Electronic Colloquium on Computational Complexity - Reports Series 1997 - available via:
ECCC
TR97-059
FTP: ftp.eccc.uni-trier.de:/pub/eccc/
WWW: http://www.eccc.uni-trier.de/eccc/
Email: ftpmail@ftp.eccc.uni-trier.de with subject 'help eccc'

Approximating the SVP to within a factor $\left(1 + \frac{1}{\dim^{\epsilon}}\right)$ is NP-hard under randomized reductions

(extended abstract)

Jin-Yi Cai * Ajay Nerurkar †

Abstract

Recently Ajtai showed that to approximate the shortest lattice vector in the l_2-norm within a factor $(1+2^{-\dim^k})$, for a sufficiently large constant k, is NP-hard under randomized reductions. We improve this result to show that to approximate a shortest lattice vector within a factor $(1 + \dim^{-\epsilon})$, for any $\epsilon > 0$, is NP-hard under randomized reductions. Our proof also works for arbitrary l_p-norms, $1 \leq p < \infty$.

*Department of Computer Science, State University of New York at Buffalo, Buffalo, NY 14260. Research supported in part by NSF grant CCR-9634665 and an Alfred P. Sloan Fellowship. Email: cai@cs.buffalo.edu

†Department of Computer Science, State University of New York at Buffalo, Buffalo, NY 14260. Research supported in part by NSF grant CCR-9634665. Email: apn@cs.buffalo.edu

1 Introduction

This paper presents the latest advance in the determination of the complexity of the famous Shortest Lattice Vector Problem.

A lattice L is a discrete additive subgroup of $\mathbf{R}^n$. It is the set of all integral linear combinations of an underlying generating set of linearly independent vectors from $\mathbf{R}^n$. The study of lattice problems has a long history dating back to Lagrange, Gauss, Dirichlet and Hermite, among others [Lag73, Gau01, Dir50, Her50]. Many problems concerning lattices are both fascinating and challenging. One of the most studied computational problems is the Shortest Lattice Vector Problem (SVP): Given an n-dimensional lattice, find the shortest non-zero lattice vector in the lattice.

Just over one hundred years ago, Minkowski proved his theorems on shortest lattice vectors and successive minima, unifying much previous work, and established the subject *Geometry of Numbers* as a bridge between geometry and Diophantine approximation and the theory of quadratic forms [Gru93, GLS88, GL87]. Our interests in lattice problems mainly lie in its computational complexity aspects, and its application to provably secure public key cryptography, as recently demonstrated by Ajtai [Ajt96], and Ajtai and Dwork [AD96].

People working in the design of secure cryptography have realized for some time that the security of a cryptographic protocol depends on the intractability of a certain computational problem *on the average*. At the moment, we lack any mathematical proof of hardness, either in an asymptotic sense or for specific values of parameters for any problem in NP. Thus NP-hardness is taken to be a weak form of a proof of intractability. But, NP-hardness only refers to the worst case complexity of the problem. It would be most desirable to prove that a problem believed to be intractable is as hard on the average as in the worst case. This is exactly what was accomplished by Ajtai [Ajt96], who established an equivalence, in some technical sense, between the average case complexity of SVP and its worst case complexity. More precisely, Ajtai [Ajt96] established a probabilistic polynomial time reduction from the problem of approximating, within a certain polynomial factor n^c, a short lattice basis in the worst case, to the problem of finding a short lattice vector for a uniformly chosen lattice in a certain random class of lattices. The Ajtai connection from worst case to average case complexity has been improved by Cai and Nerurkar [CN97]. The Ajtai connection is also the basis of the Ajtai-Dwork public-key cryptosystem, which Ajtai and Dwork [AD96] proved is secure based on only a worst case hardness assumption. The assumption is that a certain version of the SVP is not solvable in P or in BPP, namely to find the shortest lattice vector in a lattice with a n^c-unique shortest vector. (This means that every lattice vector not parallel to the unique shortest vector is longer by at least a factor of n^c.) The Ajtai-Dwork cryptosystem is the only known public-key cryptosystem provably secure, assuming only the worst case intractability of its underlying problem. Another public-key system based on lattice problems was proposed by Goldreich, Goldwasser and Halevi [GGH96].

Thus the Ajtai-Dwork system continues the tradition of cryptographic protocols based on sufficiently "famous" problems, such as factoring, for which the most able minds have labored long and hard, and have found no polynomial time algorithms. Compared to other number theoretic problems such as factoring or discrete log, the advantage for SVP at least in provable terms, is twofold. First, there is the worst case to average case connection mentioned above.

Secondly, we know that some versions of this problem are NP-hard. In contrast, neither is known to hold for factoring, and for discrete log the usual random self-reducibility is only valid for a fixed modulus p.

Regarding NP-hardness, Lagarias [Lag82] showed that SVP is NP-hard for the l_∞-norm. Van Emde Boas [vEB81] showed that finding the nearest lattice vector is NP-hard under all l_p-norms, $p \geq 1$. Arora et al [ABSS93] showed that finding an approximate solution to within any constant factor for the nearest vector problem for any l_p-norm, is NP-hard. There are no known polynomial-time algorithms to find approximate solutions to these problems within any polynomial factor, even probabilistically. The celebrated Lovász basis reduction algorithm [LLL82] finds a short vector within a factor of $2^{n/2}$ in polynomial time. One major open problem in this field has been whether SVP is NP-hard for the natural l_2-norm. This was conjectured e.g., by Lovász [Lov86].

In a tour de force, Ajtai settled this conjecture very recently [Ajt97]: SVP is NP-hard for l_2-norm under randomized reductions. Moreover Ajtai showed that to approximate the shortest vector of an n-dimensional lattice within a factor of $\left(1 + \frac{1}{2^{n^k}}\right)$ (for a sufficiently large constant k) is also NP-hard. The main result of this paper is to improve this approximation factor to $\left(1 + \frac{1}{n^\epsilon}\right)$ for any $\epsilon > 0$.

The approximation factor for which NP-hardness can be shown is most important in terms of cryptographic applications. A theorem of Lagarias, Lenstra and Schnorr [LLS90] showed that the problem of approximating the length of the shortest lattice vector within a factor of Cn, for an appropriate constant C, is not NP-hard, unless NP = coNP. Goldreich and Goldwasser showed that approximating the shortest lattice vector within a factor of $O(\sqrt{n/\log n})$ is not NP-hard unless the polynomial time hierarchy collapses [GG97]. Cai showed that finding the shortest lattice vector in a lattice with a $n^{1/4}$-unique shortest vector is not NP-hard unless the polynomial time hierarchy collapses [Cai]. The Ajtai-Dwork system is based on the intractability of finding the shortest lattice vector in a lattice with a n^c-unique shortest vector. Currently the exponent c is still rather large in their proof. Thus at this moment we cannot say that the Ajtai-Dwork system, as it stands, is NP-hard to break. To narrow the gap between those cases where NP-hardness can be proved and those where it is probably not NP-hard is most interesting and potentially very important for secure cryptography. The current gap is $(1 + \frac{1}{n^\epsilon})$ and $O(\sqrt{n/\log n})$.

2 Preliminaries

We denote by $\mathbf{R}$ the field of real numbers and by $\mathbf{Z}$ the ring of integers. The Euclidean (l_2-) norm is denoted by $\|\cdot\|$. For n linearly independent vectors $v_1, v_2, \ldots, v_n \in \mathbf{R}^m$, $m \geq n$, $P(v_1, \ldots, v_n) = \{\sum_{i=1}^n \beta_i v_i \mid \forall i \ 0 \leq \beta_i \leq 1\}$ denotes the parallelepiped defined by $v_1, \ldots, v_n$. The (n-dimensional) *volume* vol $(P(v_1, \ldots, v_n))$ of the parallelepiped $P(v_1, \ldots, v_n)$ is $|\det (B^T B)|^{1/2}$, where the $m \times n$ matrix B consists of v_i's as column vectors, $B = (v_1, \ldots, v_n)$. The n-dimensional lattice $L = L(v_1, \ldots, v_n)$, with basis $v_1, \ldots, v_n$, is the set of all integral linear combinations of the v_i. The *determinant* of the lattice L, $\det L$, is the volume of $P(v_1, \ldots, v_n)$. It is invariant under a change of basis. The length of the shortest non-zero vector of L is denoted by $\lambda_1(L)$.

The shortest vector problem (SVP) Given $b_1, \ldots, b_n$, find a shortest non-zero vector (in some fixed norm) in the lattice $L(b_1, \ldots, b_n)$.

We will reduce an NP-complete problem to the problem of finding an approximate shortest vector in a lattice. Following Ajtai [Ajt97], the NP-complete problem we use is the *restricted subset sum problem* which is a variation of the subset sum problem. This problem can be shown to be NP-hard under polynomial time many-one reductions. (A polynomial time Turing reduction was given in [Ajt97].)

The restricted subset sum problem Given integers $a_1, \ldots, a_l, A$, such that $\max\{\log_2(|A|+1), \max_{i=1}^{l} \log_2(|a_i|+1)\} \leq l^3$, find a 0-1 solution to the system $\sum_{i=1}^{l} a_i x_i = A, \sum_{i=1}^{l} x_i = [\frac{l}{2}]$.

3 A lattice with wonderful properties

We first define the values of some parameters. Let $\epsilon > 0$ be any constant. Let $\kappa = 2$, $\mu = 10$. Choose $\alpha > \frac{4}{\epsilon}$ and sufficiently larger than μ. Let $\sum_{i=1}^{l} a_i x_i = A$ be an instance of the restricted subset sum problem. Let $n = \lceil l^{1/\delta_1} \rceil$, where δ_1 is the constant whose existence is guaranteed by Theorem 1 (stated on page 8, due to Ajtai) for $\alpha_1 = 2\alpha, \alpha_2 = 1$. We can assume that l, and consequently n as well, are sufficiently large with respect to α. Let J be an integer such that $n = \left\lfloor \frac{\log J}{\alpha \log\log J} \right\rfloor$. Clearly, $e^n < J < e^{n \log^2 n}$. Let $p_1 < \ldots < p_m$ be all the primes less than $(\log J)^\alpha$. By the Prime Number Theorem, $n^\alpha \leq m \leq n^{\alpha+1}$. Let Γ denote the set of integers formed by taking all the products of n distinct elements of the set $\{p_1, \ldots, p_m\}$. Note that any element of Γ is at most $(\log J)^{\alpha n} \leq J$. Pick an integer b uniformly from Γ. Let ω be an integer such that $\omega^\mu \leq b \leq (2\omega)^\mu$. Clearly, $2^n \leq b \leq J$. Thus, both b and ω are exponential in n. Let $B = \omega^{\mu+1}$.

Using the values of the parameters, $\kappa, \mu, m, B, \omega$, and b defined above, we now review the lattice construction of Ajtai [Ajt97]. Note that the only randomness in this construction is the random choice of $b \in_U \Gamma$.

Let L_1 be the lattice spanned by the rows ν_i of the following matrix,

$$\begin{pmatrix} \sqrt{\log p_1} & \cdots & 0 & 0 & B \log p_1 \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & \cdots & \sqrt{\log p_m} & 0 & B \log p_m \\ 0 & \cdots & 0 & 0 & B \log b \\ 0 & \cdots & 0 & \omega^{-\kappa} & B \log\left(1 + \frac{\omega}{b}\right) \end{pmatrix}.$$

The following lemma proves certain properties of this lattice. Specifically, it proves that if a lattice vector is short enough, its coefficients in terms of the ν_i have a special form. The hypothesis on the length of the vector used here is stronger than the one in Lemma 3.2 in [Ajt97]. This enables us to prove NP-hardness for a larger approximation factor.

Lemma 1 *Let c be any constant strictly smaller than $2 \log 2$. Let $w = (w_1, \ldots, w_{m+2}) \in L_1$, $w \neq 0$, $w = \sum_{i=1}^{m+2} \delta_i \nu_i$, $\delta_{m+1} \geq 0$. If $\|w\|^2 \leq \log b + c$, then*

1. $|\delta_{m+2}| \leq \omega^{\kappa+1}$;

2. $\delta_{m+1} = 1$;

3. *For* $i = 1, \ldots, m$, $\delta_i \in \{0, -1\}$;

4. $\prod_{i=1}^{m} p_i^{-\delta_i} \equiv b \pmod{\omega}$;

5. *If* $g = \prod_{i=1}^{m} p_i^{-\gamma_i} = b + t\omega, \quad t \in \mathbf{Z}, \quad \gamma_i \in \{0, -1\}$ *for* $i = 1, \ldots, m$, *and* $|b - g| \leq \omega^{\kappa - 1/2}$, *then* $w' = \sum_{i=1}^{m+2} \gamma_i \nu_i$, *where* $\gamma_{m+1} = 1, \gamma_{m+2} = t$, *satisfies* $\|w'\|^2 \leq \log b + \frac{3}{\omega^2}$;

6. *For all* $v \in L$, $v \neq 0$, *we have* $\|v\|^2 \geq \log b$.

Useful Facts Define $g_0 = \prod_{\delta_i > 0,\ 1 \leq i \leq m} p_i^{\delta_i}$ and $g_1 = \prod_{\delta_i < 0,\ 1 \leq i \leq m} p_i^{-\delta_i}$. Then,

$$\begin{aligned}
\log g_0 &= \sum_{\delta_i > 0,\ 1 \leq i \leq m} \delta_i \log p_i \\
\log g_1 &= \sum_{\delta_i < 0,\ 1 \leq i \leq m} -\delta_i \log p_i \\
\log g_0 - \log g_1 &= \sum_{i=1}^{m} \delta_i \log p_i \qquad (*) \\
\log g_0 + \log g_1 &= \sum_{i=1}^{m} |\delta_i| \log p_i \leq \sum_{i=1}^{m} \delta_i^2 \log p_i = \sum_{i=1}^{m} w_i^2 \leq \|w\|^2 \qquad (**)
\end{aligned}$$

Note that w can't be a scalar multiple of ν_{m+2} because $w \neq 0$ and

$$\|\nu_{m+2}\| > \omega^{\mu+1} \log\left(1 + \frac{\omega}{b}\right) \geq \omega^{\mu+1} \frac{\omega}{2b} \geq \omega^{\mu+1} \frac{1}{2} \frac{\omega}{(2\omega)^{\mu}} \geq \sqrt{\log b + c} \geq \|w\|.$$

Proof (of Lemma 1)

1. $|\delta_{m+2}| \leq \omega^{\kappa+1}$:

$$|\delta_{m+2}| \omega^{-\kappa} = |w_{m+1}| \leq \|w\| \leq (\log b + c)^{\frac{1}{2}}.$$

Therefore, $|\delta_{m+2}| \leq \omega^{\kappa} (\log b + c)^{\frac{1}{2}} \leq \omega^{\kappa+1}$.

2. $\delta_{m+1} = 1$:

First assume $\delta_{m+1} = 0$. Since w is not parallel to ν_{m+2}, $\exists i \in \{1, \ldots, m\}$, $\delta_i \neq 0$. This means at least one of g_0 and g_1 is not equal to 1 and so $g_0 \neq g_1$, since they are products of distinct primes. Then, one of g_0 and g_1 satisfies $\log g_i \leq \frac{1}{2}(\log b + c)$, and so $g_i \leq \gamma\sqrt{b}$, where γ is a constant. This implies,

$$|\log g_0 - \log g_1| \geq |\log(\gamma\sqrt{b} + 1) - \log(\gamma\sqrt{b})| \geq \frac{1}{\gamma\sqrt{b} + 1} \geq \frac{1}{2\gamma\sqrt{b}} \geq \frac{1}{\gamma' \omega^{\mu/2}},$$

where γ' denotes the constant $\frac{1}{2^{\mu/2+1}\gamma}$. We also have,

$$B \left| \sum_{i=1}^{m} \delta_i \log p_i + \delta_{m+2} \log(1 + \frac{\omega}{b}) \right| = |w_{m+2}| \leq \|w\| \leq (\log b + c)^{1/2}.$$

From this we get,

$$\begin{aligned}
|\delta_{m+2}| &\geq \frac{1}{\log\left(1+\frac{\omega}{b}\right)}\left(\left|\sum_{i=1}^{m}\delta_i\log p_i\right| - B^{-1}(\log b+c)^{1/2}\right)\\
&\geq \frac{b}{\omega}\left(|\log g_0-\log g_1| - \frac{1}{\omega^{\mu+1}}(\log b+c)^{1/2}\right) \qquad \text{by } (*)\\
&\geq \frac{b}{\omega}\left(\frac{1}{\gamma'\omega^{\mu/2}} - \frac{1}{\omega^{\mu+1}}(\log b+c)^{1/2}\right)\\
&\geq \omega^{\mu-1}\left(\frac{1}{\gamma'\omega^{\mu/2}} - \frac{1}{\omega^{\mu+1/2}}\right)\\
&> \omega^{\mu/2-2}\\
&= \omega^{\kappa+1},
\end{aligned}$$

for sufficiently large ω. This contradicts part 1. (In the sequel, inequalities are always meant to be asymptotic statements.)

Now assume $\delta_{m+1}\geq 2$. By part 1, $\left|\delta_{m+2}\log\left(1+\frac{\omega}{b}\right)\right| \leq \omega^{\kappa+1}\frac{\omega}{b} \leq \frac{1}{\omega^2}$. We have,

$$(\log b+c)^{1/2} \geq \|w\| \geq |w_{m+2}| = B\left|\sum_{i=1}^{m}\delta_i\log p_i + \delta_{m+1}\log b + \delta_{m+2}\log\left(1+\frac{\omega}{b}\right)\right|.$$

Therefore,

$$\begin{aligned}
\left|\sum_{i=1}^{m}\delta_i\log p_i\right| &\geq |\delta_{m+1}\log b| - \left|\delta_{m+2}\log\left(1+\frac{\omega}{b}\right)\right| - B^{-1}(\log b+c)^{1/2}\\
&\geq 2\log b - \frac{1}{\omega^2} - \frac{1}{\omega^{\mu+1}}(\log b+c)^{1/2} \;\geq\; \frac{3}{2}\log b.
\end{aligned}$$

But, using $(*)$ and $(**)$,

$$\frac{3}{2}\log b > \log b + c \geq \|w\|^2 \geq \log g_0+\log g_1 \geq |\log g_0-\log g_1| = \left|\sum_{i=1}^{m}\delta_i\log p_i\right|.$$

3. For $i=1,\ldots,m$, $\delta_i\in\{0,-1\}$:

We have $(\log b+c)^{1/2}\geq\|w\|\geq|w_{m+2}| = B\left|\sum_{i=1}^{m}\delta_i\log p_i+\log b+\delta_{m+2}\log\left(1+\frac{\omega}{b}\right)\right|$, and by part 1, $\left|\delta_{m+2}\log\left(1+\frac{\omega}{b}\right)\right|\leq\frac{1}{\omega^2}$. Therefore,

$$\begin{aligned}
|\log g_0-\log g_1+\log b| &= \left|\sum_{i=1}^{m}\delta_i\log p_i+\log b\right|\\
&\leq B^{-1}(\log b+c)^{1/2}+\frac{1}{\omega^2}\\
&\leq \frac{1}{\omega^{\mu+1}}(\log b+c)^{1/2}+\frac{1}{\omega^2}\\
&\leq \frac{1}{\omega}.
\end{aligned}$$

If there is an $i \in \{1, \ldots, m\}$ such that $\delta_i > 0$, then $\log g_0 \geq \log 2$. Thus, $\log g_1 \geq \log 2 + \log b - \frac{1}{\omega}$, and

$$\log b + c \geq \|w\|^2 \geq \log g_0 + \log g_1 \geq \log b + 2\log 2 - \frac{1}{\omega},$$

which is a contradiction, since c is a constant strictly smaller than $2\log 2$. Therefore, $\forall i \in \{1, \ldots, m\}$ $\delta_i \leq 0$, which implies $\log g_0 = 0$. This means, $|\log b - \log g_1| \leq \frac{1}{\omega}$ and so, $\log g_1 \geq \log b - \frac{1}{\omega}$.

Now we will show that $\forall i \in \{1, \ldots, m\}$, $\delta_i \in \{0, -1\}$. Suppose there is a $j \in \{1, \ldots, m\}$ such that $|\delta_j| \geq 2$. Then, $\delta_j^2 \geq 2|\delta_j|$ and $\delta_i^2 \geq |\delta_i|$ for all other i. Therefore, $\|w\|^2 \geq \sum_{i=1}^m \delta_i^2 \log p_i \geq |\delta_j| \log p_j + \sum_{i=1}^m |\delta_i| \log p_i \geq 2\log 2 + \log g_1 \geq \log b + 2\log 2 - \frac{1}{\omega} > \log b + c$, a contradiction.

The proofs of *4, 5, 6* are given in the appendix. They are essentially the same as the ones in Lemma 3.2 in [Ajt97]. □

4 Normalizing the lattice

We now normalize the lattice so that every non-zero lattice vector has length at least 1. As described earlier, b is chosen randomly from the set Γ. In [Ajt97] it has been proven that, with high probability, b satisfies the following,

(i) $b \geq J^{1-\frac{1}{\alpha-2}}$

(ii) In the interval $(b - \omega^{3/2}, b + \omega^{3/2})$, there are at least $2^{n \log n}$ elements of Γ that are congruent to $b \pmod{\omega}$.

If b satisfies (i) and (ii) above, then the following lemma holds (for all sufficiently large n).

Lemma 2 *Let* $L_2 = \frac{1}{\sqrt{\log b}} L_1$, $\bar{\nu}_i = \frac{1}{\sqrt{\log b}} \nu_i$, $\bar{\rho} = \frac{3}{\omega^2 \log b}$. *Then,*

1. $v \in L_2, v \neq 0 \implies \|v\| \geq 1$;
2. *If* Z *is the set of all* $w \in L_2$, $w = \sum_{i=1}^{m+2} \gamma_i \bar{\nu}_i$, *with* $\gamma_i \in \{0, -1\}$ *for* $i \in \{1, \ldots, m\}$ *and* $\sum_{i=1}^m |\gamma_i| = n$ *and* $\|w\|^2 < 1 + \bar{\rho}$, *then* $|Z| \geq 2^{n \log n}$;
3. *If* $u_1, u_2 \in Z, u_1 \neq u_2$ *and* $u_j = \sum_{i=1}^{m+2} \gamma_i^{(j)} \bar{\nu}_i$, *then* $\exists i \in \{1, \ldots, m\}$ *such that* $\gamma_i^{(1)} \neq \gamma_i^{(2)}$;
4. *For all* $w \in L, w \neq 0$, *if* $\|w\|^2 \leq 1 + \frac{2}{m^{3\epsilon/4}}$, $w = \sum_{i=1}^{m+2} \gamma_i \bar{\nu}_i$, $\gamma_{m+1} \geq 0$, *then* $\gamma_1, \ldots, \gamma_m \in \{0, -1\}$ *and* $\gamma_{m+1} = 1$;
5. *size*$(\bar{\rho}) \leq n^2, 0 < \bar{\rho} < 2^{-\sqrt{n}}$;
6. $|\det(w_1, \ldots, w_{m+2})| \geq \left(\frac{c_0}{\sqrt{n}}\right)^n$, *where* c_0 *is a universal constant.*

Proof We prove only parts *4*, *5*, and *6* here. The proofs of the other parts are given in the appendix. They are similar to the ones in Lemma 3.1 in [Ajt97].

4. Let $\nu = \sqrt{\log b}\, w \in L_1$. Then,

$$\|\nu\|^2 = (\log b)\,\|w\|^2 \leq (\log b)\left(1 + \frac{2}{m^{3\epsilon/4}}\right) = \log b + \frac{2\log b}{m^{3\epsilon/4}}.$$

Now, $\log b \leq \log J < n\log^2 n$ and $m^{3\epsilon/4} \geq n^{3\alpha\epsilon/4} > n^3$. Therefore, $\|\nu\|^2 < \log b + c$. The conclusion follows from Lemma 1.

5. $\bar{\rho} = \frac{3}{\omega^2 \log b}$, and $\log(\omega^2 \log b) = 2\log\omega + \log\log b$. We have, $b < J < e^{n\log^2 n}$ and $\omega \leq b^{1/\mu} < e^{n\log^2 n/\mu}$. This implies, $\log\omega < \frac{n\log^2 n}{\mu}$. Therefore, $\mathrm{size}(\bar{\rho}) \leq n^2$, say.

By (i), $b \geq J^{1-1/(\alpha-2)} \geq e^{n(1-1/(\alpha-2))}$. Therefore, $\omega^2 \geq \frac{b^{2/\mu}}{4} \geq \frac{e^{\frac{2n}{\mu}\left(1-\frac{1}{\alpha-2}\right)}}{4} \geq 3\frac{2^{\sqrt{n}}}{\log b}$, say. Thus, $\bar{\rho} = \frac{3}{\omega^2 \log b} \leq 2^{-\sqrt{n}}$.

6. This follows by Minkowski's First Theorem, since $\lambda_1(L_2) \geq 1$. □

Note that L_2 is a real lattice. For computational purposes, we need to construct a rational approximation to L_2. In probabilistic polynomial time, we can produce a lattice that is a good approximation to L_2. Formally,

> $\forall c > 0\ \exists c' > 0$ and a probabilistic polynomial-time Turing machine $\mathcal{C}$ that, given an input n in binary, returns in time $(\log n)^{c'}$, an integer m, a rational $\bar{\rho} > 0$ and linearly independent vectors $\bar{v}_1, \ldots, \bar{v}_{m+2} \in \mathbf{Q}^{m+2}$, such that $\exists \bar{\nu}_1, \ldots, \bar{\nu}_{m+2} \in \mathbf{R}^{m+2}, \|\bar{v}_i - \bar{\nu}_i\| \leq 2^{-n^c}$ for $i = 1, \ldots, m+2$, and with a probability $\geq \frac{1}{2}$, $L_2 = L(\bar{\nu}_1, \ldots, \bar{\nu}_{m+2})$ satisfies parts *1 – 6* of Lemma 2.

Lemma 3 *Let $v_i = (1+\bar{\rho})\bar{v}_i$. Let $L = L(v_1, \ldots, v_{m+2})$ and $\rho = 8\bar{\rho}$. Then, for all sufficiently large n,*

1. *$v \in L$, $v \neq 0$ implies $\|v\| \geq 1$;*
2. *If Y is the set of all $v \in L$, $v = \sum_{i=1}^{m+2} \gamma_i v_i$ with $\sum_{i=1}^{m} |\gamma_i| = n$, $\gamma_i \in \{0, -1\}$ for $i \in \{1, \ldots, m\}$, and $\|v\|^2 < 1 + \rho$, then $|Y| \geq 2^{n\log n}$;*
3. *If $u_1, u_2 \in Y$, $u_1 \neq u_2$ and $u_j = \sum_{i=1}^{m+2} \gamma_i^{(j)} v_i$, $j = 1, 2$, then $\exists i \in \{1, \ldots, m\}$ such that $\gamma_i^{(1)} \neq \gamma_i^{(2)}$;*
4. *For all $v \in L, v \neq 0$, if $\|v\|^2 \leq 1 + \frac{2}{m^{3\epsilon/4}}$, $v = \sum_{i=1}^{m+2} \gamma_i v_i$ with $\gamma_{m+1} \geq 0$, then $\gamma_1, \ldots, \gamma_m \in \{0, -1\}$ and $\gamma_{m+1} = 1$.*

Proof Parts *1*, *2* and *3* easily follow from Lemma 2 and the proofs for them can be found in the appendix. We only prove *4* here.

Let T be the linear transformation $T\bar{\nu}_i = \bar{v}_i$, for $i = 1, \ldots, m+2$. Applying Lemma 5 from the appendix with $\bar{a}_i = \bar{\nu}_i$ and $\bar{b}_i = \bar{v}_i$, $i = 1, \ldots, m+2$, we get that $1-2^{-n^{c_1}} \leq \|T\| \leq 1+2^{-n^{c_1}}$ and $1-2^{-n^{c_1}} \leq \left\|T^{-1}\right\| \leq 1+2^{-n^{c_1}}$ for some constant c_1 that can be made as large as we want by making the $\bar{v}_i$ approximate the $\bar{\nu}_i$ better.

4. $v = (1+\bar{\rho})Tw$ for some $w \in L_2$, $w \neq 0$, and so

$$\|w\|^2 \leq (1+\bar{\rho})^{-2} \left\|T^{-1}\right\|^2 \|v\|^2 \leq (1+2^{-\sqrt{n}})^{-2}(1+2^{-n^{c_1}})^2 \|v\|^2 \leq \|v\|^2 \leq 1 + \frac{2}{m^{3\epsilon/4}}.$$

Therefore, by Lemma 2, $\gamma_1, \ldots, \gamma_m \in \{0, -1\}$ and $\gamma_{m+1} = 1$. □

5 The reduction

First, we state a combinatorial theorem of Ajtai [Ajt97].

Theorem 1 (Ajtai) $\forall \alpha_1 > 2, \alpha_2 > 0$, $\exists \delta_1, \delta_2, \delta_3, 0 < \delta_i < 1$, $i = 1,2,3$, *such that, for all sufficiently large* n, *the following holds. Assume that* $\langle S, X \rangle$ *is an* n*-uniform hypergraph,* $n^2 \leq |S| \leq n^{\alpha_1}, |X| \geq 2^{\alpha_2 n \log n}, k = \lfloor n^{\delta_1} \rfloor$ *and* $C = C_1, \ldots C_k$ *is a random sequence of pairwise disjoint subsets each with exactly* $|S|n^{-1-\delta_2}$ *elements, uniformly chosen from all such sequences. Then, with a probability* $\geq 1 - n^{-\delta_3}$, *for each 0,1-valued function* f *defined on* $\{1, \ldots, k\}$, $\exists T \in X$, *such that,* $\forall j \in \{1, \ldots, k\}$, $f(j) = |C_j \cap T|$.

Using the n defined earlier, apply Theorem 1 with $\alpha_1 = 2\alpha, \alpha_2 = 1, S = \{1, \ldots m\}, k = \lfloor n^{\delta_1} \rfloor \geq l$, and

$$X = \{T \subseteq \{1, \ldots, m\} \mid \exists v \in Y,\ v = \sum_{i=1}^{m+2} \gamma_i v_i,\ T = \{i \in \{1, \ldots, m\} \mid \gamma_i = -1\}\}.$$

We know that $|Y| \geq 2^{n \log n}$ and any two distinct $v_1, v_2 \in Y$ produce different T's. Thus $|X| \geq 2^{\alpha_2 n \log n}$ (since $\alpha_2 = 1$), as required by the hypothesis of Theorem 1. In what follows, we focus only on $C_1, \ldots, C_l$ (and disregard $C_{l+1}, \ldots, C_k$, if $k > l$). With high probability, a random choice of the C_i satisfies the following :

> For each 0,1-valued function f defined on $\{1, \ldots l\}$, $\exists T \in X$ such that, $\forall j \in \{1, \ldots, l\}$, $f(j) = |C_j \cap T|$.

Let $C = C_1, \ldots C_l$ be such a good choice, and $\sum_{i=1}^{l} a_i x_i = A$ be a given instance of the restricted subset sum problem. Let $g_{C,v}(i) = -\sum_{j \in C_i} \gamma_j$, where $v = \sum_{i=1}^{m+2} \gamma_i v_i$. Define a $(l+2) \times (m+1)$ matrix D as follows,

1. $d_{1,j} = a_i l$ for all $j \in C_i$, $d_{1,m+1} = Al$ and $d_{1,j} = 0$ otherwise,
2. $d_{2,j} = l$ for all $j \in \bigcup_{i=1}^{l} C_j$, $d_{2,m+1} = [\frac{l}{2}]l$ and $d_{2,j} = 0$ otherwise,
3. For all $i \in \{1, \ldots, l\}$, $d_{i+2,j} = 1$ if $j \in C_i$ and $d_{i+2,j} = 0$ otherwise.

If $C_1, \ldots, C_l$ are consecutive intervals of $\{1, \ldots, m\}$, then D is the following matrix,

$$\begin{pmatrix} a_1 l & \cdots & a_1 l & \cdots & a_i l & \cdots & a_i l & \cdots & a_l l & \cdots & a_l l & \cdots & 0 & \cdots & Al \\ l & \cdots & l & \cdots & l & \cdots & l & \cdots & l & \cdots & l & \cdots & 0 & \cdots & [\frac{l}{2}]l \\ 1 & \cdots & 1 & \cdots & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & & \vdots & & \vdots & & \vdots & & \vdots & & \vdots & & \vdots & & \vdots \\ 0 & \cdots & 0 & \cdots & 1 & \cdots & 1 & \cdots & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & & \vdots & & \vdots & & \vdots & & \vdots & & \vdots & & \vdots & & \vdots \\ 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 & \cdots & 1 & \cdots & 1 & \cdots & 0 & \cdots & 0 \end{pmatrix}.$$

For $x \in L$, $x = \sum_{i=1}^{m+2} \gamma_i v_i$, let $\Lambda(x) = \langle \gamma_1\sqrt{\tau}, \ldots, \gamma_{m+1}\sqrt{\tau} \rangle$ where $\tau = 2/m^\epsilon$. Let $L^{(D)} \subseteq \mathbf{R}^{m+l+4}$ be the lattice generated by the vectors $(v_i, \Lambda(v_i)D^T)$. It is of dimension $m+2$. Clearly $L^{(D)} = \{(v, \Lambda(v)D^T) \mid v \in L\}$. Let $L^{(D)+} = \{(v, \Lambda(v)D^T) \mid v \in L,\ v = \sum_{i=1}^{m+2} \gamma_i v_i,\ \gamma_{m+1} \geq 0\}$.

Main Theorem

(i) With high probability, a random choice of $C = C_1, \ldots, C_l$ is good, in the sense of Theorem 1.

(ii) For such a good choice of C, let D be the matrix as defined above. Then, if the restricted subset sum problem $\sum_{i=1}^{l} a_i x_i = A$ has a solution, and $\bar{w} = (w, \Lambda(w)D^T) \in L^{(D)+}$ is a $\left(1 + \frac{1}{m^\epsilon}\right)$-approximation to the shortest non-zero vector of $L^{(D)}$, i.e. $\lambda_1(L^{(D)})^2 \leq \|\bar{w}\|^2 \leq \left(1 + \frac{1}{m^\epsilon}\right) \lambda_1(L^{(D)})^2$, then $y_i = g_{C,w}(i)$ is a solution to the restricted subset sum problem.

Remark It can also be shown that the SVP under any l_p-norm, $1 \leq p < \infty$, is NP-hard to approximate to within $\left(1 + \frac{1}{\dim^\epsilon}\right)$ under randomized reductions, by using $(\log p_i)^{1/p}$ in the construction of L_1.

We first state a lemma. The proof can be found in the appendix.

Lemma 4 *Let $y_1, \ldots, y_l$ be l integers such that $\sum_{i=1}^{l} y_i = [\frac{l}{2}]$. Then, $\sum_{i=1}^{l} y_i^2$ is minimized when all y_i are either 0 or 1, and this minimum value is $[\frac{l}{2}]$. If $\exists i\ y_i \notin \{0, 1\}$, then $\sum_{i=1}^{l} y_i^2 \geq [\frac{l}{2}] + 2$.*

Proof (of Main Theorem) Part (i) is really a restatement of Theorem 1.

(ii) Suppose $\sum_{i=1}^{l} a_i x_i = A$ has a solution. Let f be the function $f(i) = s_i$ where $\sum_{i=1}^{l} a_i s_i = A$. Then $\exists T \in X$, or equivalently, $\exists v = v_T \in Y$, $v = \sum_{j=1}^{m+2} \beta_j v_j$, such that $\forall i \in \{1, \ldots, l\}$,

$$g_{C,v}(i) = -\sum_{j \in C_i} \beta_j = |C_i \cap T| = f(i) = s_i.$$

That is, $\exists v \in Y$, such that $g_{C,v}(i) = s_i$ is a solution to the given instance of the restricted subset sum problem.

Let $\bar{v} = (v, \Lambda(v)D^T)$. Since $v \in Y$, $0 < \|v\| \leq 1 + \rho$. So, $\bar{v}$ is a non-zero vector, which implies $\lambda_1(L^{(D)}) \leq \|\bar{v}\|$. Since v gives rise to a solution to the restricted subset sum instance, $\lambda_1(L^{(D)})^2 \leq \|\bar{v}\|^2 = \|v\|^2 + \left\|\Lambda(v)D^T\right\|^2 \leq (1 + \rho) + \tau[\frac{l}{2}]$. Since $\tau = \frac{2}{m^\epsilon}$ and $l \leq n^{\delta_1} \leq$

$m^{\delta_1/\alpha} \leq m^{\delta_1\epsilon/4} \leq m^{\epsilon/4}$, $\|\bar{v}\|^2 \leq 1 + \rho + \frac{1}{m^{3\epsilon/4}}$. By assumption, $\bar{w} = (w, \Lambda(w)D^T)$ is a $\left(1 + \frac{1}{m^\epsilon}\right)$-approximation to the shortest non-zero vector of $L^{(D)}$. Therefore,

$$\begin{aligned} \|w\|^2 &\leq \|\bar{w}\|^2 \\ &\leq \left(1 + \frac{1}{m^\epsilon}\right) \lambda_1(L^{(D)})^2 \\ &\leq \left(1 + \frac{1}{m^\epsilon}\right) \|\bar{v}\|^2 \\ &\leq 1 + \frac{2}{m^{3\epsilon/4}}. \end{aligned}$$

Let $w = \sum_{i=1}^{m+2} \gamma_i v_i$. Then, by part *4* of Lemma 3, and because $\bar{w} \in L^{(D)+}$, $\gamma_{m+1} = 1$. Let $u = (u_1, \ldots, u_{l+2}) = \Lambda(w)D^T$. Let $y_i = g_{C,w}(i)$. It is easy to see that since $\gamma_{m+1} = 1$, $u_1 = \sqrt{\tau} l(A - \sum_{i=1}^{l} a_i y_i)$, $u_2 = \sqrt{\tau} l([\frac{l}{2}] - \sum_{i=1}^{l} y_i)$, and for $1 \leq j \leq l$, $u_{j+2} = -\sqrt{\tau} y_j$. We show that the y_i form a solution to the restricted subset sum problem. That is, we show that

(i) $\sum_{i=1}^{l} a_i y_i = A$, and

(ii) $\sum_{i=1}^{l} y_i = [\frac{l}{2}]$, and

(iii) $\forall i \; y_i \in \{0, 1\}$.

If (i) fails, then $u_1^2 \geq \tau l^2$. Since $\|\bar{w}\| \geq \lambda_1(L^{(D)})$, $\bar{w} \neq 0$, which implies $w \neq 0$, and so $\|w\| \geq 1$. Thus, $\|\bar{w}\|^2 \geq \|w\|^2 + u_1^2 \geq 1 + \tau l^2$. This is a contradiction because,

$$\begin{aligned} \|\bar{w}\|^2 \leq \left(1 + \frac{1}{m^\epsilon}\right) \|\bar{v}\|^2 &\leq \left(1 + \frac{1}{m^\epsilon}\right) (1 + \rho + \tau[\frac{l}{2}]) \\ &< \left(1 + \frac{\tau}{2}\right) (1 + \tau l) \\ &< 1 + \tau l^2 \\ &\leq \|\bar{w}\|^2. \end{aligned}$$

Similarly, if (ii) fails, then $u_2^2 \geq \tau l^2$, and so $\|\bar{w}\|^2 \geq 1 + \tau l^2$.

Now assume (i) and (ii) hold but (iii) fails. Therefore,

$$\|\bar{w}\|^2 \geq 1 + \sum_{i=3}^{l+2} u_i^2 = 1 + \tau \sum_{i=1}^{l} y_i^2 \geq 1 + \tau \left(\left[\frac{l}{2} \right] + 2 \right),$$

where the last inequality uses Lemma 4. Thus,

$$\|\bar{w}\|^2 - \|\bar{v}\|^2 \geq 2\tau - \rho \geq \tau = \frac{2}{m^\epsilon} > \frac{\|\bar{v}\|^2}{m^\epsilon}.$$

This implies $\|\bar{w}\|^2 > \left(1 + \frac{1}{m^\epsilon}\right) \|\bar{v}\|^2 \geq \left(1 + \frac{1}{m^\epsilon}\right) \lambda_1(L^{(D)})^2$, a contradiction. □

References

[ABSS93] S. Arora, L. Babai, J. Stern, and Z. Sweedyk. The hardness of approximate optima in lattices, codes, and systems of linear equations. In *Proc. 34th IEEE Symposium on Foundations of Computer Science (FOCS)*, 724-733, 1993.

[AD96] M. Ajtai and C. Dwork. A public-key cryptosystem with worst-case/average-case equivalence. 1996. Available as TR96-065 from ECCC, *Electronic Colloquium on Computational Complexity*, at `http://www.uni-trier.de/eccc/`.

[Ajt96] M. Ajtai. Generating hard instances of lattice problems. In *Proc. 28th Annual ACM Symposium on the Theory of Computing*, 99–108, 1996. Full version available as TR96-007 from ECCC, *Electronic Colloquium on Computational Complexity*, at `http://www.uni-trier.de/eccc/`.

[Ajt97] M. Ajtai. The shortest vector problem in L_2 is NP-hard for randomized reductions. 1997. Available as TR97-047 from ECCC, *Electronic Colloquium on Computational Complexity*, at `http://www.uni-trier.de/eccc/`.

[Cai] J-Y Cai. A relation of primal-dual lattices and the complexity of shortest lattice vector problem. *Theoretical Computer Science*. To appear.

[CN97] J-Y Cai and A. Nerurkar. An improved worst-case to average-case connection for lattice problems. In *Proc. 38th IEEE Symposium on Foundations of Computer Science (FOCS)*, 468–477, 1997.

[Dir50] P. G. L. Dirichlet. Über die Reduktion der positiven quadratischen Formen mit drei unbestimmten ganzen Zahlen. *Journal für die Reine und Angewandte Mathematik*, 40:209–227, 1850.

[Gau01] C. F. Gauss. *Disquisitiones Arithmeticae*. Fleischer, Leipzig, 1801. English transl. by A. A. Clarke. Yale University Press, 1966.

[GG97] O. Goldreich and S. Goldwasser. On the limits of non-approximability of lattice problems. 1997. Available as TR97-031 from ECCC, *Electronic Colloquium on Computational Complexity*, at `http://www.uni-trier.de/eccc/`.

[GGH96] O. Goldreich, S. Goldwasser, and S. Halevi. Public-key cryptosystems from lattice reduction problems. 1996. Available as TR96-056 from ECCC, *Electronic Colloquium on Computational Complexity*, at `http://www.uni-trier.de/eccc/`.

[GL87] P. M. Gruber and C. G. Lekkerkerker. *Geometry of Numbers*. North-Holland, 1987.

[GLS88] M. Grötschel, L. Lovász, and A. Schrijver. *Geometric Algorithms and Combinatorial Optimization*. Springer Verlag, 1988.

[Gru93] P. M. Gruber. *Handbook of Convex Geometry*. Elsevier Science Publishers B.V., 1993.

[Her50] C. Hermite. Extraits de lettres de M. Ch. Hermite à M. Jacobi sur différents objets de la théorie des nombres. *Journal für die Reine und Angewandte Mathematik*, 40:261–278, 279–290, 291–307, 308–315, 1850.

[Lag73] J. L. Lagrange. Recherches d'arithmétique. *Nouv. Mém. Acad. Roy. Sc. Belles Lettres Berlin*, pages 265–312, 1773. [*Oeuvres*, Vol. 3 (Gauthier-Villars, Paris, 1869) pp. 693–758].

[Lag82] J. C. Lagarias. The computational complexity of simultaneous diophantine approximation problems. In *Proc. 23rd IEEE Symposium on Foundations of Computer Science (FOCS)*, 32-39, 1982.

[LLL82] A. K. Lenstra, H. W. Lenstra, and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261:515–534, 1982.

[LLS90] J. Lagarias, H. W. Lenstra, and C. Schnorr. Korkin-Zolotarev bases and successive minima of a lattice and its reciprocal lattice. *Combinatorica*, 10(4):333–348, 1990.

[Lov86] L. Lovász. *An Algorithmic Theory of Numbers, Graphs and Convexity.* SIAM, Philadelphia, 1986.

[vEB81] P. van Emde Boas. Another NP-complete partition problem and the complexity of computing short vectors in lattices. Technical Report 81-04, Mathematics Department, University of Amsterdam, 1981.

6 Appendix

Proof of Lemma 1 (continued).

4. $\prod_{i=1}^{m} p_i^{-\delta_i} \equiv b \pmod{\omega}$:

In fact, $\prod_{i=1}^{m} p_i^{-\delta_i} = b + \delta_{m+2}\omega$. Let $t = \delta_{m+2}$. It suffices to prove the two claims below.

Claim 1 *$b + t\omega$ is the closest integer to $b\left(1 + \frac{\omega}{b}\right)^t$.*

Proof

$$b\left(1+\frac{\omega}{b}\right)^t = b + t\omega + b\binom{t}{2}\frac{\omega^2}{b^2} + \cdots = b + t\omega + R$$

where

$$|R| \le \frac{t^2\omega^2}{b} \le \frac{\omega^{2\kappa+4}}{\omega^{\mu}} \le \frac{1}{\omega^2}$$

This proves the claim.

Claim 2 *$g = \prod_{i=1}^{m} p_i^{-\delta_i}$ is the closest integer to $b\left(1 + \frac{\omega}{b}\right)^t$.*

Proof

$$\begin{aligned}\left|\log\left(b\left(1+\frac{\omega}{b}\right)^t\right)-\log g\right| &= \left|\log b + t\log\left(1+\frac{\omega}{b}\right)-\log g\right| \\ &= B^{-1}|w_{m+2}| \\ &\leq B^{-1}(\log b + c)^{1/2} \\ &< \omega^{-\mu-1/2}.\end{aligned}$$

We have, $\log g \leq \|w\|^2 \leq \log b + c$, and so $g \leq e^c b$. So we get,

$$\left|\log\left(g+\frac{1}{2}\right)-\log g\right| \geq \frac{1}{2}\frac{1}{g+\frac{1}{2}} \geq \frac{1}{4e^c b} = \Omega\left(\frac{1}{\omega^\mu}\right)$$

Similarly, $\left|\log\left(g-\frac{1}{2}\right)-\log g\right| = \Omega\left(\frac{1}{\omega^\mu}\right)$. This proves the claim.

5. If $g = \prod_{i=1}^m p_i^{-\gamma_i} = b + t\omega,\ \ t \in \mathbf{Z},\ \ \gamma_i \in \{0,-1\}$ for $i = 1,\ldots,m$, and $|b-g| \leq \omega^{\kappa-1/2}$, then $w' = \sum_{i=1}^{m+2}\gamma_i\nu_i$, where $\gamma_{m+1}=1, \gamma_{m+2}=t$, satisfies $\|w'\|^2 \leq \log b + \frac{3}{\omega^2}$:

$$\left\|w'\right\|^2 = \sum_{i=1}^m \gamma_i^2 \log p_i + t^2\omega^{-2\kappa} + B^2[\sum_{i=1}^m \gamma_i \log p_i + \log b + t\log\left(1+\frac{\omega}{b}\right)]^2.$$

We have

$$\sum_{i=1}^m \gamma_i^2 \log p_i = \sum_{i=1}^m |\gamma_i| \log p_i = \log g = \log(b+t\omega) = \log b + \log\left(1+\frac{t\omega}{b}\right),$$

and

$$\begin{aligned}\sum_{i=1}^m \gamma_i \log p_i + \log b + t\log\left(1+\frac{\omega}{b}\right) &= -\log g + \log b + t\log\left(1+\frac{t\omega}{b}\right) \\ &= -\log(b+t\omega) + \log b + t\log\left(1+\frac{\omega}{b}\right) \\ &= -\log\left(1+\frac{t\omega}{b}\right) + t\log\left(1+\frac{\omega}{b}\right) \\ &= \left(-\frac{t\omega}{b}+\frac{t^2\omega^2}{2b^2}-\cdots\right)+\left(\frac{t\omega}{b}-\frac{1}{2}\frac{t\omega^2}{b^2}\cdots\right) \\ &< \frac{t^2\omega^2}{b^2}.\end{aligned}$$

Therefore,

$$\left\|w'\right\|^2 \leq \log b + \log\left(1+\frac{t\omega}{b}\right) + t^2\omega^{-2\kappa} + \left(\frac{t^2\omega^2}{b^2}\right)^2 B^2.$$

Since $|g-b| \leq \omega^{\kappa-1/2}$, $|t| \leq \omega^{\kappa-3/2}$. Substituting this above, we get the required result.

6. For all $v \in L$, $v \neq 0$, we have $\|v\|^2 \geq \log b$:

Let $v = \sum_{i=1}^{m+2} \delta_i \nu_i \neq 0$ and assume $\|v\|^2 < \log b$. Then $\delta_{m+1} \in \{-1, 1\}$. Wlog, let $\delta_{m+1} = 1$. Then, for $i = 1, \ldots, m$, $\delta_i \in \{0, -1\}$. Let $t = \delta_{m+2}$, and $g = \prod_{i=1}^{m} p_1^{-\delta_i}$. If $g \geq b$, then $\|v\|^2 \geq \sum_{i=1}^{m} |\delta_i| \log p_i = \log g \geq \log b$. So, $g < b$. Now, $t^2 \omega^{-2\kappa} \leq \|v\|^2 < \log b$. Therefore, $|t| < \omega^{\kappa} \sqrt{\log b}$. By part *4* above, $g = b + t\omega$. So,

$$\begin{aligned} \log b - \log g &\leq \frac{1}{g}(b - g) \\ &= \frac{1}{b + t\omega}(|t|\omega) \\ &< \frac{2}{b}|t|\omega \\ &= 2\omega^{-\mu+1}|t| < t^2\omega^{-2\kappa}. \end{aligned}$$

So,

$$\begin{aligned} \|v\|^2 &\geq \sum_{i=1}^{m} |\delta_i| \log p_i + t^2\omega^{-2\kappa} \\ &= \log g + t^2\omega^{-2\kappa} \\ &= \log b - (\log b - \log g) + t^2\omega^{-2\kappa} \\ &\geq \log b - 2\omega^{-\mu+1}|t| + t^2\omega^{-2\kappa} \\ &\geq \log b, \end{aligned}$$

a contradiction. □

Proof of Lemma 2 (continued).

1. $v \in L_2, v \neq 0 \implies \|v\| \geq 1$:

This follows from part *6* of Lemma 1.

2. $|Z| \geq 2^{n \log n}$:

From (ii), the set $Z' = \{g \in \Gamma \mid g \equiv b \pmod{\omega},\ |b - g| \leq \omega^{3/2}\}$ satisfies $|Z'| \geq 2^{n \log n}$. By Lemma 1, for every $g \in Z'$, where $g = b + t\omega$, we have $\nu = \sum_{i=1}^{m} \gamma_i \nu_i + \nu_{m+1} + t\nu_{m+2}$ satisfies $\|\nu\|^2 \leq \frac{3}{\omega^2} + \log b$. Let $w = \frac{1}{\sqrt{\log b}} \nu \in L_2$. Then, $w = \sum_{i=1}^{m+2} \gamma_i \bar{\nu}_i$, where $\gamma_{m+1} = 1, \gamma_{m+2} = t$. We have,

$$\|w\|^2 = \frac{1}{\log b} \|\nu\|^2 \leq \frac{1}{\log b} \left(\frac{3}{\omega^2} + \log b \right) = 1 + \bar{\rho}$$

and for $i \in \{1, \ldots, m\}$ $\gamma_i \in \{0, -1\}$ and $\sum_{i=1}^{m} |\gamma_i| = n$, because $g \in \Gamma$.

3. If $u_1, u_2 \in Z, u_1 \neq u_2$ and $u_j = \sum_{i=1}^{m+2} \gamma_i^{(j)} \bar{\nu}_i$, then $\exists i \in \{1, \ldots, m\}$ such that $\gamma_i^{(1)} \neq \gamma_i^{(2)}$:

Assume $\forall i \in \{1,\ldots,m\}, \gamma_i^{(1)} = \gamma_i^{(2)}$. Let $y_j = \sqrt{\log b}\, u_j = \sum_{i=1}^{m+2} \gamma_i^{(j)} \nu_i$. Then

$$\begin{aligned} \|y_j\|^2 &= (\log b)\, \|u_j\|^2 \\ &\leq (\log b)(1+\bar{\rho}) \\ &= (\log b)\left(1 + \frac{3}{\omega^2 \log b}\right) \\ &= \log b + \frac{3}{\omega^2} \leq \log b + c \end{aligned}$$

By definition of Z, $\gamma_i^{(j)} \in \{0,-1\}$, for $i \in \{1,\ldots,m\}$ and $j \in \{1,2\}$. If $\gamma_{m+1}^{(j)} < 0$ for $j = 1$ or 2, then $-y_j$ satisfies the assumptions of Lemma 1 and so $-\gamma_i^{(j)} \in \{0,-1\}$, for $i \in \{1,\ldots,m\}$. This implies $\gamma_i^{(j)} \in \{0,1\}$ for $i \in \{1,\ldots,m\}$, contrary to the definition of Z. (And $\exists i \in \{1,\ldots,m\}$ $\gamma_i^{(j)} = 1$, since by the definition of Z, $\sum_{i=1}^{m} |\gamma_i^{(j)}| = n > 0$.) Therefore, $\gamma_{m+1}^{(j)} \geq 0$, $j \in \{1,2\}$ and so by Lemma 1, $\gamma_{m+1}^{(1)} = \gamma_{m+1}^{(2)} = 1$. Thus, $y = y_1 - y_2$ is parallel to ν_{m+2} and

$$\|y\|^2 = (y_1 - y_2) \cdot (y_1 - y_2) \leq 2(\|y_1\|^2 + \|y_2\|^2) \leq 4(\log b + c).$$

But, $\|\nu_{m+2}\|^2 \geq B^2 \log\left(1 + \frac{\omega}{b}\right)^2 > 4(\log b + c)$. □

Proof of Lemma 3 (continued).

1. $v \in L, v \neq 0 \implies \|v\| \geq 1$:

Let T be the linear transformation $T\bar{\nu}_i = \bar{v}_i$, for $i = 1,\ldots,m+2$. Then, $1 - 2^{-n^{c_1}} \leq \|T\| \leq 1 + 2^{-n^{c_1}}$ and $1 - 2^{-n^{c_1}} \leq \left\|T^{-1}\right\| \leq 1 + 2^{-n^{c_1}}$ for some constant c_1 that is sufficiently large. By construction, $v = (1+\bar{\rho})Tw$, for some $w \in L_2$, $w \neq 0$. This implies $\|w\| \geq 1$. So, $\|v\| \geq (1+\bar{\rho})\left\|T^{-1}\right\| \geq (1+2^{-n^3})(1-2^{-n^{c_1}}) \geq 1$, because size$(\bar{\rho}) \leq n^2$ and c_1 is large enough .

2. $|Y| \geq 2^{n \log n}$:

Let $v = (1+\bar{\rho})Tw$, $w \in Z$. Then,

$$\|v\|^2 \leq (1+\bar{\rho})^2 \|T\|^2 \|w\|^2 \leq (1+\bar{\rho})^2(1+2^{-n^{c_1}})^2(1+\bar{\rho})^2 \leq (1+\bar{\rho})^6 \leq 1 + 8\bar{\rho} = 1 + \rho.$$

3. If $u_1, u_2 \in Y, u_1 \neq u_2$ and $u_j = \sum_{i=1}^{m+2} \gamma_i^{(j)} v_i$, $j = 1,2$, then $\exists i \in \{1,\ldots,m\}$ such that $\gamma_i^{(1)} \neq \gamma_i^{(2)}$:

Similar to 2. □

Lemma 4 *Let $y_1,\ldots,y_l$ be l integers such that $\sum_{i=1}^{l} y_i = [\frac{l}{2}]$. Then, $\sum_{i=1}^{l} y_i^2$ is minimized when all y_i are either 0 or 1, and this minimum value is $[\frac{l}{2}]$. If $\exists i$ $y_i \notin \{0,1\}$, then $\sum_{i=1}^{l} y_i^2 \geq [\frac{l}{2}] + 2$.*

Proof Consider,

$$S = \sum_{i=1}^{l} y_i^2 - \sum_{i=1}^{l} y_i = \sum_{i=1}^{l} y_i(y_i - 1).$$

For all $y \in \mathbf{Z}$, $y(y-1) \geq 0$ and is 0 iff $y \in \{0,1\}$. Therefore, $S = 0$ iff $\forall i\ y_i \in \{0,1\}$, else $S > 0$. This means that the minimum of $\sum_{i=1}^{l} y_i^2$ subject to the condition that $\sum_{i=1}^{l} y_i = [\frac{l}{2}]$ occurs when exactly $[\frac{l}{2}]$ of the y_i are 1 and the rest are 0. For $y \geq 2$ or $y \leq -1$, $y(y-1)$ increases with $|y|$. and $y(y-1) = 2$ when $y = 2$ or -1. If $\exists i\ y_i \notin \{0,1\}$, then $S \geq 2$ and so $\sum_{i=1}^{l} y_i^2 \geq [\frac{l}{2}] + 2$. □

Lemma 5 *Let $m = poly(n)$. Let $\bar{a}_1, \ldots, \bar{a}_{m+2}$ and $\bar{b}_1, \ldots, \bar{b}_{m+2}$ be two sets of linearly independent vectors in $\mathbf{R}^{m+2}$, such that $1 \leq \|\bar{a}_i\|, \left\|\bar{b}_i\right\| \leq 2^{n^\beta}$ for some constant $\beta > 0$ and for $i = 1, \ldots, m+2$. Let the matrix $W = (\bar{a}_1, \ldots, \bar{a}_{m+2})$ satisfy $|det\ W| \geq 2^{-n^{\beta'}}$ for some constant $\beta' > 0$ and $\delta_i = \bar{b}_i - \bar{a}_i$ satisfy $\|\delta_i\| \leq 2^{-n^\gamma}$, where $\gamma \geq \beta' + \beta + 2$. Let T be the linear transformation $T(\bar{a}_i) = \bar{b}_i$, for $i = 1, \ldots, m+2$. Then, $1 - 2^{-n^{\gamma-2}} \leq \|T\| \leq 1 + 2^{-n^{\gamma-2}}$ and $1 - 2^{-n^{\gamma-2}} \leq \left\|T^{-1}\right\| \leq 1 + 2^{-n^{\gamma-2}}$.*

Proof We have, $\frac{\|T(\bar{a}_i)\|}{\|\bar{a}_i\|} = \frac{\left\|\bar{b}_i\right\|}{\|\bar{a}_i\|} \geq 1 - \frac{2^{-n^\gamma}}{\|\bar{a}_i\|} \geq 1 - 2^{-n^\gamma} \geq 1 - 2^{-n^{\gamma-2}}$, since $\|\bar{a}_i\| \geq 1$ and so the lower bound follows. For the upper bound, let $\alpha = (\alpha_1, \ldots, \alpha_{m+2})$ and $W\alpha = x = (x_1, \ldots, x_{m+2})$ be a unit vector in $\mathbf{R}^{m+2}$. Let $W(i)$ = the matrix obtained by replacing the i^{th} column of W by x, and $W(j,i)$ = matrix obtained by deleting the j^{th} row and the i^{th} column of W. Let P_i denote the parallelepiped defined by $\bar{a}_j$, $j \neq i$ and $\text{proj}(P_i, j)$ denote the orthogonal projection of P_i on the space spanned by $e_1, \ldots, e_{j-1}, e_{j+1}, \ldots, e_n$, where e_i's are the standard unit vectors. Note that, $\text{vol}(\text{proj}(P_i, j)) = |\text{det } W(j,i)|$. By Cramer's Rule,

$$|\alpha_i| = \frac{|\text{det } W_i|}{|\text{det } W|}.$$

We have,

$$\begin{aligned} |\text{det } W_i| &= \left| \sum_{j=1}^{m+2} x_j (\text{det } W(j,i)) \right| \\ &\leq \sum_{j=1}^{m+2} |x_j|\ \text{vol}(\text{proj}(P_i, j)) \\ &\leq \sum_{j=1}^{m+2} |x_j|\ \text{vol}(P_i). \end{aligned}$$

Therefore,

$$\begin{aligned} |\alpha_i| &\leq \frac{\text{vol}(P_i)}{|\text{det } W|} \sum_{j=1}^{m+2} |x_j| \\ &\leq \frac{\text{vol}(P_i)}{|\text{det } W|} \sqrt{n} \sum_{j=1}^{m+2} x_j^2 \qquad \text{by Cauchy-Schwarz} \\ &\leq \frac{\text{vol}(P_i)}{|\text{det } W|} \sqrt{n} \end{aligned}$$

Since $|\det W| \geq 2^{-n^{\beta'}}$ and $\mathrm{vol}(P_i) \leq \prod_{j \neq i} \|\bar{a}_j\| \leq (2^{n^\beta})^n = 2^{n^{\beta+1}}$,

$$|\alpha_i| \leq 2^{n^{\beta+1}} 2^{n^{\beta'}} \sqrt{n} \leq 2^{n^{\beta+\beta'+1}}.$$

Now, let $y = Tx = \sum_{i=1}^{m+2} \alpha_i \bar{b}_i$. Then,

$$\begin{aligned}
\|y\| &= \left\| \sum_{i=1}^{m+2} \alpha_i \bar{b}_i \right\| \\
&= \left\| \sum_{i=1}^{m+2} \alpha_i (\bar{a}_i + \delta_i) \right\| \\
&\leq \left\| \sum_{i=1}^{m+2} \alpha_i \bar{a}_i \right\| + \left\| \sum_{i=1}^{m+2} \alpha_i \delta_i \right\| \\
&\leq \|x\| + \sum_{i=1}^{m+2} |\alpha_i| \, \|\delta_i\| \\
&\leq 1 + \sum_{i=1}^{m+2} 2^{n^{\beta+\beta'+1}} \|\delta_i\| .
\end{aligned}$$

Since $\|\delta_i\| \leq 2^{-n^\gamma}$ and $\gamma \geq \beta + \beta' + 2$,

$$\|y\| \leq 1 + \sum_{i=1}^{m+2} 2^{n^{\gamma-1}} 2^{-n^\gamma} \leq 1 + 2^{-n^{\gamma-2}}.$$

A similar proof works for T^{-1}. □