Deterministic Construction of an Approximate M-Ellipsoid and its Applications to Derandomizing Lattice Algorithms

Daniel Dadush* Santosh Vempala†

Abstract

We give a deterministic $O(\log n)^n$-time and space algorithm for the *Shortest Vector Problem (SVP)* of a lattice under *any* norm, improving on the previous best deterministic $n^{O(n)}$-time algorithms for general norms. This approaches the $2^{O(n)}$-time and space complexity of the randomized sieve based SVP algorithms (Arvind and Joglekar, FSTTCS 2008), first introduced by Ajtai, Kumar and Sivakumar (STOC 2001) for ℓ_2-SVP, and the M-ellipsoid covering based SVP algorithm of Dadush et al. (FOCS 2011).

Here we continue with the covering approach of Dadush et al., and our main technical contribution is a deterministic approximation of an M-ellipsoid for any convex body. To achieve this we exchange the M-position of a convex body by a related position, known as the minimal mean width position of the polar body. We reduce the task of computing this position to solving a semi-definite program whose objective is a certain Gaussian expectation, which we show can be approximated deterministically.

1 Introduction

The Shortest Vector Problem (SVP) on lattices is a central algorithmic problem in the geometry of numbers, with applications to Integer Programming [13], factoring polynomials over the rationals [12], cryptanalysis (e.g., [21, 9, 20]), and much more. (An n-dimensional *lattice* L is a discrete additive subgroup of $\mathbb{R}^n$, and is generated as the set of integer linear combinations of some basis vectors $b_1, \ldots, b_k \in \mathbb{R}^n$, for some $k \leq n$.) The SVP is simply: given a lattice L represented by a basis, find a nonzero $v \in L$ such that $\|v\|$ is minimized, where $\|\cdot\|$ denotes a particular norm on $\mathbb{R}^n$.

The fastest known algorithms for solving SVP in general norms, are $2^{O(n)}$ time algorithms based on the AKS sieve [1, 2]. These algorithms use an exponential amount of randomness and guarantee the correctness of their outputs with high probability. Improving on this, [6] gave a $2^{O(n)}$ Las Vegas algorithm (i.e. only the runtime is random, not the correctness) for general norm SVP which uses only a polynomial amount of randomness. In this paper, building on the ideas of [6], we give a deterministic $O(\log n)^n$ algorithm for general norm SVP, hence completely eliminating the randomness while sustaining a moderate increase in the running time. The previous best deterministic complexity for general norm SVP is $n^{\Omega(n)}$.

To place our contribution in context, we review the ideas behind [6]. For the Euclidean norm, Micciancio and Voulgaris [16] showed how to solve the SVP and CVP in time $2^{O(n)}$, using a new enumeration technique based on the Voronoi cell of a lattice (the set of points in $\mathbb{R}^n$ closer to the origin than any other lattice point). Unfortunately, the direct generalization of their technique to other norms, i.e., using the associated Voronoi cell of the norm seems very difficult, even for other ℓ_p norms. In particular, many of the crucial properties of the ℓ_2-Voronoi cell either do not carry over or are not known to carry over for Voronoi cells of other norms, for example Voronoi cells of other norms are generally non-convex, and it is unknown whether a constant factor scaling of a general Voronoi cell contains at most $2^{O(n)}$ lattice points. In [6], Dadush et al. proposed a different approach that reduces SVP in general norms to enumeration in the ℓ_2 norm. Their key idea was to use the classical M-ellipsoid covering from convex geometry to cover a given convex body K by $2^{O(n)}$ translations of an ellipsoid. To solve SVP under $\|\cdot\|_K$ and a lattice L they enumerate lattice point inside a suitable scaling of K, namely any scaling $s > 0$ such that $sK \cap L \neq \emptyset$ and $\frac{s}{2}K \cap L = \emptyset$. At this scaling, it is not hard to argue via a simple volume bound that any translation of sK contains no more than $2^{O(n)}$ lattice points. To enumerate lattice points in sK, the idea is to cover sK using translations of an ellipsoid E, and then to enumerate lattice points in each of these ellipsoids, thereby reducing the problem to enumeration in ℓ_2 (which can be solved using the algorithm of [16]).

*School of Industrial and Systems Engineering, Georgia Tech. dndadush@gatech.edu

†School of Computer Science, Georgia Tech. vempala@gatech.edu

Both authors were supported in part by NSF awards AF-0915903 and AF-0910584.

The number of points in any of the ellipsoids is easily bounded as the number of translations of sK required to cover E times the number of points in any translation of sK. Let

$$N(A,B) = \inf\{|\Lambda| : \Lambda \subseteq \mathbb{R}^n, A \subseteq B + \Lambda\}$$

denote the number of translations of B required to cover A. Then it follows that complexity of the above reduction is bounded by $N(sK,E)N(E,sK)2^{O(n)}$. We state this formally in Section 5.

Thus, the question arises: given a convex body K, what is the minimum possible value of $N(K,E)N(E,K)$ for any ellipsoid E. An M-ellipsoid of a convex body K is an ellipsoid E with the following property:

$$N(K,E)N(E,K) \leq 2^{O(n)} \tag{1.1}$$

In words, the number of copies of E required to cover K times the number of copies of K to cover E is bounded by a single exponential in n. The existence of such an ellipsoid for any convex body was established by Milman [17]. We note that an M-ellipsoid can be quite different from the more classical John ellipsoid, e.g. the largest ellipsoid contained in K, since its volume can be an $n^{O(n)}$ factor off from K (e.g., the cube vs the unit ball) implying than $N(K,E) = n^{\Omega(n)}$.

A key ingredient in the approach of [6] is finding an M-ellipsoid of K. Indeed, the paper shows that the method of Klartag [11] gives a polynomial-time *randomized* algorithm to construct an M-ellipsoid with high probability (such an algorithm was implicit in his paper). Unfortunately, the algorithm makes essential use of random sampling over convex bodies (to estimate a covariance matrix) and seems inherently difficult to derandomize.

In this paper, we give a deterministic algorithm to build an "approximate" M-ellipsoid E for any convex body K. While we do not obtain the optimal covering bounds, we will guarantee that $N(K,E) = 2^{O(n)}$ and $N(E,K) = O(\log n)^n = 2^{O(n \log\log n)}$. Moreover, we show that this ellipsoid E can be computed in $O(\sqrt{\log n})^n$ time. This result and its consequence for the SVP are stated more precisely in the following theorems.

THEOREM 1.1. *There is deterministic algorithm that given any convex body $K \subset \mathbb{R}^n$, specified by a membership oracle, finds an ellipsoid E such that $N(K,E) \leq 2^{O(n)}$ and $N(E,K) \leq O(\log n)^n$. The time complexity of the algorithm (oracle calls and arithmetic operations) is $O(\sqrt{\log n})^n$ and its space complexity is polynomial in n.*

Using this theorem, and the techniques from [6], we obtain the following result:

THEOREM 1.2. *Given a lattice L by a basis and a norm $\|.\|_K$ specified by a convex body K, the shortest vector in L under the norm $\|.\|_K$ can be found in $O(\log n)^n$ time and space.*

We note that the current space complexity of the SVP algorithm also grows as $O(\log n)^n$ although we expect this can be improved to $2^{O(n)}$. Applications to other lattice problems (closest vector, integer programming) are described in Section 5. These results are based on two main ideas. The first is a convex program inspired by an existential approximation to the M-ellipsoid based on a position called the ℓ-position, given by Pisier [22]. The second is an algorithm for solving the convex program, where the key hurdle is an efficient deterministic approximation of the objective value at any given feasible point.

In the next section, we describe the ℓ-position which leads to the approximate M-ellipsoid. Then we give our convex programming based algorithm for computing the approximate M-ellipsoid, followed by its analysis. Section 5 applies this to the SVP and other problems.

We conclude this section with a remark on the complexity of computing (approximate) M-ellipsoids (and therefore the ℓ-position). An M-ellipsoid E for a convex body K achieving covering numbers $N(K,E)$, $N(E,K)$ gives an $N(K,E)N(E,K)$ to the volume of K. It is well-known that in the oracle model for convex bodies, any deterministic algorithm that has complexity at most n^a incurs an approximation factor of $(cn/a\log n)^{n/2}$, implying in particular that an algorithm that achieves a $2^{O(n)}$ approximation must have complexity $2^{\Omega(n)}$. Theorem 1.1 readily implies an $O(\log n)^n$ approximation with $O(\sqrt{\log n})^n$ complexity, getting close to the lower bound. Fully closing this gap is an interesting open problem.

2 M-ellipsoids and the ℓ-position

As explained above, one useful view of whether an ellipsoid E "approximates" a convex body K well is if $N(K,E), N(E,K) = 2^{O(n)}$. A similar view, taken by Pisier, is to find an ellipsoid E with the property that $\mathrm{vol}(K \cap E) \geq \mathrm{vol}(E)/2$ and $\mathrm{vol}(K)$ not much larger than $\mathrm{vol}(E)$.

This is useful in light of the following elementary bound on covering numbers for centrally symmetric bodies (see [18]).

LEMMA 2.1. *Let $A, B \subseteq \mathbb{R}^n$ be symmetric convex bodies. Then*

$$N(A,B) \leq 3^n \frac{\mathrm{vol}(A)}{\mathrm{vol}(A \cap B)}$$

We are now ready for the ℓ-position which lets us

find an ellipsoid with small covering numbers using this perspective.

Let $K \subseteq \mathbb{R}^n$ be a symmetric convex body, and let $K^* = \{x : \sup_{y \in K} \langle x, y \rangle \leq 1\}$ denote the polar of K. Let $B_2^n \subseteq \mathbb{R}^n$ denote the unit euclidean ball, and $S^{n-1} = \partial B_2^n$ denote the unit sphere. Let $\gamma_n(x) = \left(\frac{1}{\sqrt{2\pi}}\right)^n e^{-\frac{1}{2}\|x\|^2}$ be the density of the canonical gaussian measure on $\mathbb{R}^n$. We define the expected norm of a random Gaussian point as

$$\ell(K) = \int \|x\|_K \gamma_n(x) dx.$$

The following lemma, see [22], provides an asymptotic estimate of this quantity.

LEMMA 2.2. *Let $K \subseteq \mathbb{R}^n$ be a symmetric convex body. Then for*

$$m = \sup\{r \geq 0 : \mathrm{vol}_{n-1}(rS^{n-1} \cap K) \geq \frac{1}{2}\mathrm{vol}_{n-1}(rS^{n-1})\}$$

we have that $\ell(K) = \Theta\left(\frac{\sqrt{n}}{m}\right)$. Furthermore, we have that $\mathrm{vol}(mB_2^n \cap K) \geq \frac{1}{2}\mathrm{vol}(mB_2^n)$.

A theorem of Pisier [22] relates the ℓ-estimate of a body with that of its dual.

THEOREM 2.1. *Let $K \subseteq \mathbb{R}^n$ be a symmetric convex body. Then*

$$\inf_{T \in SL(n)} l(TK) l(T^*K^*) \leq cn \log n$$

where $SL(n)$ is the set of $n \times n$ matrices of determinant 1 and $c > 0$ is an absolute constant.

The next theorem, known as the Blashke-Santaló inequality [5, 25], gives an upper bound on the volume product, a fundamental quantity in convex geometry.

THEOREM 2.2. (BLASHKE-SANTALÓ) *Let $K \subseteq \mathbb{R}^n$ be a symmetric convex body. Then*

$$\mathrm{vol}(K)\mathrm{vol}(K^*) \leq \mathrm{vol}(B_2^n)^2$$

with equality iff K is an ellipsoid.

Using the above estimates, we get the following well-known result, whose proof we include for completeness.

THEOREM 2.3. (PISIER) *Let $K \subseteq \mathbb{R}^n$ be a symmetric convex body. Then there exists an ellipsoid $E \subseteq \mathbb{R}^n$ such that*

- $\mathrm{vol}(E \cap K) \geq \frac{1}{2}\mathrm{vol}(E)$
- $\mathrm{vol}(K) \leq O(\log n)^n \mathrm{vol}(E \cap K)$

In addition, we get that

$$N(K, E) = O(\log n)^n \quad \text{and} \quad N(E, K) = \frac{1}{2}3^n$$

Proof. Let us first apply a measure preserving linear transformation T to K such that $l(TK)l(T^*K^*)$ is minimized, and hence by 2.1 we may assume that $\ell(K)\ell(K^*) = O(n \log n)$. Now using Lemma 2.2 we see that

$$\begin{aligned} m &= \sup\{r \geq 0 : \mathrm{vol}(rB_2^n \cap K) \geq \frac{1}{2}\mathrm{vol}(rB_2^n)\} \\ &= \Omega\left(\frac{\sqrt{n}}{\ell(K)}\right) \end{aligned}$$

and that

$$m^* = \sup\{r \geq 0 : \mathrm{vol}(rB_2^n \cap K^*) \geq \frac{1}{2}\mathrm{vol}(rB_2^n)\} = \Omega\left(\frac{\sqrt{n}}{l(K^*)}\right)$$

Hence we get that $mm^* = \Omega\left(\frac{1}{\log n}\right)$.
Using Theorem 2.2 we get that

$$\begin{aligned} \mathrm{vol}(K) &\leq \frac{\mathrm{vol}(B_2^n)^2}{\mathrm{vol}(K^*)} \leq 2\frac{\mathrm{vol}(B_2^n)^2}{\mathrm{vol}(m^*B_2^n)} = 2\left(\frac{1}{m^*}\right)^n \mathrm{vol}(B_2^n) \\ &= O(m \log n)^n \mathrm{vol}(B_2^n) = O(\log n)^n \mathrm{vol}(mB_2^n) \\ &= O(\log n)^n \mathrm{vol}(mB_2^n \cap K) \end{aligned}$$

We now see that the ellipsoid $E = mB_2^n$ satisfies the claims of the corollary. To derive the additional assertions, we simply apply Lemma 2.1 to the volume estimates above.

3 Algorithm to compute an ℓ-type Ellipsoid

Our algorithm will find an ellipsoid by (approximately) solving the following convex program (CP).

$$\begin{aligned} \inf f(A) &= \int_{\mathbb{R}^n} \|Ax\|_K \gamma_n(x) dx \\ \text{subject to} \quad & \\ A &\succeq 0 \\ \det(A) &\geq 1 \end{aligned} \tag{3.2}$$

The above program models a tractable variant of the implicit optimization problem in Theorem 2.1. It encodes what is known in the convex geometry literature as the minimal mean width position of K^* (see for example [7]). To interpret the above program, examine the ellipsoid

$$E = c\frac{\sqrt{n}}{f(A)} AB_2^n, 0 < c < 1 \text{ an absolute constant}$$

where we have that $\text{vol}(E)^{\frac{1}{n}} \approx \frac{\det(A)^{\frac{1}{n}}}{f(A)}$. By Lemma 2.2, we have that $\text{vol}(E \cap K) \geq \frac{1}{2}\text{vol}(E)$, i.e. E is "half-contained" inside K. Hence the above program in essence finds the largest volume ellipsoid that is half-contained inside K. From the existence proof of Pisier 2.3, we get that the largest such ellipsoid (corresponding to the optimal solution of the above program) indeed contains a $\Omega(\frac{1}{\log n})^n$ volume fraction of K, and hence achieves the desired covering bounds with respect to K. Hence to obtain an approximate M-ellipsoid, it suffices to solve the above program [1]. Moreover, by the same argument, any solution that achieves a constant factor approximation of the optimal for the above program, also yields an ellipsoid with the desired covering bounds.

The focus of the following sections will be to give a deterministic $O(\sqrt{\log n})^n$-time algorithm to solve the above convex program to within a $(1+o(1))$-factor. We note that the above program fits directly into the framework of stochastic convex optimization (e.g. minimizing the expectation of a convex function), and hence there are many available methods (stochastic gradient descent [23, 19], random walk based optimization [10, 14], $\cdots$) to solve it within the desired accuracy (constant factor suffices) in randomized polynomial time. Our contribution here is therefore in solving the program deterministically.

In the above program, K will be a symmetric convex body presented by a weak membership oracle, satisfying $rB_2^n \subseteq K \subseteq RB_2^n$. To solve the program, we first round K using the ellipsoid method [8] so that $B_2^n \subseteq K \subseteq nB_2^n$ (note the improvement from $n^{\frac{3}{2}}$ to n is possible since K is centrally symmetric). Next we use a discrete approximation of space to approximate the ℓ-estimate at any given A, where this approximation remains convex. Next we analyze the properties of the above convex program, showing that (1) a well sandwiched subset of the feasible region (ratio of inner contained and outer containing ball) contains the optimal solution, (2) the objective function is Lipshitz, and (3) the objective value of the optimal solution is not too small. From here, we apply the classical reduction from weak membership to weak optimization [8] (which simulates the ellipsoid method), which allows us to compute a $(1+\epsilon)$ approximation (multiplicative) of the optimal solution using at most a polynomial number of queries to the objective function.

[1] Since the $f(AO) = f(A)$, for any orthogonal transformation O, we may assume that the optimal transformation A is positive definite.

Our approximation of the ℓ-estimate is as follows:

$$\text{Let } s = \frac{1}{\sqrt{2\pi}}\sqrt{\frac{\log(2(2n+1))}{\pi}}, \quad C_s = \frac{1}{2s}[-1,1]^n \text{ and } p_x = \int_{C_s} \gamma_n(x+y)dy.$$

Define $D \subseteq \mathbb{R}^n$ be set of points from the lattice $(1/s)\mathbb{Z}^n$ that lie in the ball of radius $3\sqrt{n}$ around the origin, i.e.,

$$D = \left(\frac{1}{s}\mathbb{Z}^n\right) \bigcap \left(3\sqrt{n}B_2^n\right)$$

Then

$$\tilde{f}(A) = \sum_{x \in D} p_x \|Ax\|_K.$$

Complexity of Computing $\tilde{f}(A)$: A first step in analyzing this discretization is to bound the size of D.

We claim that $|D| = O(\sqrt{\log n})^n$. Since C_s tiles space with respect to $\frac{1}{s}\mathbb{Z}^n$ and $C_s \subseteq \sqrt{n}B_2^n$, we have that

$$|D| = \frac{\text{vol}(D + C_s)}{\text{vol}(C_s)} \leq \frac{\text{vol}(3\sqrt{n}B_2^n + C_s)}{\text{vol}(C_s)} \leq \frac{\text{vol}(4\sqrt{n}B_2^n)}{s^{-n}} = 4^n \text{vol}(\sqrt{n}B_2^n)s^n = O(\sqrt{\log n})^n$$

as claimed.

From here it is straightforward to see that for any $A \in \mathbb{R}^{n \times n}$, one can compute $\tilde{f}(A)$ (to within any reasonable accuracy) using at most $O(\sqrt{\log n})^n$ norms evaluations and poly(n)-space. To see this, we note that the points in D can be enumerated in $O(D) = O(\sqrt{\log n})^n$ time using poly(n)-space, by recursively enumerating all the integer points (scaled down) in $3\sqrt{n}B_2^n$ by induction on coordinate values. From here, we simply need to update the sum above, one summand at a time, where for $x \in D$ computing $\|Ax\|_K$ correponds to a norm evaluation, and computing $p_x = \prod_{i=1}^n \gamma_1([-\frac{1}{2s}, \frac{1}{2s}] + x_i)$, which is the product of elementary gaussian integrals, can be estimated within the necessary accuracy in poly(n) time using standard methods (e.g. the trapezoid method).

4 Analysis

The analysis is divided into two parts. First, we give an $O(\sqrt{\log n})^n$ algorithm to compute an approximation of the objective value in 3.2 on any given input. Second, we show that the optimization problem with the approximated objective 3.2 is well-behaved, i.e. that it is convex, that the feasible region can be nicely bounded, the objective function is Lipshitz. This will allow us to apply the ellipsoid algorithm to solve the problem.

4.1 Computing the ℓ-estimate In this section, we analyze the deterministic algorithm to approximately compute $\ell(K)$ in $O(\sqrt{\log n})^n$ time. Recall that our approach is to approximate the associated integral as a sum over a discrete set.

We first describe the idea. A reasonable first approach would be to check whether the integrand (i.e. $\|x\|_K$) is Lipschitz enough so that reasonably sized discretization may be used to approximate the integral $\ell(K)$. Indeed, it will be true that $|\|x\|_K - \|y\|_K| = O(\ell(K))\|x-y\|_2$. Given that the mass of the n dimensional standard Gaussian is concentrated inside of shell of constant width at radius $\sqrt{n}$, this bound on the Lipshitz constant would suggest that a discretization D of $\sqrt{n}S^{n-1}$, such that every point in $\sqrt{n}S^{n-1}$ is at distance $O(1)$ from D, should suffice to estimate $\ell(K)$. Though this will indeed be true, any such discrete set D must have size $O(\sqrt{n})^n$, i.e. far larger than $O(\sqrt{\log n})^n$. Taking a closer look however, we observe that one only needs such a Lipschitz bound "on average", since all we want is to approximate is the integral. This we are able to bound below, using some standard tail bounds and a simple monotonicity inequality about expectations.

To perform the analysis of our algorithm, we will need certain facts about the discrete Gaussian distribution. Let

$$\rho_s(x) = e^{-\pi\|\frac{x}{s}\|^2}$$

for $x \in \mathbb{R}^n$, and we write $\rho_s(A)$ to mean $\sum_{x\in A}\rho_s(x)$ for $A \subseteq \mathbb{R}^n$. For an n-dimensional lattice $L \subseteq \mathbb{R}^n$, and $c \in \mathbb{R}^n$ we define the discrete Gaussian measure on $L+c$ with parameter s as

$$D_{L+c,s}(A) = \frac{\rho_s(A)}{\rho_s(L+c)}$$

for $A \subseteq L + c$.

In our setting, we will only need the case $L = \mathbb{Z}^n$. We let U stand for the uniform distribution on $[-1/2, 1/2]^n$. We now state some useful standard lemmas. See [3, 15].

LEMMA 4.1. *Take $s \geq \sqrt{\frac{\log(2(t+1))}{\pi}}$ and let X be distributed as $D_{L+c,s}$ for $c \in \mathbb{R}^n$. Then*

$$\left(1-\frac{1}{t}\right)^n s^n \leq \rho_s(\mathbb{Z}^n + c) \leq \left(1+\frac{1}{t}\right)^n s^n$$

LEMMA 4.2. *Let X be drawn from a standard n-dimensional Gaussian $N(0,1)^n$, i.e., with density $\left(\frac{1}{\sqrt{2\pi}}\right)^n e^{-\frac{1}{2}\|x\|^2}$, then for $t \geq 1$ we have that*

$$\Pr(\|X\| \geq t\sqrt{n}) \leq e^{-\left(1-\frac{1+\ln(t^2)}{t^2}\right)\frac{1}{2}nt^2}$$

The next lemma is an inequality that we will use in the main proof. It is directly implied by Lemma 8 in [4]. For convenience we give a proof in the appendix.

LEMMA 4.3. *Let $f : \mathbb{R}^n \to \mathbb{R}$ be a convex function. Let U denote the uniform distribution on $[-\frac{1}{2}, \frac{1}{2}]^n$ and let X denote the n-dimensional Gaussian $N(0, 1/\sqrt{2\pi})$, i.e., with density $e^{-\pi\|x\|^2}$. Then we have that*

$$\mathrm{E}[f(X)] \geq \mathrm{E}[f(U)]$$

The choice of standard deviation for the Gaussian in the above lemma is to simply ensure that its maximum density is bounded by 1.

We are now ready for the main theorem of this section.

THEOREM 4.1. *Let $s = \frac{1}{\sqrt{2\pi}}\sqrt{\frac{\log(2(2n+1))}{\pi}}$ and $C_s = \frac{1}{2s}[-1,1]^n$. Define*

$$D = \left(\frac{1}{s}\mathbb{Z}^n\right) \bigcap \left(3\sqrt{n}B_2^n\right) \text{ and } p_x = \gamma_n(x + C_s)dy$$

for $x \in D$. Then for any symmetric convex body $K \subseteq \mathbb{R}^n$, we have that

$$\left(1-\frac{1}{s}\right)\ell(K) \leq \tilde{\ell}(K) \leq \left(1+\frac{1}{s}\right)\ell(K)$$

where $\tilde{l}(K) = \sum_{x\in D} p_x\|x\|_K$.

Proof. The proof proceeds as follows. First we note in Claim 1 below that we can restrict attention to a ball of radius $2\sqrt{n}$ via a tail bound on the standard Gaussian. Then, in Claim 2, we bound the error of the discrete approximation computed in terms of the norm of a random point from U (uniform in $[-1/2, 1/2]^n$). Finally, using Lemma 4.3, we can bound this norm by the ℓ-estimate itself (Claim 3 below).

Claim 1.

$$\begin{aligned}(1-e^{-0.3n})\int_{\mathbb{R}^n}\|x\|_K\gamma_n(x)dx &\leq \int_{D+C_s}\|x\|_K\gamma_n(x)dx \\ &\leq \int_{\mathbb{R}^n}\|x\|_K\gamma_n(x)dx\end{aligned}$$

Claim 2.

$$\left|\sum_{x\in D} p_x\|x\|_K - \int_{D+C_s}\|x\|_K\gamma_n(x)dx\right| \leq \frac{2}{s}\,\mathrm{E}[\|U\|_K].$$

Claim 3.

$$\mathrm{E}[\|U\|_K] \leq \frac{1}{\sqrt{2\pi}}\,\mathrm{E}[\|X\|_K]$$

where X is a standard n-dimensional Gaussian.

We prove these claims presently.

Combining Claims $(1), (2)$, and (3), we get the upper bound

$$\begin{aligned}\sum_{x\in D} p_x\|x\|_K &\le \int_{D+C_s} \|x\|_K\gamma_n(x)dx + \frac{2}{s}\,\mathrm{E}[\|U\|_K] \\ &\le \mathrm{E}[\|X\|_K] + \frac{\sqrt{2}}{\sqrt{\pi}s}\,\mathrm{E}[\|X\|_K] \\ &= \left(1+\frac{\sqrt{2}}{\sqrt{\pi}s}\right)\mathrm{E}[\|X\|_K],\end{aligned}$$

and the lower bound

$$\begin{aligned}\sum_{x\in D} p_x\|x\|_K &\ge \int_{D+C_s} \|x\|_K\gamma_n(x)dx - \frac{2}{s}\,\mathrm{E}[\|U\|_K] \\ &\ge \left(1-e^{-0.3n}\right)\mathrm{E}[\|X\|_K] - \frac{\sqrt{2}}{\sqrt{\pi}s}\,\mathrm{E}[\|X\|_K] \\ &= \left(1-e^{-0.3n}-\frac{\sqrt{2}}{\sqrt{\pi}s}\right)\mathrm{E}[\|X\|_K].\end{aligned}$$

Since $e^{-0.3n} + \frac{\sqrt{2}}{\sqrt{\pi}s} \le \frac{1}{s}$ for n large enough, we get the claimed result.

Now we prove the claims.

Proof of Claim 1: Since the scaled cube C_s tiles space with respect to the lattice $\frac{1}{s}\mathbb{Z}^n$, for $x \in 2\sqrt{n}B_2^n$, we have that $x+C_s \cap \frac{1}{s}\mathbb{Z}^n \neq \emptyset$. Since $x+C_s \subseteq 2\sqrt{n}B_2^n + \frac{\sqrt{n}}{s}B_2^n \subseteq 3\sqrt{n}B_2^n$, we get that $2\sqrt{n}B_2^n \subseteq D + C_s$. Since $\|\cdot\|_K$ is non-negative, we clearly have that

$$\begin{aligned}\int_{2\sqrt{n}B_2^n} \|x\|_K\gamma_n(x)dx &\le \int_{D+C_s} \|x\|_K\gamma_n(x)dx \\ &\le \int_{\mathbb{R}^n} \|x\|_K\gamma_n(x)dx\end{aligned}$$

Expressing the integral in polar coordinates, we have to bound the ratio between the integral

$$\int_{2\sqrt{n}B_2^n} \|x\|_K\gamma_n(x)dx = (1/\sqrt{2\pi})^n \int_{S^{n-1}}\int_0^{2\sqrt{n}} \|\theta\|_K e^{-\frac{1}{2}r^2} r^n dr d\theta.$$

and the same integral over all of $\mathbb{R}^n$. Thus,

$$\begin{aligned}\frac{\int_{2\sqrt{n}B_2^n} \|x\|_K\gamma_n(x)\,dx}{\int_{\mathbb{R}^n} \|x\|_K\gamma_n(x)\,dx} &= \frac{\int_{S^{n-1}}\int_0^{2\sqrt{n}} \|\theta\|_K e^{-\frac{1}{2}r^2} r^n dr d\theta}{\int_{S^{n-1}}\int_0^{\infty} \|\theta\|_K e^{-\frac{1}{2}r^2} r^n dr d\theta} \\ &\ge \frac{\int_0^{2\sqrt{n}} e^{-\frac{1}{2}r^2} r^n dr}{\int_0^{\infty} e^{-\frac{1}{2}r^2} r^n dr} \\ &= 1 - \int_{\mathbb{R}^{n+1}\setminus 2\sqrt{n}B_2^n} \gamma_{n+1}(x)dx \\ &\ge 1 - e^{-(1-\frac{1+\ln(\frac{4n}{n+1})}{\frac{4n}{n+1}})2n} \ge 1 - e^{-0.3n}\end{aligned}$$

using Lemma 4.2 (i.e., the standard Gaussian tailbound) with $t = 2\sqrt{\frac{n}{n+1}}$, and noting that $n \ge 1$. This proves the claim.

Proof of Claim 2: For $y \in \mathbb{R}^n$, let $r(y)$ denote the closest vector to y in $\frac{1}{s}\mathbb{Z}^n$ under the l_2 norm. Given the structure of $\mathbb{Z}^n$, a simple computation yields that

$$r(y) = \left(\frac{\lfloor sy_1\rceil}{s}, \ldots, \frac{\lfloor sy_n\rceil}{s}\right)$$

Furthermore, for $x \in \frac{1}{s}\mathbb{Z}^n$ we have that $r(y) = x$ iff $y \in x + C_s$. Now we see that

$$\begin{aligned}\sum_{x\in D} p_x\|x\|_K &= \sum_{x\in D}\int_{x+C_s} \|x\|_K\gamma_n(y)dy \\ &= \int_{D+C_s} \|r(y)\|_K\gamma_n(y)dy\end{aligned}$$

From here, using the triangle inequality, we get that

$$\begin{aligned}&\int_{D+C_s} \|r(y)\|_K\gamma_n(y)dy \le \\ &\int_{D+C_s} (\|y\|_K + \|y-r(y)\|_K)\gamma_n(y)dy = \\ &\int_{D+C_s} \|y\|_K\gamma_n(y) + \int_{D+C_s} \|y-r(y)\|_K\gamma_n(y)dy\end{aligned}$$

Similarly, we also get that

$$\begin{aligned}&\int_{D+C_s} \|r(y)\|_K\gamma_n(y)dy \ge \\ &\int_{D+C_s} \|y\|_K\gamma_n(y) - \int_{D+C_s} \|y-r(y)\|_K\gamma_n(y)dy\end{aligned}$$

Hence to get the desired upper and lower bounds on $\sum_{x\in D} p_x\|x\|_K$, we need only upper bound the quantity

$\int_{D+C_s} \|y - r(y)\|_K \gamma_n(y)dy$. Now we note that

$$\int_{D+C_s} \|y - r(y)\|_K \gamma_n(y)dy =$$
$$\int_{C_s} \|c\|_K \sum_{y \in D+c} \gamma_n(y)dc =$$
$$\left(\frac{1}{s}\right)^n \int_{C_1} \left\|\frac{c}{s}\right\|_K \sum_{y \in D+\frac{c}{s}} \gamma_n(y)dc =$$
$$\left(\frac{1}{s}\right)^n \int_{C_1} \left\|\frac{c}{s}\right\|_K \sum_{y \in sD+c} \gamma_n\left(\frac{y}{s}\right)dc =$$
$$\left(\frac{1}{\sqrt{2\pi}s}\right)^n \frac{1}{s} \int_{C_1} \|c\|_K \sum_{y \in sD+c} e^{-\pi\|\frac{y}{\sqrt{2\pi}s}\|^2}dc$$

Next note that $sD = \mathbb{Z}^n \cap 3\sqrt{n}sB_2^n$. Therefore by Lemma 4.1 we have that

$$\left(\frac{1}{\sqrt{2\pi}s}\right)^n \frac{1}{s} \int_{C_1} \|c\|_K \sum_{y \in sD+c} e^{-\pi\|\frac{y}{\sqrt{2\pi}s}\|^2}dc \leq$$
$$\left(\frac{1}{\sqrt{2\pi}s}\right)^n \frac{1}{s} \int_{C_1} \|c\|_K \sum_{y \in \mathbb{Z}^n+c} e^{-\pi\|\frac{y}{\sqrt{2\pi}s}\|^2}dc \leq$$
$$\left(\frac{1}{\sqrt{2\pi}s}\right)^n \frac{1}{s} \int_{C_1} \|c\|_K (\sqrt{2\pi}s)^n (1 + \frac{1}{2n})^n dc \leq$$
$$\frac{2}{s} \int_{C_1} \|c\|_K dc = \frac{2}{s} \mathrm{E}[\|U\|_K]$$

Proof of Claim 3: We wish to show that

$$\mathrm{E}[\|U\|_K] \leq \frac{1}{\sqrt{2\pi}} \mathrm{E}[\|X\|_K] = \mathrm{E}[\|\frac{1}{\sqrt{2\pi}}X\|_K]$$

A simple computation gives that $\frac{1}{\sqrt{2\pi}}X$ has density $e^{-\pi\|x\|^2}$ for $x \in \mathbb{R}^n$. Since $\|\cdot\|_K$ is a convex function, the above inquality follows directly from Lemma 4.3. The claim thus follows.

4.2 Efficiency of solving the convex program In what follows we will assume that our symmetric convex body K is well sandwiched, i.e. that $B_2^n \subseteq K \subseteq nB_2^n$. As mentioned previously, this can be achieved by GLS type rounding using the ellipsoid algorithm.

We recall the functions $f, \tilde{f} : \mathbb{R}^{n \times n} \to \mathbb{R}$

$$f(A) = \int_{\mathbb{R}^n} \|Ax\|_K \gamma_n(x)dx \quad \text{and} \quad \tilde{f}(A) = \sum_{x \in D} p_x \|Ax\|_K$$

We will consider an approximate version of Program 3.2:

$$\begin{aligned} \inf \tilde{f}(A) &= \sum_{x \in D} p_x \|Ax\|_K \\ \text{subject to} & \\ A &\succeq 0 \\ \det(A) &\geq 1 \end{aligned} \tag{4.3}$$

The main result of this section is the following:

THEOREM 4.2. *Let $\tilde{A}$ denote an optimal solution to Program 4.3. Then for $0 < \epsilon \leq 1$, a matrix $A \in \mathbb{R}^{n \times n}$ satisfying $\tilde{f}(A) \leq (1+\epsilon)\tilde{f}(\tilde{A})$ can be computed in deterministic $\mathrm{poly}(n, \ln \frac{1}{\epsilon})O(\sqrt{\log n})^n$ time. Furthermore, let $A \in \mathbb{R}^{n \times n}$ be any 2-approximate solution to 4.3, then for $E = \frac{\sqrt{n}}{\tilde{f}(A)}AB_2^n$ we have that*

$$N(E, K) = 2^{O(n)} \quad N(K, E) = O(\log n)^n$$

Proof. Let A^* denote an optimal solution to 3.2. Then by Theorem 4.1 we have that

$$\begin{aligned} (1 - \frac{1}{s})f(A^*) \leq (1 - \frac{1}{s})f(\tilde{A}) \leq \tilde{f}(\tilde{A}) \\ \leq \tilde{f}(A^*) \leq (1 + \frac{1}{s})f(A^*) \end{aligned} \tag{4.4}$$

where the first inequality follows by optimality of A^*, and the third inequality by optimality of $\tilde{A}$.

Claim 1: $f(A^*) = O\left(\frac{\log n}{\mathrm{vol}(K)^{\frac{1}{n}}}\right)$. Pick a linear transformation $T \in SL(n)$ minimizing $l(TK)l(T^*K)$. From the proof of Lemma 2.3, for some $c_1, c_2 = \Theta(1)$, letting $m = c_1 \frac{\sqrt{n}}{l(TK)}$ we have that

$$\frac{1}{2}\mathrm{vol}(mT^{-1}B_2^n) = \mathrm{vol}(mT^{-1}B_2^n \cap K) \geq \left(\frac{c_2}{\log n}\right)^n \mathrm{vol}(K)$$

Now

$$\begin{aligned} \mathrm{vol}(mT^{-1}B_2^n) &= \mathrm{vol}(B_2^n)\det(T^{-1})m^n = \mathrm{vol}(B_2^n)\frac{m^n}{\det(T)} \\ &= \mathrm{vol}(B_2^n)m^n. \end{aligned}$$

Therefore

$$\begin{aligned} &\mathrm{vol}(B_2^n)^{\frac{1}{n}} m \geq \frac{c_2}{\log n} \mathrm{vol}(K)^{\frac{1}{n}} \Rightarrow \\ &\frac{c_1}{c_2} \mathrm{vol}(B_2^n)^{\frac{1}{n}} \sqrt{n} \frac{\log n}{\mathrm{vol}(K)^{\frac{1}{n}}} \geq l(TK) \Rightarrow \\ &l(TK) = O\left(\frac{\log n}{\mathrm{vol}(K)^{\frac{1}{n}}}\right) \end{aligned}$$

Using the identity $\|x\|_{TK} = \|T^{-1}x\|_K$ we see that

$$\begin{aligned} l(TK) &= \int_{x \in \mathbb{R}^n} \|x\|_{TK} \gamma_n(x)dx = \int_{x \in \mathbb{R}^n} \|T^{-1}x\|_K \gamma_n(x) \\ &= f(T^{-1}) \end{aligned}$$

Let $A = T^{-1}$. For a standard gaussian vector X is $\mathbb{R}^n$, we note that $A_s = (A^tA)^{\frac{1}{2}}X$, where A_s is the unique positive definite square root of A^tA, is identically distributed to AX. Therefore $f(A_s) = E[\|A_sX\|_K] =$

$E[\|AX\|_K] = f(A) = f(T^{-1})$. Since $A_s = (A^tA)^{\frac{1}{2}} \succeq 0$ and $\det(A_s) = |\det(A)| = \det(T^{-1}) = 1$, we have that A_s is feasible for Program 3.2. Since A^* is the optimal solution to 3.2 we have that

$$f(A^*) \leq f(A_s) = f(T^{-1}) = O\left(\frac{\log n}{\mathrm{vol}(K)^{\frac{1}{n}}}\right)$$

as needed.

Claim 2: The Programs 3.2 and 4.3 are convex.

By Lemma 4.4, we know that both f and $\tilde{f}$ are convex over the feasible region. In both programs, the feasible region is the set of positive semi-definite matrices of determinant greater than 1, which is clearly convex.

Claim 3: Program 4.3 can be solved to within $(1+\epsilon)$ multiplicative error in deterministic $\mathrm{poly}(n, \ln\frac{1}{\epsilon})O(\sqrt{\log n})^n$ time.

Given that $B_2^n \subseteq K \subseteq nB_2^n$, by Lemma 4.5 we may constrain convex Program 4.3 to the well-bounded region R without removing any optimal solutions. Now by Lemma 4.4 (3) the objective function is $2\sqrt{n}$ Lipshitz over operator norm (and hence over the Frobenius norm), and by Lemma 4.5 (3) that the ratio of min and max value of the objective function over R is $O(n^{\frac{5}{2}})$. Given all this, we may apply the ellipsoid algorithm (see [8] Theorem 4.3.13 for example) to solve the convex program 4.3 to within $(1+\epsilon)$ multiplicative error using at most $\mathrm{poly}(n, \ln\frac{1}{\epsilon})$ evaluations of $\tilde{f}$ and arithmetic operations. Since each evaluation of $\tilde{f}$ can be computed in deterministic $O(\sqrt{\log n})^n$ time, this proves the claim.

Claim 4: Let A be a 2-approximation for the program 4.3. Then the ellipsoid $E = \frac{\sqrt{n}}{\tilde{f}(A)}AB_2^n$ satisfies $N(K,E) = O(\log n)^n$ and $N(E,K) = 2^{O(n)}$.

Let $\tilde{A}$ be as above. By Equation (4.4), Lemma 4.1 and Claim 1, we have that

$$\begin{aligned} f(A) &\leq \frac{s}{s-1}\tilde{f}(A) \leq 2\,\frac{s}{s-1}\,\tilde{f}(\tilde{A}) \leq \frac{s+1}{s-1}f(A^*) \\ &= O\left(\frac{\log n}{\mathrm{vol}(K)^{\frac{1}{n}}}\right). \end{aligned}$$

By Theorem 4.1, we note that $\frac{\sqrt{n}}{\tilde{f}(A)} = \Theta(1)\frac{\sqrt{n}}{f(A)}$. Hence by Lemma 2.2, there exists $c \leq 1$, where $c = \Omega(1)$, such that $\mathrm{vol}(cE \cap K) = \frac{1}{2}\mathrm{vol}(cE)$. Now note that

$$\begin{aligned} \mathrm{vol}(cE) &= \left(\frac{c\sqrt{n}}{\tilde{f}(A)}\right)^n \det(A)\mathrm{vol}(B_2^n) \geq \left(\frac{c\sqrt{n}\mathrm{vol}(B_2^n)^{\frac{1}{n}}}{\tilde{f}(A)}\right)^n \\ &= \Omega\left(\frac{1}{\log n}\right)^n \mathrm{vol}(K) \end{aligned}$$

Now since $\mathrm{vol}(E \cap K) \geq \mathrm{vol}(cE \cap K) = \frac{1}{2}\mathrm{vol}(cE) = \frac{1}{2}c^n\mathrm{vol}(E)$ and $\mathrm{vol}(E \cap K) \geq \mathrm{vol}(cE \cap K) = \Omega\left(\frac{1}{\log n}\right)^n \mathrm{vol}(K)$, applying the covering estimates of Lemma 2.1 yields the claim.

Lemma 4.4.

1. *$f, \tilde{f}$ define norms on $\mathbb{R}^{n\times n}$.*
2. *$A^tA \succeq B^tB \Rightarrow f(A) \geq f(B)$.*
3. *$|f(A)-f(B)|, |\tilde{f}(A)-\tilde{f}(B)| \leq 2\sqrt{n}\|A-B\|$, where $\|A-B\|$ denote the operator norm of $A-B$.*

Proof. Let $X \in \mathbb{R}^n$ denote a standard Gaussian random vector. Take $A, B \in \mathbb{R}^{n\times n}$ and scalars $s, t \in \mathbb{R}$. Then note that

$$\begin{aligned} f(sA+tB) &= \mathrm{E}[\|(sA+tB)X\|_K] = \mathrm{E}[\|sAX+tBX\|_K] \\ &\leq \mathrm{E}[|s|\|AX\|_K + |t|\|BX\|_K] \\ &= |s|f(A) + |t|f(B) \end{aligned}$$

where the inequality above follows since $\|\cdot\|_K$ defines a norm. Lastly, using the fact that

$$\frac{1}{n}\|x\|_2 \leq \|x\|_K \leq \|x\|_2$$

for $x \in \mathbb{R}^n$ (since $B_2^n \subseteq K \subseteq nB_2^n$) it is easy to verify that $f(A) = 0 \Leftrightarrow A = 0^{n\times n}$ and $f(A) < \infty$ for all $A \in \mathbb{R}^{n\times n}$. Hence f defines a norm on $\mathbb{R}^{n\times n}$ as claimed. The argument for $\tilde{f}$ is symmetric.

Now take A, B satisfying the condition of (2). Note that AX is an origin centered gaussian with covariance matrix $\mathrm{E}[AX(AX)^t] = \mathrm{E}[AXX^tA^t] = A^tA$. Similarly BX is origin centered with covariance B^tB. From our assumptions, the matrix $C = A^tA - B^tB \succeq 0$, hence C has a PSD square root which we denote $C^{\frac{1}{2}}$. Now let Y denote standard n-dimensional Gaussian independent from X. Now note that $BX + C^{\frac{1}{2}}Y$ is again a Gaussian vector with covariance $B^tB + C = A^tA$. Hence $BX + C^{\frac{1}{2}}Y$ is identically distributed to AX. Therefore we see that

$$\begin{aligned} f(A) &= \mathrm{E}[\|AX\|_K] = \mathrm{E}[\|BX + C^{\frac{1}{2}}Y\|_K] \\ &= \mathop{\mathrm{E}}_X\mathop{\mathrm{E}}_Y[\|BX + C^{\frac{1}{2}}Y\|_K]] \\ &\geq \mathop{\mathrm{E}}_X[\|BX + C^{\frac{1}{2}}\mathop{\mathrm{E}}_Y[Y]\|_K] = \mathrm{E}[\|BX\|_K] = f(B) \end{aligned}$$

where the inequality follows by Jensen's inequality and the convexity of $\|\cdot\|_K$.

We now prove (3). Take $A, B \in \mathbb{R}^{n\times n}$. By the triangle inequality, we have that

$$f(B) - f(A-B) \leq f(A) \leq f(B) + f(A-B).$$

Therefore $|f(B) - f(A)| \leq f(A-B)$. Since $\tilde{f}$ is also a norm, we similarly get that $|\tilde{f}(B) - \tilde{f}(A)| \leq \tilde{f}(A-B)$.

Let $\lambda = \|A - B\|$. By definition of the operator norm, we have that $(A-B)^t(A-B) \preceq \lambda^2 I_n$, where I_n denote the $n \times n$ identity matrix. Therefore by (2), we have that

$$f(A-B) = \mathrm{E}[\|(A-B)X\|_K] \leq \mathrm{E}[\|\lambda X\|_K] = \lambda \,\mathrm{E}[\|X\|_K]$$
$$\leq \lambda \,\mathrm{E}[\|X\|_2] \leq \lambda\sqrt{\mathrm{E}[\|X\|_2^2]} = \lambda\sqrt{n}$$

as needed. Next by Theorem 4.1, we have that

$$\tilde{f}(A-B) \leq 2f(A-B) \leq 2\|A-B\|\sqrt{n}$$

as required.

LEMMA 4.5. *Define the set*

$$R = \{A \in \mathbb{R}^{n\times n} : A \succeq 0, \det(A) \geq 1, \|A\| \leq 2n^{\frac{3}{2}}\}$$

where $\|A\|$ denote the operator norm of A. Then R satisfies the following:

1. *R contains an optimal solution to the programs 3.2 and 4.3.*
2. *R satisfies the following sandwiching properties:*

   $$n^{\frac{3}{2}} I_n + (n^{\frac{3}{2}} - 1)B_2^{n\times n} \subseteq R \subseteq n^{\frac{3}{2}} I_n + 3n^2 B_2^{n\times n}$$

   where I_n is the $n \times n$ identity matrix and $B_2^{n\times n} = \{A \in \mathbb{R}^{n\times n} : A = A^t, \|A\|_F \leq 1\}$, the set of $n \times n$ symmetric matrices of Frobenius norm at most 1.
3. *There is an absolute constant c such that for any $A \in R$, we have that*

   $$\frac{c}{\sqrt{n}} \leq f(A), \tilde{f}(A) \leq 3n^2$$

Proof. Let $X \in \mathbb{R}^n$ denote a standard n dimensional gaussian vector, and let $s = \frac{1}{\sqrt{2\pi}}\sqrt{\frac{\log(2(2n+1))}{\pi}}$.

We start by showing property (1). Let A be an optimal solution for Program 3.2. We wish to show that $\|A\| \leq n^{\frac{3}{2}}$. Since $\|x\|_2 \geq \|x\|_K$ for all $x \in \mathbb{R}^n$, we have that

$$f(I_n) = \mathrm{E}[\|X\|_K] \leq \mathrm{E}[\|X\|_2] \leq \sqrt{E[\|X\|_2^2]} = \sqrt{n}$$

Since I_n is feasible for 3.2, it suffices to show that if $\|A\| \geq 2n^{\frac{3}{2}}$, we get that $f(A) \geq \sqrt{n}$. Let $\lambda = \|A\|$, and let v denote an eigenvector of A satisfying $Av = \lambda v$ and $\|v\| = \frac{1}{n}$. Since $K \subseteq nB_2^n$, we have that $K \subseteq W = \{x : |\langle v, x\rangle| \leq 1\}$ (since $\|v\| = \frac{1}{n}$). Therefore

$$f(A) = \mathrm{E}[\|X\|_K] \geq \mathrm{E}[\|AX\|_W] = \mathrm{E}[|\langle v, AX\rangle|]$$
$$= \lambda \,\mathrm{E}[|\langle v, X\rangle|] = \lambda(\sqrt{\frac{2}{\pi}}\|v\|) = \frac{\lambda}{n}\sqrt{\frac{2}{\pi}}$$

Since A is optimal, we get that $\frac{\lambda}{n}\sqrt{\frac{2}{\pi}} \leq \sqrt{n} \Rightarrow \lambda \leq 2n^{\frac{3}{2}}$ as claimed. We now show the same for Program 4.3. By 4.1, $\tilde{f}(I_n) \leq (1+\frac{1}{s})f(I_n) \leq (1+\frac{1}{s})\sqrt{n}$. Now if A is an optimal solution to 4.3, letting $\lambda = \|A\|$, we have that

$$\tilde{f}(A) \geq (1 - \frac{1}{s})f(A) \geq (1-\frac{1}{s})\frac{\lambda}{n}\sqrt{\frac{2}{\pi}}$$

But then as above we have that

$$\lambda \leq \frac{1+\frac{1}{s}}{1-\frac{1}{s}}\sqrt{\frac{\pi}{2}}\, n^{\frac{3}{2}} \leq 2n^{\frac{3}{2}}$$

for n large enough as needed. Therefore R satisfies property (1) as needed.

We now show the containment relationship in (2). Take $A = n^{\frac{3}{2}} I_n + B$ where $B \in (n^{\frac{3}{2}} - 1)B_2^{n\times n}$. We must show that $A \in R$. We recall that $\|B\| \leq \|B\|_F \leq \sqrt{n}\|B\|$. First, note that

$$\|A\| \leq n^{\frac{3}{2}} + \|B\| \leq n^{\frac{3}{2}} + n^{\frac{3}{2}} - 1 < 2n^{\frac{3}{2}}$$

as needed. Next note that

$$\inf_{v\in S^{n-1}} v^t A v = \inf_{v\in S^{n-1}} v^t(n^{\frac{3}{2}} I_n + B)v$$
$$\geq \inf_{v\in S^{n-1}} n^{\frac{3}{2}} v^t v - v^t B v$$
$$= n^{\frac{3}{2}} - \sup_{v\in S^{n-1}} v^t B v \geq n^{\frac{3}{2}} - \|B\| \geq 1$$

Since A is symmetric, the above shows the A's smallest eigenvalue is at least 1, and hence $A \succeq 0$ and $\det(A) \geq 1$ as needed. To show the opposite containment, note that for $A \in R$, we have that

$$\|A - n^{\frac{3}{2}} I_n\|_F \leq \|A\|_F + \|n^{\frac{3}{2}} I_n\|_F \leq \sqrt{n}\|A\| + n^2 \leq 3n^2$$

as needed.

Now we need to show the bounds on $f(A)$ for $A \in R$ to prove property (3). First we remember that

$$\mathrm{E}[\|AX\|_2] \geq f(A) \geq \frac{1}{n}\mathrm{E}[\|AX\|_2]$$

Hence it suffices to upper and lower bound $\mathrm{E}[\|AX\|_2]$. We see that

$$c\sqrt{\mathrm{E}[\|AX\|_2^2]} \leq \mathrm{E}[\|AX\|_2] \leq \sqrt{\mathrm{E}[\|AX\|_2^2]}$$

for an absolute constant $0 \leq c < 1$. Here the first inequality follows by Borell's Lemma and the second by Jensen's inequality. Next we have that

$$\sqrt{\mathrm{E}[\|AX\|_2^2]} = \sqrt{\mathrm{E}[X^t A^t A X]} = \sqrt{\mathrm{E}[\mathrm{trace}(A^t A X X^t)]}$$
$$= \sqrt{\mathrm{trace}(A^t A)} = \|A\|_F$$

Since $A \in R$, we know that $\|A\| \leq 2n^{\frac{3}{2}}$, and hence $\|A\|_F \leq 2n^2$. Combining the above inequalities, this yields that $f(A) \leq 2n^2$ as needed. We now prove the lower bound. Since $A \in R$, we have that $\det(A) \geq 1$. Let A_i denote the i^{th} column of A. Now we have that

$$\|A\|_F \geq \sqrt{n} \prod_{i=1}^{n} \|A_i\|_2^{\frac{1}{n}} \geq \sqrt{n} \det(A)^{\frac{1}{n}} \geq \sqrt{n}$$

where the first inequality follows by the arithmetic - geometric mean inequality, and the second follows from Hadamard's inequality. Combining the above inequalities, we get that

$$f(A) \geq \frac{1}{n} \mathrm{E}[\|AX\|_2] \geq \frac{c}{n} \|A\|_F \geq \frac{c}{\sqrt{n}}$$

as needed. The bounds for $\tilde{f}(A)$ follow from the relationship $(1 - \frac{1}{s})f(A) \leq f(A) \leq (1 + \frac{1}{s})f(A)$ (Theorem 4.1).

5 Application to lattice algorithms

We now apply our construction of ℓ-type ellipsoids to lattice algorithms. Dadush et al [6] gave algorithms for SVP in any norm, CVP in any norm and Integer Programming (IP). These algorithms were all based on the construction of an M-ellipsoid. Their core result can be stated as follows. For a lattice L and convex body K in $\mathbb{R}^n$, let $G(K, L)$ be the largest number of lattice points contained in any translate of K, i.e.,

$$G(K, L) = \max_{x \in \mathbb{R}^n} |(K + x) \cap L|. \tag{5.5}$$

THEOREM 5.1. *[6] Given any convex body $K \subseteq \mathbb{R}^n$ along with an M-ellipsoid E of K and any n-dimensional lattice $L \subseteq \mathbb{R}^n$, the set $K \cap L$ can be computed in deterministic time $G(K, L) \cdot 2^{O(n)}$.*

They then proceeded to give a randomized construction of an M-ellipsoid. The necessary properties of the M-ellipsoid E are that the covering numbers $N(K, E)$ and $N(E, K)$ are both bounded by $2^{O(n)}$. In fact, the result of [6] can be stated more generally as follows.

THEOREM 5.2. *Given any convex body $K \subseteq \mathbb{R}^n$ along with an ellipsoid E of K and any n-dimensional lattice $L \subseteq \mathbb{R}^n$, the set $K \cap L$ can be computed in deterministic time $G(K, L) \cdot N(K, E)N(E, K) \cdot 2^{O(n)}$.*

Furthermore, in [6], they only require an algorithm which builds an M-ellipsoid when K is centrally symmetric. This follows since one can show that an M-ellipsoid E for $K - K$ (which is symmetric) is also an M-ellipsoid for K (of slightly worse quality). Hence from Theorem 1.1 and the bounds derived on $N(K, E)$ and $N(E, K)$, we obtain a simple corollary.

COROLLARY 5.1. *Given any convex body $K \subseteq \mathbb{R}^n$ and any n-dimensional lattice $L \subseteq \mathbb{R}^n$, the set $K \cap L$ can be computed in deterministic time $G(K, L) \cdot O(\log n)^n$.*

This lattice point enumerator is the core of subsequent algorithms for SVP, CVP and IP in [6]. We obtain similar conclusions with deterministic algorithms but with an overhead of $O(\log n)^n$. The precise statement for SVP is Theorem 1.2. For CVP the statement is as follows.

THEOREM 5.3. *There is a deterministic algorithm that, given any well-centered n-dimensional convex body K, solves CVP exactly on any n-dimensional lattice L in the semi-norm $\|\cdot\|_K$ defined by K, in $(2 + \gamma)^{O(n)} \cdot O(\log n)^n$ time and space, provided that the distance from the query point x to L is at most γ times the length of the shortest nonzero vector of L (under $\|\cdot\|_K$).*

A central motivation for solving SVP in general norms is to improve the complexity of integer programming. The IP algorithm directly uses the SVP algorithm. Moreover, in this case, the final complexity bound is already higher than $O(\log n)^n$, so we simply get the IP complexity of [6] with a deterministic algorithm.

THEOREM 5.4. *There exists a deterministic algorithm that, given a convex body $K \subseteq \mathbb{R}^n$ and an n-dimensional lattice $L \subset \mathbb{R}^n$, either decides that $K \cap L = \emptyset$ or returns a point $y \in K \cap L$ in $O(f^*(n))^n$ time, where $f^*(n)$ is the optimal bound for the "flatness" theorem.*

The flatness theorem, which we do not describe here, gives a bound on the lattice width of lattice-point-free convex bodies. The current best bound on $f^*(n)$ is $n^{4/3}$ for general convex bodies [24].

6 Conclusion

It remains open to give a deterministic $2^{O(n)}$ algorithm for M-ellipsoids and coverings. This would resolve the open problem of a deterministic $2^{O(n)}$ SVP algorithm in any norm and close the gap for the complexity of deterministic volume algorithms as noted in the introduction.

Another open problem is to fully extend the approach suggested in [6] to exact or even $(1 + \epsilon)$ CVP. At the moment, their $2^{O(n)}$ bound only holds for exact CVP when the target point's distance to the lattice is at most a constant times the minimum distance of the lattice. In particular, it is open to give a $2^{O(n)}$ algorithm for the CVP under the L_∞ norm.

Acknowledgments. We are deeply grateful to Grigoris Paouris and Chris Peikert for illuminating

discussions, and to Gilles Pisier for his book on convex bodies. We are also thankful to an anonymous referee for useful references.

References

[1] Miklós Ajtai, Ravi Kumar, and D. Sivakumar. A sieve algorithm for the shortest lattice vector problem. In *STOC*, pages 601–610, 2001.

[2] Vikraman Arvind and Pushkar S. Joglekar. Some sieving algorithms for lattice problems. In *FSTTCS*, pages 25–36, 2008.

[3] Wojciech Banaszczyk. Inequalites for convex bodies and polar reciprocal lattices in R^n. *Discrete & Computational Geometry*, 13:217–231, 1995.

[4] F. Barthe and A. Naor. Hyperplane projections of the unit ball of $\mathrm{l_p^n}$. *Discrete & Computational Geometry*, 27(2):215–226, 2002.

[5] W. Blaschke. Über affine geometry xiv: eine minimum aufgabe für legendres trägheits ellipsoid. *Ber. verh. sächs. Akad. d. Wiss.*, 70:72–75, 1918.

[6] Daniel Dadush, Chris Peikert, and Santosh Vempala. Enumerative lattice algorithms in any norm via m-ellipsoid coverings. In *FOCS*, 2011.

[7] A.A. Giannopolous, V.D. Milman, and M. Rudelson. Convex bodies with minimal mean width. *Geometric Aspects of Functional Analysis*, pages 81–93, 2001.

[8] M. Grötschel, L. Lovász, and A. Schrijver. *Geometric Algorithms and Combinatorial Optimization*. Springer, 1988.

[9] Antoine Joux and Jacques Stern. Lattice reduction: A toolbox for the cryptanalyst. *J. Cryptology*, 11(3):161–185, 1998.

[10] A. T. Kalai and S. Vempala. Simulated annealing for convex optimization. *Math. Oper. Res.*, 31(2):253–266, 2006.

[11] B. Klartag. On convex perturbations with a bounded isotropic constant. *Geometric And Functional Analysis*, 16:1274–1290, 2006.

[12] Arjen K. Lenstra, Hendrik W. Lenstra, Jr., and László Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4):515–534, December 1982.

[13] Hendrik W. Lenstra. Integer programming with a fixed number of variables. *Mathematics of Operations Research*, 8(4):538–548, November 1983.

[14] L. Lovász and S. Vempala. Fast algorithms for logconcave functions: Sampling, rounding, integration and optimization. In *FOCS '06: Proceedings of the 47th Annual IEEE Symposium on Foundations of Computer Science*, pages 57–68, Washington, DC, USA, 2006. IEEE Computer Society.

[15] Daniele Micciancio and Oded Regev. Worst-case to average-case reductions based on Gaussian measures. *SIAM J. Comput.*, 37(1):267–302, 2007. Preliminary version in FOCS 2004.

[16] Daniele Micciancio and Panagiotis Voulgaris. A deterministic single exponential time algorithm for most lattice problems based on Voronoi cell computations. In *STOC*, pages 351–358, 2010.

[17] V. Milman. Inegalites de brunn-minkowski inverse et applications at la theorie locales des espaces normes. *C. R. Acad. Sci. Paris*, 302(1):25–28, 1986.

[18] V.D. Milman and A. Pajor. Entropy and asymptotic geometry of non-symmetric convex bodies. *Advances in Mathematics*, 152(2):314 – 335, 2000.

[19] A. Nemirovski, A. Juditsky, G. Lan, and A. Shapiro. Robust stochastic programming approach to stochastic programming. *SIAM Journal on Optimization*, 19:1574–1609, 2009.

[20] Phong Q. Nguyen and Jacques Stern. The two faces of lattices in cryptology. In *CaLC*, pages 146–180, 2001.

[21] Andrew M. Odlyzko. The rise and fall of knapsack cryptosystems. In C. Pomerance, editor, *Cryptology and Computational Number Theory*, volume 42 of *Proceedings of Symposia in Applied Mathematics*, pages 75–88, 1990.

[22] G. Pisier. *The Volume of Convex Bodies and Banach Space Geometry*. Cambridge University Press, 1989.

[23] H. Robbins and S. Monro. A stochastic approximation method. *Annals of Mathematical Statistics*, 22:400–407, 1950.

[24] M. Rudelson. Distance between non-symmetric convex bodies and the MM*-estimate. *Positivity*, 4(8):161–178, 2000.

[25] Luis A. Santaló. Un invariante afin para los cuerpos convexos del espacio de n dimensiones. *Portugalie Math.*, 8:155–161, 1949.

7 Appendix

Proof. (of Lemma 4.3.) We shall prove the statement by induction. Let $C = [-\frac{1}{2}, \frac{1}{2}]$. We start with the base case $n = 1$. The density of U here is $I[x \in C]$, and the density for X is $e^{-\pi x^2}$ (this density function is chosen so that the density is at most 1 everywhere).

For our convex function $f : \mathbb{R} \to \mathbb{R}$, let ϕ denote the linear function satisfying $\phi(-\frac{1}{2}) = f(-\frac{1}{2})$ and $\phi(\frac{1}{2}) = f(\frac{1}{2})$. By convexity of f we note that $f(x) \leq \phi(x)$ for $x \in C$ and $f(x) \geq \phi(x)$ for $x \in \mathbb{R} \setminus C$. Now we note that

$$\mathrm{E}[f(X)] - \mathrm{E}[f(U)] = \int_{\mathbb{R}} f(x)(e^{-\pi x^2} - I[x \in C])dx = \int_{\mathbb{R}\setminus C} f(x)(e^{-\pi x^2})dx + \int_C f(x)(e^{-\pi x^2} - 1)dx$$

For $x \in \mathbb{R} \setminus C$, we have that $e^{-\pi x^2} \geq 0$ and $f(x) \geq \phi(x)$, and hence

$$\int_{\mathbb{R}\setminus C} f(x)(e^{-\pi x^2}) \geq \int_{\mathbb{R}\setminus C} \phi(x)(e^{-\pi x^2}).$$

For $x \in C$, we have that $e^{-\pi x^2} \leq 1$ and that $f(x) \leq$

$\phi(x)$, and hence

$$\int_C f(x)(e^{-\pi x^2} - 1) \geq \int_C \phi(x)(e^{-\pi x^2} - 1)$$

So we see that

$$\int_{\mathbb{R}\setminus C} f(x)(e^{-\pi x^2})dx + \int_C f(x)(e^{-\pi x^2} - 1)dx \geq$$
$$\int_{\mathbb{R}\setminus C} \phi(x)(e^{-\pi x^2})dx + \int_C f(x)(e^{-\pi x^2} - 1)dx =$$
$$\int_{\mathbb{R}} \phi(x)(e^{-\pi x^2} - I[x \in C])dx = \mathrm{E}[\phi(X - U)] =$$
$$\phi(\mathrm{E}[X - U]) = \phi(0) = 0.$$

Here the last equalities follow since ϕ is linear and both X and U have mean 0. The base case is thus proven.

We now assume that the claim is true for $n \geq 1$ and prove it for $n + 1$. Note that $X = (X_1, \ldots, X_{n+1})$ where the X_is are i.i.d. gaussians with density $e^{-\pi x^2}$, and that $U = (U_1, \ldots, U_{n+1})$ where the U_is are i.i.d. uniform random variables on C. We first show that

$$\mathrm{E}[f(X_1, \ldots, X_{n+1})] \geq \mathrm{E}[f(X_1, \ldots, X_n, U_{n+1})]$$

To see this, note that

$$\mathrm{E}[f(X_1, \ldots, X_{n+1})] =$$
$$\int_{\mathbb{R}^n} e^{-\pi(\sum_{i=1}^n x_i^2)} \int_{\mathbb{R}} f(x_1, \ldots, x_{n+1}) e^{-\pi x_{n+1}^2} dx_{n+1} \ldots dx_1$$

Now by convexity of f, we see that for any $x_1, \ldots, x_n \in \mathbb{R}^n$ the function $g(y) = f(x_1, \ldots, x_n, y)$ is a convex function from $\mathbb{R}$ to $\mathbb{R}$. Therefore, by the analysis of the base case, we have that

$$\int_{\mathbb{R}^n} e^{-\pi(\sum_{i=1}^n x_i^2)} \int_{\mathbb{R}} f(x_1, \ldots, x_{n+1}) e^{-\pi x_{n+1}^2} dx_{n+1} \ldots dx_1 \geq$$
$$\int_{\mathbb{R}^n} e^{-\pi(\sum_{i=1}^n x_i^2)} \int_{\mathbb{R}} f(x_1, \ldots, x_{n+1}) I[x_{n+1} \in C] dx_{n+1} \ldots dx_1 =$$
$$\mathrm{E}[f(X_1, \ldots, X_n, U_{n+1})]$$

as needed. Next by convexity of f, we get that the function

$$g(x_1, \ldots, x_n) = \mathrm{E}[f(x_1, \ldots, x_n, U_{n+1})]$$

is also convex. Therefore by the induction hypothesis, we get that

$$\mathrm{E}[f(X_1, \ldots, X_n, U_{n+1})] = \mathrm{E}[g(X_1, \ldots, X_n)]$$
$$\geq \mathrm{E}[g(U_1, \ldots, U_n)] = \mathrm{E}[f(U_1, \ldots, U_{n+1})]$$

as needed.