SIAM J. COMPUT.
Vol. 30, No. 6, pp. 2008–2035

THE SHORTEST VECTOR IN A LATTICE IS HARD TO APPROXIMATE TO WITHIN SOME CONSTANT*

DANIELE MICCIANCIO†

Abstract. We show that approximating the *shortest vector problem* (in any ℓ_p norm) to within any constant factor less than $\sqrt[p]{2}$ is hard for NP under *reverse unfaithful random* reductions with inverse polynomial error probability. In particular, approximating the *shortest vector problem* is not in RP (random polynomial time), unless NP equals RP. We also prove a proper NP-hardness result (i.e., hardness under deterministic many-one reductions) under a reasonable number theoretic conjecture on the distribution of square-free smooth numbers. As part of our proof, we give an alternative construction of Ajtai's constructive variant of Sauer's lemma that greatly simplifies Ajtai's original proof.

Key words. NP-hardness, shortest vector problem, point lattices, geometry of numbers, sphere packing

AMS subject classifications. 68Q25, 68W25, 11H06, 11P21, 11N25

PII. S0097539700373039

1. Introduction.

Lattices are geometric objects that can be pictorially described as the set of intersection points of an infinite, regular (but not necessarily orthogonal) n-dimensional grid. The rich combinatorial structure of lattices makes them very powerful tools to attack many important problems in mathematics and computer science. In particular, lattices have been used to solve integer programming with finitely many variables [25, 24, 20], factorization of polynomials over the integers [24, 31], low density subset-sum problems [23, 12, 8], and many cryptanalytic problems [32, 17, 13, 7, 6].

Despite the many successful applications of lattice techniques, the most fundamental problems on lattices resisted any attempt to devise polynomial time algorithm to solve them. These are the *shortest vector problem* (SVP) and the *closest vector problem* (CVP). In SVP, given a lattice, one must find the shortest nonzero vector in the lattice (i.e., the intersection point in the grid closest to the origin). CVP is the inhomogeneous counterpart of SVP: given a lattice and a target point (not necessarily in the lattice), find the lattice point closest to the target. Both problems can be defined with respect to any norm, but the Euclidean norm ℓ_2 is the most commonly used.

The first intractability results for lattice problems date back to 1981 when van Emde Boas [34] proved that CVP[1] is NP-hard and conjectured the same for SVP. Since then, the hardness result for CVP was considerably strengthened, proving that even finding approximate solutions to CVP is hard (see section 2 for more information). Despite the similarities between the two problems, progress in proving the hardness of

*Received by the editors May 16, 2000; accepted for publication (in revised form) September 22, 2000; published electronically March 20, 2001. A preliminary version of this paper appeared in the Proceedings of the 39th Annual IEEE Symposium on Foundations of Computer Science (FOCS '98). This work was done when the author was at MIT, supported in part by DARPA contract DABT 63-96-C-0018.

http://www.siam.org/journals/sicomp/30-6/37303.html

†Department of Computer Science and Engineering, University of California, San Diego, 9500 Gilman Drive, Mail Code 0114, La Jolla, California 92093-0114 (daniele@cs.ucsd.edu).

[1]In this van Emde Boas paper, this problem is called "Nearest Vector," and the name "Closest Vector" is used for SVP in the ℓ_∞ norm.

SVP was much slower. Even for the exact version of this problem, proving the conjectured NP-hardness remained an open problem for almost two decades. Recently, Ajtai [2] proved that the SVP is hard for NP under *reverse unfaithful random* reductions (RUR-reductions for short, see [18]). These are probabilistic reductions that map NO instances to NO instances with probability 1 and YES instances to YES instances with non-negligible probability.[2] Although not a proper NP-hardness result (i.e., hardness for NP under many-one reductions, which would imply that SVP is not in P unless NP = P), hardness under RUR-reductions also gives evidence of the intractability of a problem. In particular, it implies that SVP is not in RP unless NP = RP. (Here RP is the class of decision problems with random polynomial decision algorithms that are always correct on NO instances and "usually" correct on YES instances.) So, Ajtai's result gives the first theoretical evidence that SVP is indeed intractable, resolving (in a probabilistic sense) van Emde Boas' conjecture. In the same paper, Ajtai also remarks that his NP-hardness proof can be adapted to show the hardness of approximating the length of the shortest vector within some very small factor $1 + o(1)$ that rapidly approaches 1 as the dimension of the lattice grows.

In this paper we prove the first nonapproximability result for the shortest vector problem to within some factor bounded away from 1. Namely, we show that (for any ℓ_p norm) approximating SVP within any constant factor less than $\sqrt[p]{2}$ is hard for NP under RUR-reductions. In particular, approximating SVP in the Euclidean norm within any factor less then $\sqrt{2}$ is hard for NP. The error probability of the reduction is polynomially small, i.e., the reduction correctly maps YES instances to YES instances with probability $1 - 1/\operatorname{poly}(n)$ for some polynomial function $\operatorname{poly}(n)$. Moreover, randomness itself is used in a very restricted way and it can be removed under standard computational or number theoretic assumptions. In particular we show that

(i) SVP has no polynomial time approximation algorithm unless the polynomial hierarchy [26, 33] collapses to the second level.

(ii) Approximating SVP is NP-hard (under deterministic many-one reductions) if the following conjecture on the distribution of square-free smooth numbers holds true: for any $\epsilon > 0$ and for all sufficiently large n there exists a square-free polylog-smooth integer in the interval $[n, n + n^{\epsilon}]$, i.e., an integer whose prime factors are all less than $(\lg n)^c$ (for some constant c independent of n) and have exponent one.

The rest of the paper is organized as follows. In section 2 we give an overview of related work. In section 3 we formally define the approximation problems associated to SVP, CVP, and a variant of the latter. In section 4 we prove that SVP is NP-hard to approximate by reduction from the modified CVP using a geometric lemma which is proved in section 5. In section 6 we present deterministic reductions under various computational or number theoretic assumptions. Section 7 concludes with remarks and open problems.

In section 5 we use a combinatorial theorem (Theorem 5.9) similar to a result originally proved by Ajtai in [2]. In the appendix we present a proof of this combinatorial theorem that greatly simplifies Ajtai's original construction.

2. Related work. The complexity of lattice problems has been widely investigated since the early 1980s because of the many connections between these problems and other areas of computer science. Results are usually presented for the Euclidean

[2] In Ajtai's proof, as well in our result, the success probability is in fact $1 - 1/p(n)$ for some polynomial function $p(n)$.

(ℓ_2) norm but can be easily adapted to any ℓ_p norm, or in some cases any norm. Unless otherwise stated, the following results refer to the ℓ_2 norm.

The first polynomial time approximation algorithms for SVP was the celebrated Lenstra–Lenstra–Lovász (LLL) basis reduction algorithm [24] that achieves an approximation factor $2^{O(n)}$ exponential in the dimension n. In [4] Babai showed how to achieve a similar approximation factor for CVP combining LLL with a lattice rounding technique. To date, the best approximation factor for SVP achievable in polynomial time is $2^{O(n(\log\log n)^2/\log n)}$ using Schnorr's block reduction algorithm [29]. In fact, Schnorr gives a hierarchy of basis reduction algorithms that go from polynomial time to exponential time achieving better and better approximation factors. Unfortunately, Schnorr's result is almost ubiquitously cited as a polynomial time algorithm for approximating SVP within a factor $2^{\epsilon n}$ for any fixed $\epsilon > 0$. It turns out, as recently observed by Goldreich and Håstad [14], that one can set ϵ to a slowly decreasing function of n while maintaining the running time polynomial and achieving a slightly subexponential approximation factor $2^{O(n(\log\log n)^2/\log n)}$. A similar approximation factor can be achieved for CVP combining Schnorr's block reduction algorithm with Kannan's reduction [19] from approximate CVP to approximate SVP.

On the complexity side, CVP was proved NP-hard to solve exactly by van Emde Boas in [34]. The first inapproximability results for CVP are due to Arora et al. [3] who proved that CVP is NP-hard to approximate within any constant factor, and quasi NP-hard to approximate within factor $2^{\log^{1-\epsilon} n}$. The latter result is improved to a proper NP-hardness result by Dinur, Kindler, and Sufra in [10], but the proof is much more complicated. Interestingly, CVP remains hard to solve exactly even if the lattice is known in advance and can be arbitrarily preprocessed before the target point is revealed [28].

The NP-hardness of SVP (in the ℓ_2 norm) was conjectured in [34] but remained an open problem for a long time. The first result is due to Ajtai [2] who proved that solving the problem exactly is NP-hard for randomized reductions. Ajtai's result can also be adapted to show the inapproximability of SVP within certain factors $1 + o(1)$ that rapidly approach 1 as the dimension of the lattice grows. In this paper we prove the first NP-hardness result for approximating SVP within factors bounded away from one.

Interestingly, SVP in the ℓ_∞ norm seems to bear much more similarities to CVP than SVP in the ℓ_2 norm. In fact, the NP-hardness of SVP in the ℓ_∞ norm was already proved in [34]. The quasi NP-hardness of approximating SVP within $2^{\log^{0.5-\epsilon} n}$ appeared in [3], and a proper NP-hardness result is proved in [9] using techniques similar to [10].

The unlikelihood of the NP-hardness of approximating SVP and CVP within polynomial factors has also been investigated. In [22], Lagarias, Lenstra, and Schnorr showed that approximating SVP and CVP within factors $O(n)$ and $O(n^{1.5})$ is in coNP. This result is improved by Banaszczyk [5] where both problems are shown in coNP for $O(n)$ approximation factors. These results imply that approximating SVP and CVP within $\Omega(n)$ polynomial factors cannot be NP-hard, unless NP=coNP. Under the stronger assumption that NP is not contained in coAM, Goldreich and Goldwasser [15] show that approximating SVP and CVP within $\Omega(\sqrt{n}/\log n)$ cannot be NP-hard.

Our results are achieved by reducing the approximate SVP from a variant of CVP which was shown NP-hard to approximate in [3]. The techniques we use to reduce CVP to SVP are related to those used in [30, 1] and [2]. In particular all these works use variants of the "prime number lattice" originally defined by Schnorr in [30] to

(empirically) reduce factoring to lattice reduction. The intent in [30] was to find new factoring algorithms and the method is not formally analyzed. In [1] Adleman attempts to give a formal reduction from factoring to the shortest vector problem. Although based on relatively complicated number theoretic conjectures, Adleman's work marks an important step in the study of the hardness of the shortest vector problem because the reduction from factoring to SVP is presented for the first time as theoretical evidence that SVP is hard. Trying to remove the number theoretic conjectures from Adleman's proof, Ajtai had the fundamental intuition that variants of the prime number lattice could be used to reduce any NP problem (not necessarily related to factoring) to SVP. In the breakthrough paper [2] Ajtai uses an enhanced version of the prime number lattice to reduce an NP-complete problem (a variant of subset sum) to SVP.

In this paper we use a variant of the prime number lattice which is much closer to the original lattice introduced by Schnorr. However, it should be noted that the enhanced lattice defined by Ajtai was the starting point of our investigation, and we rediscovered Schnorr's prime number lattice while trying to understand and simplify Ajtai's construction.

In our proof the prime number lattice is for the first time explicitly connected to sphere packing, giving a simpler and more geometric interpretation of the combinatorics underlying the lattice. The simpler and more geometric approach used in this paper allows us to translate some of the techniques to other settings. In fact, similar techniques have been recently used by Dumer, Micciancio, and Sudan [11] to prove similar results for the minimum distance problem for linear codes.

3. Definitions. Let $\mathbb{R}$ and $\mathbb{Z}$ be the sets of the reals and the integers, respectively. The m-dimensional Euclidean space is denoted $\mathbb{R}^m$. A *lattice* in $\mathbb{R}^m$ is the set of all integer combinations $\mathcal{L} = \{\sum_{i=1}^{n} x_i \mathbf{b}_i : x_i \in \mathbb{Z}\}$ of n linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$ in $\mathbb{R}^m$ $(m \geq n)$. The set of vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$ is said to form a *basis* of the lattice, and the integer n is called the *rank* of the lattice. A basis can be compactly represented by the matrix $\mathbf{B} = [\mathbf{b}_1 | \ldots | \mathbf{b}_n] \in \mathbb{R}^{m \times n}$ having the basis vectors as columns. The lattice generated by $\mathbf{B}$ is denoted $\mathcal{L}(\mathbf{B})$. Notice that $\mathcal{L}(\mathbf{B}) = \{\mathbf{Bx} : \mathbf{x} \in \mathbb{Z}^n\}$, where $\mathbf{Bx}$ is the usual matrix-vector multiplication.

For any $p \geq 1$, the ℓ_p norm of a vector $\mathbf{x} \in \mathbb{R}^n$ is defined as $\|\mathbf{x}\|_p = \sqrt[p]{\sum x_i^p}$. The following definitions can be given with respect to any norm. Since in the rest of this paper the norm being used will always be clear from the context, we omit explicit references to a norm in order to keep notation simple, but it should be noted that the definitions are norm dependent. The *minimum distance* of a lattice, $\lambda(\mathcal{L})$, is the minimum distance between any two distinct lattice points and equals the length of the shortest nonzero lattice vector:

$$\lambda(\mathcal{L}) = \min\{\|\mathbf{x} - \mathbf{y}\| : \mathbf{x} \neq \mathbf{y} \in \mathcal{L}\} = \min\{\|\mathbf{x}\| : \mathbf{x} \in \mathcal{L}, \mathbf{x} \neq \mathbf{0}\}.$$

For vector $\mathbf{x} \in \mathbb{R}^n$ and set $S \subseteq \mathbb{R}^n$, let $\operatorname{dist}(\mathbf{v}, S) = \min_{\mathbf{w} \in S} \|\mathbf{v} - \mathbf{w}\|$ be the distance between $\mathbf{v}$ and S. For vector $\mathbf{x} \in \mathbb{R}^n$ and real r, let $\mathcal{B}(\mathbf{v}, r) = \{\mathbf{w} \in \mathbb{R}^n : \|\mathbf{v} - \mathbf{w}\| \leq r\}$ be the ball of radius r centered in $\mathbf{v}$.

When discussing computational issues related to lattices, it is customary to assume that the lattices are represented by a basis matrix $\mathbf{B}$ and that $\mathbf{B}$ has integer entries. In order to study the computational complexity of lattice problems, we formulate them in terms of promise problems. A *promise* problem is a generalization of the familiar notion of decision problem. The difference is that in a promise problem not every string is required to be either a YES or a NO instance. Given a string with

the promise that it is either a YES or NO instance, one has to decide which of the two sets it belongs to.

Following [15], we formulate the approximation problems associated with the shortest vector problem and the closest vector problem in terms of the following promise problems.

DEFINITION 3.1 (approximate SVP). *The promise problem* GAPSVP_γ *(where* $\gamma \geq 1$ *is a function of the dimension) is defined as follows. Instances are pairs* $(\mathbf{B}, d)$*, where* $\mathbf{B} \in \mathbb{Z}^{n \times k}$ *is a lattice basis and* d *a positive number such that*

(i) $(\mathbf{B}, d)$ *is a* YES *instance if* $\lambda(\mathbf{B}) \leq d$*, i.e.,* $\|\mathbf{Bz}\| \leq d$ *for some* $\mathbf{z} \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$*;*

(ii) $(\mathbf{B}, d)$ *is a* NO *instance if* $\lambda(\mathbf{B}) > \gamma \cdot d$*, i.e.,* $\|\mathbf{Bz}\| > \gamma \cdot d$ *for all* $\mathbf{z} \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$*.*

DEFINITION 3.2 (approximate CVP). *The promise problem* GAPCVP_γ *(where* $\gamma \geq 1$ *is a function of the dimension) is defined as follows. Instances are triples* $(\mathbf{B}, \mathbf{y}, d)$*, where* $\mathbf{B} \in \mathbb{Z}^{n \times k}$ *is a lattice basis,* $\mathbf{y} \in \mathbb{Z}^n$ *a vector, and* d *a positive number such that*

(i) $(\mathbf{B}, \mathbf{y}, d)$ *is a* YES *instance if dist*$(\mathbf{y}, \mathcal{L}(\mathbf{B})) \leq d$*, i.e.,* $\|\mathbf{Bz} - \mathbf{y}\| \leq d$ *for some* $\mathbf{z} \in \mathbb{Z}^n$*;*

(ii) $(\mathbf{B}, \mathbf{y}, d)$ *is a* NO *instance if dist*$(\mathbf{y}, \mathcal{L}(\mathbf{B})) > \gamma \cdot d$*, i.e.,* $\|\mathbf{Bz} - \mathbf{y}\| > \gamma \cdot d$ *for all* $\mathbf{z} \in \mathbb{Z}^n$*.*

The relation between the promise problems above and the corresponding lattice optimization problems is easily explained. On one hand, if one can compute a γ-approximation $d' \in [\lambda(\mathbf{B}), \gamma \cdot \lambda(\mathbf{B})]$ to the length of the shortest nonzero lattice vector, then one can solve GAPSVP_γ by checking whether $d' \leq \gamma \cdot d$ or $d' > \gamma \cdot d$. On the other hand, assume one has a decision oracle O that solves GAPSVP_γ. (By definition, when the input does not satisfy the promise, the oracle can return any answer.) Let $u \in \mathbb{Z}$ be an upper bound to $\lambda(\mathbf{B})$ (for example, let u be the length of any of the basis vectors). Notice that $O(\mathbf{B}, u)$ always returns YES, while $O(\mathbf{B}, 0)$ always returns NO. Using binary search find an integer $d \in \{0, \ldots, u^2\}$ such that $O(\mathbf{B}, \sqrt{d}) = \text{YES}$ and $O(\mathbf{B}, \sqrt{d-1}) = \text{NO}$. Then, $\lambda(\mathbf{B})$ must lie in the interval $[\sqrt{d}, \gamma \cdot \sqrt{d}]$. A similar argument holds for the closest vector problem.

Reductions between promise problems are defined in the obvious way. A function $f\colon \{0,1\}^* \to \{0,1\}^*$ is a reduction from $(\Pi_{\text{YES}}, \Pi_{\text{NO}})$ to $(\Sigma_{\text{YES}}, \Sigma_{\text{NO}})$ if it maps YES instances to YES instances and NO instances to NO instances, i.e., $f(\Pi_{\text{YES}}) \subseteq \Sigma_{\text{YES}}$ and $f(\Pi_{\text{NO}}) \subseteq \Sigma_{\text{NO}}$. Clearly any algorithm A to solve $(\Sigma_{\text{YES}}, \Sigma_{\text{NO}})$ can be used to solve $(\Pi_{\text{YES}}, \Pi_{\text{NO}})$ as follows: on input $I \in \Pi_{\text{YES}} \cup \Pi_{\text{NO}}$, run A on $f(I)$ and output the result. Notice that $f(I)$ always satisfies the promise $f(I) \in \Sigma_{\text{YES}} \cup \Sigma_{\text{NO}}$, and $f(I)$ is a YES instance iff I is a YES instance.

We define one last promise problem that will be useful in the sequel. The problem is a modification of GAPCVP in which YES instances are required to have a boolean solution, and in the NO instances the target vector can be multiplied by any nonzero integer.

DEFINITION 3.3 (modified CVP). *The promise problem* GAPCVP'_γ *(where* $\gamma \geq 1$ *is a function of the dimension) is defined as follows. Instances are triples* $(\mathbf{B}, \mathbf{y}, d)$ *where* $\mathbf{B} \in \mathbb{Z}^{n \times k}$ *is a full rank matrix,* $\mathbf{y} \in \mathbb{Z}^n$ *a vector, and* d *a positive number such that*

(i) $(\mathbf{B}, \mathbf{y}, d)$ *is a* YES *instance if* $\|\mathbf{Bz} - \mathbf{y}\| \leq d$ *for some* $\mathbf{z} \in \{0,1\}^n$*;*

(ii) $(\mathbf{B}, \mathbf{y}, d)$ *is a* NO *instance if* $\|\mathbf{Bz} - w\mathbf{y}\| > \gamma \cdot d$ *for all* $\mathbf{z} \in \mathbb{Z}^n$ *and all* $w \in \mathbb{Z} \setminus \{\mathbf{0}\}$*.*

In [3] it is proved that GAPCVP_γ and its variant GAPCVP'_γ are NP-hard for any constant factor $\gamma \geq 1$.

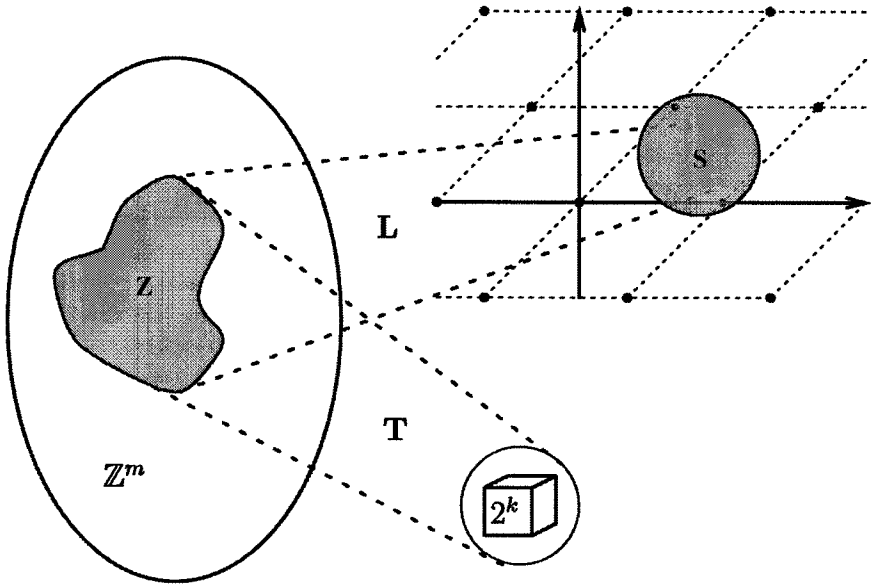

FIG. 4.1. *Lattice $\mathcal{L}(\mathbf{L})$ has minimum distance $\widetilde{\gamma} \approx \sqrt[p]{2}$ times the radius of sphere $\mathcal{B}(\mathbf{s}, r)$ and all boolean vectors of length k can be expressed as $\mathbf{Tz}$ for some lattice vector $\mathbf{Lz}$ inside the sphere.*

4. Hardness of approximating SVP. In this section we present the main result of this paper: for any ℓ_p norm ($p \geq 1$), and for any constant $\gamma \in [1, \sqrt[p]{2})$, the promise problem GAPSVP$_\gamma$ is hard for NP (under RUR-reductions). The proof is by reduction from a variant of the closest vector problem (GAPCVP$'$) and is based on the following simple idea: Assume one wants to find the point in a lattice $\mathcal{L}(\mathbf{B})$ (approximately) closest to some vector $\mathbf{y}$. One may look for the shortest nonzero vector in the lattice generated by the matrix $[\mathbf{B}|\mathbf{y}]$, i.e., the Minkowski sum of the original lattice $\mathcal{L}(\mathbf{B})$ and the lattice $\mathcal{L}(\mathbf{y}) = \mathbb{Z} \cdot \mathbf{y}$ of all integer multiples of the target vector. If the shortest vector in $\mathcal{L}([\mathbf{B}|\mathbf{y}])$ is of the form $\mathbf{Bx} - \mathbf{y}$ then $\mathbf{Bx}$ necessarily is the lattice vector in $\mathcal{L}(\mathbf{B})$ closest to $\mathbf{y}$. However, if the original lattice $\mathcal{L}(\mathbf{B})$ contains vectors as short as the distance of $\mathbf{y}$ from $\mathcal{L}(\mathbf{B})$, then solving the shortest vector problem in the lattice $\mathcal{L}([\mathbf{B}|\mathbf{y}])$ might find a vector of the form $\mathbf{Bx}$, unrelated to the target $\mathbf{y}$. (Notice that the shortest vector in $\mathcal{L}([\mathbf{B}|\mathbf{y}])$ might also correspond to a vector in $\mathcal{L}(\mathbf{B})$ close to a multiple of $\mathbf{y}$, but this is not a problem if we are reducing from GAPCVP$'$.)

We solve this problem by embedding the lattice $\mathcal{L}([\mathbf{B}|\mathbf{y}])$ in a higher dimensional space; i.e., we introduce new coordinates and extend the basis vectors in $[\mathbf{B}|\mathbf{y}]$ with appropriate values. The embedding is based on the construction of a lattice $\mathcal{L}(\mathbf{L})$ and a sphere $\mathcal{B}(\mathbf{s}, r)$ with the property that the minimum distance between lattice points in $\mathcal{L}(\mathbf{L})$ is bigger than the radius r of the sphere (by a constant factor $\widetilde{\gamma} > \gamma$) and at the same time the sphere contains exponentially many lattice vectors from $\mathcal{L}(\mathbf{L})$. We use the lattice points in the sphere to represent all potential solutions to the GAPCVP$'$ problem. In particular, we also build a linear integer transformation $\mathbf{T}$ such that any boolean vector $\mathbf{x} \in \{0,1\}^k$ (i.e., any potential solution to the GAPCVP$'$ problem) can be expressed as $\mathbf{Tz}$ ($\mathbf{z}$ an integer vector) for some lattice point $\mathbf{Lz}$ in the ball $\mathcal{B}(\mathbf{s}, r)$. These requirements are summarized in the following lemma (see Figure 4.1).

LEMMA 4.1. *For any ℓ_p norm ($p \geq 1$) and any constant $\widetilde{\gamma} \in [1, \sqrt[p]{2})$ there exists a (probabilistic) algorithm that on input $k \in \mathbb{Z}^+$ outputs, in* $\mathrm{poly}(k)$ *time, two positive integers $m, r \in \mathbb{Z}^+$, a lattice basis $\mathbf{L} \in \mathbb{Z}^{(m+1)\times m}$, a vector $\mathbf{s} \in \mathbb{Z}^{m+1}$, and a linear integer transformation $\mathbf{T} \in \mathbb{Z}^{k\times m}$ such that*

(i) $\lambda(\mathbf{L}) > \widetilde{\gamma} \cdot r$,

(ii) *with probability at least* $1 - 1/\mathrm{poly}(k)$ *for all $\mathbf{x} \in \{0,1\}^k$ there exists a $\mathbf{z} \in \mathbb{Z}^m$ such that $\mathbf{Tz} = \mathbf{x}$ and $\mathbf{Lz} \in \mathcal{B}(\mathbf{s}, r)$.*

Remark. From the proof of Lemma 4.1 in section 5 it appears that the lemma can be stated in a stronger form asserting the existence of a single algorithm that takes p and $\widetilde{\gamma}$ as additional parameters. However, it should be noted that for every ℓ_p norm, the algorithm can be used only for factors $\widetilde{\gamma} < \sqrt[p]{2}$, and the complexity of the algorithm (e.g., running time or output size) grows to infinity as $\widetilde{\gamma}$ gets closer to $\sqrt[p]{2}$. Stating the result as a single algorithm would require to determine the dependency of the running time on how close $\widetilde{\gamma}$ is to $\sqrt[p]{2}$. In order to keep the notation simple, we will state all the results in this paper for fixed norms ℓ_p and factors γ, but a generalization of the results to variable ℓ_p and γ (subject to the constraint $\gamma < \sqrt[p]{2}$) is indeed possible and the dependency of the running time on p and γ can (in principle) be extracted from the proofs presented in this paper. It should also be noted that as p gets larger and larger, the maximum constant for which we can prove hardness of SVP in the ℓ_p norm approaches 1. This is quite counterintuitive, as we know that SVP in the ℓ_∞ norm is hard to approximate within any constant [3, 9]. So, it is natural to expect that SVP in the ℓ_p norm is harder when p is large.

We defer the proof of the above lemma to section 5 and move straight to the main theorem.

THEOREM 4.2. *For any ℓ_p norm ($p \geq 1$) and for any constant $\gamma \in [1, \sqrt[p]{2})$, the promise problem* GAPSVP_γ *is hard for* NP *under RUR-reductions with inverse polynomial error probability.*

Proof. Fix an ℓ_p norm and a constant $\gamma \in [1, \sqrt[p]{2})$. Let $\widetilde{\gamma}$ be a real between γ and $\sqrt[p]{2}$ and let γ' be a real greater than $(\gamma^{-p} - \widetilde{\gamma}^{-p})^{-1/p}$, and assume without loss of generality that γ'/γ and $\widetilde{\gamma}/\gamma$ are rational numbers. We prove that GAPSVP_γ is hard for NP by reduction from the promise problem $\mathrm{GAPCVP}'_{\gamma'}$ which is known to be NP-hard (see [3]).

Let $(\mathbf{B}, \mathbf{y}, d)$ be an instance of $\mathrm{GAPCVP}'_{\gamma'}$ with $\mathbf{B} \in \mathbb{Z}^{n\times k}$, $\mathbf{y} \in \mathbb{Z}^n$, and $d \in \mathbb{Z}$. We define an instance $(\mathbf{V}, t)$ of GAPSVP_γ such that if $(\mathbf{B}, \mathbf{y}, d)$ is a NO instance of $\mathrm{GAPCVP}'_{\gamma'}$ then $(\mathbf{V}, t)$ is a NO instance of GAPSVP_γ, and if $(\mathbf{B}, \mathbf{y}, d)$ is a YES instance of $\mathrm{GAPCVP}'_{\gamma'}$ then $(\mathbf{V}, t)$ is a YES instance of GAPSVP_γ with high probability.

Run the (randomized) algorithm from Lemma 4.1 on input k to obtain a lattice basis $\mathbf{L} \in \mathbb{Z}^{(m+1)\times m}$, a vector $\mathbf{s} \in \mathbb{Z}^{m+1}$, a linear integer transformation $\mathbf{T} \in \mathbb{Z}^{k\times m}$ and a integer $r \in \mathbb{Z}$ such that

(i) $\|\mathbf{Lz}\|_p > \widetilde{\gamma} \cdot r$ for all $\mathbf{z} \in \mathbb{Z}^m \setminus \{\mathbf{0}\}$,

(ii) with probability at least $1 - 1/\mathrm{poly}(k)$, for all vectors $\mathbf{x} \in \{0,1\}^k$ there exists a $\mathbf{z} \in \mathbb{Z}^m$ such that $\mathbf{Tz} = \mathbf{x}$ and $\|\mathbf{Lz} - \mathbf{s}\|_p \leq r$.

Define the lattice

$$\mathbf{V} = \left[\begin{array}{c|c} a \cdot \mathbf{BT} & a \cdot \mathbf{y} \\ b \cdot \mathbf{L} & b \cdot \mathbf{s} \end{array}\right],$$

where a and b are two integer scaling factors such that $\frac{a}{b} = \frac{r\widetilde{\gamma}}{d\gamma'}$ and $t = a \cdot d\gamma'/\gamma = b \cdot r\widetilde{\gamma}/\gamma$ is integer. We want to prove that if $(\mathbf{B}, \mathbf{y}, d)$ is a NO instance of $\mathrm{GAPCVP}'_{\gamma'}$

then $(\mathbf{V}, t)$ is a NO instance of GAPSVP$_\gamma$, and (provided the construction in the lemma succeeds) if $(\mathbf{B}, \mathbf{y}, d)$ is a YES instance of GAPCVP$'_{\gamma'}$ then $(\mathbf{V}, t)$ is a YES instance of GAPSVP$_\gamma$.

First assume $(\mathbf{B}, \mathbf{y}, d)$ is a NO instance and consider a generic nonzero integer vector

$$\mathbf{w} = \begin{bmatrix} \mathbf{z} \\ w \end{bmatrix}.$$

We want to prove that $\|\mathbf{V}\mathbf{w}\|_p^p > (\gamma t)^p$. Notice that

$$\|\mathbf{V}\mathbf{w}\|_p^p = (a \cdot \|\mathbf{B}\mathbf{x} + w\mathbf{y}\|_p)^p + (b \cdot \|\mathbf{L}\mathbf{z} + w\mathbf{s}\|_p)^p,$$

where $\mathbf{x} = C\mathbf{z}$. We prove that

$$a \cdot \|\mathbf{B}\mathbf{x} + w\mathbf{y}\|_p > \gamma t, \qquad \text{or} \qquad b \cdot \|\mathbf{L}\mathbf{z} + w\mathbf{s}\|_p > \gamma t.$$

We distinguish two cases:

1. If $w \neq 0$, then by definition of GAPCVP$'_{\gamma'}$,
$$a \cdot \|\mathbf{B}\mathbf{x} + w\mathbf{y}\|_p > a \cdot \gamma' d = \gamma t;$$
2. if $w = 0$, then $\mathbf{z} \neq 0$ and by construction
$$b \cdot \|\mathbf{L}\mathbf{z} + w\mathbf{s}\|_p = b \cdot \|\mathbf{L}\mathbf{z}\|_p > b \cdot \widetilde{\gamma} r = \gamma t.$$

Now assume that $(\mathbf{B}, \mathbf{y}, d)$ is a YES instance, i.e., there exists a boolean vector $\mathbf{x} \in \{0,1\}^k$ such that $\|\mathbf{B}\mathbf{x} - \mathbf{y}\|_p \leq d$. By construction, there exists a vector $\mathbf{z} \in \mathbb{Z}^m$ such that $\mathbf{T}\mathbf{z} = \mathbf{x}$ and $\|\mathbf{L}\mathbf{z} - \mathbf{s}\|_p \leq r$. Define

$$\mathbf{w} = \begin{bmatrix} \mathbf{z} \\ -1 \end{bmatrix}$$

and compute the norm of the corresponding lattice vector:

$$\begin{aligned} \|\mathbf{V}\mathbf{w}\|_p^p &= (a \cdot \|\mathbf{B}\mathbf{x} - \mathbf{y}\|_p)^p + (b \cdot \|\mathbf{L}\mathbf{z} - \mathbf{s}\|_p)^p \\ &\leq (ad)^p + (br)^p \\ &= \left(\frac{\gamma t}{\gamma'}\right)^p + \left(\frac{\gamma t}{\widetilde{\gamma}}\right)^p \\ &\leq t^p \gamma^p \left(\left(\frac{1}{\gamma^p} - \frac{1}{\widetilde{\gamma}^p}\right) + \frac{1}{\widetilde{\gamma}^p}\right) \\ &= t^p, \end{aligned}$$

proving that $(\mathbf{V}, t)$ is a YES instance of GAPSVP$_\gamma$. ∎

5. Proof of the geometric lemma. In this section we prove Lemma 4.1. As explained in section 4, this lemma asserts the existence of an integer lattice $\mathcal{L}(\mathbf{L})$ with large minimum distance, a sphere $\mathcal{B}(\mathbf{s}, r)$ of radius less than $\lambda(\mathbf{L})$ (by a constant factor $\widetilde{\gamma}$) containing a large number of lattice points, and a linear integer transformation that maps the coordinates (with respect to $\mathbf{L}$) of the lattice points in the sphere onto the set of all binary strings of some shorter length. Moreover, $\mathbf{L}, \mathbf{s}$, and $\mathbf{T}$ can be computed in (random) polynomial time.

The lattice and the sphere are more easily defined using arbitrary real numbers. So, we first drop the requirement that $\mathbf{L}$ and $\mathbf{s}$ have integer entries and define a real matrix $\widetilde{\mathbf{L}}$ and a real vector $\widetilde{\mathbf{s}}$ with the desired properties. Then, we show how to approximate $\widetilde{\mathbf{L}}$ and $\widetilde{\mathbf{s}}$ with integer matrices. Finally, we prove Lemma 4.1 combining the integer lattice construction with a combinatorial theorem on low-degree hypergraphs.

5.1. The real lattice. In the next lemma we define a real lattice $\mathcal{L}(\widetilde{\mathbf{L}})$ and prove a lower bound on the length of its nonzero vectors. The definition of $\widetilde{\mathbf{L}}$ is parametric with respect to an ℓ_p norm ($p \geq 1$), a real number $\alpha > 0$, and a set of positive integers $A = \{a_1, \ldots, a_m\}$. The idea is to map the multiplicative structure of the integers $a_1, \ldots, a_m$ to the additive structure of the lattice $\mathcal{L}(\widetilde{\mathbf{L}})$, defining a basis vector for each a_i and expressing its entries in terms of the logarithm of a_i. This way the problem of finding a sphere containing many lattice points is reduced to the problem of finding a small interval containing many products of the a_i's. At the end we will set α to some large number (exponential in m), and A to a set of small primes. The existence of a sphere containing many lattice points will follow from the density of the primes and a simple averaging argument.

LEMMA 5.1. *Let $A = \{a_1, \ldots, a_m\}$ be a set of relatively prime odd positive integers. Then for any ℓ_p norm ($p \geq 1$), and any real $\alpha > 0$, all nonzero vectors in the lattice generated by the (columns of the) matrix*

$$\widetilde{\mathbf{L}} = \begin{bmatrix} \sqrt[p]{\ln a_1} & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \sqrt[p]{\ln a_m} \\ \alpha \ln a_1 & \cdots & \alpha \ln a_m \end{bmatrix} \in \mathbb{R}^{(m+1)\times m} \tag{5.1}$$

have ℓ_p norm bigger than $\sqrt[p]{2 \ln \alpha}$.

Proof. We want to prove that for all nonzero integer vectors $\mathbf{z} \in \mathbb{Z}^m$,

$$\|\widetilde{\mathbf{L}}\mathbf{z}\|_p^p \geq 2 \ln \alpha.$$

We first introduce some notation. Let $\mathbf{R} \in \mathbb{R}^m$ be the row vector

$$\mathbf{R} = [\ln a_1, \ln a_2, \ldots, \ln a_m] \tag{5.2}$$

and $\mathbf{D} \in \mathbb{R}^{m\times m}$ be the diagonal matrix

$$\mathbf{D} = \begin{bmatrix} \sqrt[p]{\ln a_1} & 0 & \cdots & 0 \\ 0 & \sqrt[p]{\ln a_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \sqrt[p]{\ln a_m} \end{bmatrix}. \tag{5.3}$$

Notice that

$$\widetilde{\mathbf{L}} = \begin{bmatrix} \mathbf{D} \\ \alpha \mathbf{R} \end{bmatrix}$$

and $\|\widetilde{\mathbf{L}}\mathbf{z}\|_p^p = \|\mathbf{D}\mathbf{z}\|_p^p + \alpha^p |\mathbf{R}\mathbf{z}|^p$. We bound the two terms separately. Define the integers

$$\hat{g} = \prod\{a_i^{z_i} : z_i > 0\}, \qquad \check{g} = \prod\{a_i^{-z_i} : z_i < 0\}, \qquad g = \hat{g}\check{g} = \prod_{i=1}^{m} a_i^{|z_i|}.$$

Using this notation, the first term satisfies

$$\begin{aligned}\|\mathbf{Dz}\|_p^p &= \sum_i |z_i|^p \ln a_i \\ &\geq \sum_i |z_i| \ln a_i \\ &= \ln g\end{aligned}$$

because $p \geq 1$ and the z_i's are integers. Bounding the second term is slightly more complex:

$$\begin{aligned}|\mathbf{Rz}| &= \left| \sum_i z_i \ln a_i \right| \\ &= |\ln \hat{g} - \ln \check{g}| \\ &= \ln \left(1 + \frac{|\hat{g} - \check{g}|}{\min\{\hat{g}, \check{g}\}} \right).\end{aligned}$$

Now notice that since $\mathbf{z}$ is nonzero, $\hat{g}$ and $\check{g}$ are distinct odd integers and therefore $|\hat{g} - \check{g}| \geq 2$. Moreover, $\min\{\hat{g}, \check{g}\} < \sqrt{\hat{g}\check{g}} = \sqrt{g}$. By monotonicity and concavity of function $\ln(1 + x)$ over the interval $[0, 2]$, one gets

$$\ln \left(1 + \frac{|\hat{g} - \check{g}|}{\min\{\hat{g}, \check{g}\}} \right) > \ln \left(1 + \frac{2}{\sqrt{g}} \right) > \frac{2}{\sqrt{g}} \cdot \frac{\ln 3}{2} > \frac{1}{\sqrt{g}}.$$

Combining the two bounds one gets

$$\|\widetilde{\mathbf{L}}\mathbf{z}\|_p^p = \|\mathbf{Dz}\|_p^p + \alpha^p (\mathbf{Rz})^p > \ln g + \frac{\alpha^p}{g^{p/2}}$$

which is a continuous function of g with derivative

$$\frac{1}{g} \left(1 - \frac{p}{2} \cdot \frac{\alpha^p}{g^{p/2}} \right).$$

The function is minimized (over the reals) when $g = \alpha^2 \left(\frac{p}{2}\right)^{2/p}$ with minimum

$$2 \ln \alpha + \left(\frac{2}{p} \right) \ln \left(\frac{p}{2} \right) + \left(\frac{2}{p} \right) > 2 \ln \alpha + \left(\frac{2}{p} \right) \ln p > 2 \ln \alpha.$$

Therefore, for all nonzero integer vectors $\mathbf{z}$, $\|\widetilde{\mathbf{L}}\mathbf{z}\|_p^p > 2 \ln \alpha$. □

Consider now a sphere centered in

$$\widetilde{\mathbf{s}} = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ \alpha \ln \beta \end{bmatrix}, \tag{5.4}$$

where β is a positive real to be specified. We now show that there is a close relationship between finding lattice vectors close to $\widetilde{\mathbf{s}}$ and approximating β as a product of the a_i's.

LEMMA 5.2. *Let* $\widetilde{\mathbf{L}}$ *and* $\widetilde{\mathbf{s}}$ *be defined as in* (5.1) *and* (5.4). *For any* ℓ_p *norm* ($p \geq 1$), *reals* $\alpha, \beta \geq 1$, *positive integers* $a_1, \ldots, a_m$, *and boolean vector* $\mathbf{z} \in \{0,1\}^m$, *if the integer* $g = \prod_i a_i^{z_i}$ *belongs to the interval* $[\beta, \beta(1+1/\alpha)]$, *then*

$$\|\widetilde{\mathbf{L}}\mathbf{z} - \widetilde{\mathbf{s}}\|_p \leq \sqrt[p]{\ln \beta + 2}.$$

Proof. Let $\mathbf{D}$ and $\mathbf{R}$ be as defined in (5.3) and (5.2). Notice that since $\mathbf{z}$ is a 0-1 vector,

$$\|\mathbf{D}\mathbf{z}\|_p^p = \mathbf{R}\mathbf{z} = \ln g,$$

and therefore

$$\begin{aligned}\|\widetilde{\mathbf{L}}\mathbf{z} - \widetilde{\mathbf{s}}\|_p^p &= \|\mathbf{D}\mathbf{z}\|_p^p + \alpha^p |\mathbf{R}\mathbf{z} - \ln \beta|^p \\ &= \ln g + \alpha^p |\ln g - \ln \beta|^p \\ &= \ln \beta + \ln \frac{g}{\beta} + \left|\alpha \ln \frac{g}{\beta}\right|^p.\end{aligned}$$

From the assumption $g \in [\beta, \beta(1+1/\alpha)]$ and using the inequality $\ln(1+x) < x$ (true for all $x \neq 0$) one gets

$$0 \leq \ln \frac{g}{\beta} \leq \ln\left(1 + \frac{1}{\alpha}\right) < \frac{1}{\alpha}$$

which, substituted in the above expression, gives

$$\|\widetilde{\mathbf{L}}\mathbf{z} - \widetilde{\mathbf{s}}\|_p^p < \ln \beta + \frac{1}{\alpha} + 1 \leq \ln \beta + 2 \qquad \square$$

Now let ϵ be a small positive real constant and set $\alpha = \beta^{(1-\epsilon)}$. From Lemma 5.1, the minimum distance between lattice points is bigger than $\lambda = \sqrt[p]{2(1-\epsilon)\ln \beta}$, and there are many lattice points within distance $\sqrt[p]{\ln \beta + 2} \approx \lambda / \sqrt[p]{2}$ from $\widetilde{\mathbf{s}}$, provided that the interval $[\beta, \beta + \beta^\epsilon]$ contains many products of the form $\prod_{i \in S} a_i$ ($S \subseteq \{1, \ldots, m\}$). If $a_1, \ldots, a_m$ are the first m odd prime numbers, this is the same as saying that $[\beta, \beta + \beta^\epsilon]$ contains many square-free odd (a_m)-smooth numbers. We now informally estimate for which values of m and β one should expect $[\beta, \beta + \beta^\epsilon]$ to contain a large number of such products. A rigorous probabilistic analysis will follow right after.

Fix some integer $c > 1/\epsilon$, let h be a sufficiently large integer and set $m = h^c$. Let $a_1, \ldots, a_m$ be the first m odd primes, and consider the set of products

$$M = \left\{ \prod_{i \in S} a_i : S \subset \{1, \ldots, m\}, |S| = h \right\}.$$

Notice that

$$|M| = \binom{m}{h} = \prod_{i=0}^{h-1} \frac{m-i}{h-i} \geq \prod_{i=0}^{h-1} \frac{m}{h} = h^{(c-1)h} \tag{5.5}$$

and all elements of M belong to the interval $[1, (a_m)^h]$. If we choose β uniformly at random in this interval, the expected size of $[\beta, \beta + \beta^\epsilon]$ is $\Omega((a_m)^{\epsilon h})$ and we can estimate the number of elements of M contained in $[\beta, \beta + \beta^\epsilon]$ to be

$$\Omega((a_m)^{\epsilon h}) \cdot \frac{|M|}{(a_m)^h} \geq \Omega\left(\frac{h^{c-1}}{(a_m)^{1-\epsilon}}\right)^h.$$

By the prime number theorem, $a_m = O(m \ln m) = O(h^c \ln h)$ and therefore our estimate is $\Omega(h^{\epsilon c - 1}/\ln h)^h > 2^h$ for all sufficiently large h.

Making the above argument more formal, one can prove that there exists an interval $[\beta, \beta + \beta^\epsilon]$ containing exponentially (in h) many products from M. Still, it is not clear how to find the right β. If square-free smooth numbers are distributed uniformly enough, any choice of β is good. Unfortunately, we do not know enough about the distribution of smooth numbers to prove such a statement about small intervals $[\beta, \beta + \beta^\epsilon]$. (It can be proved that for all β the interval $[\beta, 2\beta]$ contains square-free smooth numbers, but not much is known about interval of sublinear size.)

So, we exploit the smooth number distribution (whatever it is) to bias the choice of the interval toward those containing many smooth numbers. The idea is to set β to the product of a random (size h) subset of the a_i's. This way, the interval $[\beta, \beta + \beta^\epsilon]$ is selected with a probability roughly proportional to the number of square-free (a_m)-smooth numbers contained in it. So, for example, intervals containing no smooth numbers are never selected, and intervals containing few smooth numbers are selected with very small probability. The probability of choosing an interval containing few products is bounded in the next lemma. In fact the lemma is quite general and applies to any set M of real numbers bigger than 1.

LEMMA 5.3. *For every positive real numbers $\epsilon \in [0, 1)$, $\mu > 1$, integer $H \geq 1$, and any finite subset $M \subset [1, \mu)$, if β is chosen uniformly at random from M, then the probability that $[\beta, \beta + \beta^\epsilon)$ contains less than H elements from M is at most*

$$\Pr_{\beta \in M}\{|[\beta, \beta + \beta^\epsilon) \cap M| < H\} \leq \frac{\mu^{1-\epsilon} \cdot H}{\kappa(\epsilon) \cdot |M|},$$

where $\kappa(\epsilon) = 1 - 2^{1-\epsilon}$.

Proof. Let B be the set of all $\beta \in M$ such that $|[\beta, \beta + \beta^\epsilon) \cap M| < H$. We show that $|B|$ can be partitioned into at most $K = \mu^{1-\epsilon}/\kappa(\epsilon)$ subsets, each containing less than H elements. It follows that

$$\Pr_{\beta \in M}\{\beta \in B\} = \frac{|B|}{|M|} \leq \frac{K(H-1)}{|M|} = \frac{\mu^{1-\epsilon} \cdot H}{\kappa(\epsilon) \cdot |M|}.$$

Divide $[1, \mu)$ into $\lceil \log_2 \mu \rceil$ intervals $[2^k, 2^{k+1})$ for $k = 0, \ldots, \lceil \log_2 \mu \rceil - 1$. Then divide each interval $[2^k, 2^{k+1})$ into $2^k/2^{\epsilon k} = 2^{(1-\epsilon)k}$ subintervals of size $2^{\epsilon k}$. Notice that each subinterval is of the form $[x, x + y)$ for some $y \leq x^\epsilon$, therefore it contains at most $H - 1$ points from B. It remains to count the total number of subintervals. Adding up the number of subintervals for each interval $[2^k, 2^{k+1})$ we get

$$\begin{aligned} K &= \sum_{k=0}^{\lceil \log_2 \mu \rceil - 1} 2^{(1-\epsilon)k} \\ &= \frac{2^{(1-\epsilon)\lceil \log_2 \mu \rceil} - 1}{2^{1-\epsilon} - 1} \\ &< \frac{(2\mu)^{1-\epsilon}}{2^{1-\epsilon} - 1} = \frac{\mu^{1-\epsilon}}{\kappa(\epsilon)}. \end{aligned}$$

□

Applying this lemma to the set of square free smooth numbers we get the following proposition.

PROPOSITION 5.4. *For all reals $\epsilon, \delta > 0$, there exists an integer c such that for all sufficiently large integer h, the following holds. Let $m = h^c$, $a_1, \ldots, a_m$ be the*

first m odd primes, and M the set of all products $\prod_{i\in S} a_i$, where S is a size h subset of $\{1,\ldots,m\}$. If β is chosen uniformly at random from M then the probability that $[\beta,\beta+\beta^\epsilon)$ contains less than $h^{\delta h}$ elements of M is at most 2^{-h}.

Proof. Fix some $\epsilon,\delta>0$ and let c be an integer bigger than $(1+\delta)/\epsilon$. Let $\mu=a_m^h$. Notice that M is contained in $[1,\mu)$ and $|M|\geq h^{(c-1)h}$ (see (5.5)). Applying Lemma 5.3 to set M with $H=h^{\delta h}$, we get

$$\begin{aligned}\Pr\{|[\beta,\beta+\beta^\epsilon)\cap M|<H\} &< \frac{h^{\delta h}\cdot\mu^{1-\epsilon}}{\kappa(\epsilon)|M|}\\ &< \frac{h^{\delta h}a_m^{(1-\epsilon)h}}{\kappa(\epsilon)h^{(c-1)h}}.\end{aligned}$$

By the prime number theorem, $a_m=O(m\ln m)=O(h^c\ln h)$, which substituted in the above expression gives

$$\begin{aligned}\Pr\{|[\beta,\beta+\beta^\epsilon]\cap M|\leq H\} &< \frac{h^{\delta h}\,O(h^c\ln h)^{(1-\epsilon)h}}{\kappa(\epsilon)h^{(c-1)h}}\\ &= \left(\frac{O(\ln h)^{(1-\epsilon)}}{h^{\epsilon c-(1+\delta)}}\right)^h\\ &< \left(\frac{O(\ln h)}{h^{\epsilon c-(1+\delta)}}\right)^h\\ &< 2^{-h}\end{aligned}$$

for all sufficiently large h because $\epsilon c-(1+\delta)>0$. □

Combining Lemma 5.1, Lemma 5.2, and Proposition 5.4, we immediately get the following theorem.

THEOREM 5.5. *For all reals $\epsilon,\delta>0$, there exists an integer c such that the following holds. Let h be a positive integer, $m=h^c$, and $a_1,\ldots,a_m$ be the first m odd primes. Let β be the product of a random subset of $\{a_1,\ldots,a_m\}$ of size h and set $\alpha=\beta^{1-\epsilon}$. Define $\widetilde{\mathbf{L}}$ and $\widetilde{\mathbf{s}}$ as in (5.1) and (5.4), and let $\widetilde{r}=\sqrt[p]{(1+\epsilon)\ln\beta}>1$. Then*

(i) *all nonzero vectors in $\mathcal{L}(\widetilde{\mathbf{L}})$ have ℓ_p norm greater than $\sqrt[p]{2\left((1-\epsilon)/(1+\epsilon)\right)}r$.*

(ii) *For all sufficiently large h, with probability at least $1-2^{-h}$, the ball $\mathcal{B}(\widetilde{\mathbf{s}},r)$ contains more than $h^{\delta h}$ lattice points of the form $\mathbf{Lz}$ where $\mathbf{z}$ is a 0-1 vector with exactly h ones.*

5.2. Working over the integers. In the previous subsection we proved that as far as real entries are allowed one can easily define a basis $\widetilde{\mathbf{L}}$ and probabilistically find a vector $\widetilde{\mathbf{s}}$ with the property that a sphere of radius slightly more then $\lambda(\widetilde{\mathbf{L}})/\sqrt[p]{2}$ contains many lattice points. We now prove that the same result can be achieved using a suitable integer approximation of $\widetilde{\mathbf{L}}$ and $\widetilde{\mathbf{s}}$. The error incurred by approximating a multiple of $\widetilde{\mathbf{L}}$ and $\widetilde{\mathbf{s}}$ with integers is bounded in the following two lemmas.

LEMMA 5.6. *For all $\eta\geq 1$ and all integer vectors $\mathbf{z}\in\mathbb{Z}^m$,*

$$\|\mathbf{Lz}\|_p\geq(\eta-1)m\|\widetilde{\mathbf{L}}\mathbf{z}\|_p,$$

where $\mathbf{L}=\lfloor(m\eta)\widetilde{\mathbf{L}}\rceil$ is the matrix obtained multiplying $\widetilde{\mathbf{L}}$ by $m\eta$ and rounding each entry to the closest integer.

Proof. By triangular inequality

$$\|\mathbf{Lz}\|_p=\|(m\eta)\widetilde{\mathbf{L}}\mathbf{z}+(\mathbf{L}-(m\eta)\widetilde{\mathbf{L}})\mathbf{z}\|_p$$

$$\begin{aligned}&\geq \|(m\eta)\widetilde{\mathbf{L}}\mathbf{z}\|_p - \|(\mathbf{L}-(m\eta)\widetilde{\mathbf{L}})\mathbf{z}\|_p\\&= \eta m\|\widetilde{\mathbf{L}}\mathbf{z}\|_p - \|(\mathbf{L}-(m\eta)\widetilde{\mathbf{L}})\mathbf{z}\|_p.\end{aligned}$$

It remains to prove that $\|(\mathbf{L}-(m\eta)\widetilde{\mathbf{L}})\mathbf{z}\|_p \leq m\|\widetilde{\mathbf{L}}\mathbf{z}\|_p$. Notice that all entries in $(\mathbf{L}-(m\eta)\widetilde{\mathbf{L}})$ are at most $1/2$ in absolute value. Therefore

$$\begin{aligned}\|(\mathbf{L}-(m\eta)\widetilde{\mathbf{L}})\mathbf{z}\|_p &\leq \frac{1}{2}\sqrt[p]{\|\mathbf{z}\|_p^p + \left(\sum|z_i|\right)^p}\\&\leq \frac{1}{2}\sqrt[p]{\|\mathbf{z}\|_p^p + m^p\|\mathbf{z}\|_p^p}\\&\leq m\|\mathbf{z}\|_p.\end{aligned}$$

Furthermore,

$$\begin{aligned}\|\widetilde{\mathbf{L}}\mathbf{z}\|_p^p &= \|\mathbf{D}\mathbf{z}\|_p^p + \alpha^p|\mathbf{R}\mathbf{z}|^p\\&\geq \|\mathbf{D}\mathbf{z}\|_p^p\\&\geq \|\mathbf{z}\|_p^p\end{aligned}$$

because $\mathbf{D}$ is diagonal with all entries greater than 1. This proves that $\|(\mathbf{L}-(m\eta)\widetilde{\mathbf{L}})\mathbf{z}\|_p \leq m\|\widetilde{\mathbf{L}}\mathbf{z}\|_p$ and therefore $\|\mathbf{L}\mathbf{z}\|_p \geq (\eta-1)m\|\widetilde{\mathbf{L}}\mathbf{z}\|_p$. □

LEMMA 5.7. *For all $\eta > 0$ and all integer vectors $\mathbf{z} \in \mathbb{Z}^m$*

$$\|\mathbf{L}\mathbf{z}-\mathbf{s}\|_p \leq (\eta+1)m\|\widetilde{\mathbf{L}}\mathbf{z}-\widetilde{\mathbf{s}}\|_p,$$

where $\mathbf{L} = \lfloor(m\eta)L\rceil$ and $\mathbf{s} = \lfloor(m\eta)\mathbf{s}\rceil$ are the matrices obtained multiplying $\widetilde{\mathbf{L}}$ and $\widetilde{\mathbf{s}}$ by $m\eta$ and rounding each entry to the closest integer.

Proof. By triangular inequality

$$\begin{aligned}\|\mathbf{L}\mathbf{z}-\mathbf{s}\|_p &= \|((m\eta)\widetilde{\mathbf{L}}\mathbf{z}-(m\eta)\widetilde{\mathbf{s}}) + (\mathbf{L}-(m\eta)\widetilde{\mathbf{L}})\mathbf{z} - (\mathbf{s}-(m\eta)\widetilde{\mathbf{s}})\|_p\\&\leq \|((m\eta)\widetilde{\mathbf{L}}\mathbf{z}-(m\eta)\widetilde{\mathbf{s}})\|_p + \|(\mathbf{L}-(m\eta)\widetilde{\mathbf{L}})\mathbf{z} - (\mathbf{s}-(m\eta)\widetilde{\mathbf{s}})\|_p\\&= \eta m\|\widetilde{\mathbf{L}}\mathbf{z}-(m\eta)\widetilde{\mathbf{s}}\|_p + \|(\mathbf{L}-(m\eta)\widetilde{\mathbf{L}})\mathbf{z} - (\mathbf{s}-(m\eta)\widetilde{\mathbf{s}})\|_p.\end{aligned}$$

Notice that all entries in $(\mathbf{L}-(m\eta)\widetilde{\mathbf{L}})$ and $(\mathbf{s}-(m\eta)\widetilde{\mathbf{s}})$ are at most $1/2$ in absolute value. Therefore

$$\|(\mathbf{L}-(m\eta)\widetilde{\mathbf{L}})\mathbf{z} - (\mathbf{s}-(m\eta)\widetilde{\mathbf{s}})\|_p^p \leq \left(\frac{1}{2}\right)^p\left(\|\mathbf{z}\|_p^p + \left(\sum|z_i|+1\right)^p\right) < m^p\|\mathbf{z}\|_p^p.$$

Furthermore,

$$\|\widetilde{\mathbf{L}}\mathbf{z}-\widetilde{\mathbf{s}}\|_p \geq \|\mathbf{D}\mathbf{z}\|_p \geq \|\mathbf{z}\|_p$$

because $\mathbf{D}$ is diagonal with all entries greater than 1. This proves that

$$\|(\mathbf{L}-(m\eta)\widetilde{\mathbf{L}})\mathbf{z} - (\mathbf{s}-(m\eta)\widetilde{\mathbf{s}})\|_p \leq m\|\widetilde{\mathbf{L}}\mathbf{z}-\widetilde{\mathbf{s}}\|_p,$$

and therefore

$$\|\mathbf{L}\mathbf{z}-\mathbf{s}\|_p \leq (\eta+1)\|\mathbf{L}\mathbf{z}-\mathbf{s}\|_p \qquad \square$$

We can now prove a variant of Theorem 5.5 where all the numbers are integers.

THEOREM 5.8. *For every $p \geq 1$, $\gamma \in [1, \sqrt[p]{2})$ and $\delta > 0$ there exists a probabilistic algorithm that on input an integer h outputs (in $\mathrm{poly}(h)$ time) integers m, r, a matrix $\mathbf{L} \in \mathbb{Z}^{(m+1)\times m}$, and an integer vector $\mathbf{s} \in \mathbb{Z}^{m+1}$ such that*

(i) *all vectors in* $\mathcal{L}(\mathbf{L})$ *have* ℓ_p *norm bigger than* γr*;*
(ii) *for all sufficiently large* h*, with probability at least* $1-2^{-h}$ *the sphere* $\mathcal{B}(\mathbf{s},r)$ *contains at least* $h^{\delta h}$ *lattice points of the form* $\mathbf{Lz}$ *where* $\mathbf{z}$ *is a* 0-1 *vector with exactly* h *ones.*

Proof. We show that for all $p \geq 1, \delta > 0$ and $\epsilon > 0$ the theorem is satisfied with

$$\gamma = \left(\frac{(1-\epsilon)^{1+1/p}}{(1+\epsilon)^{2+1/p}}\right) \cdot \sqrt[p]{2}.$$

Let c be as in Theorem 5.5. On input h, algorithm A computes $m = h^c$, and the first m odd primes $a_1, a_2, \ldots, a_m$. Let $\widetilde{\mathbf{L}}$, $\widetilde{\mathbf{s}}$, and $\widetilde{r}$ be as defined in Theorem 5.5, and compute the approximations

$$\mathbf{L} = \lfloor (m/\epsilon)\widetilde{\mathbf{L}} \rceil, \qquad \mathbf{s} = \lfloor (m/\epsilon)\widetilde{\mathbf{s}} \rceil, \qquad r = \lceil (1+1/\epsilon) m\widetilde{r} \rceil.$$

Let $\mathbf{z} \in \mathbb{Z}^m$ be a nonzero integer vector. We want to bound $\|\mathbf{Lz}\|_p$. We know from Theorem 5.5 that

$$\|\widetilde{\mathbf{L}}\mathbf{z}\|_p > \sqrt[p]{2\frac{1-\epsilon}{1+\epsilon}}\widetilde{r}. \tag{5.6}$$

Using Lemma 5.6 (with $\eta = 1/\epsilon$) and (5.6) we get

$$\begin{aligned} \|\mathbf{Lz}\|_p &\geq \left(\frac{1}{\epsilon} - 1\right) m \|\widetilde{\mathbf{L}}\mathbf{z}\|_p \\ &> \left(\frac{(1-\epsilon)^{1+1/p}}{\epsilon(1+\epsilon)^{1/p}}\right) m \sqrt[p]{2} \cdot \widetilde{r}. \end{aligned} \tag{5.7}$$

Notice that r satisfies the bounds $r < (1+1/\epsilon)m\widetilde{r} + 1$ and $r > (1+1/\epsilon)$ because $\widetilde{r} > 1$. Thus, we can bound $\widetilde{r}$ as follows:

$$\begin{aligned} \widetilde{r} &> \frac{r-1}{(1+1/\epsilon)m} \\ &= \frac{1-1/r}{(1+1/\epsilon)m} \cdot r \\ &> \frac{1-1/(1+1/\epsilon)}{(1+1/\epsilon)m} \cdot r \\ &= \frac{\epsilon}{(\epsilon+1)^2 m} \cdot r. \end{aligned} \tag{5.8}$$

Combining (5.7) and (5.8) we get

$$\|\mathbf{Lz}\|_p > \left(\frac{(1-\epsilon)^{1+1/p}}{\epsilon(1+\epsilon)^{1/p}}\right) \sqrt[p]{2} \frac{\epsilon}{(\epsilon+1)^2} r = \gamma r.$$

Now consider the sphere $\mathcal{B}(\mathbf{s}, r)$. By Theorem 5.5, for all sufficiently large h, with probability at least $1-2^{-h}$, the ball $\mathcal{B}(\widetilde{\mathbf{s}}, \widetilde{r})$ contains at least $h^{\delta h}$ lattice points of the form $\widetilde{\mathbf{L}}\mathbf{z}$ where $\mathbf{z}$ is a 0-1 vector with exactly h ones. For each such point $\widetilde{\mathbf{L}}\mathbf{z}$, we can use Lemma 5.7 (with $\eta = 1/\epsilon$) to bound the distance of $\mathbf{Lz}$ from $\mathbf{s}$ as follows:

$$\begin{aligned} \|\mathbf{Lz} - \mathbf{s}\|_p &\leq (1+1/\epsilon) m \|\widetilde{\mathbf{L}}\mathbf{z} - \widetilde{\mathbf{s}}\|_p \\ &\leq (1+1/\epsilon) m\widetilde{r} \leq r. \end{aligned}$$

Therefore $\mathbf{Lz}$ belongs to the sphere $\mathcal{B}(\mathbf{s}, r)$. This proves that $\mathcal{B}(\mathbf{s}, r)$ also contains at least $h^{\delta h}$ lattice points of the desired form. ∎

5.3. Projecting lattice points to binary strings. In order to complete the proof of Lemma 4.1 we need the following combinatorial theorem from [27]. (See the proof in the appendix.)

THEOREM 5.9. *Let $\mathcal{Z} \subseteq \{0,1\}^m$ be a set of vectors containing exactly h ones. If $|\mathcal{Z}| \geq h! m^{\frac{4\sqrt{h}k}{\epsilon}}$, and $\mathbf{T} \in \{0,1\}^{k \times m}$ is chosen setting each entry to 1 independently at random with probability $p = \frac{1}{4hk}$, then the probability that all binary vectors $\{0,1\}^k$ are contained in $\mathbf{T}(\mathcal{Z}) = \{\mathbf{Tz} : \mathbf{z} \in \mathcal{Z}\}$ is at least $1 - 6\epsilon$.*

We remark that a similar theorem was already proved in [2], and we could have used that result instead of Theorem 5.9. However, our construction and analysis are much simpler than those in [2] and are probably more efficient.

We can now prove Lemma 4.1. Fix an ℓ_p norm ($p \geq 1$) and a constant $\gamma \in [1, \sqrt[p]{2})$. Let k be a sufficiently large integer. We want to build in $\text{poly}(k)$ time an integer lattice $\mathbf{L}$, an integer vector $\mathbf{s}$, an integer transformation matrix $\mathbf{T}$, and an integer radius r such that

(i) all nonzero vectors in $\mathcal{L}(\mathbf{L})$ have ℓ_p norm greater than γr;

(ii) with probability at least $1 - 1/\text{poly}(k)$, for all $\mathbf{x} \in \{0,1\}^k$ there exists a $\mathbf{z} \in \mathbb{Z}^m$ such that $\mathbf{Tz} = \mathbf{x}$ and $\|\mathbf{Lz} - \mathbf{s}\|_p \leq r$.

Let $\delta = 2$ and run the algorithm from Theorem 5.8 on input $h = k^4$. This algorithm outputs an integer matrix $\mathbf{L} \in \mathbb{Z}^{(m+1) \times m}$ and a vector $\mathbf{s} \in \mathbb{Z}^m$ and $r \in \mathbb{Z}$. Notice that since $\mathbf{s}$ is computed in polynomial time, m must be polynomial in h, i.e., $m < h^c$ for some constant c independent of h. Let $\mathcal{Z}$ be the set of all vectors $\mathbf{z} \in \{0,1\}^m$ with exactly h ones, such that $\mathbf{Lz} \in \mathcal{B}(\mathbf{s}, r)$. We know from Theorem 5.8 that all nonzero vectors in $\mathcal{L}(\mathbf{L})$ have ℓ_p norm greater than γr, and with probability at least $1 - 2^{-h}$ the set $\mathcal{Z}$ contains at least h^{2h} elements.

Now, choose matrix $\mathbf{T} \in \{0,1\}^{k \times m}$ by setting each entry to one independently with probability $1/(4hk)$. Notice that

$$|\mathcal{Z}| \geq h^{2h} > h! m^{h/c} = h! m^{\frac{4\sqrt{h}k}{\epsilon}},$$

where $\epsilon = 4c/k$. So, by Theorem 5.9, the probability that for each $\mathbf{x}$ there exists a vector $\mathbf{z}$ such that $\mathbf{x} = \mathbf{Tz}$ and $\mathbf{Lz} \in \mathcal{B}(\mathbf{s}, r)$ is at least $1 - 1/O(k)$. This concludes the proof of Lemma 4.1.

6. Deterministic reductions. In section 4 we proved that approximating SVP is hard for NP under RUR-reductions. In particular, this proves that approximating SVP is not in RP unless NP = RP. In this section we address the question whether SVP is hard under deterministic reductions.

A quick inspection of the proof of Theorem 4.2 immediately shows that the only place in the reduction where randomness is used is Lemma 4.1. A deterministic polynomial time algorithm satisfying the conditions in Lemma 4.1 would immediately give a proper NP-hardness result (under deterministic many-one reductions) for GAPSVP.

To date, we do not know if such a deterministic polynomial time algorithm exists. However, one can show that such an algorithm exists if one assumes a reasonable number theoretic conjecture, or allows for nonuniform reductions.

6.1. Nonuniform reductions. The reduction presented in the proof of Theorem 4.2 always maps NO instances to NO instances and YES instances to YES instances provided that the probabilistic algorithm in the lemma succeeds. Notice that the construction in the lemma depends only on the dimension k of the GAPCVP$'$ instance we are reducing. Moreover, the success of the algorithm does not depend on the particular instance we are reducing.

Therefore, if we allow for nonuniform reductions in the proof of Theorem 4.2, we can encode the objects $\mathbf{L}, \mathbf{T}, \mathbf{s}, r$ satisfying Lemma 4.1 directly in the reduction as polynomial size nonuniform hints. Notice that the existence of $\mathbf{L}, \mathbf{T}, \mathbf{s}, r$ is guaranteed by the (probabilistic) proof of Lemma 4.1.

This gives the following variant of Theorem 4.2.

THEOREM 6.1. *For any ℓ_p norm ($p \geq 1$) and for any constant $\gamma \in [1, \sqrt[p]{2})$, the promise problem* GAPSVP$_\gamma$ *is hard for* NP *under deterministic nonuniform polynomial reductions. In particular,* GAPSVP$_\gamma$ *is not in* P/poly *unless* NP $\subseteq$ P/poly.

Using standard results on nonuniform complexity [21], this also implies the following corollary.

COROLLARY 6.2. *For any ℓ_p norm ($p \geq 1$) and for any constant $\gamma \in [1, \sqrt[p]{2})$, the promise problem* GAPSVP$_\gamma$ *is not in* P *unless the polynomial hierarchy* [26, 33] *collapses to the second level.*

6.2. NP-hardness under a number theoretic conjecture. In this section we show how the proof of the geometric lemma can be made deterministic using a number theoretic conjecture. This results in a proper NP-hardness result for GAPSVP (i.e. NP-hardness under deterministic many-one reductions) but relies on an unproven assumption on the distribution of square-free smooth numbers. The conjecture is the following.

CONJECTURE 1. *For any $\epsilon > 0$ there exists a d such that for all large enough n, there exists an (odd) integer in $[n, n + n^\epsilon]$ which is square-free and $(\log^d n)$-smooth; i.e., all of its prime factors have exponent 1 and are less than $\log^d n$.*

We remark that although the above conjecture is very plausible, proving it seems to be beyond current mathematical techniques. We now show that if the above conjecture is true, then there exists a deterministic (uniform) polynomial time algorithm satisfying the requirements of Lemma 4.1. For simplicity, we show how to build real matrices $\mathbf{L}, \mathbf{s}, r$ satisfying the condition in the lemma. $\mathbf{L}, \mathbf{s}, r$ can be easily transformed into integer matrices as explained in subsection 5.2 using Lemma 5.6 and Lemma 5.7 to bound the errors incurred in the approximation process.

Let ϵ be a positive real between 0 and 1. Let d be an integer (whose existence is guaranteed by the conjecture) such that for all large enough n there exists a $(\log^d n)$-smooth square-free (odd) integer in the interval $[n, n+n^{\epsilon/2}]$. Let $\mathbf{L}$ and $\mathbf{s}$ be as defined in (5.1) and (5.4) with $m = k^{d+1} + k$, $a_1, \ldots, a_m$ the first m (odd) prime numbers, $\beta = a_m^{\frac{2k}{\epsilon}}$ and $\alpha = \beta^{1-\epsilon}$. Finally, let $\mathbf{T} \in \{0,1\}^{k \times m}$ be the matrix $\mathbf{T} = [\mathbf{0}_{k \times k^{d+1}} | \mathbf{I_k}]$.

From Lemma 5.1 we know that for all nonzero vectors $\mathbf{z} \in \mathbb{Z}^m$,

$$\|L\mathbf{z}\|_p \geq \sqrt[p]{2(1-\epsilon)\ln\beta}.$$

We now show that for all $\mathbf{x} \in \{0,1\}^k$ there exists a $\mathbf{y} \in \mathbb{Z}^{k^{d+1}}$ such that

$$\left\| \mathbf{L} \begin{bmatrix} \mathbf{y} \\ \mathbf{x} \end{bmatrix} - \mathbf{s} \right\|_p < \sqrt[p]{\ln\beta + 2} = r. \tag{6.1}$$

Since the equality

$$\mathbf{T} \begin{bmatrix} \mathbf{y} \\ \mathbf{x} \end{bmatrix} = \mathbf{x}$$

follows directly from the definition to $\mathbf{T}$, (6.1) proves the second condition in Lemma 4.1. By Lemma 5.2 it is sufficient to show that for every integer $g_{\mathbf{x}} = \prod_{i=1}^k a_{k^{d+1}+i}^{x_i}$

(with $x_i \in \{0,1\}$) there exists an integer $g_{\mathbf{y}} = \prod_{i=1}^{k^{d+1}} a_i^{y_i}$ (with $y_i \in \{0,1\}$) such that $g = g_{\mathbf{x}} g_{\mathbf{y}} \in [\beta, \beta + \beta^{\epsilon}]$. Fix some $g_{\mathbf{x}} = \prod_{i=1}^{k} a_{k^{d+1}+i}^{x_i}$. Notice that

$$\frac{\beta}{g_{\mathbf{x}}} > \frac{\beta}{a_m^k} = a_m^{(\frac{2}{\epsilon}-1)k} > 2^k$$

so for all sufficiently large k, there exists a $\log^d(\beta/g_{\mathbf{x}})$-smooth square-free (odd) integer in the interval

$$[\beta/g_{\mathbf{x}}, (\beta/g_{\mathbf{x}}) + (\beta/g_{\mathbf{x}})^{\epsilon/2}].$$

But

$$\log^d(\beta/g_{\mathbf{x}}) \leq \log^d(\beta) = O(k \log k)^d < k^{d+1}.$$

So, this smooth number can be expressed as $g_{\mathbf{y}} = \prod_{i=1}^{k^{d+1}} a_i^{y_i}$ with $y_i \in \{0,1\}$. Therefore,

$$g_{\mathbf{x}} g_{\mathbf{y}} \in [\beta, \beta + g_{\mathbf{x}}(\beta/g_{\mathbf{x}})^{\epsilon/2}].$$

Finally, notice that $g_{\mathbf{x}} \leq a_m^k = \beta^{\epsilon/2}$. So, if we define

$$\mathbf{z} = \begin{bmatrix} \mathbf{y} \\ \mathbf{x} \end{bmatrix}$$

then

$$\prod a_i^{z_i} = g_{\mathbf{x}} g_{\mathbf{y}} \in [\beta, \beta + \beta^{\epsilon}]$$

and by Lemma 5.2 the lattice vector $\mathbf{Lz}$ belongs to the sphere $\mathcal{B}(\mathbf{s}, r)$.

This completes the proof that if Conjecture 1 is true, then $\mathbf{L}, \mathbf{T}, \mathbf{s}, r$ satisfy the conditions of Lemma 4.1. Then, the reduction in the proof of Theorem 4.2 gives the following corollary.

COROLLARY 6.3. *If Conjecture* 1 *holds true, then for any ℓ_p norm and any constant $\gamma < \sqrt[p]{2}$,* GAPSVP$_\gamma$ *is* NP*-hard (under deterministic many-one reductions).*

7. Discussion. We proved that approximating the shortest vector problem in any ℓ_p within factors less than $\sqrt[p]{2}$ is not in polynomial time under any of the following assumptions:

1. NP $\neq$ RP,
2. NP $\not\subseteq$ P/poly,
3. Conjecture 1 is true and NP $\neq$ P.

Although all of these results give theoretical evidence that SVP cannot be approximated in polynomial time, the problem whether solving SVP (even exactly) is NP-hard under deterministic many-one reductions remains open. We notice that the only place where randomness (or nonuniform hints, or the number theoretic conjecture) is used in our reduction is the proof of Lemma 4.1. A deterministic polynomial time solution to Lemma 4.1 would immediately give an NP-hardness result for SVP under deterministic many-one reductions. We leave finding a deterministic algorithm satisfying Lemma 4.1 as an open problem.

Our NP-hardness proof is by reduction from approximate CVP. In particular we reduced instances of CVP of size n to instances of SVP of size $m = n^c$, where $c > 2$

is a constant independent of n. Although this gives a polynomial relation between n and m it should be noted that m can be much bigger than n. Therefore, in order to assert that an instance of SVP is hard to solve in practice, the dimension m must be rather large. Finding a more efficient reduction, where, for example, $m = O(n)$, is left as an open problem. Interestingly, a dimension and approximation preserving reduction is possible in the other direction from SVP to CVP [16].

The geometric lemma used in our reduction is in a certain sense optimal (in the ℓ_2 norm): it can be formally proved that any lattice $\mathbf{L}$ satisfying the lemma must have vectors of length less than $r/\sqrt{2}$ (see [27]). Proving that SVP is NP-hard to approximate within factors larger than $\sqrt{2}$ cannot be done by simply improving the geometric lemma. We leave as an open problem to prove that SVP is NP-hard to approximate within any constant factor.

Appendix. A combinatorial theorem on low-degree hyper-graphs.

In this appendix we prove Theorem 5.9. We want to prove that if $\mathcal{Z} \subset \{0,1\}^m$ is a set of vectors of weight h, and $|\mathcal{Z}| \geq h! m^{\frac{4\sqrt{h}k}{\epsilon}}$, then the probability that $\{0,1\}^k \subseteq \mathbf{T}(\mathcal{Z})$ (where $\mathbf{T} \in \{0,1\}^{k\times m}$ is a linear transformation chosen at random setting each entry to 1 independently with probability $p = \epsilon/(4hk)$) is at least $1 - 6\epsilon$.

The theorem can be reformulated in terms of hyper-graphs as follows. Let $(N, \mathcal{Z})$ be an h-regular hyper-graph, i.e., a hyper-graph all of whose hyper-edges have size h. Let $\mathbf{T} = (T_1, \ldots, T_k)$ be a collection of subsets of N chosen at random including each element of N in T_i independently with probability $p = \epsilon/(4hk)$. For any subset $U \subseteq N$, let

$$\mathbf{T}(U) = (|T_1 \cap U|, |T_2 \cap U|, \ldots, |T_k \cap U|)$$

and define $\mathbf{T}(\mathcal{Z}) = \{\mathbf{T}(U) : U \in \mathcal{Z}\}$. We want to prove that if $|\mathcal{Z}| > h!|N|^{4\sqrt{h}k/\epsilon}$, then $\{0,1\}^k \subseteq \mathbf{T}(\mathcal{Z})$ with probability at least $1 - 6\epsilon$.

The correspondence between the matrix and hyper-graph formulation is immediate: identify the hyper-edges with the corresponding characteristic vectors in $\{0,1\}^{|N|}$ and the collection $\mathbf{T}$ with a matrix whose rows are the characteristic vectors of the sets T_i. Then $\mathbf{T}(U) = \mathbf{Tu}$ where $\mathbf{u}$ is the characteristic vector of set U.

We first prove a weaker result: we show for every vector $\mathbf{x} \in \{0,1\}^k$, $\mathbf{x} \in \mathbf{T}(\mathcal{Z})$ with high probability. Consider the target vector $\mathbf{x}$ as fixed. We want to bound the probability that $\mathbf{T}(U) \neq \mathbf{x}$ for all $U \in \mathcal{Z}$. Since the set $\mathcal{Z}$ is very big, the expected number of $U \in \mathcal{Z}$ such that $\mathbf{T}(U) = \mathbf{x}$ is also very high. Unfortunately, this is not sufficient to conclude that with high probability there exists a $U \in \mathcal{Z}$ such that $\mathbf{T}(U) = \mathbf{x}$, because the events $\mathbf{T}(U) = \mathbf{x}$ (indexed by the hyper-edges $U \in \mathcal{Z}$) might be strongly correlated. Notice that if U and V are disjoint (i.e., $U \cap V = \emptyset$), then the corresponding events are independent. In fact the size of the intersection $|U \cap V|$ is a good measure of the correlation between the events $\mathbf{T}(U) = \mathbf{x}$ and $\mathbf{T}(V) = \mathbf{x}$. Notice that if $|\mathcal{Z}|$ is big, then many hyper-edges in $\mathcal{Z}$ will intersect because there cannot be more than m/h mutually disjoint hyper-edges. However, one can still hope that for most of the pairs $U, V \in \mathcal{Z}$, the intersection $U \cap V$ is very small. This is not necessarily true for any hyper-graph $\mathcal{Z}$, but one can show that if $\mathcal{Z}$ is sufficiently large, then it must contain a large hyper-graph with this small intersection property.

The proof of the theorem is divided in four major steps:

1. We first show that the probability that $\mathbf{x} \notin \mathbf{T}(\mathcal{Z})$ can be bounded by the expectation

$$\operatorname*{Exp}_R[e^{\gamma R} - 1], \tag{A.1}$$

where γ is a small positive real, and $R = |U \cap V|$ is the random variable defined as the size of the intersection of two randomly chosen hyper-edges $U, V \in \mathcal{Z}$.

2. We show that $\mathcal{Z}$ "contains" a hyper-graph such that the intersection of two randomly selected hyper-edges is very small with high probability.

3. Then, we prove the weak version of the theorem applying the bound (A.1) to this hyper-graph contained in $\mathcal{Z}$.

4. Finally, we derive the strong version of our theorem from the weak one.

Each of the above steps is described in the following subsections.

A.1. The exponential bound. We start by computing the probability that $\mathbf{T}(U) = \mathbf{x}$ for some fixed set U. In the next lemma we prove a more general statement concerning the probability that two events $\mathbf{T}(U) = \mathbf{x}$ and $\mathbf{T}(V) = \mathbf{x}$ are simultaneously satisfied and relate it to the size of the intersection $r = |U \cap V|$ of the two sets U, V.

LEMMA A.1. *Let $\mathbf{x} \in \{0,1\}^k$ be any boolean vector, $U, V \subset N$ be two sets of size d and let $\mathbf{T} \in \{0,1\}^{k \times |N|}$ be chosen at random by setting each entry to 1 independently with probability p. Then, the probability (over the choice of $\mathbf{T}$) that both $\mathbf{T}(U)$ and $\mathbf{T}(V)$ equal $\mathbf{x}$ is*

$$\Phi(r) = (1-p)^{(2d-r)k} \left[\frac{pr}{1-p} + \left(\frac{p(d-r)}{1-p} \right)^2 \right]^{\|\mathbf{x}\|_1},$$

where $r = |U \cap V|$.

Proof. Since the rows of matrix $\mathbf{T}$ are chosen independently,

$$\Pr_{\mathbf{T}}\{\mathbf{T}(U) = \mathbf{T}(V) = \mathbf{x}\} = \prod_{i=1}^{k} \Pr_{T_i}\{|T_i \cap U| = |T_i \cap V| = x_i\}.$$

We prove that for all $i = 1, \ldots, k$,

$$\Pr_{T_i}\{|T_i \cap U| = |T_i \cap V| = x_i\} = (1-p)^{(2d-r)} \left[\frac{pr}{1-p} + \left(\frac{p(d-r)}{1-p} \right)^2 \right]^{x_i}.$$

First consider the case $x_i = 0$ and compute the probability (over the choice of T_i) that $|T_i \cap U| = |T_i \cap V| = 0$. This is true iff none of the elements of $U \cup V$ belongs to T_i, so the probability is

$$\Pr_{T_i}\{|T_i \cap U| = |T_i \cap V| = 0\} = (1-p)^{|U \cup V|} = (1-p)^{2d-r}.$$

Now consider the case $x_i = 1$ and compute the probability (over the choice of T_i) that $|T_i \cap U| = |T_i \cap V| = 1$. This is true iff either (1) T_i contains one element of $U \cap V$ and no other element of $U \cup V$, or (2) T_i contains one element of $U \setminus V$, one element of $V \setminus U$, and no other element of $U \cup V$. Event (1) has probability

$$|U \cap V| \cdot p(1-p)^{|U \cup V|-1} = (1-p)^{2d-r} \left(\frac{pr}{1-p} \right)$$

while event (2) has probability

$$|U \setminus V| \cdot |V \setminus U| \cdot p^2 (1-p)^{|U \cup V|-2} = (1-p)^{2d-r} \left(\frac{p(d-r)}{1-p} \right)^2.$$

Adding up the two probabilities, we get

$$\Pr_{T_i}\{|T_i \cap U| = |T_i \cap V| = 1\} = (1-p)^{(2d-r)}\left(\frac{pr}{1-p} + \left(\frac{p(d-r)}{1-p}\right)^2\right). \qquad \square$$

By choosing $U = V$ in the previous lemma one gets the following corollary.

COROLLARY A.2. *Let $\mathbf{x} \in \{0,1\}^k$ be a boolean vector, $U \subseteq N$ a subset of size d, and $\mathbf{T} \in \{0,1\}^{k \times |N|}$ a random matrix chosen by setting each entry to 1 independently with probability p. Then,*

$$\Pr_{\mathbf{T}}\{\mathbf{T}(U) = \mathbf{x}\} = \Phi(d) = (1-p)^{dk}\left(\frac{pd}{1-p}\right)^{\|\mathbf{x}\|_1}.$$

Notice that when $U \cap V = \emptyset$,

$$\Pr\{\mathbf{T}(U) = \mathbf{T}(V) = \mathbf{x}\} = \Phi(0) = \Phi(d)^2 = \Pr\{\mathbf{T}(U) = \mathbf{x}\}\Pr\{\mathbf{T}(V) = \mathbf{x}\},$$

i.e., the events $\mathbf{T}(U) = \mathbf{x}$ and $\mathbf{T}(V) = \mathbf{x}$ are independent. We can now prove the following proposition.

PROPOSITION A.3. *Let $(N, \mathcal{Z})$ be a d-regular hyper-graph and let $\mathbf{T} \in \{0,1\}^{k \times |N|}$ be chosen at random by setting each entry to 1 independently with probability p. Then, for each $\mathbf{x} \in \{0,1\}^k$ the probability (over the choice of $\mathbf{T}$) that $\mathbf{x} \notin \mathbf{T}(\mathcal{Z})$ is at most $\mathrm{Exp}_R[e^{\gamma R}] - 1$, where $\gamma = \frac{kp}{1-p} + \frac{k}{pd^2}$ and $R = |U \cap V|$ is the random variable defined as the size of the intersection of two randomly chosen elements of $\mathcal{Z}$.*

Proof. Fix some vector $\mathbf{x} \in \{0,1\}^k$ and choose $\mathbf{T}$ at random as specified in the proposition. For all $U \in \mathcal{Z}$, let X_U be the indicator random variable

$$X_U = \begin{cases} 1 & \text{if } \mathbf{T}(U) = \mathbf{x}, \\ 0 & \text{otherwise.} \end{cases}$$

Define the random variable $X = \sum_{U \in \mathcal{Z}} X_U$. Notice that $X = 0$ iff $\mathbf{x} \notin \mathbf{T}(\mathcal{Z})$. Moreover, if $X = 0$ then $|X - \mathrm{Exp}[X]| \geq \mathrm{Exp}[X]$. Using Chebyshev's inequality we get the following bound:

$$\begin{aligned} \Pr\{\mathbf{x} \notin \mathbf{T}(\mathcal{Z})\} &= \Pr\{X = 0\} \\ &\leq \Pr\{|X - \mathrm{Exp}[X]| \geq \mathrm{Exp}[X]\} \\ &\leq \frac{\mathrm{Var}[X]}{\mathrm{Exp}[X]^2} = \frac{\mathrm{Exp}[X^2]}{\mathrm{Exp}[X]^2} - 1. \end{aligned}$$

So, let us compute the moments $\mathrm{Exp}[X]$ and $\mathrm{Exp}[X^2]$. For the first moment we have

$$\mathop{\mathrm{Exp}}_{\mathbf{T}}[X] = \sum_{U \in \mathcal{Z}} \Pr_{\mathbf{T}}\{\mathbf{T}(U) = \mathbf{x}\} = |\mathcal{Z}| \cdot \Phi(d),$$

and for the second one

$$\begin{aligned} \mathop{\mathrm{Exp}}_{\mathbf{T}}[X^2] &= \mathop{\mathrm{Exp}}_{\mathbf{T}}\left[\left(\sum_{U \in \mathcal{Z}} X_U\right)^2\right] \\ &= \mathop{\mathrm{Exp}}_{\mathbf{T}}\left[\sum_{U,V \in \mathcal{Z}} X_U \cdot X_V\right] \\ &= \sum_{U,V \in \mathcal{Z}} \Pr_{\mathbf{T}}\{\mathbf{T}(U) = \mathbf{T}(V) = \mathbf{x}\} \\ &= |\mathcal{Z}|^2 \cdot \mathop{\mathrm{Exp}}_{R}[\Phi(R)], \end{aligned}$$

where $R = |U \cap V|$ is the size of two randomly chosen $U, V \in \mathcal{Z}$. Therefore,

$$\begin{aligned}
\Pr_{\mathbf{T}}\{\mathbf{x} \notin \mathbf{T}(\mathcal{Z})\} &= \frac{\operatorname{Exp}_R[\Phi(R)]}{\Phi(d)^2} - 1 \\
&= \operatorname*{Exp}_R\left[(1-p)^{-kR}\left(\frac{(1-p)R}{pd^2} + \left(1 - \frac{R}{d}\right)^2\right)^{\|\mathbf{x}\|_1}\right] - 1 \\
&< \operatorname*{Exp}_R\left[\left(1 + \frac{p}{1-p}\right)^{kR}\left(\frac{R}{pd^2} + 1\right)^k\right] - 1 \\
&< \operatorname*{Exp}_R\left[e^{\frac{pkR}{1-p}} e^{\frac{kR}{pd^2}}\right] - 1 \\
&= \operatorname*{Exp}_R[e^{\gamma R} - 1],
\end{aligned}$$

where $\gamma = \frac{kp}{1-p} + \frac{k}{pd^2}$. ∎

A.2. Well spread hyper-graphs. In the previous section we showed that the probability that $\mathbf{x} \notin \mathbf{T}(\mathcal{Z})$ is at most $\operatorname{Exp}_R[e^{\gamma R}] - 1$. Obviously, the bound is interesting only when $\operatorname{Exp}_R[e^{\gamma R}] < 2$. Notice that this can be true only if

$$\Pr_R\{R = r\} < e^{-\gamma r}$$

for all but a single value of r. Therefore the probability $\Pr_R\{R = r\}$ must decrease exponentially fast in r. This is not necessarily true for any low degree regular hyper-graph $\mathcal{Z}$. In this section we show that if $\mathcal{Z}$ is sufficiently large, then $\mathcal{Z}$ must "contain" a hyper-graph such that

$$\Pr_R\{R = r\} \le 1/r!.$$

More precisely we show that $\mathcal{Z}$ contains a hyper-graph satisfying the following property.

DEFINITION A.4. *Let $(N, \mathcal{Z})$ be a d-regular hyper-graph. $\mathcal{Z}$ is* well spread *if for all $W \subseteq N$ of size at most d, the fraction of hyper-edges containing W is at most*

$$\frac{|\{U \in \mathcal{Z} : W \subseteq U\}|}{|\mathcal{Z}|} \le \frac{1}{d(d-1)\cdots(d-|W|+1)} = \frac{(d-|W|)!}{d!}.$$

Well spread hyper-graphs have the important property that the size of the intersection of two randomly selected hyper-edges is small with very high probability, as shown in the next lemma.

LEMMA A.5. *Let $(N, \mathcal{Z})$ a regular well spread hyper-graph. Choose $U, V \in \mathcal{Z}$ independently and uniformly at random and let $R = |U \cap V|$. For all $r > 0$,*

$$\Pr_R\{R \ge r\} < \frac{1}{r!}.$$

Proof. Let d be the degree of the hyper-graph. We prove that for any fixed set U of size d, the probability that $|U \cap V| \ge r$ when V is chosen at random from $\mathcal{Z}$ is at most $\frac{1}{r!}$. If $|U \cap V| \ge r$ then V contains a subset of U of size r. Therefore, by union bound,

$$\Pr_{V \in \mathcal{Z}}\{|U \cap V| \ge r\} \le \sum_{W \in \binom{U}{r}} \Pr_{V \in \mathcal{Z}}\{W \subseteq V\} = \sum_{W \in \binom{U}{r}} \frac{|\{V \in \mathcal{Z} : W \subseteq V\}|}{|\mathcal{Z}|},$$

where $\binom{U}{r}$ denotes the set of all the size r subsets of U. Since $\mathcal{Z}$ is well spread, the fraction $|\{V \in \mathcal{Z} : W \subseteq V\}|/|\mathcal{Z}|$ is at most $\frac{(d-r)!}{d!}$, which substituted in the previous expression, gives

$$\Pr_{V \in \mathcal{Z}}\{|U \cap V| \geq r\} \leq \binom{d}{r}\frac{(d-r)!}{d!} = \frac{1}{r!}. \qquad \square$$

We now show how to find well spread hyper-graphs "inside" any sufficiently big regular hyper-graph. For any subset $W \subseteq N$, define the induced hyper-graph

$$\mathcal{Z}_W = \{A \subseteq N \setminus W : A \cup W \in \mathcal{Z}\}.$$

In other words, $\mathcal{Z}_W$ is the set of hyper-edges containing W, with the nodes in W removed. Notice the following basic facts:

1. Hyper-graph $\mathcal{Z}$ is well spread if for every set W of size at most d, $|\mathcal{Z}_W| \leq \frac{(d-|W|)!}{d!}|\mathcal{Z}|$.
2. $\mathcal{Z}_W$ is d'-regular with $d' = d - |W|$.
3. If $W = \emptyset$ then $\mathcal{Z}_W = \mathcal{Z}$.
4. $(\mathcal{Z}_W)_V = \mathcal{Z}_{W \cup V}$ if $U \cap V = \emptyset$, and $(\mathcal{Z}_W)_V = \emptyset$ otherwise.
5. If $|W| > d$ then $\mathcal{Z}_W = \emptyset$.

In the following lemma we prove that for any regular hyper-graph $\mathcal{Z}$, there exists a set W such that $\mathcal{Z}_W$ is well spread.

LEMMA A.6. *Let $(N, \mathcal{Z})$ be an h-regular hyper-graph. Then there exists a set $W \subset N$ such that $(N, \mathcal{Z}_W)$ is well spread and $|\mathcal{Z}_W| > |\mathcal{Z}|/h!$.*

Proof. If $(N, \mathcal{Z})$ is well spread, let $W = \emptyset$ and the statement is obviously true. Otherwise, there exists some set W of size at most h such that $|\mathcal{Z}_W| > \frac{(h-|W|)!}{h!} \cdot |\mathcal{Z}|$. Let W be maximal (with respect to the set inclusion ordering relation) among these sets. Obviously, $|\mathcal{Z}_W| > |\mathcal{Z}|/h!$. Notice that $\mathcal{Z}_W$ is d-regular, with $d = h - |W|$. We prove that $(N, \mathcal{Z}_W)$ is well spread. Let V be a subset of N of size at most d. There are three cases:

(i) If $V \cap W \neq \emptyset$ then $|(\mathcal{Z}_W)_V| = 0 \leq \frac{(d-|V|)!}{d!} \cdot |\mathcal{Z}_W|$.
(ii) If $V = \emptyset$, then $|(\mathcal{Z}_W)_V| = |\mathcal{Z}_W| = \frac{d!}{d!} \cdot |\mathcal{Z}_W|$.
(iii) Finally assume $V \neq \emptyset$ and $V \cap W = \emptyset$. By the maximality of W one gets

$$\begin{aligned} |(\mathcal{Z}_W)_V| &= |\mathcal{Z}_{V \cup W}| \\ &\leq \frac{(h-|V \cup W|)!}{h!}|\mathcal{Z}| \\ &= \frac{(d-|V|)!}{d!}\frac{(h-|W|)!}{h!}|\mathcal{Z}| \\ &< \frac{(d-|V|)!}{d!}|\mathcal{Z}_W|. \qquad \square \end{aligned}$$

A.3. Weak probabilistic construction. We now combine the tools developed in the previous sections to prove the following theorem.

THEOREM A.7. *For every sufficiently small constant $\epsilon > 0$, positive integer k and h-regular hyper-graph $(N, \mathcal{Z})$ of size $|\mathcal{Z}| > h!|N|^{\sqrt{h}k/\epsilon}$ the following holds. Define matrix $\mathbf{T} \in \{0,1\}^{k \times |N|}$ at random by setting each entry to 1 independently with probability $p = \frac{\epsilon}{hk}$. Then, for every $\mathbf{x} \in \{0,1\}^k$,*

$$\Pr\{\mathbf{x} \in \mathbf{T}(\mathcal{Z})\} > 1 - 5\epsilon.$$

From Lemma A.6, there exists a subset $W \subset N$ such that $(N, \mathcal{Z}_W)$ is well spread and $|\mathcal{Z}_W| \geq |\mathcal{Z}|/h! > |N|^{\sqrt{h}k/\epsilon}$. Choose $\mathbf{T} \in \{0,1\}^{k \times |N|}$ at random by setting each entry to one independently with probability $p = \frac{\epsilon}{hk}$. Let F be the event that all entries in $\mathbf{T}$ that belongs to the columns corresponding to elements in W are 0. Notice that $\Pr\{\neg F\} \leq |W|kp \leq hkp = \epsilon$. Notice also that

$$\Pr_{\mathbf{T}}\{\mathbf{x} \notin \mathbf{T}(\mathcal{Z}) \mid F\} \leq \Pr_{\mathbf{T}}\{\mathbf{x} \notin \mathbf{T}(\mathcal{Z}_W)\}$$

Let d be the degree of $\mathcal{Z}_W$. Since $|\mathcal{Z}_W| \leq \binom{|N|}{d} < |N|^d$ and $|\mathcal{Z}_W| > |N|^{\sqrt{h}k/\epsilon}$, hyper-graph $\mathcal{Z}_W$ has degree at least $d > \sqrt{h}k/\epsilon$.

Applying Proposition A.3 to d-regular hyper-graph $\mathcal{Z}_W$, the probability (over the choice of $\mathbf{T}$) that $\mathbf{x} \notin \mathbf{T}(\mathcal{Z}_W)$ is at most $\mathrm{Exp}_R[e^{\gamma R}] - 1$, where R is the size of the intersection of two random elements in $\mathcal{Z}_W$ and

$$\begin{aligned}\gamma &= \frac{kp}{1-p} + \frac{k}{pd^2} \\ &= \frac{\epsilon}{h - \epsilon/k} + \frac{hk^2}{\epsilon d^2} \\ &< \frac{\epsilon}{1-\epsilon} + \epsilon.\end{aligned}$$

But $\mathcal{Z}_W$ is well spread, so by lemma A.5, $\Pr_R\{R \geq r\} < 1/r!$ and the expectation $\mathrm{Exp}_R[e^{\gamma R}]$ can be bounded as follows:

$$\begin{aligned}\mathop{\mathrm{Exp}}_R[e^{\gamma R}] &= \sum_{r \geq 0} e^{\gamma r} \Pr_R\{R = r\} \\ &= \sum_{r \geq 0} e^{\gamma r} \left(\Pr_R\{R \geq r\} - \Pr_R\{R \geq r+1\}\right) \\ &= \sum_{r \geq 0} e^{\gamma r} \Pr_R\{R \geq r\} - \sum_{r \geq 1} e^{\gamma(r-1)} \Pr_R\{R \geq r\} \\ &= 1 + (1 - e^{-\gamma}) \sum_{r \geq 1} e^{\gamma r} \Pr_R\{R \geq r\} \\ &< 1 + \gamma \sum_{r \geq 1} \frac{e^{\gamma r}}{r!} \\ &= 1 + \gamma(e^{e^\gamma} - 1).\end{aligned}$$

So, the probability that $\mathbf{x} \notin \mathbf{T}(\mathcal{Z})$ given F is less than $\gamma(e^{e^\gamma} - 1)$ and

$$\begin{aligned}\Pr_{\mathbf{T}}\{\mathbf{x} \notin \mathbf{T}(\mathcal{Z})\} &\leq \Pr\{\neg F\} + \Pr\{\mathbf{x} \notin \mathbf{T}(\mathcal{Z}) \mid F\} \\ &\leq \epsilon + \gamma(e^{e^\gamma} - 1).\end{aligned}$$

Using the bound $\gamma < \epsilon(1 + 1/(1-\epsilon))$, we get that for all sufficiently small ϵ

$$\Pr_{\mathbf{T}}\{\mathbf{x} \notin \mathbf{T}(\mathcal{Z})\} \leq 5\epsilon.$$

A.4. Strong probabilistic construction. We proved that for every boolean vector $\mathbf{x}$, if $\mathbf{T}$ is chosen as described in Theorem A.7, then with high probability there

exists a $U \in \mathcal{Z}$ such that $\mathbf{T}(U) = \mathbf{x}$. It follows by an averaging argument that with high probability the size of $\mathbf{T}(\mathcal{Z}) \cap \{0,1\}^k$ (the set of all boolean vectors that can be represented as $\mathbf{T}(U)$ for some $U \in \mathcal{Z}$) is almost equal to the size of the whole $\{0,1\}^k$. We now show how to project $\mathbf{T}(\mathcal{Z}) \cap \{0,1\}^k$ onto the set of all binary strings of some shorter length.

For any vector $\mathbf{x} \in \{0,1\}^n$ and subset $G \subseteq \{1,\ldots,n\}$, define the projection $\mathbf{x}|_G \in \{0,1\}^{|G|}$ as the vector obtained taking the coordinates of $\mathbf{x}$ with index in G. The projection operation is extended to set of vectors in the obvious way: $\mathcal{W}|_G = \{\mathbf{x}|G : \mathbf{x} \in \mathcal{W}\}$. The next lemma shows that the probability that a random projection $\mathcal{W}|_G$ covers the whole set $\{0,1\}^G$ of binary strings is at least equal to the density of $|\mathcal{W}|$ in $\{0,1\}^n$.

LEMMA A.8. *Let $\mathcal{W}$ be a subset of $\{0,1\}^n$. If G is chosen uniformly at random among all subsets of $\{1,\ldots,n\}$, then*

$$\Pr_G\left\{\mathcal{W}|_G = \{0,1\}^G\right\} \geq \frac{|\mathcal{W}|}{2^n}.$$

Proof. By induction on n. The base case $n = 0$ is trivially true. (Notice that $\{0,1\}^G = \{0,1\}^n = \{\varepsilon\}$ and $\mathcal{W}|_G = \mathcal{W} = \{0,1\}^G$ iff $|\mathcal{W}| = 1$.) So, assume the statement holds for all $\mathcal{W} \subseteq \{0,1\}^n$ and let us prove it for $\mathcal{W} \subseteq \{0,1\}^{n+1}$. Choose G at random and let $G' = G \setminus \{n+1\}$. Notice that G' is a random subset of $\{1,\ldots,n\}$. Define the following sets:

$$\mathcal{W}_0 = \left\{\mathbf{x} : \begin{bmatrix}\mathbf{x}\\0\end{bmatrix} \in \mathcal{W}\right\}, \qquad \mathcal{W}_1 = \left\{\mathbf{x} : \begin{bmatrix}\mathbf{x}\\1\end{bmatrix} \in \mathcal{W}\right\}.$$

Notice that $|\mathcal{W}| = |\mathcal{W}_0| + |\mathcal{W}_1| = |\mathcal{W}_0 \cup \mathcal{W}_1| + |\mathcal{W}_0 \cap \mathcal{W}_1|$. Moreover, if

(i) either $(n+1) \in G$ and $(\mathcal{W}_0 \cap \mathcal{W}_1)|_{G'} = \{0,1\}^{G'}$
(ii) or $(n+1) \notin G$ and $(\mathcal{W}_0 \cup \mathcal{W}_1)|_{G'} = \{0,1\}^{G'}$,

then $\mathcal{W}|_G = \{0,1\}^G$. Therefore, using the inductive hypothesis, we get

$$\begin{aligned}
\Pr\{\mathcal{W}|_G = \{0,1\}^G\} &\geq \Pr\{(n+1) \in G\} \Pr\{(\mathcal{W}_0 \cup \mathcal{W}_1)|_{G'} = 2^{G'}\} \\
&\quad + \Pr\{(n+1) \notin G\} \Pr\{(\mathcal{W}_0 \cap \mathcal{W}_1)|_{G'} = 2^{G'}\} \\
&\geq \frac{1}{2}\left(\frac{|\mathcal{W}_0 \cup \mathcal{W}_1|}{2^n}\right) + \frac{1}{2}\left(\frac{|\mathcal{W}_0 \cap \mathcal{W}_1|}{2^n}\right) \\
&= \frac{|\mathcal{W}_0 \cup \mathcal{W}_1| + |\mathcal{W}_0 \cap \mathcal{W}_1|}{2^{n+1}} \\
&= \frac{|\mathcal{W}|}{2^{n+1}}. \qquad \square
\end{aligned}$$

Now, we can easily derive Theorem 5.9 from Lemma A.8 and Theorem A.7. Instead of choosing the matrix $\mathbf{T} \in \{0,1\}^{k \times m}$ as specified in Theorem 5.9, we do the following mental experiment. First choose a bigger matrix $\mathbf{T}' \in \{0,1\}^{4k \times n}$ at random by setting each entry to 1 independently with probability $p = \frac{4\epsilon}{dk}$. Then choose a random subset $G \subseteq 1,\ldots,4k$ of its rows. If G has size at least k, set $\mathbf{T}$ to the submatrix of $\mathbf{T}'$ with rows corresponding to the first k elements of G. (If G has less than k elements, the experiment fails.)

Let $\mathcal{W} = \mathbf{T}'(\mathcal{Z}) \cap \{0,1\}^{4k}$. Notice that the probability distribution of matrix $\mathbf{T}$ (conditioned on the event $|G| \geq k$) is the same as in Theorem 5.9. Moreover, if $|G| \geq k$ and $\{0,1\}^G \subseteq \mathcal{W}|_G$ then $\{0,1\}^k \subseteq \mathbf{T}(\mathcal{Z})$. So, we can bound the probability

that matrix $\mathbf{T}$ does not satisfy Theorem 5.9 as the sum of the probabilities that $|G| < k$ and $\{0,1\}^k \not\subseteq \mathbf{T}(\mathcal{Z})$.

Notice that $\mathrm{Exp}[|G|] = 2k$ and $\mathrm{Var}[|G|] = k$. So, by Chebychev's inequality

$$\begin{aligned}\Pr\{|G| < k\} &< \Pr\{||G| - \mathrm{Exp}[|G|]| < k\} \\ &< \frac{\mathrm{Var}[|G|]}{k^2} \\ &= \frac{1}{k} < \epsilon\end{aligned}$$

for all sufficiently large k. Now, let us bound the probability that $\{0,1\}^G \subseteq \mathcal{W}|_G$ when G and $\mathbf{T}'$ are chosen at random. Using Lemma A.8 and the independence of G and $\mathbf{T}'$, one gets

$$\begin{aligned}\Pr_{G,\mathbf{T}'}\{\{0,1\}^G \subseteq \mathcal{W}|_G\} &= \mathop{\mathrm{Exp}}_{\mathbf{T}'}[\Pr_G\{\{0,1\}^G \subseteq \mathcal{W}|_G\}] \\ &\geq \mathop{\mathrm{Exp}}_{\mathbf{T}'}\left[\frac{|\mathcal{W}|}{2^{4k}}\right] \\ &= \mathop{\mathrm{Exp}}_{\mathbf{T}'}\left[\Pr_{\mathbf{x}\in\{0,1\}^{4k}}[\mathbf{x} \in \mathcal{W}]\right] \\ &= \mathop{\mathrm{Exp}}_{\mathbf{x}\in\{0,1\}^{4k}}\left[\Pr_{\mathbf{T}'}[\mathbf{x} \in \mathbf{T}'(\mathcal{Z})]\right] \\ &\geq \min_{\mathbf{x}\in\{0,1\}^{4k}} \Pr_{\mathbf{T}'}\{\mathbf{x} \in \mathbf{T}'(\mathcal{Z})\} \\ &\geq 1 - 5\epsilon.\end{aligned}$$

Therefore the probability that $\{0,1\}^k \not\subseteq \mathbf{T}(\mathcal{Z})$ is at most 5ϵ. By union bound, with probability at least $1 - 6\epsilon$ matrix $\mathbf{T}$ satisfies Theorem 5.9.

Acknowledgments. Many people contributed to this work with useful discussions and comments. I wish to thank all of them. I will not attempt to list them all here, but some of them deserve a special mention. Special thanks to Shafi Goldwasser who convinced me that SVP was NP-hard to approximate and encouraged me to work on this problem, Oded Goldreich who patiently listened to my proofs when I had not even started writing this paper and actively contributed to the proof of Theorem 5.9, and Muli Safra who suggested an important simplification in Lemma 5.2. Thanks also to Miklós Ajtai, whose work has largely inspired the results presented in this paper.

REFERENCES

[1] L. M. Adleman, *Factoring and Lattice Reduction*, manuscript, 1995.

[2] M. Ajtai, *The shortest vector problem in L_2 is NP-hard for randomized reductions (extended abstract)*, in Proceedings of the 30th Annual ACM Symposium on Theory of Computing, Dallas, TX, 1998, pp. 10–19.

[3] S. Arora, L. Babai, J. Stern, and E. Z. Sweedyk, *The hardness of approximate optima in lattices, codes, and systems of linear equations*, J. Comput. System Sci., 54 (1997), pp. 317–331. Preliminary version in FOCS'93.

[4] L. Babai, *On Lovasz' lattice reduction and the nearest lattice point problem*, Combinatorica, 6 (1986), pp. 1–13.

[5] W. Banaszczyk, *New bounds in some transference theorems in the geometry of numbers*, Math. Ann., 296 (1993), pp. 625–635.

[6] M. Bellare, S. Goldwasser, and D. Micciancio, *"Pseudo-random" generators within cryptographic applications: the DSS case*, in Advances in Cryptology—CRYPTO '97, B. S.

Kaliski Jr., ed., Lecture Notes in Comput. Sci. 1294, Springer-Verlag, New York, 1997, pp. 277–291.

[7] D. Coppersmith, *Small solutions to polynomial equations, and low-exponent RSA vulnerabilities*, J. Cryptology, 10 (1997), pp. 233–260.

[8] M. J. Coster, A. Joux, B. A. LaMacchia, A. M. Odlyzko, C.-P. Schnorr, and J. Stern, *Improved low-density subset sum algorithms*, Comput. Complexity, 2 (1992), pp. 111–128.

[9] I. Dinur, *Approximating SVP_∞ to within almost-polynomial factors is NP-hard*, in Algorithms and Complexity, 4th Italian Conference, CIAC 2000, Proceedings, G. Bongiovanni, G. Gambosi, and R. Petreschi, eds., Lecture Notes in Comput. Sci. 1767, Rome, Italy, 2000, Springer-Verlag, New York, pp. 263–276.

[10] I. Dinur, G. Kindler, and S. Safra, *Approximating CVP to within almost-polynomial factors is NP-hard*, in 39th Annual IEEE Symposium on Foundations of Computer Science, Palo Alto, CA, 1998.

[11] I. Dumer, D. Micciancio, and M. Sudan, *Hardness of approximating the minimum distance of a linear code*, in 40th Annual IEEE Symposium on Foundations of Computer Science, New York, 1999, pp. 475–484.

[12] A. M. Frieze, *On the Lagarias-Odlyzko algorithm for the subset sum problem*, SIAM J. Comput., 15 (1986), pp. 536–539.

[13] A. M. Frieze, J. Håstad, R. Kannan, J. C. Lagarias, and A. Shamir, *Reconstructing truncated integer variables satisfying linear congruences*, SIAM J. on Comput., 17 (1988), pp. 262–280.

[14] O. Goldreich, *private communication*, 1999.

[15] O. Goldreich and S. Goldwasser, *On the limits of nonapproximability of lattice problems*, J. Comput. System Sci., 60 (2000), pp. 540–563. Preliminary version in STOC'98.

[16] O. Goldreich, D. Micciancio, S. Safra, and J.-P. Seifert, *Approximating shortest lattice vectors is not harder than approximating closest lattice vectors*, Inform. Process. Lett., 71 (1999), pp. 55–61.

[17] J. Håstad, *Solving simultaneous modular equations of low degree*, SIAM J. Comput., 17 (1988), pp. 336–341. Preliminary version in Crypto85.

[18] D. S. Johnson, *A catalog of complexity classes*, in Handbook of Theoretical Computer Science, vol. A (Algorithms and Complexity), Elsevier Science, Amsterdam, 1990, chap. 2, pp. 67–161.

[19] R. Kannan, *Algorithmic geometry of numbers*, in Annual Reviews of Computer Science, Vol. 2, Annual Review Inc., Palo Alto, CA, 1987, pp. 231–267.

[20] R. Kannan, *Minkowski's convex body theorem and integer programming*, Math. Oper. Res., 12 (1987), pp. 415–440.

[21] R. M. Karp and R. J. Lipton, *Some connections between nonuniform and uniform complexity classes*, in Proceedings of the Twelfth Annual ACM Symposium on Theory of Computing, Los Angeles, CA, 1980, pp. 28–30. Appeared in journal form as R. M. Karp and R. J. Lipton, *Turing machines that take advice*, Enseign. Math., 28 (1982) pp. 191–209.

[22] J. C. Lagarias, H. W. Lenstra, Jr., and C.-P. Schnorr, *Korkine-Zolotarev bases and successive minima of a lattice and its reciprocal lattice*, Combinatorica, 10 (1990), pp. 333–348.

[23] J. C. Lagarias and A. M. Odlyzko, *Solving low-density subset sum problems*, J. ACM, 32 (1985), pp. 229–246.

[24] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann., 261 (1982), pp. 513–534.

[25] H. W. Lenstra, *Integer programming with a fixed number of variables*, Math. Oper. Res., 8 (1983), pp. 538–548.

[26] A. R. Meyer and L. J. Stockmeyer, *The equivalence problem for regular expression with squaring requires exponential space*, in Proceedings of the 13th IEEE Symposium on Switching and Automata Theory, 1972, pp. 25–29.

[27] D. Micciancio, *On the Hardness of the Shortest Vector Problem*, Ph.D. thesis, Massachusetts Institute of Technology, Cambridge, MA, 1998.

[28] D. Micciancio, *The hardness of the closest vector problem with preprocessing*, IEEE Trans. Inform. Theory, 47 (2001).

[29] C.-P. Schnorr, *A hierarchy of polynomial time lattice basis reduction algorithms*, Theoret. Comput. Sci., 53 (1987), pp. 201–224.

[30] C.-P. Schnorr, *Factoring integers and computing discrete logarithms via Diophantine approximation*, in Advances in Computational Complexity 13, DIMACS Ser. Discrete Math. Theoret. Comput. Sci., AMS, Providence, RI, 1993, pp. 171–182. Preliminary version in Eurocrypt'91, Springer-Verlag, LNCS 547.

[31] A. Schönhage, *Factorization of univariate integer polynomials by Diophantine approximation and an improved basis reduction algorithm*, in Automata, Languages and Programming, 11th Colloquium, J. Paredaens, ed., Lecture Notes in Comput. Sci. 172, Antwerp, Belgium, 1984, Springer-Verlag, New York, pp. 436–447.

[32] A. Shamir, *A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem*, IEEE Trans. Inform. Theory, 30 (1984), pp. 699–704. Preliminary version in FOCS'82.

[33] L. J. Stockmeyer, *The polynomial-time hierarchy*, Theoret. Comput. Sci., 3 (1977), pp. 1–22.

[34] P. van Emde Boas, *Another NP-Complete Problem and the Complexity of Computing Short Vectors in a Lattice*, Tech. Report 81-04, Mathematische Instituut, Universiry of Amsterdam, 1981; also available online from http://turing.wins.uva.nl/∼peter/.