Approximating the SVP to within $1 + \frac{1}{\text{dim}}$ is NP-hard under randomized reductions

Jin-Yi Cai and Ajay Nerurkar
Department of Computer Science, State University of New York, Buffalo, New York 14260
E-mail: cai@cs.buffalo.edu, apn@cs.buffalo.edu

Received April 15, 1998; revised April 30, 1999

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

1. INTRODUCTION

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

A lattice $L$ is a discrete additive subgroup of $\mathbb{R}^n$. It is the set of all integral linear combinations of an underlying generating set of linearly independent vectors from $\mathbb{R}^n$. 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 nonzero 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 their computational complexity aspects, and their application to provably secure public-key cryptography, as recently demonstrated by Ajtai [Ajt96], and Ajtai and Dwork [AD97].

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

\footnote{Research supported in part by NSF Grant CCR-9634665 and an Alfred P. Sloan Fellowship.}
certain computational problem on 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 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 for the Ajtai–Dwork public-key cryptosystem, which Ajtai and Dwork [AD97] proved is secure, based on only a worst case hardness assumption. The assumption is that there is no P or BPP algorithm for a certain version of the SVP, namely to find the shortest lattice vector in a lattice with an $n^c$-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. Second, 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 of lattice problems, Lagarias [Lag82] showed that SVP is NP-hard for the $l_{\infty}$-norm. Van Emde Boas [vEB81] showed that, given a point in space, finding the closest lattice vector to it (the closest vector problem, CVP) 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 CVP 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 [Ajt98]: 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 $(1 + 1/2^c)$ (for
a sufficiently large constant \( k \) is also NP-hard under randomized reductions. The main result of this paper is to improve this approximation factor to \( (1+1/n) \) for any \( \epsilon > 0 \). Very recently, Micciancio [Mic98] has raised the factor further, to any constant smaller than \( \sqrt{2} \).

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 an \( n^{1/4} \)-unique shortest vector is not NP-hard unless the polynomial time hierarchy collapses [Cai98].

The Ajtai-Dwork system is based on the intractability of finding the shortest lattice vector in a lattice with an \( n^{1/4} \)-unique shortest vector. Currently the exponent \( \epsilon \) is still rather large in their proof. Thus, we could conjecture that the Ajtai-Dwork system, as it stands, is not NP-hard to break. In fact, Nguyen and Stern [NS98] prove a converse to the Ajtai-Dwork result. They show that if CVP (or SVP) can be approximated to within a certain polynomial factor, the Ajtai-Dwork system can be broken. 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.

2. PRELIMINARIES

We denote by \( \mathbb{R} \) the field of real numbers and by \( \mathbb{Z} \) the ring of integers. The Euclidean \( (l_2 \text{-}) \) norm is denoted by \( \| \cdot \| \). For \( n \) linearly independent vectors \( v_1, v_2, ..., v_n \in \mathbb{R}^m \), \( m \geq n \), \( P(v_1, ..., v_n) = \{ \sum_{i=1}^n \beta_i v_i \mid 0 \leq \beta_i \leq 1 \} \) denotes the parallelepiped defined by \( v_1, ..., v_n \). The \( (n\text{-dimensional}) \) volume \( vol(P(v_1, ..., v_n)) \) of the parallelepiped \( P(v_1, ..., v_n) \) is \( \sqrt{ \det(B^TB) } \), where the \( m \times n \) matrix \( B \) consists of \( v_i \)'s as column vectors, \( B = (v_1, ..., v_n) \). The \( n \text{-dimensional} \) lattice \( L = L(v_1, ..., v_n) \), with basis \( v_1, ..., v_n \), is the set of all integral linear combinations of the \( v_i \). The determinant of the lattice \( L \), \( \det L \), is the volume of \( P(v_1, ..., v_n) \). It is invariant under a change of basis. The length of the shortest nonzero vector of \( L \) is denoted by \( \lambda_1(L) \).

The number of bits needed to represent \( x \) is notated as \( \text{size}(x) \). All logarithms are to the base \( e \) unless specified otherwise.

The Shortest Vector Problem. Given \( b_1, ..., b_n \), find a shortest nonzero vector (in some fixed norm) in the lattice \( L(b_1, ..., b_n) \).

We will reduce an NP-complete problem to the problem of finding an approximate shortest vector in a lattice. Following Ajtai [Ajt98], 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 [Ajt98].)
The Restricted Subset Sum Problem. Given integers \(a_1, \ldots, a_l, A\), such that 
\[
\max\left\{ \log_2(|A|+1), \max_{i=1}^l \log_2(|a_i|+1) \right\} \leq l^\kappa,
\]
find a 0–1 solution to the system 
\[
\sum_{i=1}^l a_i x_i = A, \quad \sum_{i=1}^l x_i = \lfloor l/2 \rfloor.\]
Here, \(|\cdot|\) denotes absolute value.

3. A LATTICE WITH WONDERFUL PROPERTIES

We first define the values of some parameters. Let \(\varepsilon > 0\) be any constant. Let \(\kappa = 2, \mu = 10\). Choose \(\alpha > 4/\varepsilon\) and sufficiently larger than \(\mu\). Let \(\sum_{i=1}^l a_i x_i = A\) be an instance of the restricted subset sum problem. Let \(n = \lceil l^{1/4} \rceil\), where \(\delta_i\) is the constant whose existence is guaranteed by Theorem 2 (stated in Section 5, due to Ajtai) for \(x_1 = 2x, x_2 = 1\). We can assume that \(l\), and consequently \(n\) as well, are sufficiently large with respect to \(\alpha\). Let \(J\) be an integer such that \(n = \lfloor (\log J)/\alpha \log \log J \rfloor\). Clearly, \(e^\varepsilon < J < e^\varepsilon \log^\varepsilon\). Let \(p_1 < \cdots < p_m\) be all the primes less than \((\log J)^\varepsilon\). By the Prime Number Theorem, \(n^\varepsilon m \leq n^{\varepsilon+1}\). Let \(I\) denote the set of integers formed by taking the products of \(n\) distinct elements of the set \([p_1, \ldots, p_m]\). Note that any element of \(I\) is at most \((\log J)^m \leq J\). Pick an integer \(b\) uniformly from \([1, n]\). Let \(\omega\) be any integer such that \(\omega^\varepsilon b \leq 2(\omega^\varepsilon)^\varepsilon\). It may be chosen deterministically. Clearly, \(2^\varepsilon b \leq J\). Thus, both \(b\) and \(\omega\) are exponential in \(n\). Let \(B = \omega^\varepsilon + 1\).

Using the values of the parameters, \(\kappa, \mu, m, B, \omega\), and \(b\) defined above, we now review the lattice construction of Ajtai [Ajt98].

Let \(L_1\) be the lattice spanned by the rows \(v_i\) of the matrix
\[
\begin{pmatrix}
\sqrt{\log p_1} & \cdots & 0 & 0 & B \log p_1 \\
\vdots & \ddots & \vdots & \vdots & \vdots \\
0 & \cdots & \sqrt{\log p_m} & 0 & B \log p_m \\
0 & \cdots & 0 & 0 & B \log b \\
0 & \cdots & 0 & \omega^{-\varepsilon} & B \log(1 + \frac{\omega^\varepsilon}{b})
\end{pmatrix}.
\]

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 \(v_i\) have a special form. The hypothesis on the length of the vector \(w\) used here is weaker than the one in Lemma 3.2 in [Ajt98]. 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 \(w = (w_1, \ldots, w_{m+2}) \in L_1, \ w \neq 0, \ w = \sum_{i=1}^{m+2} \delta_i v_i, \ \delta_{m+1} \neq 0. \ If \ |w|^2 \leq \log b + c, \ then\)

1. \(|\delta_{m+2}| \leq \omega^\varepsilon + 1;\)
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 \( g = \prod_{i=1}^{m} p_i^{-\gamma_i} = b + \mathbf{w} \), \( t \in \mathbb{Z} \), \( \gamma_i \in \{0, -1\} \) for \( i = 1, \ldots, m \), and \( |b - g| < \omega^{n - 1/2} \), then \( \mathbf{w'} = \sum_{i=1}^{m+2} \gamma_i \mathbf{v}_i \), where \( \gamma_{m+1} = 1 \), \( \gamma_{m+2} = t \), satisfies \( \|\mathbf{w'}\|^2 \leq \log b + 3\omega^2 \).

6. For all \( v \in L_1, v \neq 0 \), 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,

\[
\log g_0 = \sum_{\delta_i > 0, 1 \leq i \leq m} \delta_i \log p_i
\]

\[
\log g_1 = \sum_{\delta_i < 0, 1 \leq i \leq m} -\delta_i \log p_i
\]

\[
\log g_0 - \log g_1 = \sum_{i=1}^{m} \delta_i \log p_i
\]

\[
\log g_0 + \log g_1 = \sum_{i=1}^{m} |\delta_i| \log p_i
\]

\[
\leq \sum_{i=1}^{m} \delta_i^2 \log p_i
\]

\[
= \sum_{i=1}^{m} w_i^2 \leq \|\mathbf{w}\|^2.
\]

Also,

\[
B \left| \sum_{i=1}^{m} \delta_i \log p_i + \delta_{m+1} \log b + \delta_{m+2} \log \left(1 + \frac{\omega}{b}\right) \right|
\]

\[
= |\mathbf{w}_{m+2}| \leq \|\mathbf{w}\| \leq (\log b + c)^{1/2}.
\]

Note that \( \mathbf{w} \) cannot be a scalar multiple of \( v_{m+2} \) because \( \mathbf{w} \neq 0 \) and

\[
\|v_{m+2}\| > \omega^{n+1} \log \left(1 + \frac{\omega}{b}\right) \geq \omega^{n+1} \frac{\omega}{2b}
\]

\[
> \omega^{n+1} \frac{1}{2} \frac{\omega}{(2\omega)^2}
\]

\[
> \sqrt{\log b + c} \geq \|\mathbf{w}\|.
\]

**Proof of Lemma 1.**

1. \( |\delta_{m+2}| \omega^{-n} = |\mathbf{w}_{m+2}| \leq \|\mathbf{w}\| \leq (\log b + c)^{1/2} \). Therefore,

\[
|\delta_{m+2}| \leq \omega^n (\log b + c)^{1/2} \leq \omega^{n+1}.
\]

2. First assume \( \delta_{m+1} = 0 \). Since \( \mathbf{w} \) is not parallel to \( v_{m+2}, \exists i \in \{1, \ldots, m\}, \delta_i \neq 0 \). 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 $g_i \leq \sqrt[\gamma]{b}$, where $\gamma$ is a constant. This implies 

$$|log g_0 - log g_1| \geq |log(\sqrt[\gamma]{b} + 1) - log(\sqrt[\gamma]{b})|$$

$$\geq \frac{1}{\sqrt[\gamma]{b} + 1}$$

$$\geq \frac{1}{2\sqrt[\gamma]{b}} \geq \frac{1}{\gamma^2\omega^{n/2}},$$

where $\gamma'$ denotes the constant $1/2^{n/2 + 1/\gamma}$.

From (1) and (3) and since $\delta_{m+1} = 0$ and $log(1 + \omega/b) \leq \omega/b$, we get

$$|\delta_{m+2}| \geq \frac{b}{\omega}\left( |log g_0 - log g_1| - \frac{(log b + c)^{1/2}}{\omega^{n+1}} \right)$$

$$\geq \frac{b}{\omega}\left( \frac{1}{\gamma^2\omega^{n/2}} - \frac{1}{\omega^{n+1}} (log b + c)^{1/2} \right)$$

$$\geq \omega^{n-1}\left( \frac{1}{\gamma^2\omega^{n/2}} - \frac{1}{\omega^{n+1}} \right)$$

$$> \omega^{n-2}$$

$$= \omega^{n+1},$$

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

Now assume $\delta_{m+1} \geq 2$. We know that $(log b + c)^{1/2} \geq |w| \geq |w_{m+2}|$ and, by part 1, $|\delta_{m+2} log(1 + \omega/b)| \leq \omega^{n+1}\omega/b \leq 1/\omega^2$.

By (3) and because of the lower bound on $\delta_{m+1}$,

$$\left| \sum_{1}^{m} \delta_i log p_i \right| \geq 2 log b - \frac{1}{\omega^2} - \frac{1}{\omega^{n+1}} (log b + c)^{1/2}$$

$$\geq \frac{3}{2} log b.$$

But using (1) and (2),

$$\frac{3}{2} log b > |w|^2$$

$$\geq \log g_0 + \log g_1$$

$$\geq |log g_0 - log g_1|$$

$$= \left| \sum_{1}^{m} \delta_i log p_i \right|.$$
3. By part 1, $|\delta_{m+2} \log (1 + \omega/b)| \leq 1/\alpha^2$. Therefore, by (3) and since $\delta_{m+1} = 1$,

$$|\log g_0 - \log g_1 + \log b| = \left| \sum_{i=1}^{m} \delta_i \log p_i + \log b \right|$$

$$\leq B^{-1} (\log b + c)^{1/2} + \frac{1}{\alpha^2}$$

$$\leq \frac{1}{\alpha^2} (\log b + c)^{1/2} + \frac{1}{\alpha^2}$$

$$\leq \frac{1}{\alpha}.$$

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

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

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, $|\log b - \log g_1| \leq 1/\alpha$ and, so, $\log g_1 \geq \log b - 1/\alpha$.

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 $\delta_j^2 \geq |\delta_j|$ for all other $i$. Therefore, $\|w\|^2 \geq \sum_{i=1}^{m} \delta_i^2 \log p_i \geq |\delta_j| \log p_j + \sum_{i=1}^{m} |\delta_i| \log p_i \geq 2 \log 2 + \log g_1 \geq \log b + 2 \log 2 - 1/\alpha > \log b + c$, a contradiction.

4. 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 $b(1 + \omega/b)^t$.

**Proof.**

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

where

$$|R| \leq \frac{t^2 \omega^2}{b} \leq \frac{\omega^{2+4}}{\alpha^2} \leq \frac{1}{\alpha^2}.$$

This proves the claim. □

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


Proof.

\[
\left| \log \left( b \left( 1 + \frac{\omega}{b} \right) \right) - \log g \right|
\]

\[
= \left| \log b + t \log \left( 1 + \frac{\omega}{b} \right) - \log g \right|
\]

\[
= B^{-1} \left| w_m + 1 \right|
\]

\[
\leq B^{-1} (\log b + c)^{1/2}
\]

\[
< \omega^{-\mu - 1/2}.
\]

We have, \( \log g \leq \|w\|^2 \leq \log b + c \), and so \( g \leq e^{\varepsilon b} \). So we get

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

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

5. \( \|w\|^2 \) is the sum of the quantities \( \sum_{i=1}^m \gamma_i^2 \log p_i, \omega \omega^{-2\varepsilon}, \) and \( B^2 \left[ \sum_{i=1}^m \gamma_i \log p_i + \log b + t \log(1 + \omega b) \right]^2 \). We have

\[
\sum_{i=1}^m \gamma_i^2 \log p_i = \sum_{i=1}^m |\gamma_i| \log p_i
\]

\[
= \log g
\]

\[
= \log b + \log \left( 1 + \frac{\omega}{b} \right)
\]

and

\[
\sum_{i=1}^m \gamma_i \log p_i + \log b + t \log \left( 1 + \frac{\omega}{b} \right)
\]

\[
= - \log g + \log b + t \log \left( 1 + \frac{\omega}{b} \right)
\]

\[
= - \log(1 + t/\omega) + \log b + t \log \left( 1 + \frac{\omega}{b} \right)
\]

\[
= - \log \left( 1 + \frac{\omega}{b} \right) + t \log \left( 1 + \frac{\omega}{b} \right)
\]

\[
= \left( - \frac{t/\omega}{b} + \frac{t^2\omega^2}{2b^2} \cdots \right) + \left( \frac{t/\omega}{b} - \frac{1}{2} \frac{t^2\omega^2}{b^2} \cdots \right)
\]

\[
< \frac{t^2\omega^2}{b^2}.
\]
Therefore,

$$\|w\|^2 \leq \log b + \log \left( 1 + \frac{t\omega}{b} \right) + \frac{t^2}{\omega^2\rho} + \left( \frac{Bt^2\omega^2}{b^2} \right)^2.$$  

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

6. Let $v = \sum_{i=1}^{m+2} \delta_i v_i \neq 0$ and assume $\|v\|^2 < \log b$. Then $\delta_{m+1} \in \{-1, 1\}$. W.l.o.g. let $\delta_{m+1} = 1$. Then, for $i = 1, \ldots, m$, $\delta_i \in \{0, -1\}$. Let $t = \delta_{m+2}$, and $g = \prod_{i=1}^{m} p_i^{-\delta_i}$. 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, $t^2\omega^{-2\epsilon} \leq \|v\|^2 < \log b$. Therefore, $|t| \leq \omega^n \sqrt{\log b}$. By part 4 above, $g = b + t\omega$. So,

$$\log b - \log g \leq \frac{1}{g} (b - g)$$

$$= \frac{1}{b + t\omega} (|t| \omega)$$

$$< \frac{2}{b} |t| \omega$$

$$\leq 2\omega^{-n+1} |t| < t^2\omega^{-2\epsilon}.$$  

So,

$$\|v\|^2 \geq \sum_{i=1}^{m} |\delta_i| \log p_i + t^2\omega^{-2\epsilon}$$

$$= \log g + t^2\omega^{-2\epsilon}$$

$$= \log b - (\log b - \log g) + t^2\omega^{-2\epsilon}$$

$$\geq \log b,$$

a contradiction.

4. NORMALIZING THE LATTICE

We now normalize the lattice so that every nonzero lattice vector has length at least 1. As described earlier, $b$ is chosen randomly from the set $\mathcal{I}$. In [Ajt98] it has been proven that with probability $\geq \frac{1}{2}$, $b$ satisfies the following:

(i) $b \geq 2^{1-1/(n-2)}$

(ii) In the interval $(b - \omega^{1/2}, b + \omega^{3/2})$, there are at least $2^n \log n$ elements of $\mathcal{I}$ that are congruent to $b$ modulo $\omega$.

**Lemma 2.** Let $b$ satisfy (i) and (ii) above and let $n$ be sufficiently large. Let $L_2 = (1/\sqrt{\log b}) L_1$, $\bar{v}_i = (1/\sqrt{\log b}) v_i$, $\bar{b} = (3/\omega^2 \log b)$. Then
1. \( v \in L_2, v \neq 0 \Rightarrow \|v\| \geq 1 \).

2. If \( Z \) is the set of all \( w \in L_2 \), \( w = \sum_{i=1}^{m+2} \gamma_i \bar{v}_i \), with \( \gamma_i \in \{0, -1\} \) for \( i \in \{1, \ldots, m\} \) and \( \sum_{i=1}^{m} |\gamma_i| = n \) and \( \|w\|^2 > 1 + \rho \), then \( |Z| \geq 2^n \log^a n \).

3. If \( u_1, u_2 \in Z, u_1 \neq u_2 \), and \( u_j = \sum_{i=1}^{m+2} \gamma_i^{(j)} \bar{v}_i \), 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 \( \|w\|^2 \leq 1 + 2/m^{1/4}, w = \sum_{i=1}^{m+2} \gamma_i \bar{v}_i, \gamma_{m+1} \geq 0 \), then \( \gamma_1, \gamma_m \in \{0, -1\} \) and \( \gamma_{m+1} = 1 \).

5. \( \det(\gamma_1, \ldots, \gamma_{m+2}) \geq (c_0/\sqrt{n})^a \), where \( c_0 \) is a universal constant.

**Proof.** 1. This follows from part 6 of Lemma 1.

2. From (iii) above, the set \( Z' = \{ g \in \Gamma \mid g \equiv b \pmod{o}, |b - g| \leq \omega^{1/2} \} \) satisfies \( |Z'| \geq 2^n \log^a n \). By part 5 of Lemma 1, for every \( g \in Z' \), where \( g = b + tw = \prod_{i=1}^{m} p_i \gamma_i \) we have \( v = \sum_{i=1}^{m} \gamma_i \bar{v}_i + tv_{m+1} + tv_{m+2} \) satisfies \( \|v\|^2 < 3/\omega^2 + \log b \). Let \( \omega = (1/\sqrt{\log b})v \in L_2 \). Then, \( w = \sum_{i=1}^{m+2} \gamma_i \bar{v}_i \), where \( \gamma_{m+1} = 1, \gamma_{m+2} = t \). We have

\[
\|w\|^2 = \frac{1}{\log b} \|v\|^2 \leq \frac{1}{\log b} \left( \frac{3}{\omega^2} \log b \right) = 1 + \rho,
\]

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

\[
\|y_j\|^2 = (\log b) \|u_j\|^2 \leq (\log b)(1 + \rho)
\]

\[
= (\log b) \left( 1 + \frac{3}{\omega^2 \log b} \right)
\]

\[
= \log b + \frac{3}{\omega^2} \leq \log b + c.
\]

By definition of \( Z \), \( \gamma_i^{(j)} \in \{0, -1\} \) for \( i \in \{1, \ldots, m\} \) and \( j \in \{1, 2\} \). If \( \gamma_{m+1} \neq 0 \) 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, \( \gamma_{m+1} = 0, j \in \{1, 2\} \), and so by Lemma 1, \( \gamma_m^{(2)} = 1 \). Thus, \( y_{m+1} = y_2 \) is parallel to \( v_{m+2} \). But this is not possible since

\[
\|y\|^2 = (y_1 - y_2) \cdot (y_1 - y_2) \leq 2(||y_1||^2 + ||y_2||^2) \leq 4(\log b + c),
\]

and \( \|v_{m+2}\|^2 \geq B^2 \log(1 + \omega/b)^2 > 4(\log b + c) \).
4. Let $v_1 = (\sqrt{\log b}) w \in L_1$. Then,

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

Now, $\log b \ll \log J < n \log^2 n$ and $m^{3/4} \gg n^{3/4} > n^2$. Therefore, $||v||^2 < \log b + c$. The conclusion follows from Lemma 1.

5. $\tilde{p} = 3/\omega^2 \log b$ and $\log(\omega^2 \log b) = 2 \log \omega + \log \log b$. We have $b < J < e^{n \log^2 n}$ and $\omega \ll b^{1/2} < e^{n \log^2 n^{1/2}}$. This implies $\log \omega < n \log^2 n/\mu$. Therefore, $\text{size} (\tilde{p}) \leq n^2$, say. By (i), $b \geq J^{1-1/(n-2)} \geq e^{2(1-1/(n-2))}$. Therefore,

$$4 \log \omega \geq \frac{b^{2n}}{4} \geq e^{2(\omega(1-1/(n-2))} \geq \frac{3}{4} \frac{2\sqrt{n}}{\log b^2},$$

say. Thus, $\tilde{p} = 3/\omega^2 \log b \ll 2^{-\sqrt{n}}$.

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,

For all $c > 0$, there exists $\rho_0 > 0$ and a probabilistic polynomial-time Turing machine $\mathcal{M}$ that, given an input $n$ in binary, returns in time $(\log n)^{\rho}$, an integer $m$, a rational $\rho > 0$, and linearly independent vectors $\bar{v}_1, ..., \bar{v}_{m+2} \in \mathbb{Q}^{m+2}$, such that $3\bar{v}_1, ..., \bar{v}_{m+2} \in \mathbb{R}^{m+2}$, $||\bar{v}_i - \bar{v}_j|| \leq 2^{-\rho'}$ for $i = 1, ..., m+2$, and with probability $\geq \frac{1}{2}$, $L_2 = L(\bar{v}_1, ..., \bar{v}_{m+2})$ satisfies (1)–(6) of Lemma 2.

If $L(\bar{v}_1, ..., \bar{v}_{m+2})$ is a good approximation to a lattice $L_2$ satisfying (1)–(6) of Lemma 2, then the following holds.

Lemmata 3. Let $v_1 = (1 + \rho) \bar{v}_i$. Let $L = L(v_1, ..., v_{m+2})$ and $\rho = 3\rho$. 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 $\sum_{i=1}^{m+2} |\gamma_i| = n$, $\gamma_i \in \{0, -1\}$ for $i \in \{1, ..., m\}$, and $||v||^2 < 1 + \rho$, then $|Y| \geq 2n \log n$.

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

4. For all $v \in L$, $v \neq 0$, if $||v||^2 \leq 1 + 2/m^{3/4}$, $v = \sum_{i=1}^{m+2} \gamma_i v_i$ with $\gamma_{m+1} \geq 0$, then $\gamma_1, ..., \gamma_m \in \{0, -1\}$ and $\gamma_{m+1} = 1$.
Proof. Let $T$ be the linear transformation $T \vec{v}_i = \vec{e}_i$ for $i = 1, ..., m + 2$. Apply Lemma 5 from the Appendix. Since $m = \text{poly}(n)$, we get that $1 - 2^{-\alpha_m} \leq \|T\| \leq 1 + 2^{-\alpha_m}$ and $1 - 2^{-\alpha_1} \leq \|T^{-1}\| \leq 1 + 2^{-\alpha_1}$ for some constant $c_1$ that can be made as large as we want by making the $\vec{e}_i$ approximate the $\vec{v}_i$ better.

1. By construction, $v = (1 + \rho) Tw$ for some $w \in L_2$, $w \neq 0$. This implies $\|w\| \geq 1$. So, $\|v\| \geq (1 + \rho) \|T^{-1}\| \geq (1 + 2^{-\alpha_i})(1 + 2^{-\alpha_1})^{-1} \geq 1$, because $\text{size}(\rho) \leq n^2$ and $c_1$ is large enough.

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

$$
\|v\| \leq (1 + \rho)^2 \|w\|^2 \\
\leq (1 + \rho)^2 (1 + 2^{-\alpha_i})^2 (1 + \rho)^2 \\
\leq (1 + \rho)^2 \leq 1 + 8\rho = 1 + \rho.
$$

Thus, the conclusion follows from part 2 of Lemma 2.

3. Similar to 2.

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

$$
\|w\| \leq (1 + \rho)^{-2} \|T^{-1}\|^2 \|v\|^2 \\
\leq (1 + 2^{-\alpha_i})^{-2} (1 + 2^{-\alpha_1})^2 \|v\|^2 \\
\leq \|v\|^2 \\
\leq 1 + \frac{2}{n^{\alpha_i}}.
$$

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

5. THE REDUCTION

We now randomly extend the lattice $L$ constructed in the last section. With high probability, given an approximate shortest vector in this extended lattice, we will be able to produce a solution to the restricted subset sum instance, if one exists.

Let $\sum_{i=1}^{l} a_i \vec{x}_i = A$ be the given instance of the restricted subset sum problem, and let $C = C_1, ..., C_l$ be a random sequence of subsets of $\{1, ..., m\}$, where $m$ is as defined in Section 3.

Define a $(l + 2) \times (m + 1)$ matrix $D$ as follows:

1. $d_{1,j} = a_j$ for all $j \in C_i$, $d_{1,m+1} = A$, and $d_{1,j} = 0$ otherwise;

2. $d_{2,j} = l$ for all $j \in \bigcup_{i=1}^{l} C_j$, $d_{2,m+1} = \lceil l/2 \rceil$, and $d_{2,j} = 0$ otherwise;

3. For all $i \in \{1, ..., l\}$, $d_{i+2,j} = 1$ if $j \in C_i$, and $d_{i+2,j} = 0$ otherwise.
If $C_1, ..., C_l$ are consecutive intervals of $\{1, ..., m\}$, then $D$ is the matrix

$$
\begin{pmatrix}
  a_1 l & \cdots & a_i l & \cdots & a_l l & \cdots & A_i \\
  \vdots & & \vdots & & \vdots & & \vdots \\
  1 & \cdots & 1 & \cdots & 1 & \cdots & \left(\frac{1}{2}\right) l \\
  \vdots & & \vdots & & \vdots & & \vdots \\
  0 & \cdots & 0 & \cdots & 1 & \cdots & 0 \\
\end{pmatrix}
$$

Define $r = 2/m^l$. For $v \in L$, let $A(v) = \langle \gamma_1, \sqrt{\tau}, ..., \gamma_{m+1}, \sqrt{\tau} \rangle$. Let $L^{(D)} \subseteq \mathbb{R}^{m+4}$ be the lattice generated by the vectors $(v_i, A(v_i)D^T)$, where the $v_i$ are the basis vectors of $L$. It is of dimension $m+2$. Clearly, $L^{(D)} = \{ (v, A(v)D^T) \mid v \in L \}$. Let $L^{(D)}^+ = \{ (v, A(v)D^T) \mid v \in L, \ v = \sum_{i=1}^{m+2} \gamma_i v_i, \ \gamma_{m+1} \geq 0 \}$. Let $g_{C,v}(i) = -\sum_{i \in C} \gamma_i v_i$, where $v = \sum_{i=1}^{m+2} \gamma_i v_i$ is a vector in $L$.

**Theorem 1.** This construction satisfies the following:

(i) Let $X = \{ T \subseteq \{1, ..., m\} \mid \exists \in Y, \ v = \sum_{i=1}^{m+2} \gamma_i v_i, \ T = \{ i \in \{1, ..., m\} \mid \gamma_i = -1 \} \}$. With high probability, a random choice of $C = C_1, ..., C_l$ is such that, has property $P$.

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

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

Before we present the proof of this theorem we show how it can be used to prove our main result.

**Main Theorem.** Approximating the SVP to within a factor $(1 + 1/\dim^l)$ is NP-hard under randomized reductions, where $\dim$ denotes the dimension of the lattice.

**Proof.** The proof is obtained by putting together the results established so far. We show NP-hardness by reducing the restricted subset sum problem to the problem of finding an approximate shortest vector in an appropriate lattice. It is easy to see that the reduction can be done in randomized polynomial time.

An input to the restricted subset sum problem is integers $a_1, ..., a_l$ and $A$, such that max $\{ \log_2(|A| + 1), \max_{i=1}^l \log_2(|a_i| + 1) \} \leq \hat{p}$. We are required to find a $0$–$1$ solution to the system $\sum_{i=1}^{m+2} a_i x_i = A$, $\sum_{i=1}^l x_i = \lfloor l/2 \rfloor$. Here $\lfloor \cdot \rfloor$ denotes absolute value. Clearly, the input size is $O(\hat{p}^3)$. First, we construct a lattice $L$. This lattice is a rational approximation of a scaled version of lattice $L_1$, which has been defined in Section 3. The only randomness in the construction is the random choice of $b$, all other parameters are chosen deterministically. Note that every entry in the basis matrix for $L_1$, and hence $L$, has length polynomial in $l$. With probability $\geq \frac{1}{2}$ over the choice of $b$, $L$ has the properties described in Lemma 3.
Next, we pick random subsets $C_1, ..., C_l$ of $\{1, ..., m\}$, and use them to construct the matrix $D_l$ as outlined earlier in this section. This matrix defines an extension $L(D_l)$ of $L$. By Theorem 1, with high probability, a random choice of the $C_i$ is good, and then a solution to the restricted subset sum instance can be computed from a vector of $L(D_l)$ whose squared norm is within a factor $(1 + 1/dim')$ of $\lambda_1(L(D_l))^2$.

**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 $(1 + 1/dim')$ under randomized reductions, by using $(\log n)^{1/p}$ in the construction of $L_1$.

**Proof of Theorem 1.** (i) First, we state a combinatorial theorem of Ajtai [Ajt98].

**Theorem 2 (Ajtai).** For all $\alpha_1 \geq 2, \alpha_2 > 0$, $\exists \delta_1, \delta_2, \delta_3, 0 < \delta_i < 1, i = 1, 2, 3$, such that, for all sufficiently large $n$, the following holds: Assume that $\langle S, X \rangle$ is an $n$-uniform hypergraph, $n^2 \leq |S| \leq n^{\alpha_1}$, $|X| \geq 2^{\alpha_2 n \log n}$. Let $k = \lfloor n^{\delta_1} \rfloor$ and $C = C_1, ..., C_k$ be a random sequence of pairwise disjoint subsets of $S$, 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 $\{1, ..., k\}$, $\exists T \in X$, such that, $\forall j \in \{1, ..., k\}, f(j) = |C_j \cap T|$.

Using the $n$ defined in Section 3, apply Theorem 2 with $\alpha_1 = 2\alpha, \alpha_2 = 1, S = \{1, ..., m\}, k = \lfloor n^{\delta_1} \rfloor \geq l$, and $X = \{ T \subseteq \{1, ..., m\} | \exists v \in Y, \ v = \sum_{i=1}^{m+2} \#_i v_i, \ T = \{ i \in \{1, ..., m\} | \#_i = 1 \} \}$. We know that $|Y| \geq 2^{n \log n}$ and any two distinct $v_1, v_2 \in Y$ produce different $T$'s. Thus, $|X| \geq 2^{n \log n}$ (since $\alpha_2 = 1$), as required by the hypothesis of Theorem 2. Therefore, with high probability a random choice of the $C_1, ..., C_l$ satisfies Property P (because $k \geq l$).

(ii) We first state a lemma whose proof can be found in the Appendix.

**Lemma 4.** Let $y_1, ..., y_l$ be $l$ integers such that $\sum_{i=1}^l y_i = \lfloor l/2 \rfloor$. Then, $\sum_{i=1}^l y_i^2$ is minimized when all $y_i$ are either 0 or 1, and this minimum value is $\lfloor l/2 \rfloor + 2$.

Suppose $\sum_{i=1}^l a_i y_i = A$ has a solution $x_i = s_i$. Let $f$ be the function $f(i) = s_i$. 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 $\forall i \in \{1, ..., l\}$,

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

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

Let $\bar{v} = (v, A(v) D^T)$. Since $v \in Y$, $0 < \|v\| \leq 1 + \rho$. So, $\bar{v}$ is a nonzero vector, which implies $\lambda_1(L(D)) \leq \|v\|$. Since $v$ gives rise to a solution to the restricted subset sum instance, $\lambda_1(L(D))^2 \leq \|v\|^2 \leq \|A(v) D^T\|^2 \leq (1 + \rho)^2 \lfloor l/2 \rfloor$. Since $\tau = 2/m^2$ and $1 \leq n^{\delta_1} \leq n^{\delta_2/\delta_3} \leq m^{\delta_4/\delta_3} \leq m^{\delta_4}$, $\|v\|^2 \leq 1 + \rho + 1/m^{\delta_4}$. By assumption, $\bar{w} = (w, A(w) D^T)$ is a $(1 + 1/m^2)$-approximation to the shortest nonzero vector of $L(D)$. 


Therefore,

\[ \|w\|^2 \leq \|\tilde{w}\|^2 \]
\[ \leq \left( 1 + \frac{1}{m^2} \right) \lambda_1(L^{(D)})^2 \]
\[ \leq \left( 1 + \frac{1}{m^2} \right) \|\epsilon\|^2 \]
\[ \leq 1 + \frac{2}{m\sqrt{\lambda^*}}. \]

Let \( w = \sum_{i=1}^{m+2} y_i v_i \). Then, by part 4 of Lemma 3 and because \( \tilde{w} \in L^{(D)^+}, \gamma_{m+1} = 1 \). Let \( u = (u_1, ..., u_{l+2}) = A(w)D^T \). Let \( y_i = g_{C_{\omega}}(i) \). It is easy to see that since \( \gamma_{m+1} = 1 \), \( u_1 = \sqrt{\tau} (A - \sum_{i=1}^{m} a_i y_i) \), \( u_2 = \sqrt{\tau} (l[l/2] - \sum_{i=1}^{m} y_i) \), 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) \( \sum_{i=1}^{l} a_i y_i = A \)
(ii) \( \sum_{i=1}^{l} y_i = \lfloor l/2 \rfloor \), and
(iii) \( \forall i, y_i \in \{0, 1\} \).

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

\[ \|\tilde{w}\|^2 \leq \left( 1 + \frac{1}{m^2} \right) \|\epsilon\|^2 \]
\[ \leq \left( 1 + \frac{1}{m^2} \right) \left( 1 + \rho + \tau \left( \frac{l}{2} \right) \right) \]
\[ < \left( 1 + \frac{\tau}{2} \right) \left( 1 + \tau l \right) \]
\[ < 1 + \tau l^2 \]
\[ \leq \|\tilde{w}\|^2. \]

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

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

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

where the last inequality uses Lemma 4. Thus,

\[ \|\tilde{w}\|^2 - \|\epsilon\|^2 \geq 2\tau - \rho \geq \frac{2}{m^2} \geq \frac{\|\epsilon\|^2}{m^2}. \]
This implies

\[ \| \vec{w} \|^2 > \left( 1 + \frac{1}{m^2} \right) \| \vec{v} \|^2 > \left( 1 + \frac{1}{m^2} \right) \lambda_1(L^{(D)})^2, \]

a contradiction. \[\Box\]

**APPENDIX**

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

**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 \( y \in \mathbb{Z} \), \( y(y - 1) \geq 0 \) and is 0 iff \( y \in \{0, 1\} \). Therefore, \( S = 0 \) iff \( \forall y \in \{0, 1\} \), else \( S > 0 \). This means that the minimum of \( \sum_{i=1}^l y_i^2 \), subject to the condition that \( \sum_{i=1}^l y_i = [l/2] \), occurs when exactly \([l/2]\) 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 \( \sum_{i=1}^l y_i^2 \geq [l/2] + 2 \) \[\Box\]

**Lemma 5.** Let \( \beta > 0, \beta' > 0, \gamma \geq \beta' + \beta + 3 \) be any constants. Let \( \vec{a}_1, \ldots, \vec{a}_{m+2} \) and \( \vec{b}_1, \ldots, \vec{b}_{m+2} \) be two sets of linearly independent vectors in \( \mathbb{R}^{n+2} \), such that \( 1 \leq |\vec{a}_i| \), \( |\vec{b}_i| \leq 2^m \) for \( i = 1, \ldots, m + 2 \). Let the matrix \( W = (\vec{a}_1, \ldots, \vec{a}_{m+2}) \) satisfy \( |\det W| \geq 2^{-m} \), and \( \tilde{\delta}_i = \vec{b}_i - \vec{a}_i \) satisfy \( |\tilde{\delta}_i| \leq 2^{-m} \). Let \( T \) be the linear transformation \( T(\vec{a}_i) = \vec{b}_i \) for \( i = 1, \ldots, m + 2 \). Then, \( 1 - 2^{-m-2} \leq \| T \| \leq 1 + 2^{-m-2} \).

**Proof.** We have, \( \| T(\vec{a}_i) \| / |\vec{a}_i| = |\vec{b}_i| / |\vec{a}_i| = 1 - 2^{-m} / |\vec{a}_i| \geq 1 - 2^{-m} \geq 1 - 2^{-m-2} \), since \( |\vec{a}_i| \geq 1 \) and, so, the lower bound follows. For the upper bound, let \( \vec{x} = (x_1, \ldots, x_{m+2}) \) and \( W\vec{x} = \vec{x}_1, \ldots, x_{m+2}) \) be a unit vector in \( \mathbb{R}^{n+2} \). Let \( W(i) \) be the matrix obtained by replacing the \( i \)th column of \( W \) by \( \vec{x} \), and \( W(j, i) \) = matrix obtained by deleting the \( j \)th row and the \( i \)th column of \( W \). Let \( P \) denote the parallelepiped defined by \( \vec{a}_j, j \neq i \) and \( \text{proj}(P, j) \) denote the orthogonal projection of \( P \) on the space spanned by \( e_1, \ldots, e_{j-1}, e_{j+1}, \ldots, e_{m+2} \), where \( e_i \)'s are the standard unit vectors. Note that, \( \text{vol}(\text{proj}(P, j)) = |\det W(j, i)| \). By Cramer's rule,

\[ |x_i| = \frac{|\det W(i)|}{|\det W|}. \]

We have

\[ |\det W(i)| \leq \sum_{j=1}^{m+2} |x_j| |(\det W(j, i))| \]

\[ = \sum_{j=1}^{m+2} |x_j| \text{vol}(\text{proj}(P, j)) \]

\[ \leq \sum_{j=1}^{m+2} |x_j| \text{vol}(P). \]
Therefore,

\[ |x_i| \leq \frac{\text{vol}(P_i)}{|\det W|} \sum_{j=1}^{m+2} |x_j|. \]

Applying Cauchy–Schwarz, we get

\[ |x_i| \leq \frac{\text{vol}(P_i)}{|\det W|} \sqrt{m+2} \sqrt{\sum_{j=1}^{m+2} x_j^2} \]

\[ = \frac{\text{vol}(P_i)}{|\det W|} \sqrt{m+2}. \]

Since \(|\det W| \geq 2^{-m}\) and \(\text{vol}(P_i) \leq \prod_{j \neq i} \| \delta_j \| \leq (2^{m^2})(m+1) \leq 2^{m^2+2}, \)

\[ |x_i| \leq 2^{m^2+1} \sqrt{\frac{m+2}{m+2}} \leq 2^{m^2+m+2}. \]

Now, let \(y = T x = \sum_{i=1}^{m+2} x_i \delta_i\). Then,

\[ \|y\| = \left\| \sum_{i=1}^{m+2} x_i \delta_i \right\| \]

\[ \leq \left\| \sum_{i=1}^{m+2} x_i (\tilde{a}_i + \delta_i) \right\| \]

\[ \leq \left\| \sum_{i=1}^{m+2} x_i \tilde{a}_i \right\| + \left\| \sum_{i=1}^{m+2} x_i \delta_i \right\| \]

\[ \leq \|x\| + \sum_{i=1}^{m+2} |x_i| \|\delta_i\| \]

\[ \leq 1 + \sum_{i=1}^{m+2} 2^{m^2+m+2} \|\delta_i\|. \]

Since \(\|\delta_i\| \leq 2^{-m}\) and \(\gamma \geq \beta + \beta' + 3, \)

\[ \|y\| \leq 1 + \sum_{i=1}^{m+2} 2^{m^2-1} 2^{-m} \leq 1 + 2^{-m^2-2}. \]

**ACKNOWLEDGMENT**

We thank an anonymous referee for very helpful comments and suggestions.
REFERENCES


APPROMATING THE SVP