一步的相关工作

整数规划与无界子集和。Lenstra 证明了，固定变量数量的整数规划可以在多项式时间内求解 [Len83]; Kannan 将其依赖关系改进为 $n^{O(n)}$ [Kan83, Kan87], Frank 和 Tardos 展示了如何缩小所涉及数字的规模 [FT87], Kannan 和 Lov´asz 通过覆盖极小值研究了其背后的平坦性现象 [KL88], Hildebrand 和 K¨oppe 将该方法扩展到拟凸多项式目标函数 [HK13], Dadush 对一般凸体获得了时间$n^n 2^{O(n)}$ ，并提出了用于近似整数规划的随机筛法框架 [Dad12, Dad14], Dadush、Eisenbrand 和 Rothvoss 将精确整数规划归约为近似整数规划 [DER25], 而 Reis 和 Rothvoss 达到了 $(\log 2n)^{O(n)}$ [RR23]; 综述请参见 [Eis10] 。约束较少且系数较小的整数规划具有伪多项式算法 [Pap81, EW19, JR19]。整数规划是否可以在时间 $2^{O(n)}$ 内求解仍是一个开放问题。

端点 $p = 1$ 通过无界子集和将精确最近向量问题与以下问题联系起来：给定正整数 a_1、...、a_M和 T，判断 $\sum_i a_i z_i = T$ 是否存在解 $\boldsymbol{z} \in \mathbb{Z}^M_{\ge 0}$。令 $Q = T + 1$，使 $B \in \mathbb{Z}^{(M+1)\times M}$ 的行分别为 diag(a_1、 ... 、 a_M) 和 (Qa_1、 ... 、 Qa_M)，并令 $\boldsymbol{t}$ =(0 、 ... 、 0 、 QT)。那么 $\|B\boldsymbol{z} - \boldsymbol{t}\|_1 = \sum_i a_i|z_i| + Q\left|\sum_i a_i z_i - T\right|$，因此 dist$_1$($\boldsymbol{t}$ 、 $\mathcal{L}$) $\le T$ 当且仅当该实例是可行的；若有一种精确最近向量问题算法 $_1$ 能在关于维数呈单指数的时间内运行，那么它将以 $2^{O(M)}$ 乘以一个多项式的时间解决无界子集和问题。这个问题仍未解决：目前最好的通用界是 $(\log\ M)^{O(M)}$的 [RR23], ；当目标向量较大时，已知多项式时间算法 [AJSW24、CMZ25], ，特殊情形见 [SM21], ，而伪多项式算法 [BL07、Bri17、JR19、Kle22、CH22]彼此不可比较。密切相关的 Frobenius问题一般是 NP-困难的，而在固定维数下是多项式时间可解的 [RA96、Kan92、RA05]。我们的最近向量问题算法尚未达到 $p = 1$，而我们的最短向量问题算法则涵盖了这一情形。

一个自然遗留的开放性问题是，我们的技术能否扩展到适用于 $p = 1$。我们的算法至关重要地利用了这样一个事实：对于 $1 < p < 2$， ℓ_p 球是严格凸的。因此，近似最近向量问题解能够提供其邻域的有用几何信息，而算法正是利用了这些信息。对于 ℓ_1，这一点并不成立。然而，混合恒等式对 ℓ_1 成立，并且具有许多可以加以利用的良好性质。

致谢

本工作得到了 NRF 基金 NRF-NRFI09-0005 的支持。AM 获得新加坡的 NQSS 奖学金资助。AM 感谢 Li Zeyong、Saswata Mukherjee 和 Rishav Gupta 提供了许多有益的讨论。

[4]这正是我们需要假设 $p > 1$的地方。具体而言，该算法能够利用 ℓ_2 度量来近似 ℓ_p 度量的曲率。然而， $p = 1$ 这一最有趣的情形没有可供我们利用的有用曲率，因此无法在局部近似 ℓ_1 目标函数。

人工智能使用声明

最初提出使用 ℓ_2 目标函数来解决 ℓ_1 问题，是通过关联相应的（超）高斯分布实现的，这一想法源于作者。我们通过一项关于贝叶斯学习的先前工作，从 [Nol20] 中发现了稳定分布，并最终得到了一个用于最短向量问题$_p$ 的 $1 \le p < 2$ 算法，其性能优于先前工作。然而，我们无法让这一想法适用于精确的最近向量问题。最终，AI 数学时代到来；在对先前尝试进行了长时间审慎思考后，GPT Sol 和 Astra 帮助我们证明，类似的算法也适用于精确的最近向量问题。我们后来了解到，GPT 从迭代加权最小二乘和 Dikin随机游走的文献中提取了这些技术；这些技术最初是为了解决连续优化问题和进行采样而发明的（见 [KV24、Gen24]）。本稿中的最短向量问题算法，是我们与 ChatGPT 5.6 交流后得到的版本，其指数中的常数得到了进一步改进。所有文字均由作者撰写。

2 预备知识

2.1 记号与计算模型

对于 $\boldsymbol{x} \in \mathbb{R}^n$ 和 $p \ge 1$，令 $\|\boldsymbol{x}\|_p := (\sum_j |x_j|^p)^{1/p}$，当 $p = 2$ 时，我们省略 p。对于定义在 $\mathbb{R}^n$ 上的函数 f 和可数集 S，我们记 $f(S) := \sum_{\boldsymbol{x} \in S} f(\boldsymbol{x})$。我们用 ln 表示自然对数，用 log 表示以 2 为底的对数，并用 $|I|$ 表示所求解问题输入的位长度。

集合 $\mathcal{S}$ 上两个概率分布 P 和 Q 之间的统计距离为

$$\mathsf{SD}(P;Q) := \frac{1}{2}\sum_{x \in \mathcal{S}} |P(x) - Q(x)| \,.$$

对于任意事件 E，有 $|P(E) - Q(E)| \le \mathsf{SD}(P; Q)$。

计算模型。 为简化阐述，我们在实数RAM模型中分析我们的算法：实数可以精确存储；算术运算、比较以及 $\ln x$、$\sin x$ 和 x^y 的求值均需单位时间；并且可以在单位时间内从 $[0, 1]$ 中均匀分布地抽取一个随机实数。然而，对于任意固定的有理数 $p \in 1 < p < 2$，这些结果在字RAM模型中同样成立，只需额外承担 poly($|I|$) 的开销，其中 $|I|$ 是输入规模。特别地，我们的算法会在“扰动”格上调用欧几里得最短向量问题$_2$ 和最近向量问题$_2$ 子程序，而这些格可能含有实数条目。下面的引理表明，我们可以将这些条目近似到 poly($|I|$) 位精度，同时只需额外承担 poly($|I|$) 的开销。

引理2.1。 设 $B \in \mathbb{R}^{n \times k}$ 是一个满列秩格的基，其最小奇异值为$\sigma_{\min}(B)$。假设对于 $b \in \mathbb{N}$，矩阵 $\widehat{B} \in \mathbb{Q}^{n \times k}$ 满足

$$\max_{i,j} |B_{ij} - \widehat{B}_{ij}| \le 2^{-b}.$$

那么，对于任意 $\boldsymbol{z} \in \mathbb{Z}^k$,

$$\left\| \widehat{B}\boldsymbol{z} - B\boldsymbol{z} \right\|_2 \le \frac{\sqrt{nk}\,2^{-b}}{\sigma_{\min}(B)} \|B\boldsymbol{z}\|_2 \,.$$

证明。根据矩阵-向量乘法的次乘性以及奇异值的定义，

$$\left\|\widehat{B}\boldsymbol{z} - B\boldsymbol{z}\right\|_2 \le \sqrt{nk}2^{-b}\left\|\boldsymbol{z}\right\|_2 \le \frac{\sqrt{nk}2^{-b}}{\sigma_{\min}(B)}\left\|B\boldsymbol{z}\right\|_2 .$$ □

如果我们的输入格基 B 是有理的，那么有 $\sigma_{\min}(B)^{-1} \le 2^{\mathsf{poly}(|I|)}$. 因此，通过适当地选择 b，我们可以使格向量长度的失真达到指数级小（关于 $|I|$）。此外，我们在定理 4.1的证明中给出的上界足够宽松，可以从这些舍入后的最近向量问题$_p$ 解中恢复精确的 ℓ_2 解。特别地，它们被用于求解一种最近向量问题$_2$ 变体，其中等值集是椭球（见推论 2.12）。最后，来自第 3 节 的所有采样器都可以实现为返回所需精度的样本（即多项式（$|I|$））。

以下不等式用于引理 4.4；这里需要 $p > 1$。

引理 2.2。 令 $0 < \tau \le 1/2$ 和 $1 < p < 2$。对于 a、$b \in \mathbb{R}$，定义

$$J_\tau(a,b) \coloneqq \left((1-\tau)a^2 + \tau b^2\right)^{p/2} - (1-\tau)|a|^p - \tau|b|^p.$$

那么，

$$J_\tau(a,b) \le \frac{64}{p-1}\tau^{p/2}\left(\frac{|a|^p+|b|^p}{2} - \left|\frac{a+b}{2}\right|^p\right). \tag{2.1}$$

证明。 当 $a = b = 0$ 时，该断言显然成立。将 a, b 替换为 $|a|, |b|$ 会使 J_τ 保持不变，并且只会减小 公式 (2.1)右侧的表达式。因此不妨设 $a, b \ge 0$ 并写成$M = \max(a,b) > 0$。

函数

$$z \longmapsto z^p - \frac{p(p-1)}{2}M^{p-2}z^2$$

在 $[0, M]$ 上是凸的：其二阶导数为 $p(p-1)(z^{p-2} - M^{p-2}) \ge 0$ 当 $0 < z \le M$ 时，其一阶导数在零点处连续。在 $(a+b)/2$ 处应用凸性，可得

$$\frac{a^p+b^p}{2} - \left(\frac{a+b}{2}\right)^p \ge \frac{p(p-1)}{8}M^{p-2}(a-b)^2. \tag{2.2}$$

现在考虑两种情况。

情况 1： $\min(a,b) \le M/2$。 $z^{p/2}$ 的次可加性给出

$$\begin{aligned} J_\tau(a,b) &\le \left((1-\tau)^{p/2} - (1-\tau)\right)a^p + \left(\tau^{p/2} - \tau\right)b^p \\ &\le \tau^{p/2}(a^p+b^p) \le 2\tau^{p/2}M^p. \end{aligned}$$

由于 $|a-b| \ge M/2$，因此

$$J_\tau(a,b) \le 8\tau^{p/2}M^{p-2}(a-b)^2. \tag{2.3}$$

结合 方程 (2.2) 和 (2.3) 并利用 $1/p \le 1$ 即可证明这种情况下的断言。

情况 2： $\min(a, b) > M/2$。 如果 $a = b$，断言显然成立，因此假设 $a \ne b$。固定 a，并且对于 $z > 0$，定义

$$\begin{aligned} q(z) &\coloneqq (1-\tau)a^2 + \tau z^2, \\ f(z) &\coloneqq J_\tau(a,z) = q(z)^{p/2} - (1-\tau)a^p - \tau z^p. \end{aligned}$$

求导得

$$f'(z) = p\tau z\, q(z)^{p/2-1} - p\tau z^{p-1}.$$

由于 $q(a) = a^2$，我们有

$$f(a) = f'(a) = 0. \tag{2.4}$$

再次求导，

$$f''(z) = p\tau q(z)^{p/2-1} + p(p-2)\tau^2 z^2 q(z)^{p/2-2} - p(p-1)\tau z^{p-2}.$$

最后两项均非正，因为 $1 < p < 2$。对于介于 a 和 b 之间的每个 z， a， $z \geq M/2$ 均成立，因此

$$q(z) \geq (1-\tau)\frac{M^2}{4} + \tau\frac{M^2}{4} = \frac{M^2}{4}.$$

由于 $p/2 - 1 < 0$，可得

$$f''(z) \leq p\tau q(z)^{p/2-1} \leq p\tau\left(\frac{M^2}{4}\right)^{p/2-1} = p\,2^{2-p}\tau M^{p-2}. \tag{2.5}$$

根据泰勒定理，对于介于 a 和 b 之间的某个 ξ，

$$f(b) = f(a) + f'(a)(b-a) + \frac{1}{2}f''(\xi)(b-a)^2.$$

利用方程 (2.4) 和 (2.5)，我们得到

$$J_\tau(a,b) = f(b) \leq p\,2^{1-p}\tau M^{p-2}(a-b)^2. \tag{2.6}$$

结合等式 (2.2)与(2.6)，并利用 $2^{1-p} \leq 1$ 和 $\tau \leq \tau^{p/2}$，即可证明等式 (2.1)在这种情况下也成立。

□

定理 2.3 (H¨older 不等式；定理 3.5 出自 [Rud87])。设 p， $q > 1$ 满足

$$\frac{1}{p} + \frac{1}{q} = 1.$$

那么，

$$\int_S |f(\boldsymbol{s})g(\boldsymbol{s})|\,d\boldsymbol{s} \leq \left(\int_S |f(\boldsymbol{s})|^p\,d\boldsymbol{s}\right)^{1/p}\left(\int_S |g(\boldsymbol{s})|^q\,d\boldsymbol{s}\right)^{1/q}.$$

2.2 稳定分布

注意，对于 $y \in [0,\infty)$ 和 $0 < p < 2$，函数

$$y \mapsto \exp\left(-y^{p/2}\right)$$

是完全单调的，也就是说，对于所有的 $k \geqq 0$ 和 $y > 0$， $(-1)^k \frac{d^k}{dy^k}\exp(-y^{p/2}) \geq 0$。

因此，根据伯恩斯坦定理 [Ber29](参见 [Ber08，定理 1。5])，该函数是定义在 $\mu_{p/2}$ 上的正测度的 $[0,\infty$拉普拉斯变换，

$$\exp\left(-y^{p/2}\right) = \int_0^\infty \exp\left(-ay\right)\,d\mu_{p/2}(a).$$

由此可得

$$\mu_{p/2}([0,\infty)) = \lim_{y\to 0^+} \exp\left(-y^{p/2}\right) = 1,$$

因此，$\mu_{p/2}$ 它是一个概率测度。众所周知，对应的随机变量是正的 $p/2$-稳定随机变量 [Nol20]。

记 $\mu_{p/2}(\quad da) = g_{p/2}(a)\,da$ 为该 $p/2$-稳定随机变量的密度[5]，我们有 th at

$$\exp\left(-y^{p/2}\right) = \int_0^\infty \exp\left(-ay\right) g_{p/2}(a) da. \tag{2.7}$$

将 $y = (x/r)^2$ 代入 $x \in \mathbb{R}$、$r > 0$ 和 $a = \pi r^2/s^2$，可得

$$\exp\left(-\frac{|x|^p}{r^p}\right) = \int_0^\infty \exp\left(-\pi\frac{x^2}{s^2}\right) g_{p/2}\left(\frac{\pi r^2}{s^2}\right) \frac{2\pi r^2}{s^3} ds. \tag{2.8}$$

现在我们提及 一些关于稳定密度的事实，这些事实将在本文中始终发挥作用。Le t

$$\alpha = \frac{p}{2}, \qquad q = \frac{\alpha}{1-\alpha} = \frac{p}{2-p}, \qquad \kappa_p = (1-\alpha)\alpha^q, \qquad \beta = 2^{1/q}.$$

注意，我们有

$$\beta^q = 2, \qquad (2\beta)^\alpha = 2. \tag{2.9}$$

对于 $0 < \theta < \pi$，定义

$$A_\alpha(\theta) := \frac{\sin(\alpha\theta)^q \sin((1-\alpha)\theta)}{\sin(\theta)^{q+1}}.$$

Zolotarev [Zol86]给出了稳定分布的分布函数的如下积分表示（参见 [Dev09，公式（1）]）：对于 $a > 0$,

$$\int_0^a g_\alpha(u)\,du = \frac{1}{\pi}\int_0^\pi e^{-A_\alpha(\theta)a^{-q}}\,d\theta. \tag{2.10}$$

对公式（2.10）关于 a求导，得到

$$g_\alpha(a) = \frac{q}{\pi a^{q+1}}\int_0^\pi A_\alpha(\theta) e^{-A_\alpha(\theta)a^{-q}}\,d\theta. \tag{2.11}$$

Kanter 利用表示式 公式（2.10）还给出了从密度 g_α中进行简单抽样的方法[Kan75]（另见 [CMS76]）。

事实 2.4。令 U 服从 $(0,\pi)$上的均匀分布，令 E 为与 U 独立的标准指数随机变量。那么 $(A_\alpha(U)/E)^{1/q}$的密度为 g_α。

证明。对于 $a > 0$,

$$\Pr\left[(A_\alpha(U)/E)^{1/q} \le a\right] = \Pr\left[E \ge A_\alpha(U)\, a^{-q}\right] = \mathbb{E}_U\left[e^{-A_\alpha(U)a^{-q}}\right],$$

这是公式（2.10）的右侧。 □

[5]已知该随机变量具有密度，参见 [Nol20，定理 1。1]。

我们需要以下技术引理。

引理 2.5。对于 $a > 0$,

$$g_\alpha(a) \exp\left(\frac{\kappa_p a^{-q}}{2}\right) \le 2\beta\, g_\alpha(\beta a).$$

证明。由于 sin x for $x \in [0, \pi]$ 是凹函数，因此我们有

$$\sin(\alpha\theta) \ge \alpha \sin\theta, \qquad \sin((1-\alpha)\theta) \ge (1-\alpha)\sin\theta,$$

这意味着

$$A_\alpha(\theta) \ge \kappa_p \implies A_\alpha(\theta) - \kappa_p/2 \ge A_\alpha(\theta)/2.$$

利用方程 (2.11) 可得

$$\begin{aligned} g_\alpha(a) e^{\kappa_p a^{-q}/2} &= \frac{q}{\pi a^{q+1}} \int_0^\pi A_\alpha(\theta) e^{-(A_\alpha(\theta) - \kappa_p/2) a^{-q}}\, d\theta \\ &\le \frac{q}{\pi a^{q+1}} \int_0^\pi A_\alpha(\theta) e^{-A_\alpha(\theta) a^{-q}/2}\, d\theta \\ &\le 2\beta g_\alpha(\beta a), \end{aligned}$$

其中，在最后一个不等式中，我们再次使用了方程 (2.9) 和方程 (2.11) 。 □

对于 $\lambda \ge 0$，指数倾斜的稳定分布 $G_{\alpha,\,\lambda}$ 是定义在 $(0,\ \infty)$ 上、密度为

$$\exp\left(\lambda^\alpha - \lambda a\right) g_\alpha(a);$$

由 公式 (2.7) 可知，这是一个概率密度，并且$G_{\alpha,\,0}$ 具有密度 g_α。Devroye [Dev09，定理 3]给出了一个从中采样的算法。

引理 2.6 ([Dev09], 定理 3)**：** 存在一种算法，给定 $\alpha \in (0、1)$ 和 $\lambda \ge 0$，可从 $G_{\alpha,\,\lambda}$中输出一个样本。该算法在所有 $\alpha \in (0、1)$ 和 $\lambda \ge 0$ 上的一致期望运行时间为 $\mathcal{O}(1)$。

2.3 格

在 $\mathbb{R}^n$ 中的秩为 k 的格是集合 $\mathcal{L} = \mathcal{L}(B) := B\mathbb{Z}^k$，其中 $B \in \mathbb{R}^{n\times k}$ 具有线性无关列$\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k$；矩阵 B是 $\mathcal{L}$的基，并且当 $k = n$时， $\mathcal{L}$具有满秩。对于 $p \ge 1$和 $\boldsymbol{t} \in \mathbb{R}^m$，我们记作

$$\lambda_1^{(p)}(\mathcal{L}) := \min_{\boldsymbol{x}\in\mathcal{L}\setminus\{\boldsymbol{0}\}} \|\boldsymbol{x}\|_p \qquad \text{and} \qquad \operatorname{dist}_p(\mathcal{L}, \boldsymbol{t}) := \min_{\boldsymbol{x}\in\mathcal{L}} \|\boldsymbol{x} - \boldsymbol{t}\|_p .$$

具有 $\|\boldsymbol{x} - \boldsymbol{t}\|_p = \operatorname{dist}_p(\mathcal{L},\ \boldsymbol{t})$ 的向量 $\boldsymbol{x} \in \mathcal{L}$ 是 $\boldsymbol{t}$的最近向量。

事实 2.7 (格的陪集)。 设 $\mathcal{L} = \mathcal{L}(B)$ 是一个秩为 n 的格。

1. $\mathcal{L}$ 是 2^n 个陪集 $2\mathcal{L} + B\boldsymbol{c}$、 $\boldsymbol{c} \in \{0,1\}^n$ 的不交并。
2. 如果 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 属于同一个陪集，那么 $\frac{\boldsymbol{x}+\boldsymbol{y}}{2} \in \mathcal{L}$。
3. 此外，如果 $\mathcal{L} \subseteq \mathbb{Z}^m$ 和 $\boldsymbol{x} \ne \boldsymbol{y}$，那么 $\|\boldsymbol{x} - \boldsymbol{y}\|_2 \ge 2$。

证明。 (1) 用 $\boldsymbol{z} \in \mathbb{Z}^n$ 写出 $\boldsymbol{x} = B\boldsymbol{z}$，并将 $\boldsymbol{z}$ 模 2 化简；由于 B 的列向量线性无关，这些陪集彼此不相交。(2) $\frac{\boldsymbol{x}+\boldsymbol{y}}{2} = \boldsymbol{y} + \frac{\boldsymbol{x}-\boldsymbol{y}}{2}$ 和 $\boldsymbol{x} - \boldsymbol{y} \in 2\mathcal{L}$。~~(3)~~ $\boldsymbol{x} - \boldsymbol{y}$ 是~~$2\mathcal{L}$~~ $\subseteq 2\mathbb{Z}^m$ 的非零向量，因此其某个坐标是非零偶整数。 □

离散超高斯分布。对于 $1 \le p < 2$、 $r > 0$ 和 $\boldsymbol{x} \in \mathbb{R}^n$，定义

$$f_p(\boldsymbol{x}, r) \coloneqq \exp\left(-\frac{\|\boldsymbol{x}\|_p^p}{r^p}\right) ,$$

对于格 $\mathcal{L} \subseteq \mathbb{R}^n$ 和 $\boldsymbol{t} \in \mathbb{R}^n$，令

$$f_p(\mathcal{L} - \boldsymbol{t}, r) \coloneqq \sum_{\boldsymbol{x} \in \mathcal{L} - \boldsymbol{t}} \exp\left(-\frac{\|\boldsymbol{x}\|_p^p}{r^p}\right) ,$$

其为有限集。 ℓ_p 离散高斯分布 $D_p(\mathcal{L} - \boldsymbol{t},\ r)$ 是定义在 $\mathcal{L} - \boldsymbol{t}$ 上的分布，其定义为

$$\Pr_{X \sim D_p(\mathcal{L}-\boldsymbol{t}, r)}[X = \boldsymbol{x}] = \frac{f_p(\boldsymbol{x}, r)}{f_p(\mathcal{L} - \boldsymbol{t}, r)} \qquad \text{for } \boldsymbol{x} \in \mathcal{L} - \boldsymbol{t} . \tag{2.12}$$

对于 $s > 0$，欧几里得离散高斯分布 $D_{\mathcal{L},\ s}$ 是定义在 $\mathcal{L}$ 上的分布，其中元素的概率与 $e^{-\pi\|\boldsymbol{x}\|^2/s^2}$ 到 $\boldsymbol{x} \in \mathcal{L}$ 成正比；它是 $D_2(\mathcal{L},\ s/\sqrt{\pi})$。

2.4 计算问题与算法。

我们是我们主要关注格上的以下两个优化问题。

定义 2.8 （最短向量问题，最短向量问题$_p$）。 对于 $p \ge 1$，问题最短向量问题$_p$ 是：给定格 $\mathcal{L} \subseteq \mathbb{Q}^n$ 的一组基，输出一个向量 $\boldsymbol{x} \in \mathcal{L} \setminus \{\boldsymbol{0}\}$，使其满足 $\|\boldsymbol{x}\|_p = \lambda_1^{(p)}(\mathcal{L})$。

定义 2.9 （最近向量问题，最近向量问题$_p$）。 对于 $p \ge 1$，问题最近向量问题$_p$ 是：给定格 $\mathcal{L} \subseteq \mathbb{Q}^n$ 的一组基和一个目标向量 $\boldsymbol{t} \in \mathbb{Q}^n$，输出一个向量 $\boldsymbol{x} \in \mathcal{L}$，使其满足 $\|\boldsymbol{x} - \boldsymbol{t}\|_p =$ 最小值$_{\boldsymbol{y} \in \mathcal{L}} \|\boldsymbol{y} - \boldsymbol{t}\|_p$。

在欧几里得范数下，这两个问题都可以在时间 $2^{n+o(n)}$多项式（$|I|$）内 [ADRS15、ADS15]。我们将使用以下两个结果。

定理2.10 （[ADS15], 推论 6.5）。 存在一种随机化算法，给定一组基，基于格$\mathcal{L} \subseteq \mathbb{Q}^n$ 的秩为 n 且目标向量为 $\boldsymbol{t} \in \mathbb{Q}^n$，输出一个属于 $\mathcal{L}$ 的向量；其以至少 $1/2$的概率是 $\boldsymbol{t}$ 在 ℓ_2 范数下的最近向量。[6] 其运行时间为 $2^{n+o(n)}$多项式（$|I|$）。

注意到，最近向量问题也可以等价地定义为在格平移中寻找一个最短向量。我们将经常采用这一视角。

我们将使用以下采样器，来自 [ADRS15]。

定理 2.11 ([ADRS15], 定理 3.7)。 存在一种算法，给定一个秩为 n 的格 $\mathcal{L} \subseteq \mathbb{Q}^n$ 的基、参数 $s > 0$ 和 $\kappa \ge \Omega(n)$，输出 $2^{n/2}$ 个 $\mathcal{L}$ 的向量，其联合分布与从 $D_{\mathcal{L},\ s}$ 中抽取 $2^{n/2}$ 个独立样本的分布之间的统计距离至多为 $e^{-\Omega(\kappa)}$。该算法的运行时间为 $2^{n+\mathsf{poly}\log(\kappa)+o(n)}$多项式($|I|$)。

[6] [ADS15，推论 6。5] 给出了常数成功概率。将算法重复 k 次，并保留与 $\boldsymbol{t}$ 最接近的输出 $1 - 2^{-\Omega(k)}$，即可将其提升至 $1/2$；我们只需使用这一概率。

在我们的 CVP 算法中，欧几里得CVP算法是在 $2\mathcal{L}$ 的一个陪集上、依据对角度量应用的。

推论 2.12。 存在一种随机化算法，给定秩为 n的格 $\mathcal{L}$的一组基 B 、一个向量$\boldsymbol{w} \in \mathbb{R}^n$ 和宽度 $\boldsymbol{s} \in \mathbb{R}^n_{>0}$，输出陪集 $2\mathcal{L} + \boldsymbol{w}$ 中的一个向量，该向量以至少 $1/2$的概率使

$$\sum_{j=1}^{n} \frac{y_j^2}{s_j^2} \qquad over\ \boldsymbol{y} \in 2\mathcal{L} + \boldsymbol{w}.$$

其运行时间为 $2^{n+o(n)}$多项式($|I|$)。

证明。 令 $D := \mathrm{diag}(1/s_1, \ldots, 1/s_n)$。每个 $\boldsymbol{y} \in 2\mathcal{L} + \boldsymbol{w}$ 都可以写成 $\boldsymbol{y} = 2B\boldsymbol{z} + \boldsymbol{w}$，其中 $\boldsymbol{z} \in \mathbb{Z}^n$，于是

$$\sum_{j=1}^{n} \frac{y_j^2}{s_j^2} = \|D\boldsymbol{y}\|^2 = \|2DB\boldsymbol{z} - (-D\boldsymbol{w})\|^2 .$$

因此， $\boldsymbol{y} = 2B\boldsymbol{z} + \boldsymbol{w}$ 是最小化元，当且仅当 $2DB\boldsymbol{z}$ 是格 $\mathcal{L}(2DB)$中 $-D\boldsymbol{w}$ 的最近向量，且采用 ℓ_2 范数。对基 $2DB$ 和目标向量 $-D\boldsymbol{w}$运行定理2.10 中的算法；如果返回$\boldsymbol{v}$，则输出 $D^{-1}\boldsymbol{v} + \boldsymbol{w}$。（如果 $\boldsymbol{v} \notin \mathcal{L}($ $2DB$，可通过求解线性方程组来检验，则输出 $\boldsymbol{w}$代替。）

□

用 [MV13]替代定理2.10中的确定性算法后，推论 2.12中的算法总会输出一个最小化元，运行时间为 $2^{2n+o(n)}$ 多项式($|I|$)。

3 离散高斯混合

本节中 $p \in [1, 2)$ 和 $\alpha = p/2$。我们证明 $D_p(\mathcal{L} - \boldsymbol{t},\ r)$，其定义见公式 (2.12)，是欧几里得离散高斯分布的混合。按照公式 (2.8)，考虑一对取值于（X，S）的随机变量$\mathcal{L} - \boldsymbol{t}$）$\times\, \mathbb{R}^n_{>0}$ 及其联合密度

$$\Pr[X = \boldsymbol{x},\ S \in d\boldsymbol{s}] = \frac{\exp\left(-\pi \sum_{j=1}^{n} x_j^2/s_j^2\right)}{f_p(\mathcal{L} - \boldsymbol{t}, r)} \prod_{j=1}^{n} \left[g_{p/2}\left(\frac{\pi r^2}{s_j^2}\right) \frac{2\pi r^2}{s_j^3}\, ds_j \right]. \tag{3.1}$$

根据公式 (2.8)，将其应用于每个坐 标后， X 的边缘分布恰好是 $D_p(\mathcal{L} - \boldsymbol{t},\ r$).

对于 $\boldsymbol{s} \in \mathbb{R}^n_{>0}$ 和 $r > 0$，定义

$$h_p(\boldsymbol{s}, r) := \prod_{j=1}^{n} g_{p/2}\left(\frac{\pi r^2}{s_j^2}\right) \frac{2\pi r^2}{s_j^3},$$

对于 $\boldsymbol{x} \in \mathbb{R}^n$，定义

$$\rho(\boldsymbol{x}, \boldsymbol{s}) := \exp\left(-\pi \sum_{j} \frac{x_j^2}{s_j^2}\right).$$

Given $S = \boldsymbol{s}$, X 的分布是各向异性欧几里得离散高斯分布

$$\Pr[X = \boldsymbol{x} \mid S = \boldsymbol{s}] = \frac{\rho(\boldsymbol{x}, \boldsymbol{s})}{\rho(\mathcal{L} - \boldsymbol{t}, \boldsymbol{s})}. \tag{3.2}$$

利用公式（2.8），我们得到以下恒等式

$$f_p(\boldsymbol{x}, r) = \int_{\mathbb{R}^n_{>0}} \rho(\boldsymbol{x}, \boldsymbol{s}) h_p(\boldsymbol{s}, r) d\boldsymbol{s} \,. \tag{3.3}$$

因此，给定 $X = \boldsymbol{x}$ 时 S 的条件密度为

$$P_{\boldsymbol{x},r}(\boldsymbol{s}) \coloneqq \frac{\rho(\boldsymbol{x}, \boldsymbol{s})\, h_p(\boldsymbol{s}, r)}{f_p(\boldsymbol{x}, r)}, \tag{3.4}$$

而 S 的边缘密度为

$$\frac{h_p(\boldsymbol{s}, r)\, \rho(\mathcal{L} - \boldsymbol{t}, \boldsymbol{s})}{f_p(\mathcal{L} - \boldsymbol{t}, r)}. \tag{3.5}$$

我们将 $h_p(\cdot,\ r)$ 称为 $\boldsymbol{x}$ 处的先验分布，将 $P_{\boldsymbol{x},\ r}$ 称为后验分布。对于每个 $\boldsymbol{x} \in \mathbb{R}^n$，后验分布由公式（3.4）定义，并且只取决于 $\boldsymbol{x}$ 和 r，而不取决于 $\mathcal{L}$ 或 $\boldsymbol{t}$。用精度 $\pi r^2/s_j^2$ 表示时，它是倾斜稳定分布的乘积。事实上，公式（3.4）中每个坐标对应一个因子，并且当 $a_j \colon = \pi r^2/s_j^2$ 和 $\lambda_j \colon = x_j^2/r^2$ 时，我们有 $\pi x_j^2/s_j^2 = \lambda_j a_j$ 和 $|x_j|^p / r^p = \lambda_j^\alpha$；因此，变量代换 $a_j = \pi r^2/s_j^2$ 将第 j 个因子变为 G_α 的密度 $e^{\lambda_j^\alpha - \lambda_j a_j} g_\alpha(a_j)$，$\lambda_j$。因此，

$$\text{if } \boldsymbol{s} \sim P_{\boldsymbol{x},r}, \text{ then } \frac{\pi r^2}{s_1^2}, \ldots, \frac{\pi r^2}{s_n^2} \text{ are independent, and } \frac{\pi r^2}{s_j^2} \sim G_{\alpha,\, x_j^2/r^2}. \tag{3.6}$$

引理 3.1 (后验采样)。 存在一种算法，给定 $\boldsymbol{x} \in \mathbb{R}^n$ 和 $r > 0$，可从密度 $P_{\boldsymbol{x},\ r}$中输出一个样本，期望时间为 $O(n)$。

证明。 对于 $j = 1, \ldots, n$，分别独立地使用引理 2.6从 $G_{\alpha, x_j^2/r^2}$ 中采样得到 a_j，并输出满足$s_j \colon = r\sqrt{\pi/a_j}$的 $\boldsymbol{s}$。根据公式（3.6），$\boldsymbol{s}$ 的密度为 $P_{\boldsymbol{x},\ r}$。 □

引理 3.2 (先验采样)。 存在一种算法，给定 n 和 $r > 0$，可从定义在 $\mathbb{R}^n_{>0}$上的密度 $h_p(\cdot, r)$ 中输出一个样本，时间为 $O(n)$。

证明。 对于 $j \in [n]$，采样 a_j，从 G_α 中独立采样，使用 事实 2.4，并输出 $\boldsymbol{s}$，满足 $s_j = r\sqrt{\pi/a_j}$。根据公式（3.6），取 $\boldsymbol{x} = \boldsymbol{0}$。 □

备注： 我们从不从 D_p（$\mathcal{L}-\boldsymbol{t}$，$r$）中采样，也不从公式（3.5）的边缘分布 S中采样，该边缘分布包含格点和 ρ（$\mathcal{L}-\boldsymbol{t}$，$\boldsymbol{s}$）。对于较小的 r，分布 D_p（$\mathcal{L}-\boldsymbol{t}$，$r$）集中在 $\mathcal{L} - \boldsymbol{t}$的最短向量上，因此针对该分布的采样器将解决最近向量问题$_p$。我们的算法仅从先验分布（附录 A）和后验分布（第 4 节）中采样；这些分布不依赖于格，而只通过在所采样的对角度量中运行欧几里得算法来使用格。

4 $2^{O(n)}$ 最近向量问题$_p$算法

在本节中，$p \in$ （1，2）是固定的。将基和目标向量同时乘以基的各个条目的公分母，这只会使输入长度发生多项式级别的变化，并使所有距离乘以同一个因子，因此我们可以假设 $\mathcal{L} \subseteq \mathbb{Z}^n$；这一点仅用于引理 4.6。我们证明以下定理。

算法 1 最近向量问题$_p$ 用于 $p \in (1,2)$

输入： 格基 $B \in \mathbb{Z}^{n \times n}$；目标向量 $\boldsymbol{t} \in \mathbb{R}^n$；参数 T、N。

输出： $\boldsymbol{v}^* =$ 最近向量问题$_p(\mathcal{L}(B)\ \boldsymbol{t})$。

1: $r_1 = n \cdot$ 最大值$_j \|\boldsymbol{b}_j\|_p + \|\boldsymbol{t}\|_p$

2: **对于** $\boldsymbol{c} \in \{0,1\}^n$ **执行**

3: $\quad \boldsymbol{x}_{\boldsymbol{c}}^{(1)} = B\boldsymbol{c}$

4: $\quad$ **对** $i \in [T]$ **执行**

5: $\quad\quad r_i = r_1/2^{i-1}$

6: $\quad\quad$ **对** $j \in [N]$ **执行**

7: $\quad\quad\quad$ 示例 $\boldsymbol{s}_j \sim P_{\boldsymbol{x}_{\boldsymbol{c}}^{(i)} - \boldsymbol{t}, r_i}$

8: $\quad\quad\quad$ 求解$\boldsymbol{y}_j \leftarrow \underset{\boldsymbol{y} \in 2\mathcal{L} + \boldsymbol{x}_{\boldsymbol{c}}^{(i)} - \boldsymbol{t}}{\arg\min} \left(\sum_{k=1}^{n} \frac{y_k^2}{s_j^2,\ k} \right)$ ▷使用 推论 2.12中的算法

9: $\quad\quad$ **结束循环**

10: $\quad\quad$ 设 $\boldsymbol{w}$ 是 $\left\{ \boldsymbol{x}_{\boldsymbol{c}}^{(i)} - \boldsymbol{t}, \boldsymbol{y}_1, \ldots \boldsymbol{y}_N \right\} \subset \mathcal{L} - \boldsymbol{t}$ 中范数最小的向量

11: $\quad\quad$ 设置 $\boldsymbol{x}_{\boldsymbol{c}}^{(i+1)} = \boldsymbol{w} + \boldsymbol{t} \in 2\mathcal{L} + B\boldsymbol{c}$

12: $\quad$ **结束循环**

13: **结束循环**

14: **返回** 具有最小 $\|$值的向量 $\boldsymbol{x}_{\boldsymbol{c}}^{(T+1)}$ $\|\boldsymbol{x}_{\boldsymbol{c}}^{(T+1)} - \boldsymbol{t}\|_p$ 关于 $\boldsymbol{c} \in \{0,1\}^n$

定理 4.1。 设 $p \in (1, 2)$。给定一个秩为 n 的格 $\mathcal{L} \subseteq \mathbb{Q}^n$ 的基以及一个目标向量 $\boldsymbol{t} \in \mathbb{Q}^n$，*算法 1*（经过上述缩放）以至少 e^{-1} 的概率，在期望时间 $2^{(2+C_p)n+o(n)}\mathrm{poly}(|I|)$内输出一个在 ℓ_p 范数下距 $\boldsymbol{t}$ 最近的向量 $\mathcal{L}$，其中 C_p 的定义如下。

独立运行算法 $\lceil e\ln(1/\delta) \rceil$ 次，并返回距 $\boldsymbol{t}$ 最近的输出 $1-\delta$，即可得到一个至少以 $1-\delta$ 的概率获得最近向量，这证明了 定理 1.1。本节的其余部分将证明 定理 4.1。

设 $C_p := 2\left(\frac{2048}{p-1}\right)^{2/p}$ 和 $\boldsymbol{v}^* \in$ 最近向量问题$_p(\mathcal{L}(B)\ \boldsymbol{t})$。令

$$T = 1 + \left\lceil \frac{1}{p} \log_2 \left(\frac{16 n r_1^2}{p(p-1)} \right) \right\rceil$$

and

$$N = \left\lceil 2^{C_p n + 1} \log(T+1) \right\rceil .$$

考虑陪集 $M := 2\mathcal{L} + \boldsymbol{v}^* - \boldsymbol{t}$，并设 $d := \mathrm{dist}_p(\mathcal{L},\ \boldsymbol{t})$。我们将证明，该算法会在第 2 行中 $B\boldsymbol{c} \in 2\mathcal{L} + \boldsymbol{v}^*$的那次迭代中找到一个最近向量；在该次迭代中，每个 $\boldsymbol{x}_{\boldsymbol{c}}^{(i)}$都属于 $2\mathcal{L} + \boldsymbol{v}^*$，而第 $2\mathcal{L} + \boldsymbol{x}_{\boldsymbol{c}}^{(i)} - \boldsymbol{t}$ 8 行中的集合 为 。

该算法通过不断缩小 $\boldsymbol{x_c}$ 与目标向量之间的距离来运行。证明分为三个步骤。对于 $\boldsymbol{s} \in \mathbb{R}^n_{>0}$，令 $Y(\boldsymbol{s}) \subseteq M$ 为 $\sum_k y_k^2/s_k^2$ 在 M上的最小化元集合；当第 8 行中的 Corollary 2.12 调用成功时，它会返回 $Y(\boldsymbol{s}_j$中的一个元素。首先，我们证明，若 $\boldsymbol{x_c}$ 是最短向量 $\boldsymbol{v}^* - \boldsymbol{t}$，那么以高概率，每个 $\boldsymbol{y} \in Y(S)$ 的 $\|\boldsymbol{y}\|_p^p$ 都只比 d^p稍大。

接下来，我们将证明，当$P_{\boldsymbol{v}^*-\boldsymbol{t}、r}$ 和$P_{\boldsymbol{x}-\boldsymbol{t}、r}$ 满足 $\boldsymbol{x}$ 足够接近时，它们的密度 $\boldsymbol{t}$之间存在较大的重叠。最后，我们将这些结果结合起来，得出算法以足够大的概率成功缩短当前向量 $\boldsymbol{x_c}$ 的距离。现在，我们将证明这三个结果，然后证明定理 4.1。

引理 4.2。 对于任意 $r > 0$，都有

$$\Pr_{S\sim P_{\boldsymbol{v}^*-\boldsymbol{t},r}}\left[\|\boldsymbol{y}\|_p^p - d^p \le 8nr^p \text{ for every } \boldsymbol{y} \in Y(S)\right] \ge 1 - 2^n \cdot e^{-4n}.$$

证明。 固定一个坐标 $j \in [n]$，并记 $u = v_j^* - t_j$。对于固定的 $s > 0$，考虑函数

$$f(z) \coloneqq |z|^p - \frac{\pi r^p}{s^2} z^2,$$

它表示第8行中求解的二次目标函数与所需目标函数之间的差距。容易验证， f 在处取得最大值

$$z_{\max} \coloneqq \left(\frac{ps^2}{2\pi r^p}\right)^{1/(2-p)}$$

with

$$f(z_{\max}) = \left(1 - \frac{p}{2}\right)\left(\frac{ps^2}{2\pi r^p}\right)^{p/(2-p)}.$$

因此，对于每个 $z \in \mathbb{R}$,

$$|z|^p \le \frac{\pi r^p}{s^2} z^2 + \left(1 - \frac{p}{2}\right)\left(\frac{ps^2}{2\pi r^p}\right)^{p/(2-p)}. \tag{4.1}$$

定义

$$\Delta_{j,r}(s) \coloneqq \frac{\pi r^p u^2}{s^2} + \left(1 - \frac{p}{2}\right)\left(\frac{ps^2}{2\pi r^p}\right)^{p/(2-p)} - |u|^p.$$

将其代入公式（4.1）并重新整理，可得

$$|z|^p - |u|^p \le \frac{\pi r^p}{s^2}(z^2 - u^2) + \Delta_{j,r}(s).$$

令 $\boldsymbol{y} \in Y(S)$。代入 $z = y_j$ 并对 j 求和，可得

$$\begin{aligned}\|\boldsymbol{y}\|_p^p - d^p &\le \pi r^p \sum_j \frac{y_j^2 - (v_j^* - t_j)^2}{S_j^2} + \sum_j \Delta_{j,r}(S_j) \\ &\le \sum_j \Delta_{j,r}(S_j),\end{aligned}$$

其中 最后一个不等式成立是因为 $\boldsymbol{v}^* - \boldsymbol{t} \in M$ 和 $\boldsymbol{y}$ 使 $\sum_k y_k^2/S_k^2$ 在 M 上取得最小值 .

接下来，我们有如下断言。

命题 4.3。

$$\mathbb{E}_{S\sim P_{\boldsymbol{v}^*-\boldsymbol{t},r}}\left[\exp\left(\frac{\Delta_{j,r}(S_j)}{2r^p}\right)\right]\le 2.$$

证明 命题 4.3。 固定一个坐标 $j\in[n]$，令 $u=v_j^*-t_j$ 和 $a=\pi r^2/s^2$。根据 公式（3.4），我们有，在一维情况下，

$$P_{u,r}(s)=\frac{e^{-\pi u^2/s^2}h_p(s,r)}{e^{-|u|^p/r^p}}=\frac{e^{-\pi u^2/s^2}}{e^{-|u|^p/r^p}}\cdot g_\alpha\left(\frac{\pi r^2}{s^2}\right)\frac{2\pi r^2}{s^3}.$$

a 的条件密度为

$$g_\alpha(a)\exp\left(-\frac{u^2}{r^2}a+\frac{|u|^p}{r^p}\right).$$

此外，

$$\frac{\Delta_{j,r}(s)}{r^p}=\frac{u^2}{r^2}a+\kappa_p a^{-q}-\frac{|u|^p}{r^p},$$

其中，在中间一项中，我们使用了以下事实： $p(q+1)=2q$。

因此，

$$\begin{aligned}
\mathbb{E}\left[e^{\Delta_{j,r}(S_j)/(2r^p)}\right]&=e^{|u|^p/(2r^p)}\int_0^\infty g_\alpha(a)e^{-u^2a/(2r^2)+\kappa_p a^{-q}/2}\,da\\
&\le 2\beta\, e^{|u|^p/(2r^p)}\int_0^\infty g_\alpha(\beta a)e^{-u^2a/(2r^2)}\,da, && \text{(Lemma 2.5)}\\
&=2\exp\left(\frac{|u|^p}{2r^p}\right)\exp\left(-\frac{|u|^p}{(2\beta)^{p/2}r^p}\right) && \text{(Equation (2.7))}\\
&=2 && \text{(since } (2\beta)^{p/2}=2\text{).}
\end{aligned}$$

命题的证明到此结束。 □

因此，如果某个 $\boldsymbol{y}\in Y(S)$ 具有 $\|\boldsymbol{y}\|_p^p-d^p>8nr^p$，那么 $\sum_j \Delta_{j,\,r}(S_j)>8nr^p$。现在，根据 公式（3.6），$S\sim P_{\boldsymbol{v}^*-\boldsymbol{t}\text{的坐标}r}$ 相互独立，因此根据马尔可夫不等式和命题 4.3，

$$\Pr_{S\sim P_{\boldsymbol{v}^*-\boldsymbol{t},r}}\left[\sum_j\Delta_{j,r}(S_j)>8nr^p\right]=\Pr\left[\prod_j e^{\Delta_{j,r}(S_j)/(2r^p)}>e^{4n}\right]\le e^{-4n}\prod_j\mathbb{E}\left[e^{\Delta_{j,r}(S_j)/(2r^p)}\right]\le 2^n e^{-4n}.$$

□

引理 4.4。 令 $0<\tau\le 1/2$，并令 $\boldsymbol{x}\in 2\mathcal{L}+\boldsymbol{v}^*$ 满足 $\|\boldsymbol{x}-\boldsymbol{t}\|_p^p\le d^p+8n(2r)^p$。我们有

$$I_\tau:=\int P_{\boldsymbol{v}^*-\boldsymbol{t},r}(\boldsymbol{s})^{1-\tau}P_{\boldsymbol{x}-\boldsymbol{t},r}(\boldsymbol{s})^\tau d\boldsymbol{s}\ge\exp\left(-\frac{1024\tau^{p/2}n}{p-1}\right).$$

证明。 根据 公式（3.4），我们有

$$
\begin{aligned}
I_\tau &= \exp\left(\frac{(1-\tau)d^p + \tau\left\|\boldsymbol{x}-\boldsymbol{t}\right\|_p^p}{r^p}\right) \\
&\quad \times \int \exp\left(-\pi \sum_j \left(\frac{(1-\tau)(v_j^*-t_j)^2 + \tau(x_j-t_j)^2}{s_j^2}\right)\right) h_p(\boldsymbol{s}, r)d\boldsymbol{s} \\
&= \exp\left(-\frac{\sum_j J_\tau(v_j^*-t_j, x_j-t_j)}{r^p}\right),
\end{aligned}
$$

其中我们已使用了最后一个等式中使用了公式（3.3），并且 J 的定义见引理 2.2。

回顾由于 $\boldsymbol{x}-\boldsymbol{t}$，$\boldsymbol{v}^*-\boldsymbol{t} \in M$，我们有

$$
\frac{\boldsymbol{x}+\boldsymbol{v}^*}{2} \in \mathcal{L},
$$

因此

$$
\left\|\frac{\boldsymbol{x}+\boldsymbol{v}^*}{2} - \boldsymbol{t}\right\|_p^p \geq d^p. \tag{4.2}
$$

利用引理 2.2,

$$
\begin{aligned}
\sum_j J_\tau(v_j^*-t_j, x_j-t_j) &\leq \frac{64\tau^{p/2}}{p-1}\sum_j \left(\frac{|x_j-t_j|^p + \left|v_j^*-t_j\right|^p}{2} - \left|\frac{x_j+v_j^*}{2} - t_j\right|^p\right) \\
&= \frac{64\tau^{p/2}}{p-1}\left(\frac{\|\boldsymbol{x}-\boldsymbol{t}\|_p^p + \|\boldsymbol{v}^*-\boldsymbol{t}\|_p^p}{2} - \left\|\frac{\boldsymbol{x}+\boldsymbol{v}^*}{2} - \boldsymbol{t}\right\|_p^p\right) \\
&\leq \frac{32\tau^{p/2}}{p-1}\left(\|\boldsymbol{x}-\boldsymbol{t}\|_p^p - d^p\right) \qquad (4.3) \\
&\leq \frac{1024\tau^{p/2}nr^p}{p-1}, \qquad (4.4)
\end{aligned}
$$

其中在等式 (4.3) 中我们使用了等式 (4.2)，并且在等式 (4.4) 中我们使用了假设$\|\boldsymbol{x}-\boldsymbol{t}\|_p^p \leq d^p + 8n\,(2r)^p$ 以及对于 $p \in (1, 2)$，$2^p \leq 4$这一事实。将其代入 I_τ的定义即可得到该断言。

□

引理 4.5。 对于任意满足$\|\boldsymbol{x}-\boldsymbol{t}\|_p^p \leq d^p + 8n\,(2r)^p$ 的 $r > 0$ 和 $\boldsymbol{x} \in 2\mathcal{L} + \boldsymbol{v}^*$，我们有

$$
\Pr_{S \sim P_{\boldsymbol{x}-\boldsymbol{t}, r}}\left[\|\boldsymbol{y}\|_p^p \leq d^p + 8nr^p \text{ for every } \boldsymbol{y} \in Y(S)\right] \geq 2^{-C_p n}.
$$

证明。 令 $\tau_p = 2/C_p$ 代入 引理 4.4 并注意到

$$
I_{\tau_p} \geq e^{-n/2}. \tag{4.5}
$$

Let

$$
E := \left\{\boldsymbol{s} : \|\boldsymbol{y}\|_p^p \leq d^p + 8nr^p \text{ for every } \boldsymbol{y} \in Y(\boldsymbol{s})\right\}.
$$

由引理 4.2 可知

$$
P_{\boldsymbol{v}^*-\boldsymbol{t}, r}(E^c) \leq \exp\left(-\left(4 - \ln 2\right)n\right). \tag{4.6}
$$

接下来，回顾 I_τ 的定义，该定义来自引理 4.4。将积分拆分到 E 和 E^c上，并使用 H¨older 不等式（定理 2.3）以及 $f = P_{\boldsymbol{v}^*-\boldsymbol{t},\ r}$, $g = P_{\boldsymbol{x}-\boldsymbol{t},\ r}$ $p = 1/(1-\tau)$、 $q = 1/\tau$，可得

$$\begin{aligned} I_\tau &\le P_{\boldsymbol{v}^*-\boldsymbol{t},r}(E)^{1-\tau} \cdot P_{\boldsymbol{x}-\boldsymbol{t},r}(E)^{\tau} + P_{\boldsymbol{v}^*-\boldsymbol{t},r}(E^c)^{1-\tau} \cdot P_{\boldsymbol{x}-\boldsymbol{t},r}(E^c)^{\tau} \\ &\le P_{\boldsymbol{x}-\boldsymbol{t},r}(E)^{\tau} + P_{\boldsymbol{v}^*-\boldsymbol{t},r}(E^c)^{1-\tau}. \end{aligned} \tag{4.7}$$

结合公式 (4.5) 至(4.7) 并令 $\tau = \tau_p \le \frac{1}{2}$，可得 $P_{\boldsymbol{x}-\boldsymbol{t},\ r}(E)^{\tau_p} \ge e^{-n/2} - e^{-(4-\ln 2)n/2} \ge \frac{1}{2} e^{-n/2}$，从而

$$P_{\boldsymbol{x}-\boldsymbol{t},r}(E) \ge \left(\tfrac{1}{2} e^{-n/2}\right)^{C_p/2} = 2^{-C_p/2} e^{-C_p n/4} \ge 2^{-C_p n},$$

其中，最后一个不等式对所有 $n \ge 1$ 都成立，因为 $n \ln 2 - \frac{n}{4} \ge \ln 2$。 □

引理 4.6。 设 $p \in (1,\ 2)$， $\mathcal{L} \subset \mathbb{Z}^n$ 为格，且 $\boldsymbol{t} \in \mathbb{R}^n$。任取满足$\mathrm{dist}_p(\mathcal{L},\ \boldsymbol{t}) < \|\boldsymbol{x} - \boldsymbol{t}\|_p$ 的 $\boldsymbol{x} \in 2\mathcal{L} + \boldsymbol{v}^*$。令 $r \in \mathbb{R}$ 满足 $\|\boldsymbol{x} - \boldsymbol{t}\|_p \le r$ 且$\mathrm{dist}_p(\mathcal{L},\ \boldsymbol{t}) \le r$. 那么，

$$\|\boldsymbol{x} - \boldsymbol{t}\|_p^p \ge \mathrm{dist}_p(\mathcal{L}, \boldsymbol{t})^p + p(p-1) r^{p-2}.$$

证明。令 $\boldsymbol{v}^* \in \mathcal{L}$ 使得 $\|\boldsymbol{v}^* - \boldsymbol{t}\|_p = \mathrm{dist}_p(\mathcal{L},\ \boldsymbol{t})$。对于 $-r \le z \le r$，考虑函数

$$z \longmapsto |z|^p - \frac{p(p-1)}{2} r^{p-2} z^2.$$

该函数是凸函数，因此我们有，对于 $z_1,\ z_2 \in [-r, r]$,

$$\frac{|z_1|^p + |z_2|^p}{2} - \left|\frac{z_1 + z_2}{2}\right|^p \ge \frac{p(p-1) r^{p-2}}{8} (z_1 - z_2)^2 .$$

逐坐标应用这一点，我们得到

$$\begin{aligned} \frac{\|\boldsymbol{x} - \boldsymbol{t}\|_p^p + \mathrm{dist}_p(\mathcal{L}, \boldsymbol{t})^p}{2} - \left\|\frac{\boldsymbol{x} + \boldsymbol{v}^*}{2} - \boldsymbol{t}\right\|_p^p \\ \ge \frac{p(p-1)}{8} r^{p-2} \|\boldsymbol{x} - \boldsymbol{v}^*\|_2^2. \end{aligned}$$

由于 $\boldsymbol{x} - \boldsymbol{v}^* \in 2\mathcal{L}$，我们有 $\|\boldsymbol{x} - \boldsymbol{v}^*\|_2^2 \ge 4$，因此

$$\begin{aligned} \|\boldsymbol{x} - \boldsymbol{t}\|_p^p - d^p &\ge \frac{p(p-1)}{4} r^{p-2} \|\boldsymbol{x} - \boldsymbol{v}^*\|_2^2 \\ &\ge p(p-1) r^{p-2}, \end{aligned}$$

这就证明了该断言。 □

现在我们可以证明主要结果了。

证明定理 *4.1*。 **正确性**。 设 $\boldsymbol{c}$ 满足 $B\boldsymbol{c} \in 2\mathcal{L} + \boldsymbol{v}^*$。我们将证明，算法在线 2 的这次迭代中成功。假设在第 i 次循环迭代（第 4 行）开始时，我们有 $\left\|\boldsymbol{x}_{\boldsymbol{c}}^{(i)} - \boldsymbol{t}\right\|_p^p \le d^p + 8n\,(2r_i)^{\ p}$；对于 $i = 1$，这是因为 $\|B\boldsymbol{c} - \boldsymbol{t}\|_p \le r_1$。于是，对于第 j 行中的任意6,

根据 引理 4.5 ，当 $r = r_i$ 且 $\boldsymbol{x} = \boldsymbol{x}_{\boldsymbol{c}}^{(i)}$时，并且由于 推论 2.12 的调用以至少 $1/2$ 的概率成功，且独立于 $\boldsymbol{s}_j$,

$$\Pr[\|\boldsymbol{y}_j\|_p^p \le d^p + 8nr_i^p] \ge \tfrac{1}{2} \cdot 2^{-C_p n}.$$

N 样本相互独立（在给定先验分布的条件下），因此

$$\begin{aligned}\Pr[\forall j \in [N], \|\boldsymbol{y}_j\|_p^p > d^p + 8nr_i^p] &\le (1 - 2^{-C_p n - 1})^N \\ &\le \exp\left(-N \cdot 2^{-C_p n - 1}\right) \\ &\le \frac{1}{T+1},\end{aligned}$$

如果某个 $\boldsymbol{y}_j$满足 $\|\boldsymbol{y}_j\|_p^p \le d^p + 8nr_i^p = d^p + 8n(2r_{i+1})^p$，那么 $\boldsymbol{x}_{\boldsymbol{c}}^{(i+1)} - \boldsymbol{t}$也满足该条件，而 $\boldsymbol{x}_{\boldsymbol{c}}^{(i+1)} - \boldsymbol{t}$是候选项中最短的一个。通过对 T 次迭代进行归纳,

$$\Pr\left[\left\|\boldsymbol{x}_{\boldsymbol{c}}^{(T+1)} - \boldsymbol{t}\right\|_p^p \le d^p + 8nr_T^p\right] \ge \left(1 - \frac{1}{T+1}\right)^T \ge e^{-1}. \tag{4.8}$$

经过 T 次迭代，我们有

$$\begin{aligned}8nr_T^p &= 8nr_1^p \cdot 2^{-p(T-1)} \\ &\le \frac{1}{2}p(p-1)r_1^{p-2}\end{aligned} \tag{4.9}$$

根据我们对 T的选择。

由于每次迭代中保留的候选项都是最短的，$\left\|\boldsymbol{x}_{\boldsymbol{c}}^{(T+1)} - \boldsymbol{t}\right\|_p \le \|B\boldsymbol{c} - \boldsymbol{t}\|_p \le r_1$，并且$d \le \|\boldsymbol{t}\|_p \le r_1$。因此等式（4.9）和引理 4.6结合 $r = r_1$，以及等式（4.8），可推出以至少 e^{-1}的概率，$\boldsymbol{x}_{\boldsymbol{c}}^{(T+1)}$是 $\boldsymbol{t}$的一个最近向量；于是，所返回的向量与 $\boldsymbol{t}$的距离至少同样近，因此它也是一个最近向量。

复杂度。经过缩放后，$r_1 \ge 1$且 $\log r_1 \le \mathrm{poly}(|I|)$，因此 $T = \mathcal{O}_p(\log n + \log r_1) \le \mathrm{poly}(|I|)$。每次迭代中，第 6 行采样 $\boldsymbol{s}_j$，期望时间为 $O(n)$（引理 3.1），并调用推论 2.12 的算法，耗时为 $2^{n+o(n)}\mathrm{poly}(|I|)$。因此该算法的期望运行时间为

$$2^n \cdot T \cdot N \cdot 2^{n+o(n)}\mathrm{poly}(|I|) = 2^{(2+C_p)n+o(n)}\mathrm{poly}(|I|)$$

如断言所述。

□

注（非满秩格）。本节中的所有内容都适用于秩为 $k < n$、基为 $B \in \mathbb{Z}^{n\times k}$ 的格 $\mathcal{L} \subseteq \mathbb{Z}^n$，以及任意目标向量 $\boldsymbol{t} \in \mathbb{Q}^n$，该目标向量不一定属于 $\mathcal{L}$ 的张成空间。此时，$\mathcal{L}$ 中有 2^k 个 $2\mathcal{L}$ 的陪集，并且将推论 2.12 应用于秩为 k 的格。不过，宽度 $\boldsymbol{s}$ 仍然为 $\mathbb{R}^n$ 的 n 个坐标各对应一个坐标；而引理 4.2 、 4.4 和4.5 中的界限保持不变，因为它们是逐坐标乘积。因此，运行时间为 $2^{2k+C_p n+o(n)}\mathrm{poly}(|I|)\log(2/\delta)$，关于维数 n 为单指数。

参考文献

[ABB+23] Divesh Aggarwal、Huck Bennett、Zvika Brakerski、Alexander Golovnev、Rajendra Kumar、Zeyong Li、Spencer Peters、Noah Stephens-Davidowitz 和 Vinod Vaikuntanathan。超越多项式时间的格问题。载于第 55 届年度ACM计算理论研讨会（STOC）论文集，第 1516–1526 页，2023 年。https://arxiv.org/abs/2211. 11693. 1[ABGS21] Divesh Aggarwal、Huck Bennett、Alexander Golovnev 和 Noah Stephens-Davidowitz。CVP(P) 的精细化困难性——我们能证明的一切（以及其他无从证明的内容）。载于第 32 届年度ACM-SIAM离散算法研讨会（SODA）论文集，第 1816–1835 页。SIAM，2021 年。https://arxiv.org/abs/1911.02440. 1, 2[ABSS97] Sanjeev Arora、L´aszl´o Babai、Jacques Stern 和 Z. Sweedyk。格、编码和线性方程组中近似最优解的困难性。《计算机与系统科学杂志》，54(2):317–331，1997 年。https://doi.org/10.1006/jcss.1997.1472. 1[AC21] Divesh Aggarwal 和 Eldon Chung。关于格中最短线性无关向量具体困难性的一则注记。《信息处理快报》，167:106065，2021 年。https: //arxiv.org/abs/2005.11654. 1[ACK+21] Divesh Aggarwal、Yanlin Chen、Rajendra Kumar、Zeyong Li 和 Noah Stephens-Davidowitz。不同 p 范数下 SVP 与最近向量问题之间的保维归约。载于第 32 届年度ACM-SIAM离散算法研讨会（SODA）论文集，第 2444–2462 页。SIAM，2021 年。https://arxiv.org/abs/2104.06576. 3, 5[AD97] Mikl´os Ajtai 和 Cynthia Dwork。具有最坏情况与平均情况等价性的公钥密码系统。载于第 29 届年度ACM计算理论研讨会（STOC）论文集，第 284–293 页，1997 年。https://doi.org/10.1145/258533.258604. 1[AdFM24] Sunil Arya、Guilherme D. da Fonseca 和 David M. Mount。经济的凸覆盖及其应用。《SIAM计算杂志》，53(4):1002–1038，2024 年。初步版本发表于 SODA 2023。https://arxiv.org/abs/2303.08349. 5[ADRS15] Divesh Aggarwal、Daniel Dadush、Oded Regev 和 Noah Stephens-Davidowitz。使用离散高斯采样在 2^n 时间内求解最短向量问题：扩展摘要。载于第四十七届年度ACM计算理论研讨会论文集，STOC ’15，第 733–742 页，美国纽约州纽约，2015 年。计算机协会。https: //arxiv.org/abs/1412.7994. 2, 4, 15[ADS15] Divesh Aggarwal、Daniel Dadush 和 Noah Stephens-Davidowitz。用 2^n 时间求解最近向量问题——离散高斯再显神威！载于 2015 年 IEEE 第 56 届年度计算机科学基础研讨会（FOCS），第 563–582 页。IEEE，2015 年。https://arxiv.org/abs/1504.01995. 2, 3, 4, 5, 7, 8, 15[AEPS25] Divesh Aggarwal、Thomas Espitau、Spencer Peters 和 Noah Stephens-Davidowitz。递归格约化——寻找短格向量的框架。载于算法简洁性研讨会（SOSA 2025），第 533–573 页。SIAM，2025 年。https://arxiv.org/ abs/2311.15064. 1, 2

[AEVZ02] Erik Agrell、Thomas Eriksson、Alexander Vardy 和 Kenneth Zeger。《格点中的最近点搜索》。《IEEE 信息论汇刊》，48(8):2201–2214，2002。https://doi.org/10.1109/TIT.2002.800499。1[AGMZ26] Divesh Aggarwal、Rishav Gupta、Aditya Morolia 和 Chuanqi Zhang。《注意差距？在指数时间假设下，最短向量问题的困难性不受影响！》载于第53届国际自动机、语言与程序设计学术会议（ICALP 2026），LIPIcs 第374卷，页码 8:1–8:24。Schloss Dagstuhl– Leibniz-Zentrum f¨ur Informatik，2026。https://arxiv.org/abs/2504.02695。1[AJ08] Vikraman Arvind 和 Pushkar S. Joglekar。《格问题的若干筛法算法》。载于 IARCS 软件技术基础与理论计算机科学年会（FSTTCS 2008），LIPIcs 第2卷，页码 25–36。Schloss Dagstuhl–Leibniz-Zentrum f¨ur Informatik，2008。https://doi.org/10.4230/LIPIcs.FSTTCS.2008.1738。2, 4[AJSW24] Divesh Aggarwal、Antoine Joux、Miklos Santha 和 Karol Wegrzycki。《完全区域内整数规划与无界子集和的多项式时间算法》。arXiv 预印本 arXiv:2407.05435，2024。https://arxiv.org/abs/2407.05435。9[Ajt96] Mikl´os Ajtai。《生成格问题的困难实例（扩展摘要）》。载于第28届 ACM 计算理论研讨会年会论文集（STOC），页码 99–108，1996。https://doi.org/10.1145/237814.237838。1[Ajt98] Mikl´os Ajtai。《 L_2 在随机化归约下是 NP-困难的》。载于第30届 ACM 计算理论研讨会年会论文集（STOC），页码 10–19，1998。https://doi.org/10.1145/276698.276705。1[AKKV11] Mikhail Alekhnovich、Subhash Khot、Guy Kindler 和 Nisheeth K. Vishnoi。《带预处理的最近向量问题近似的困难性》。《计算复杂性》，20(4):741–753，2011。初步版本发表于 FOCS 2005。https://doi.org/10.1007/ s00037-011-0031-3。1[AKS01] Mikl´os Ajtai、Ravi Kumar 和 D. Sivakumar。《最短格向量问题的筛法算法》。载于第33届 ACM 计算理论研讨会年会论文集（STOC），页码 601–610，2001。https://doi.org/10.1145/380752.380857。2[AKS02] Mikl´os Ajtai、Ravi Kumar 和 D. Sivakumar。《短格向量采样与最近格向量问题》。载于第17届 IEEE 计算复杂性会议年会论文集（CCC），页码 53–57，2002。https://doi.org/10.1109/CCC.2002.1004339。2[ALNS20] Divesh Aggarwal、Jian wei Li、Phong Q. Nguyen 和 Noah Stephens-Davidowitz。《重新审视滑动规约——填补最短向量问题近似中的空白》。载于《密码学进展—CRYPTO 2020》，计算机科学讲义第12171卷，页码 274–295。施普林格，2020。https://arxiv.org/abs/1908.03724。1, 2[AM74] David F. Andrews 和 Colin L. Mallows。《正态分布的尺度混合》。《皇家统计学会杂志》B辑，36(1):99–102，1974。6[AM18] Divesh Aggarwal 和 Priyanka Mukhopadhyay。《无穷范数下最短向量问题和最近向量问题的改进算法》。载于第29届国际算法与计算研讨会（ISAAC 2018），LIPIcs 第123卷，页码 35:1–35:13。Schloss Dagstuhl–Leibniz-Zentrum f¨ur Informatik，2018。https://arxiv.org/abs/ 1801.02358。2

[AR05] Dorit Aharonov 和 Oded Regev。《NP ∩与 coNP 中的格问题》。《ACM学报》，52(5):749–765，2005。https://doi.org/10.1145/1089023.1089025。1[AS18a] Divesh Aggarwal 和 Noah Stephens-Davidowitz。《最短向量问题的 (Gap/S)ETH困难性》。载于第50届 ACM SIGACT计算理论研讨会年会论文集（STOC），页码 228–238，2018。https://arxiv.org/abs/1712.00942。1[AS18b] Divesh Aggarwal 和 Noah Stephens-Davidowitz。《取平均值就行！一个简单得令人难以置信的 2^n 时间算法，用于最短向量问题（及最近向量问题）》。载于第1届算法简洁性研讨会（SOSA 2018），信息学开放获取丛书（OASIcs）第61卷，页码 12:1–12:19。Schloss Dagstuhl–Leibniz-Zentrum f¨ ur Informatik，2018。https://arxiv.org/ abs/1709.01535。2, 3[Bab86] L´aszl´o Babai。《论 Lov´ ász 格约化与最近格点问题》。《Combinatorica》，6(1):1–13，1986。https://doi.org/10.1007/BF02579403。1, 2[BD15] Nicolas Bonifas 和 Daniel Dadush。《Voronoi图上的短路径与带预处理的最近向量问题》。载于第26届 ACM-SIAM离散算法研讨会年会论文集（SODA），页码 295–314。SIAM，2015。https://arxiv.org/abs/1412. 6168。2[Ben23] Huck Bennett。《最短向量问题的复杂度》。《ACM SIGACT新闻》，54(1):37–61，2023。https://doi.org/10.1145/3586165.3586172。1[Ber29] Serge Bernstein。《关于绝对单调函数》。《数学学报》，52(1):1–66，1929。https://doi.org/10.1007/BF02592679。12[Ber08] Christian Berg。《Stieltjes–Pick–Bernstein–Schoenberg 及其与完全单调性的联系》。载于 Jorge Mateu 和 Emilio Porcu（编），《正定函数：从 Schoenberg 到时空挑战》，页码 15–45。海梅一世大学数学系，2008。12[BGS17] Huck Bennett、Alexander Golovnev 和 Noah Stephens-Davidowitz。《CVP的定量困难性》。载于第58届 IEEE计算机科学基础研讨会年会论文集（FOCS），页码 13–24，2017。https://arxiv.org/abs/1704.03928。1, 2[BK18] Johannes Bl¨omer 和 Kathl´en Kohn。《任意范数下格的 Voronoi 胞》。《SIAM应用代数与几何学报》，2(2):314–338，2018。https://arxiv.org/ abs/1512.00720。3[BL07] Sebastian B¨ocker 和 Zsuzsanna Lipt´ak。《一种快速简洁的找零钱问题算法》。《算法学》，48(4):413–432，2007。https://doi.org/10.1007/ s00453-007-0162-8。9[BLP+13] Zvika Brakerski、Adeline Langlois、Chris Peikert、Oded Regev 和 Damien Stehl´e。《带误差学习的经典困难性》。载于第45届 ACM 计算理论研讨会年会论文集（STOC），页码 575–584，2013。https://arxiv.org/abs/1306.0281。1[BN09] Johannes Bl¨omer 和 Stefanie Naewe。《最短向量、最近向量和连续最小值的采样方法》。《理论计算机科学》，410(18):1648–1665，2009。初步版本发表于 ICALP 2007。https://doi.org/10.1016/j.tcs.2008.12.045。2, 4, 5

[BN11] Johannes Bl¨omer 和 Stefanie Naewe。关于 ℓ_p范数下最近向量问题的求解。arXiv:1104.3720，2011。https://arxiv.org/abs/1104.3720。3，4[BP23] Huck Bennett 和 Chris Peikert。（近似）最短向量问题的困难性：通过 Reed–Solomon 码给出的简单证明。载于近似、随机化与组合优化（APPROX/RANDOM 2023），LIPIcs 第 275 卷，第 37:1–37:20 页。Schloss Dagstuhl–Leibniz-Zentrum f¨ur Informatik，2023。https://arxiv.org/abs/2202.07736。1[BPT22] Huck Bennett、Chris Peikert 和 Yi Tang。在 Gap-(S)ETH 下 BDD 和 SVP 的改进困难性。载于第 13 届理论计算机科学创新会议（ITCS 2022），LIPIcs 第 215 卷，第 19:1–19:12 页。Schloss Dagstuhl–Leibniz-Zentrum f¨ur Informatik，2022。https://arxiv.org/abs/2109.04025。1[Bri17] Karl Bringmann。一个用于子集和的近线性伪多项式时间算法。载于第二十八届 ACM-SIAM 离散算法研讨会论文集，SODA 2017，第 1073–1084 页。SIAM，2017。https://arxiv.org/abs/1610.04712。9[CH22] Timothy M. Chan 和 Qizheng He。关于找零及相关问题的进一步研究。《计算机与系统科学杂志》，124：159–169，2022。https://arxiv.org/abs/2110.02503。9[CMS76] John M. Chambers、Colin L. Mallows 和 B. W. Stuck。模拟稳定随机变量的一种方法。《美国统计学会杂志》，71(354)：340–344，1976。https://doi.org/10.1080/01621459.1976.10480344。13[CMZ25] Lin Chen、Yuchen Mao 和 Guochuan Zhang。和集与子集和中的长等差数列：构造性证明与高效见证。arXiv:2503.19299，2025。发表于第 57 届 ACM 计算理论研讨会（STOC 2025）论文集，第 2086–2097 页。https://arxiv.org/abs/2503.19299。9[CN99] Jin-Yi Cai 和 Ajay Nerurkar。将 SVP 近似到因子（$1+1/$维$^{\varepsilon}$）以内在随机化归约下是 NP-困难的。《计算机与系统科学杂志》，59(2)：221–239，1999。https://doi.org/10.1006/jcss.1999.1649。1[Dad12] Daniel Dadush。整数规划、格算法与确定性体积估计。博士论文，佐治亚理工学院，2012。https://hdl.handle.net/1853/44807。1，2，3，9[Dad14] Daniel Dadush。用于近似整数规划的随机筛法算法。《Algorithmica》，70(2)：208–244，2014。LATIN 2012 的预备版本。https://arxiv.org/abs/1109.2477。9[DER25] Daniel Dadush、Friedrich Eisenbrand 和 Thomas Rothvoss。从近似整数规划到精确整数规划。《Mathematical Programming》，210：223–241，2025。IPCO 2023 的预备版本。https://arxiv.org/abs/2211.03859。3，9[Dev09] Luc Devroye。指数倾斜与多项式倾斜稳定分布的随机变量生成。《ACM建模与计算机仿真汇刊》，19(4)：18:1–18:20，2009。https://doi.org/10.1145/1596519.1596523。13，14[Din02] Irit Dinur。将 SVP 近似到近多项式因子以内是 NP-困难的。《理论计算机科学》，285(1)：55–71，2002。https://doi.org/10.1016/S0304-3975(01)00290-0。1

[DK16] Daniel Dadush 和 G´abor Kun。格点稀疏化与近似最近向量问题。《计算理论》，12(2)：1–34，2016。SODA 2013 的预备版本。https://arxiv.org/abs/1212.6781。2，5[DKRS03] Irit Dinur、Guy Kindler、Ran Raz 和 Shmuel Safra。将 CVP 近似到近多项式因子以内是 NP-困难的。Combinatorica，23(2)：205–243，2003。https://doi.org/10.1007/s00493-003-0019-y。1[DPV11] Daniel Dadush、Chris Peikert 和 Santosh Vempala。在任意范数下通过 M-椭球覆盖实现枚举型格点算法。载于第 52 届 IEEE计算机科学基础研讨会（FOCS）论文集，第 580–589 页。IEEE，2011。https://arxiv.org/abs/1011.5666。2，3，4[DRSD14] Daniel Dadush、Oded Regev 和 Noah Stephens-Davidowitz。关于带距离保证的最近向量问题。载于 2014 年 IEEE 第 29 届计算复杂性会议（CCC），第 98–109 页，2014。https://arxiv.org/abs/1409.8063。2[DV12] Daniel Dadush 和 Santosh S. Vempala。近似 M-椭球的确定性构造及其在格算法去随机化中的应用。载于第 23 届 ACM-SIAM 离散算法研讨会（SODA）论文集，第 1445–1456 页。SIAM，2012。https://arxiv.org/abs/1107.5478。2，3，4[DV13] Daniel Dadush 和 Santosh S. Vempala。通过 M-椭球计算体积的近最优确定性算法。《美国国家科学院院刊》，110(48)：19237–19245，2013。https://arxiv.org/abs/1201.5972。2，4[EHN11] Friedrich Eisenbrand、Nicolai H¨ahnle 和 Martin Niemeier。立方体覆盖与最近向量问题。载于第 27 届计算几何研讨会（SoCG）论文集，第 417–423 页，2011。https://arxiv.org/abs/1012.2289。2，5[Eis10] Friedrich Eisenbrand。整数规划与数的算法几何。载于 Michael J¨unger 等编，《整数规划50年》1958–2008，第 505–559 页。施普林格，2010。https://doi.org/10.1007/978-3-540-68279-0_14。1，9[EV22] Friedrich Eisenbrand 和 Moritz Venzin。在时间 $2^{0.802n}$ 内求近似 CVP。《计算机与系统科学杂志》，124：129–139，2022。ESA 2020 的预备版本。https://arxiv.org/abs/2005.04957。2，5[EW19] Friedrich Eisenbrand 和 Robert Weismantel。使用 Steinitz引理的邻近性结果与更快的整数规划算法。《ACM算法汇刊》（TALG），16(1)：1–14，2019。https://arxiv.org/abs/1707.00481。9[Fel71] William Feller。《概率论及其应用导论》，第二卷。John Wiley & Sons，第二版，1971。5[FM04] Uriel Feige 和 Daniele Micciancio。带预处理的格与编码问题的不可近似性。《计算机与系统科学杂志》，69(1)：45–67，2004。https://doi.org/10.1016/j.jcss.2004.01.002。1[FP85] Ulrich Fincke 和 Michael Pohst。改进的格中短长度向量计算方法，包括复杂度分析。《数学计算》，44(170)：463–471，1985。
h
t
t
p
s://
w
w
w.a
ms.org/journals/mcom/1985-44-170/S0025-5718-1985-0777278-8/S0025-5718-1985-0777278-8。

pdf。2

[FT87] Andr´as Frank 和 ´Eva Tardos。组合优化中同时丢番图逼近的一项应用。Combinatorica，7:49–65，1987。https://doi.org/10.1007/ BF02579200。1，3，9[Gen24] James E. Gentle。《矩阵代数：统计学中的理论、计算与应用》。Springer统计学丛书。施普林格，Cham，第三版，2024。https://doi.org/10. 1007/978-3-031-42144-0。7，10[GFH26a] Yiming Gao、Yansong Feng 和 Honggang Hu。离散高斯采样与 BDGL 解码相遇：在 $2^{0.5596n+o(n)}$ 时间内求解最短向量问题。密码学电子预印本档案，论文 2026/1844，2026。https://eprint.iacr.org/2026/1844。2[GFH26b] Yiming Gao、Yansong Feng 和 Honggang Hu。通过在超晶格上进行离散高斯采样，在 $2^{0.7314n+o(n)}$ 时间内求解最短向量问题。密码学电子预印本档案，论文 2026/1587，2026。https://eprint.iacr.org/2026/1587。2[GG00] Oded Goldreich 和 Shafi Goldwasser。论格问题不可近似性的界限。《计算机与系统科学杂志》，60(3):540–563，2000。https://doi.org/10.1006/jcss.1999.1686。1[GN08] Nicolas Gama 和 Phong Q. Nguyen。在 Mordell不等式范围内寻找短格向量。载于第40届年度 ACM计算理论研讨会（STOC）论文集，第207–216页，2008。https://doi.org/10.1145/1374376.1374408。1，2[GPV08] Craig Gentry、Chris Peikert 和 Vinod Vaikuntanathan。困难格的陷门与新的密码学构造。载于第40届年度 ACM计算理论研讨会（STOC）论文集，第197–206页，2008。https://eprint.iacr.org/2007/432。1[Hel85] Bettina Helfrich。构造 Minkowski 约化格基和 Hermite约化格基的算法。《理论计算机科学》，41(2–3):125–139，1985。https://www.sciencedirect. com/science/article/pii/0304397585900672。2[Hha26a] Minki Hhan。使用 q元陪集差分树，在 $2^{n/2+o(n)}$ 时间内寻找最短向量及其他。arXiv:2609.02764，2026。https://arxiv.org/abs/2609.02764。2[Hha26b] Minki Hhan。通过中点Hessian，在 $2^{0.6039n}$ 时间内求解最短向量问题。arXiv:2608.02478，2026。https://arxiv.org/abs/2608.02478。2[HK13] Robert Hildebrand 和 Matthias K¨oppe。一种用于拟凸多项式整数最小化的新型 Lenstra型算法，复杂度为 $2^{O(n \log n)}$。《离散优化》，10(1):69–84，2013。https://arxiv.org/abs/1006.4661。3，9[HKW26] Jeremy Ahrens Huang、Young Kun Ko 和 Chunhao Wang。近似CVP和最大割的（经典及量子）细粒度复杂性。载于第53届国际自动机、语言与程序设计学术会议（ICALP 2026），LIPIcs第374卷，第111:1–111:17页。Schloss Dagstuhl–Leibniz-Zentrum f¨ur Informatik，2026。https://arxiv.org/abs/2411.04124。1[HR12] Ishay Haviv 和 Oded Regev。最短向量问题几乎多项式因子范围内的基于张量的困难性。《计算理论》，8(23):513–531，2012。早期版本发表于 STOC 2007。https://arxiv.org/abs/1806.04087。1

[HRS20] Christoph Hunkenschr¨oder、Gina Reuland 和 Matthias Schymura。关于格的 Voronoi 单元的紧凑表示。《Mathematical Programming》，183：337–358，2020。https://arxiv.org/abs/1811.08532。2[HS07] Guillaume Hanrot 和 Damien Stehl´e。Kannan 最短格向量算法的改进分析。载于《密码学进展——CRYPTO 2007》，《计算机科学讲义》第 4622 卷，第 170–186 页。施普林格，2007。https://arxiv.org/abs/0705.0965。2, 4[JR19] Klaus Jansen 和 Lars Rohwedder。关于整数规划与卷积。载于第十届理论计算机科学创新会议（ITCS 2019），LIPIcs 第 124 卷，第 43:1–43:17 页。 Schloss Dagstuhl - Leibniz-Zentrum f¨ur Informatik，2019。https://arxiv. org/abs/1803.04744。9[Kan75] Marek Kanter。尺度变换下的稳定密度与全变差不等式。《概率年刊》，3(4)：697–707，1975。https://doi.org/10.1214/aop/1176996309。13[Kan83] Ravi Kannan。整数规划及相关格问题的改进算法。载于《第十五届 ACM 年度计算理论研讨会论文集》，1983 年 4 月 25–27 日，美国马萨诸塞州波士顿，第 193–206 页。ACM，1983。https://doi.org/10.1145/ 800061.808749。1, 2, 3, 9[Kan87] Ravi Kannan。闵可夫斯基凸体定理与整数规划。《数学运筹研究》，12：415–440，1987。https://doi.org/10.1287/moor.12.3.415。1, 2, 3, 4, 9[Kan92] Ravi Kannan。多胞体的格平移与Frobenius问题。《Combinatorica》，12(2)：161–177，1992。https://doi.org/10.1007/BF01204720。9[Kho05] Subhash Khot。格上最短向量问题近似的困难性。《ACM学报》，52(5)：789–808，2005。初步版本发表于 FOCS 2004。https://doi.org/10. 1145/1089023.1089027。1[Kim26] Jiseung Kim。一次离散高斯采样所需的 $2^{n/2+o(n)}$ 时间。arXiv:2608.03220，2026。https: //arxiv.org/abs/2608.03220。2[KL88] Ravi Kannan 和 L´aszl´o Lov´asz。覆盖极小值与无格点凸体。《数学年刊》，128(3)：577–602，1988。https://annals.math.princeton.edu/1988/ 128-3/p06。9[Kle22] Kim-Manuel Klein。无界子集和与Frobenius问题的细粒度复杂性。载于《2022 年 ACM-SIAM 离散算法研讨会论文集》（SODA 2022），第 3567–3582 页。SIAM，2022。https://arxiv.org/abs/2108. 05581。9[KPV12] Subhash Khot、Preyas Popat 和 Nisheeth K. Vishnoi。带预处理的最近向量问题的 $2^{\log^{1-\varepsilon} n}$ 困难性。载于第 44 届 ACM 年度计算理论研讨会（STOC）论文集，第 277–288 页，2012。https://arxiv.org/abs/1109.2176。1[KV24] Yunbum Kook 和 Santosh S. Vempala。高斯冷却与 Dikin 随机游走：用于对数凹采样的内点法。载于 Shipra Agrawal 和 Aaron Roth 编，《第三十七届学习理论会议论文集》，第 247 卷，《Proceedings of Machine

Learning Research》，第 3137–3240 页。PMLR，2024 年 6 月 30 日至 7 月 3 日。https://arxiv.org/abs/ 2307.12943。10[Len83] Hendrik W. Lenstra。固定变量数下的整数规划。《数学运筹研究》，8(4)：538–548，1983。https://doi.org/10.1287/MOOR.8.4.538。1, 3, 9[LLL82] Arjen K. Lenstra、Hendrik W. Lenstra, Jr. 和 L´aszl´o Lov´asz。具有有理系数的多项式因式分解。《Mathematische Annalen》，261(4)：515–534，1982。https://doi.org/10. 1007/BF01457454。1, 37[LLM06] Yi-Kai Liu、Vadim Lyubashevsky 和 Daniele Micciancio。一般格上的有界距离译码。载于《近似、随机化与组合优化》（APPROX-RANDOM 2006），《计算机科学讲义》第 4110 卷，第 450–461 页。施普林格，2006。https://doi.org/10.1007/11830924_41。2[LPR13] Vadim Lyubashevsky、Chris Peikert 和 Oded Regev。理想格与环上的带误差学习。《ACM学报》，60(6)：43:1–43:35，2013。初步版本发表于 EUROCRYPT 2010。https://eprint.iacr.org/2012/230。1[MG02] Daniele Micciancio 和 Shafi Goldwasser。《格问题的复杂性：密码学视角》，第 671 卷，《Kluwer 国际工程与计算机科学系列》。Kluwer Academic Publishers，2002。https://doi.org/10.1007/978-1-4615-0897-7。1[Mic01a] Daniele Micciancio。带预处理的最近向量问题的困难性。《IEEE 信息论汇刊》，47(3)：1212–1215，2001。https://doi.org/10.1109/ 18.915688。1[Mic01b] Daniele Micciancio。格中的最短向量难以在某个常数因子内近似。《SIAM计算杂志》，30(6)：2008–2035，2001。初步版本发表于 FOCS 1998。https://doi.org/10.1137/S0097539700373039。1[Mic04] Daniele Micciancio。近乎完美格、覆盖半径问题及其在 Ajtai连接因子中的应用。《SIAM计算杂志》，34(1)：118–169，2004。https: // doi.org/10.1137/S0097539703433511。1[Mic12] Daniele Micciancio。最短向量问题的不可近似性：迈向确定性归约。《计算理论》，8(22)：487–512，2012。https://doi.org/10.4086/toc. 2012.v008a022。1[MP12] Daniele Micciancio 和 Chris Peikert。格陷门：更简单、更紧凑、更快速、更小巧。载于《密码学进展——EUROCRYPT 2012》，《计算机科学讲义》第 7237 卷，第 700–718 页。施普林格，2012。https://eprint.iacr.org/2011/501。1[MR07] Daniele Micciancio 和 Oded Regev。基于高斯测度的最坏情况到平均情况归约。《SIAM计算杂志》，37(1)：267–302，2007。初步版本发表于 FOCS 2004。https://doi.org/10.1137/S0097539705447360。1[MR09] Daniele Micciancio 和 Oded Regev。基于格的密码学。载于 Daniel J. Bernstein、Johannes Buchmann 和 Erik Dahmen 编，《后量子密码学》，第 147–191 页。施普林格，2009。https://doi.org/10.1007/978-3-540-88702-7_5。1

[Muk21] Priyanka Mukhopadhyay。《最短向量问题和格上最近向量问题的更快可证明筛法算法》，适用于 ℓ_p 范数。《Algorithms》，14(12):362，2021年。https: //arxiv.org/abs/1907.04406。2, 4[MV10] Daniele Micciancio 和 Panagiotis Voulgaris。《最短向量问题的更快指数时间算法》。载于第21届 ACM-SIAM离散算法研讨会（SODA）论文集，第1468–1480页。SIAM，2010年。https://doi.org/10.1137/1. 9781611973075.119。2[MV13] Daniele Micciancio 和 Panagiotis Voulgaris。《一种基于 Voronoi 胞计算、用于大多数格问题的确定性单指数时间算法》。《SIAM计算杂志》，42(3):1364–1391，2013年。初步版本发表于 STOC 2010。https://doi.org/10.1137/100811970。2, 3, 4, 5, 16[MW15] Daniele Micciancio 和 Michael Walter。《开销极低的快速格点枚举》。载于第26届 ACM-SIAM离散算法研讨会（SODA）论文集，第276–294页。SIAM，2015年。https://eprint.iacr.org/2014/569。2[Nat24] 美国国家标准与技术研究院。《基于模格的密钥封装机制标准》。联邦信息处理标准出版物 FIPS 203，美国商务部，2024年8月。https://doi.org/10.6028/NIST.FIPS.203。1[Nol20] John P. Nolan。《单变量稳定分布：重尾数据模型》。Springer运筹学与金融工程系列。施普林格，Cham，瑞士，2020年。5, 6, 10, 13[NV08] Phong Q. Nguyen 和 Thomas Vidick。《用于最短向量问题的筛法算法具有实用性》。《数学密码学杂志》，2(2):181–207，2008年。https://doi.org/10. 1515/JMC.2008.009。2[NV22] M´arton Nasz´odi 和 Moritz Venzin。《凸体覆盖与最近向量问题》。《离散与计算几何》，67:1191–1210，2022年。https://arxiv.org/abs/1908. 08384。2, 5[Ope26] OpenAI。《欧几里得最近向量问题的 $n^{1/400}$-困难性》。载于《数学与理论计算机科学的十项进展》，第7章。OpenAI，2026年。技术手稿，2026年8月6日版本。https://cdn.openai.com/pdf/ten-proofs-oai.pdf。1[Pap81] Christos H. Papadimitriou。《整数规划的复杂度》。《ACM杂志》，28(4):765–768，1981年。https://doi.org/10.1145/322276.322287。9[Pei08] Chris Peikert。《格问题在 ℓ_p 范数下的困难性界限》。《计算复杂度》，17(2):300–351，2008年。初步版本发表于 CCC 2007。https://doi.org/10.1007/ s00037-008-0251-3。1[Pei09] Chris Peikert。《基于最坏情形最短向量问题的公钥密码系统》。载于第41届 ACM计算理论研讨会（STOC）论文集，第333–342页，2009年。https://eprint.iacr.org/2008/481。1[Pei16] Chris Peikert。《格密码学十年》。《理论计算机科学基础与趋势》，10(4):283–424，2016年。https://eprint.iacr.org/2015/939。1

[Poh81] Michael Pohst。《关于最小长度格向量、连续最小值和约化基的计算及其应用》。《ACM SIGSAM Bulletin》，15(1):37–44，1981年。https: //doi.org/10.1145/1089242.1089247。2[PS09] Xavier Pujol 和 Damien Stehl´e。《以 $2^{2.465n}$时间求解最短格向量问题》。密码学电子预印本档案，论文 2009/605，2009年。https://eprint.iacr.org/2009/605。2[RA96] Jorge L Ram´ırez-Alfons´ın。《Frobenius问题的复杂度》。《Combinatorica》，16:143–147，1996年。https://doi.org/10.1007/BF01300131。9[RA05] Jorge L. Ram´ırez Alfons´ın。《丢番图Frobenius问题》，牛津数学及其应用讲座系列第30卷。牛津大学出版社，2005年。https://doi.org/10.1093/acprof:oso/9780198568209.001.0001。9[Reg04a] Oded Regev。《通过预处理改进格问题和编码问题的不可近似性》。《IEEE 信息论汇刊》，50(9):2031–2037，2004年。初步版本发表于 CCC 2003。https://doi.org/10.1109/TIT.2004.833350。1[Reg04b] Oded Regev。《计算机科学中的格》。https://cims.nyu.edu/~regev/teaching/ lattices_fall_2004/，2004年。 [在线；访问日期：11-Jan-2025]。1[Reg09] Oded Regev。《关于格、带误差学习、随机线性码与密码学》。《ACM学报》，56(6):34:1–34:40，2009年。初步版本发表于 STOC 2005。https://arxiv.org/ abs/2401.03703。1[RR06] Oded Regev 和 Ricky Rosen。《格问题与范数嵌入》。载于第38届 ACM计算理论研讨会（STOC）论文集，第447–456页，2006年。https://doi.org/10.1145/1132516.1132581。2, 3[RR23] Victor Reis 和 Thomas Rothvoss。《子空间平坦性猜想与更快的整数规划》。载于第64届 IEEE计算机科学基础年会（FOCS 2023），美国加利福尼亚州圣克鲁斯，2023年11月6–9日，第974–988页。IEEE，2023年。https://arxiv.org/abs/2303.14605。1, 3, 4, 9[Rud87] Walter Rudin。《实分析与复分析》。McGraw-Hill，纽约，第3版，1987年。12[RV22] Thomas Rothvoss 和 Moritz Venzin。《在 $2^{0.802n}$时间内近似求解最近向量问题——现已适用于任意范数！》。载于《整数规划与组合优化》（IPCO 2022），计算机科学讲义第13265卷，第440–453页。施普林格，2022年。https://arxiv.org/abs/2110. 02387。2, 5[Sch38] I. J. Schoenberg。《度量空间与正定函数》。《美国数学会汇刊》，44(3):522–536，1938年。https://www.ams.org/journals/tran/1938-044-03/S0002-9947-1938-1501980-0/S0002-9947-1938-1501980-0.pdf。5[Sch87] Claus-Peter Schnorr。《多项式时间格基约化算法的层次结构》。《理论计算机科学》，53(2–3):201–224，1987年。https://doi.org/10.1016/ 0304-3975(87)90064-8。1, 2[SM21] Majid Salimi 和 Hamid Mala。《一种用于无界子集和问题特殊情形的多项式时间算法》。CoRR，abs/2103.09080，2021年。https://arxiv.org/abs/2103. 09080。9

[Ste16] Noah Stephens-Davidowitz。《离散高斯采样可归约为CVP和SVP》。载于《第27届ACM-SIAM离散算法年会》（SODA）论文集，第1748–1764页。SIAM，2016年。https://arxiv.org/abs/1506.07490。3[Ste17] Noah Stephens-Davidowitz。《格上的高斯测度》。博士学位论文，纽约大学，2017年。https://cs.nyu.edu/media/publications/stephens-davidowitz_noah.pdf。5[vEB81] Peter van Emde Boas。《另一个NP完全划分问题与格中短向量计算的复杂度》。技术报告MI-UvA-81-04，数学研究所，阿姆斯特丹大学，1981年。1[Wes87] Mike West。《正态分布的尺度混合》。Biometrika，74(3)：646–648，1987年9月。https://doi.org/10.1093/biomet/74.3.646。5，6[Zol86] V. M. Zolotarev。《一维稳定分布》，《数学专著译著》第65卷。美国数学学会，罗德岛州普罗维登斯，1986年。https: //doi.org/10.1090/mmono/065。13

一个用于最短向量问题的$2^{O(k)}$ 算法^p

我们将需要以下关于该格的超高斯质量的界。

引理 A.1。 设 $p \in [1,2)$，设 $\mathcal{L} \subseteq \mathbb{R}^n$ 为秩为 k的格，并设 $r > 0$。则

$$f_p(\mathcal{L}, r) \le 1 + 2^k k! \left(\frac{r}{\lambda_1^{(p)}}\right)^{pk} \exp\left(\frac{(\lambda_1^{(p)})^p}{2r^p}\right),$$

其中 $\lambda_1^{(p)} = \lambda_1^{(p)}(\mathcal{L})$。

证明。 对于 $u \ge 1$，设

$$N(u) := \left|\left\{\boldsymbol{y} \in \mathcal{L} \setminus \{\mathbf{0}\} : \|\boldsymbol{y}\|_p \le u\lambda_1^{(p)}\right\}\right|.$$

以 $\lambda_1^{(p)}/2$ 为半径、以 $\mathcal{L}$ 中的点为球心的开 ℓ_p 球两两不相交；以$\mathbf{0}$ 为球心的球，以及以所计数的 $N(u)$ 个点为球心的球，都包含于球 $\mathcal{B}_p^n(\mathbf{0},\ (u+1/2)\lambda_1^{(p)})$ 中。在张成空间 $\mathrm{span}(\mathcal{L})$ 中比较体积，

$$N(u) \le \frac{\mathrm{vol}_k\left(\mathcal{B}_p^n(\mathbf{0}, (u+1/2)\lambda_1^{(p)}) \cap \mathrm{span}(\mathcal{L})\right)}{\mathrm{vol}_k\left(\mathcal{B}_p^n(\mathbf{0}, \lambda_1^{(p)}/2) \cap \mathrm{span}(\mathcal{L})\right)} \le (1+2u)^k. \tag{A.1}$$

考虑函数

$$g(u) := \exp\left(-\left(\frac{u\lambda_1^{(p)}}{r}\right)^p\right).$$

对于任意非零的 $\boldsymbol{y} \in \mathcal{L}$，我们有

$$f_p(\boldsymbol{y}, r) = p\left(\frac{\lambda_1^{(p)}}{r}\right)^p \int_{\|\boldsymbol{y}\|_p/\lambda_1^{(p)}}^{\infty} u^{p-1} g(u) du.$$

由于对每个非零的 $\boldsymbol{y} \in \mathcal{L}$，都有 $\|\boldsymbol{y}\|_p / \lambda_1^{(p)} \ge 1$，对这些 $\boldsymbol{y}$ 求和可得

$$\begin{aligned} f_p(\mathcal{L}, r) &= 1 + \sum_{\boldsymbol{y} \in \mathcal{L}\setminus\{\mathbf{0}\}} \exp\left(-\frac{\|\boldsymbol{y}\|_p^p}{r^p}\right) \\ &= 1 + p\left(\frac{\lambda_1^{(p)}}{r}\right)^p \int_1^{\infty} u^{p-1} N(u) g(u)\, du \\ &\le 1 + p\left(\frac{\lambda_1^{(p)}}{r}\right)^p \int_1^{\infty} u^{p-1}(1+2u)^k g(u)\, du, \end{aligned}$$

其中，在最后一个不等式中，我们使用了公式 (A.1)。代入 $v = u^p$，因此 $dv = pu^{p-1}\, du$，即可得到

$$f_p(\mathcal{L}, r) \le 1 + \left(\frac{\lambda_1^{(p)}}{r}\right)^p \int_1^{\infty} (1+2v^{1/p})^k e^{-(\lambda_1^{(p)}/r)^p v}\, dv.$$

由于 $p \ge 1$ 和 $v \ge 1$，因此有 $v^{1/p} \le v$。于是

$$f_p(\mathcal{L}, r) \le 1 + \left(\frac{\lambda_1^{(p)}}{r}\right)^p \int_1^\infty (1+2v)^k e^{-(\lambda_1^{(p)}/r)^p v}\, dv.$$

现在我们来估计右侧的积分。代入

$$t = \frac{1}{2}\left(\frac{\lambda_1^{(p)}}{r}\right)^p (1+2v).$$

Then

$$dv = \left(\frac{r}{\lambda_1^{(p)}}\right)^p dt, \qquad 1 + 2v = 2\left(\frac{r}{\lambda_1^{(p)}}\right)^p t,$$

and

$$e^{-(\lambda_1^{(p)}/r)^p v} = e^{(\lambda_1^{(p)}/r)^p/2} e^{-t}.$$

因此，

$$\begin{aligned} f_p(\mathcal{L}, r) &\le 1 + 2^k \left(\frac{r}{\lambda_1^{(p)}}\right)^{pk} e^{(\lambda_1^{(p)}/r)^p/2} \int_{\frac{3}{2}(\lambda_1^{(p)}/r)^p}^\infty t^k e^{-t}\, dt \\ &\le 1 + 2^k \left(\frac{r}{\lambda_1^{(p)}}\right)^{pk} e^{(\lambda_1^{(p)}/r)^p/2} \int_0^\infty t^k e^{-t}\, dt \\ &= 1 + 2^k k! \left(\frac{r}{\lambda_1^{(p)}}\right)^{pk} e^{(\lambda_1^{(p)}/r)^p/2} \end{aligned}$$

其中，最后一个积分通过重复分部积分等于 $k!$。 □

我们以下述形式定理 1.2证明。

定理 A.2。 设 $p \in [1, 2)$。存在一种算法，给定秩为 k 的格 $\mathcal{L} \subseteq \mathbb{Q}^n$ 的一组基，能够以至少 $1 - e^{-k}$ 的概率输出格 $\mathcal{L}$ 中关于 ℓ_p 范数的最短非零向量。其运行时间为$2^{\sigma k + o(k)}$多项式$(|I|)$，其中 $\sigma := 1 + \log(2 + 1/\sqrt{2}) < 2.4368$。

我们在以下取值处应用 引理 A.1： r。

推论 A.3。 令 $p \in [1, 2)$ 和 $c > 0$，设 $\mathcal{L} \subseteq \mathbb{R}^n$ 是秩为 k 的格，设 $\lambda := \lambda_1^{(p)}(\mathcal{L})$，设$\lambda \le \lambda' \le (1 + \frac{1}{k+2})\lambda$，并设$r := \lambda'/(ck)^{1/p}$。那么 $b := (\lambda/r)^p$ 满足 $\frac{ck^2}{k+2} \le b \le ck$，并

$$f_p(\mathcal{L}, r) \le 1 + e^3\sqrt{k}\left(\frac{2}{c}\, e^{c/2-1}\right)^k.$$

证明。我们有 $b = ck(\lambda/\lambda')^p$。由于 $\lambda' \ge \lambda$，$b \le ck$。由于 $p \le 2$ 且 $(1+x)^{-2} \ge 1 - 2x$，我们有 $(\lambda/\lambda')^p \ge (1 + \frac{1}{k+2})^{-2} \ge \frac{k}{k+2}$，因此 $b \ge \frac{ck^2}{k+2}$。根据引理 A.1，$f_p(\mathcal{L}, r) - 1 \le 2^k\, k!\; b^{-k} e^{b/2}$。利用 $k! \le e\sqrt{k}(k/e)^k$，$b \ge \frac{ck^2}{k+2}$，$e^{b/2} \le e^{ck/2}$ 且 $(1 + \frac{2}{k})^k \le e^2$，

$$f_p(\mathcal{L}, r) - 1 \le e\sqrt{k}\left(1 + \frac{2}{k}\right)^k \left(\frac{2}{ec}\right)^k e^{ck/2} \le e^3\sqrt{k}\left(\frac{2}{c}\, e^{c/2-1}\right)^k.$$

□

算法 2 最短向量问题$_p$，适用于 $p \in [1,2)$ 输入：格 $\mathcal{L} \subseteq \mathbb{Q}^n$ 的一个秩为 k 的基 B。输出：$\mathcal{L}$ 中按 ℓ_p 范数衡量的一个最短非零向量。1：$c \leftarrow \frac{2}{1+2\sqrt{2}}$，$\gamma \leftarrow 1+\frac{1}{k+2}$，$K \leftarrow (n+2)^2$，$N \leftarrow \lceil 88\,k^{3/2}(2+1/\sqrt{2})^k \rceil$ 2：计算 $\mathcal{L}$ 的一个 LLL约化基，并令 ℓ 为其第一个向量的欧几里得长度 3：$\mathcal{C} \leftarrow \{\boldsymbol{b}_1\}$，其中 $\boldsymbol{b}_1$ 是LLL约化基中的第一个向量。4：对于 $j = 0, 1, \ldots, K$，执行 5：$\lambda' \leftarrow 2^{-(k-1)/2}\,\ell\,\gamma^j$，$r \leftarrow \lambda'/(ck)^{1/p}$ 6：对于 $i = 1, \ldots, N$，执行 7：从密度 $h_p(\cdot, r)$ 中采样 $\boldsymbol{s}$ ▷ 引理 3.2 8：在 $\mathcal{L}_{\boldsymbol{s}} := \mathrm{diag}(1/s_1, \ldots, 1/s_n)\mathcal{L}$ 上运行定理 2.11 的算法，参数为 1 且 $\kappa := C_1 k$；将每个输出向量乘以 $\mathrm{diag}(s_1, \ldots, s_n)$，并将其加到 $\mathcal{C}$ 9：结束循环 10：结束循环 11：返回 $\mathcal{C} \setminus \{\mathbf{0}\}$ 中范数 ℓ_p 最小的向量

这里 C_1 是一个足够大的常数，使得 定理 2.11中的统计距离至多为

$$\varepsilon := \frac{(2+1/\sqrt{2})^{-k}}{88\sqrt{k}} \qquad \text{for every } k \geq 1.$$

定理 *A.2* 的证明。设 $\boldsymbol{v}$ 是 $\mathcal{L}$ 在 ℓ_p 范数下的最短非零向量，并且 $\lambda := \|\boldsymbol{v}\|_p = \lambda_1^{(p)}(\mathcal{L})$。

正确的猜测。对于 $p \in [1,2]$，我们有 $\|\cdot\|_2 \leq \|\cdot\|_p \leq \sqrt{n}\,\|\cdot\|_2$，而 LLL-约化基的第一个向量的欧几里得长度为 $\ell \leq 2^{(k-1)/2}\lambda_1^{(2)}(\mathcal{L})$ [LLL82]。因此 $\lambda_0' := 2^{-(k-1)/2}\ell \leq \lambda \leq \sqrt{n}\,\ell$。设 j 为满足 $\lambda_j' := \lambda_0'\gamma^j \geq \lambda$的最小指标；则 $\lambda \leq \lambda_j' \leq \gamma\lambda$。此外 $j \leq K$，因为$\gamma^K \geq 2^{(k-1)/2}\sqrt{n} \geq \lambda/\lambda_0'$；事实上，$K \ln\gamma \geq \frac{(n+2)^2}{k+3} \geq \frac{(n+2)^2}{n+3} \geq n+1 \geq \ln(2^{(k-1)/2}\sqrt{n})$。我们考虑具有此 j 的外层循环迭代；其他迭代只会将 $\mathcal{L}$ 的向量添加到 $\mathcal{C}$ 中，这不会造成影响。

一次试验。固定 $\boldsymbol{s}$，并令 $q(\boldsymbol{s}) := \rho(\boldsymbol{v}, \boldsymbol{s})/\rho(\mathcal{L}, \boldsymbol{s})$。由于 $\rho(\boldsymbol{x}, \boldsymbol{s}) = e^{-\pi\|\mathrm{diag}(1/s_1,\ldots,1/s_n)\boldsymbol{x}\|^2}$，$q(\boldsymbol{s})$ 是在 $D_{\mathcal{L}_{\boldsymbol{s}},1}$ 下 $\mathrm{diag}(1/s_1, \ldots, 1/s_n)\boldsymbol{v}$ 的概率。令 m 为采样器输出的向量数；$m \geq \lfloor 2^{k/2} \rfloor \geq 2^{k/2-1}$。如果这些是来自 $D_{\mathcal{L}_{\boldsymbol{s}},1}$ 的 m 个独立样本，那么以 $(1-q)^m \leq e^{-mq} \leq 1/(1+mq)$ 的概率不会抽到 $\boldsymbol{v}$。因此，以至少.....的概率将 $\boldsymbol{v}$ 加入 $\mathcal{C}$

$$\frac{mq}{1+mq} - \varepsilon = \frac{\rho(\boldsymbol{v}, \boldsymbol{s})}{\rho(\mathcal{L}, \boldsymbol{s})/m + \rho(\boldsymbol{v}, \boldsymbol{s})} - \varepsilon.$$

现在对 $\boldsymbol{s} \sim h_p(\cdot, r)$ 取平均。对于随机变量 $X \geq 0$ 和 $Y \geq 0$，根据柯西–施瓦茨不等式应用于 $X = \frac{X}{\sqrt{Y}} \cdot \sqrt{Y}$，有 $\mathbb{E}[X^2/Y] \geq (\mathbb{E}\,X)^2/\mathbb{E}\,Y$。结合 $X = \rho(\boldsymbol{v}, \boldsymbol{s})^{1/2}$，得到

$$\Pr[\boldsymbol{v} \text{ is found in this trial}] \geq \frac{\left(\mathbb{E}\,\rho(\boldsymbol{v}, \boldsymbol{s})^{1/2}\right)^2}{\mathbb{E}\,\rho(\mathcal{L}, \boldsymbol{s})/m + \mathbb{E}\,\rho(\boldsymbol{v}, \boldsymbol{s})} - \varepsilon.$$

根据公式（3.3），对每个 $\boldsymbol{x} \in \mathbb{R}^n$，有 $\mathbb{E}\,\rho(\boldsymbol{x}, \boldsymbol{s}) = f_p(\boldsymbol{x}, r)$。因此，$\mathbb{E}\,\rho(\mathcal{L}, \boldsymbol{s}) = f_p(\mathcal{L}, r)$，$\mathbb{E}\,\rho(\boldsymbol{v}, \boldsymbol{s}) = f_p(\boldsymbol{v}, r)$，并且 $\mathbb{E}\,\rho(\boldsymbol{v}, \boldsymbol{s})^{1/2} = \mathbb{E}\,\rho(\boldsymbol{v}/\sqrt{2}, \boldsymbol{s}) = f_p(\boldsymbol{v}/\sqrt{2}, r)$。由于 $1/m \leq 2^{1-k/2}$，

$$\Pr[\boldsymbol{v} \text{ is found in this trial}] \geq \frac{f_p(\boldsymbol{v}/\sqrt{2}, r)^2}{2^{1-k/2} f_p(\mathcal{L}, r) + f_p(\boldsymbol{v}, r)} - \varepsilon. \tag{A.2}$$

分子和分母。令 $b := (\lambda/r)^p$；根据推论 A.3，$\frac{ck^2}{k+2} \le b \le ck$。于是 $f_p(\boldsymbol{v},r) = e^{-b} \le 1$，并且由于 $2^{1-p/2} \le \sqrt{2}$ 对 $p \ge 1$，$f_p(\boldsymbol{v}/\sqrt{2},r)^2 = e^{-2^{1-p/2}b} \ge e^{-\sqrt{2}\,ck}$。取 $c = \frac{2}{1+2\sqrt{2}}$ 得到 $c(\sqrt{2}+\frac{1}{2}) = 1$，即 $\frac{c}{2} - 1 = -\sqrt{2}c$。因此，根据推论 A.3，

$$2^{1-k/2} f_p(\mathcal{L},r) \le 2^{1-k/2} + 2e^3\sqrt{k}\,\Lambda^k, \qquad \text{where } \Lambda := \frac{\sqrt{2}}{c}\,e^{c/2-1} = \frac{\sqrt{2}}{c}\,e^{-\sqrt{2}c} \approx 1.2932.$$

由于 $\Lambda > 1$，方程 (A.2) 中的分母至多为 $(2 + 2e^3 + 1)\sqrt{k}\,\Lambda^k \le 44\sqrt{k}\,\Lambda^k$。由于 $e^{-\sqrt{2}c}/\Lambda = c/\sqrt{2} = (2+1/\sqrt{2})^{-1}$，

$$\Pr[\boldsymbol{v} \text{ is found in this trial}] \ge \frac{(2+1/\sqrt{2})^{-k}}{44\sqrt{k}} - \varepsilon = \frac{(2+1/\sqrt{2})^{-k}}{88\sqrt{k}}.$$

结论。 对于正确的猜测，N 次试验相互独立，因此 $\boldsymbol{v}$ 被所有试验漏掉的概率至多为

$$\left(1 - \frac{(2+1/\sqrt{2})^{-k}}{88\sqrt{k}}\right)^N \le \exp\left(-\frac{N}{88\sqrt{k}\,(2+1/\sqrt{2})^k}\right) \le e^{-k}.$$

如果 $\boldsymbol{v} \in \mathcal{C}$，则输出是一个最短非零向量。

运行时间。LLL 的运行时间为 $\mathrm{poly}(|I|)$。共有 $(K+1)N$ 次试验。每次试验以时间 $O(n)$ 对 $\boldsymbol{s}$ 进行采样（引理 3.2），调用定理 2.11 的算法，耗时 $2^{k+o(k)}\mathrm{poly}(|I|)$，并计算 $O(2^{k/2})$ 个向量及其 ℓ_p 范数。由于 $(K+1)N = O(n^2k^{3/2}(2+1/\sqrt{2})^k)$，总运行时间为 $2^{\sigma k+o(k)}\mathrm{poly}(|I|)$，其中 $\sigma = 1 + \log(2+1/\sqrt{2}) < 2.4368$。 □