On the Inapproximability of the Shortest Vector in a Lattice within some constant factor (preliminary version)

Daniele Micciancio*

MIT Laboratory for Computer Science
Cambridge, MA 02139

MIT/LCS/TM-574

February 1998

Abstract

We show that computing the approximate length of the shortest vector in a lattice within a factor c is NP-hard for randomized reductions for any constant $c < \sqrt{2}$.

*email: miccianc@theory.lcs.mit.edu. Partially supported by DARPA contract DABT63-96-C-0018.

1 Introduction

In this paper we show that approximating the shortest vector in a lattice within any constant factor less than $\sqrt{2}$ is NP-hard for randomized reductions.

The first intractability results for lattice problems date back to [10] where van Emde Boas proved that the closest vector problem (CVP) is NP-hard and conjectured that the shortest vector problem was also NP-hard.

Altough much progress was done in proving the hardness of CVP [3], where the problem is proved NP-hard to approximate within any constant factor and quasi-NP-hard within quasi-polynomial factors, the hardness of computing even the exact solution to the SVP remained an open question until recently when Ajtai [2] proved that the SVP is NP-hard for randomized reductions. In the same paper it is shown that approximating the length of the shortest vector within a factor $1 + \frac{1}{2^{n^c}}$ is also NP-hard for some constant c and in [5] is shown how to improve the inapproximability factor to $1 + \frac{1}{n^{\epsilon}}$, but still a factor that rapidly approachs 1 as the dimention of the lattice grows.

In this paper we prove the first inapproximability result for the shortest vector problem within some constant factor greater than 1. This result is achieved by reducing the approximate SVP from a variant of the CVP which can be proven NP-hard to approximate using essentially the same arguments as in [3]. The techniques to reduce CVP to SVP are similar to those used in [2] where the problem is reduced from a variant of subset sum. However the similarities between the CVP and the SVP leads both to a much simpler proof and a much stronger result.

The rest of the paper is organized as follows. In section 2 we formally define the shortest vector and closest vector approximation problems. In section 3 we prove the NP-hardness of a variant of the closest vector approximation problem. In section 4 we prove that the SVP is NP-hard to approximate by reduction from the modified CVP using a technical lemma which is proved in section 5.

2 Definitions

We formalize the approximation problems associated to the shortest vector problem and the closest vector problem in terms of the following promise problems, as done in [6].

Definition 1 (Approximate SVP) *The promise problem* $\mathtt{GapSVP_g}$*, where* g *(the gap function) is a function of the dimension, is defined by*

- YES *instances are pairs* (V, d) *where* V *is a basis for a lattice in* R^n*,* $d \in R$ *and* $\|V\vec{\mathbf{z}}\|^2 \leq d$ *for some* $\vec{\mathbf{z}} \in Z^n \setminus \{\vec{\mathbf{0}}\}$*.*
- NO *instances are pairs* (V, d) *where* V *is a basis for a lattice in* R^n*,* $d \in R$ *and* $\|V\vec{\mathbf{z}}\|^2 > g(n)d$ *for all* $\vec{\mathbf{z}} \in Z^n \setminus \{\vec{\mathbf{0}}\}$*.*

Definition 2 (Approximate CVP) *The promise problem* $\mathtt{GapCVP_g}$*, where* g *(the gap function) is a function of the dimension, is defined by*

- YES *instances are triples* $(V, \vec{\mathbf{y}}, d)$ *where* $V \in Z^{k\times n}$*,* $\vec{\mathbf{y}} \in R^k$*,* $d \in R$ *and* $\|V\vec{\mathbf{z}} - \vec{\mathbf{y}}\|^2 \leq d$ *for some* $\vec{\mathbf{z}} \in Z^n$*.*
- NO *instances are triples* $(V, \vec{\mathbf{y}}, d)$ *where* $V \in Z^{k\times n}$*,* $\vec{\mathbf{y}} \in R^k$*,* $d \in R$ *and* $\|V\vec{\mathbf{z}} - \vec{\mathbf{y}}\|^2 > g(n)d$ *for all* $\vec{\mathbf{z}}$*.*

We also define a variant of CVP, which will be used as an intermediate step in proving the hardness of approximating the shortest vector in a lattice. The difference is that the YES instances are required to have a boolean solution, and in the NO instances the target vector can be multiplied by any non-zero integer.

Definition 3 (Modified CVP) *The promise problem* $\mathtt{GapCVP'_g}$*, where* g *(the gap function) is a function of the dimension, is defined by*

- YES *instances are triples* $(V, \vec{\mathbf{y}}, d)$ *where* $V \in Z^{k\times n}$*,* $\vec{\mathbf{y}} \in R^k$*,* $d \in R$ *and* $\|V\vec{\mathbf{z}} - \vec{\mathbf{y}}\|^2 \leq d$ *for some* $\vec{\mathbf{z}} \in \{0,1\}^n$*.*
- NO *instances are triples* $(V, \vec{\mathbf{y}}, d)$ *where* $V \in Z^{k\times n}$*,* $\vec{\mathbf{y}} \in R^k$*,* $d \in R$ *and* $\|V\vec{\mathbf{z}} - w\vec{\mathbf{y}}\|^2 > g(n)d$ *for all* $\vec{\mathbf{z}} \in Z^n$ *and all* $w \in Z$*.*

3 Hardness of approximating CVP

In this section we prove that the modified CVP is NP-hard to approximate within any constant factor. The proof is by reduction from set cover and is essentially the same as in [3].

Definition 4 (Set-Cover) *An instance of* set-cover *consists of a ground set U and a collection of subsets $S_1, \ldots, S_m$ of U. A* cover *is a subcollection of the S_i's whose union is U. The cover is said to be* exact *if the sets in the cover are pairwise disjoint.*

In [4], Bellare, Goldwasser et al. show that for every constant $c > 1$ there is a polynomial time reduction that, on input an instance ϕ of SAT, produces an instance of set-cover and an integer d with the following properties:

- If ϕ is satisfiable, there is an exact cover of size d,
- If ϕ is not satisfiable, then no set cover has size less than cd.

This result is used in [3] to show that the closest vector problem is hard to approximate within any constant factor. In fact, the same reduction can be used to prove that the modified CVP is NP-hard to approximate within any constant factor.

Theorem 1 *For every constant $c > 1$ the promise problem $\mathtt{GapCVP}'_{\mathtt{c}}$ is NP-hard.*

Proof: Let c be a constant greater than one. We reduce SAT to $\mathtt{GapCVP}'_{\mathtt{c}}$. Let ϕ be an instance of SAT. Apply the reduction from Bellare, Goldwasser et al. [4] to the formula ϕ, to obtained instance of set-cover $U, S_1, \ldots, S_m$ and integer k. Let n be the size of U and let $S \in \{0,1\}^{n \times m}$ be the matrix defined by $S_{i,j} = 1$ iff $i \in S_j$.

Define N and y as follows:

$$N = \begin{bmatrix} \alpha S \\ I \end{bmatrix} \qquad \vec{\mathbf{y}} = \begin{bmatrix} \alpha \vec{\mathbf{1}} \\ \vec{\mathbf{0}} \end{bmatrix}$$

where α is an integer such that $\alpha^2 > ck$.

- Assume ϕ is satisfiable. Then, U has an exact cover $\{S_i\}_{i\in I}$ of size $|I| = k$. Let $\vec{\mathbf{x}} \in \{0,1\}^m$ be the indicator vector of set I. We have $S\vec{\mathbf{x}} = \vec{\mathbf{1}}$ and $\|x\|^2 = \sum x_i = k$. Therefore

  $$\|N\vec{\mathbf{x}} - \vec{\mathbf{y}}\|^2 = \alpha^2\|S\vec{\mathbf{x}} - \vec{\mathbf{1}}\|^2 + \|x\|^2 = k,$$

  i.e., $(N, \vec{\mathbf{y}})$ is a YES instance of the modified CVP.

- Assume ϕ is not satisfiable. Then every subset $\{S_i\}_{i\in I}$ of size $|I| < ck$ is not a cover. Let $\vec{\mathbf{x}} \in Z^m$ and $w \in Z \setminus \{0\}$. We want to prove that $\|N\vec{\mathbf{x}} - w\vec{\mathbf{y}}\|^2 > ck$. Notice that $\|N\vec{\mathbf{x}} - w\vec{\mathbf{y}}\|^2 = \alpha^2\|S\vec{\mathbf{x}} - w\vec{\mathbf{1}}\|^2 + \|\vec{\mathbf{x}}\|^2$. We show that either $\alpha^2\|S\vec{\mathbf{x}} - w\vec{\mathbf{1}}\|^2$ or $\|\vec{\mathbf{x}}\|^2$ is greater than ck. Assume $\|\vec{\mathbf{x}}\|^2 \leq ck$. We will prove that $\|S\vec{\mathbf{x}} - w\vec{\mathbf{1}}\|^2 \geq 1$, which by our choice of α implies $\alpha^2\|S\vec{\mathbf{x}} - w\vec{\mathbf{1}}\|^2 > ck$. Let I be the set of all i such that $x_i \neq 0$. Notice that $|I| \leq \sum |x_i| \leq \sum x_i^2 = \|x\|^2 \leq ck$. Therefore $\{S_i\}_{i\in I}$ is not a cover. Let $j \in U$ be such that $j \notin \bigcup_{i\in I} S_i$. We have $[S\vec{\mathbf{x}}]_j = 0$ and therefore $\|S\vec{\mathbf{x}} - w\vec{\mathbf{1}}\|^2 \geq ([S\vec{\mathbf{x}}]_j - w)^2 \geq w^2 \geq 1$.

□

4 Hardness of approximating SVP

In this section we use the hardness of approximating the closest vector in a lattice to show that the shortest vector problem is also hard to approximate within some constant factor. The proof uses the following technical lemma.

Lemma 1 *For any constant $\epsilon > 0$ there exists a PPT algorithm that on input 1^k computes a lattice $L \in R^{(m+1)\times m}$, a vector $\vec{\mathbf{s}} \in R^{m+1}$ and a matrix $C \in Z^{k\times m}$ such that with probability arbitrarily close to one,*

- *For every non-zero $\vec{\mathbf{z}} \in Z^m$, $\|Lz\|^2 > 2$.*
- *For all $\vec{\mathbf{x}} \in \{0,1\}^k$ there exists a $\vec{\mathbf{z}} \in Z^m$ such that $C\vec{\mathbf{z}} = \vec{\mathbf{x}}$ and $\|L\vec{\mathbf{z}} - \vec{\mathbf{s}}\|^2 < 1 + \epsilon$.*

The proof of the above lemma will be given in the next section. We can now prove the main theorem.

Theorem 2 *The shortest vector in a lattice is NP-hard to approximate within any constant factor less than* $\sqrt{2}$.

Proof: We will show that for any $\epsilon > 0$ the squared norm of the shortest vector is NP-hard to approximate within a factor $2/(1+2\epsilon)$. The proof is by reduction from the modified closest vector problem. Formally, we give a reduction from $\mathtt{GapCVP}'_{\mathtt{c}}$ to $\mathtt{GapSVP}_{\mathtt{g}}$ with $c = 2/\epsilon$ and $g = 2/(1+2\epsilon)$.

Let $(N, \vec{\mathbf{y}}, d)$ be an instance of $\mathtt{GapCVP}'_{\mathtt{c}}$. We define an instance (V, t) of $\mathtt{GapSVP}_{\mathtt{g}}$ such that if $(N, \vec{\mathbf{y}}, d)$ is a YES instance of $\mathtt{GapCVP}'_{\mathtt{c}}$ then (V, t) is a YES instance of $\mathtt{GapSVP}_{\mathtt{g}}$, and if $(N, \vec{\mathbf{y}}, d)$ is a NO instance of $\mathtt{GapCVP}'_{\mathtt{c}}$ then (V, t) is a NO instance of $\mathtt{GapSVP}_{\mathtt{g}}$.

Let $L, \vec{\mathbf{s}}$ and C be as defined in lemma 1. Let $t = 1 + 2\epsilon$ and let V be the matrix

$$V = \left[\begin{array}{c|c} L & -\vec{\mathbf{s}} \\ \beta \cdot N \circ C & -\beta \cdot \vec{\mathbf{y}} \end{array} \right]$$

where $\beta = \sqrt{\epsilon/d}$.

- Assume that $(N, \vec{\mathbf{y}}, d)$ is a YES instance, i.e., there exists a vector $\vec{\mathbf{x}} \in \{0,1\}^k$ such that $\|N\vec{\mathbf{x}} - \vec{\mathbf{y}}\|^2 \leq d$. From lemma 1 there exists a vector $\vec{\mathbf{z}} \in Z^m$ such that $C\vec{\mathbf{z}} = \vec{\mathbf{x}}$ and $\|L\vec{\mathbf{z}} - \vec{\mathbf{s}}\|^2 < 1 + \epsilon$. Define the vector $\vec{\mathbf{w}} = \begin{bmatrix} \vec{\mathbf{z}} \\ 1 \end{bmatrix}$. We have

  $$\|V\vec{\mathbf{w}}\|^2 = \|L\vec{\mathbf{z}} - \vec{\mathbf{s}}\|^2 + \beta^2 \|N\vec{\mathbf{x}} - \vec{\mathbf{y}}\|^2 \leq 1 + 2\epsilon = t$$

  i.e., (V, t) is a YES instance of $\mathtt{GapSVP}_{\mathtt{g}}$.

- Now assume that $(N, \vec{\mathbf{y}}, d)$ is a NO instance and let $\vec{\mathbf{w}} = \begin{bmatrix} \vec{\mathbf{z}} \\ w \end{bmatrix} \in Z^{m+1}$ be a non-zero vector. We want to prove that $\|V\vec{\mathbf{w}}\|^2 \geq g \cdot t = 2$. Notice that $\|V\vec{\mathbf{w}}\|^2 = \|L\vec{\mathbf{z}} - w\vec{\mathbf{s}}\|^2 + \beta^2\|N\vec{\mathbf{x}} - w\vec{\mathbf{y}}\|^2$. We prove that either $\|L\vec{\mathbf{z}} - w\vec{\mathbf{s}}\|^2$ or $\beta^2\|N\vec{\mathbf{x}} - w\vec{\mathbf{y}}\|^2$ is greater than 2. If $w = 0$ then $\vec{\mathbf{z}} \neq 0$ and $\|L\vec{\mathbf{z}} - w\vec{\mathbf{y}}\|^2 = \|L\vec{\mathbf{z}}\|^2 > 2$. If $w \neq 0$ then $\beta^2\|N\vec{\mathbf{x}} - w\vec{\mathbf{y}}\|^2 \geq \beta^2 cd = 2$.

□

5 Proof of the Technical Lemma

To prove lemma 1 we need a result from [2] and two other lemmas.

Lemma 2 *For all $\epsilon > 0$, for all sufficiently large integers b, the following holds. Let $p_1, \ldots, p_m$ be m relatively prime positive integers. Let $P \in R^m$ be the vector $P_i = \log_b p_i$ and let $D \in R^{m\times m}$ be the diagonal matrix $D_{i,i} = \sqrt{\log_b p_i}$. Define the matrix*

$$L = \begin{bmatrix} D & 0 \\ 0 & 1/a \\ \beta P & \beta/b\ln b \end{bmatrix} = \left[\begin{array}{ccc|c} \sqrt{\log_b p_1} & & & 0 \\ & \ddots & & \vdots \\ & & \sqrt{\log_b p_m} & 0 \\ \hline 0 & \cdots & 0 & 1/a \\ \hline \beta\log_b p_1 & \cdots & \beta\log_b p_m & \beta/b\ln b \end{array}\right]$$

where $a = \frac{1}{3}b^{\epsilon/2}$ and $\beta > \sqrt{2}b\ln b$. Then for all non-zero integer vectors $\vec{\mathbf{z}} \in Z^{m+1}$, $\|L\vec{\mathbf{z}}\|^2 \geq (2-\epsilon)$.

Proof: Let $\vec{\mathbf{z}} \in Z^{m+1}$ be a non-zero vector. Define the vector $\vec{\mathbf{z}}' = [z_1, \ldots, z_m]^T$. Notice that

$$\|L\vec{\mathbf{z}}\|^2 = \|D\vec{\mathbf{z}}'\|^2 + \left(\frac{z_{m+1}}{a}\right)^2 + \beta^2\left(P\vec{\mathbf{z}}' + \frac{z_{m+1}}{b\ln b}\right)^2.$$

We want to prove that $\|L\vec{\mathbf{z}}\|^2 \geq 2-\epsilon$.

If $\vec{\mathbf{z}}' = 0$, then $z_{m+1} \neq 0$ and

$$\|L\vec{\mathbf{z}}\|^2 \geq \beta^2\left(P\vec{\mathbf{z}}' + \frac{z_{m+1}}{b\ln b}\right)^2 = \left(\frac{\beta}{b\ln b}\right)^2 z_{m+1}^2 \geq \left(\frac{\beta}{b\ln b}\right)^2 \geq 2.$$

So, assume $\vec{\mathbf{z}}' \neq 0$. Let $\vec{\mathbf{z}}^+, \vec{\mathbf{z}}^- \in Z^m$ be the vectors defined by $z_i^+ = \max\{z_i', 0\}$ and $z_i^- = \max\{-z_i', 0\}$. Define the integers $g^+ = b^{P\vec{\mathbf{z}}^+} = \Pi_i p_i^{z_i^+}$ and $g^- = b^{P\vec{\mathbf{z}}^-} = \Pi_i p_i^{z_i^-}$. Notice that $\vec{\mathbf{z}}' \neq \vec{\mathbf{0}}$ implies $\vec{\mathbf{z}}^+ \neq \vec{\mathbf{z}}^-$ and since the p_i's are relatively prime, $g^+ \neq g^-$. We observe that for any positive integers $x \neq y$, $|\log_b x - \log_b y| \geq \frac{1}{\sqrt{xy}\lg b}$ (proof: $|\log_b x - \log_b y| = \log_b(\max\{x,y\}/\min\{x,y\}) = \log_b(1+|x-y|/\min\{x,y\}) \geq \log_b(1+1/\sqrt{xy}) \geq \log_b 2/\sqrt{xy} = 1/(\sqrt{xy}\lg b)$.) In particular, $|P\vec{\mathbf{z}}'| = |\log_b g^+ - \log_b g^-| \geq$

$(\sqrt{g^+g^-}\lg b)^{-1}$, and since $\log_b g^+g^- = P\vec{\mathbf{z}}^+ + P\vec{\mathbf{z}}^- \leq \|D\vec{\mathbf{z}}^+\|^2 + \|D\vec{\mathbf{z}}^-\|^2 = \|D\vec{\mathbf{z}}'\|^2$ we have

$$|P\vec{\mathbf{z}}'| \geq \frac{1}{b^{\frac{\|D\vec{\mathbf{z}}'\|^2}{2}}\lg b}.$$

Now assume for contradiction that $\|L\vec{\mathbf{z}}\|^2 < 2-\epsilon$. We have $\|D\vec{\mathbf{z}}'\|^2 < 2-\epsilon$ and $|z_{m+1}| < a\sqrt{2}$. It follows

$$\begin{aligned}
\|L\vec{\mathbf{z}}\| &\geq \beta\left|P\vec{\mathbf{z}}' + \frac{z_{m+1}}{b\ln b}\right| \\
&\geq \beta\left(|P\vec{\mathbf{z}}'| - \left|\frac{z_{m+1}}{b\ln b}\right|\right) \\
&\geq \beta\left(\frac{1}{b^{1-\epsilon/2}\lg b} - \frac{a\sqrt{2}}{b\ln b}\right) \\
&> \left(\frac{\beta}{b\ln b}\right)\left(b^{\epsilon/2}\ln 2 - a\sqrt{2}\right) \\
&> \sqrt{2}b^{\epsilon/2}(\ln 2 - \sqrt{2}/3) > \sqrt{2}
\end{aligned}$$

□

Lemma 3 *Let L be the matrix defined in lemma 2 and assume $\beta < b^{2-\epsilon}$. Define the vector $\vec{\mathbf{s}} = [0,\ldots,0,\beta]^T \in R^{m+2}$. For every vector $\vec{\mathbf{z}}' \in \{0,1\}^m$, let $g = \Pi_{i=1}^m p_i^{z_i}$ and $\vec{\mathbf{z}} = [(\vec{\mathbf{z}}')^T, b-g]^T$. For every positive $\delta < 1/2$, if $|z_{m+1}| = |b-g| \leq \delta a$, then $\|L\vec{\mathbf{z}} - \vec{\mathbf{s}}\|^2 \leq 1+\delta$.*

Proof: Notice that

$$\|D\vec{\mathbf{z}}'\|^2 = P\vec{\mathbf{z}}' = \log_b g = \log_b(b - z_{m+1}) = 1 + \log_b\left(1 - \frac{z_{m+1}}{b}\right).$$

Therefore, using the inequality $|\ln(1+x) - x| < x^2$ valid for all $|x| \leq 1/2$, we have

$$\begin{aligned}
\|L\vec{\mathbf{z}} - \vec{\mathbf{s}}\|^2 &= \|D\vec{\mathbf{z}}'\|^2 + \left(\frac{z_{m+1}}{a}\right)^2 + \beta^2\left(P\vec{\mathbf{z}}' + \frac{z_{m+1}}{b\ln b} - 1\right)^2 \\
&= 1 + \log_b\left(1 - \frac{z_{m+1}}{b}\right) + \left(\frac{z_{m+1}}{a}\right)^2 \\
&\quad + \left(\frac{\beta}{\ln b}\right)^2\left(\ln\left(1 - \frac{z_{m+1}}{b}\right) + \frac{z_{m+1}}{b}\right)^2
\end{aligned}$$

$$
\begin{aligned}
&\leq \ 1 - \frac{z_{m+1}}{b \ln b} + \left(\frac{z_{m+1}}{a}\right)^2 + \left(\frac{\beta}{\ln b}\right)^2 \left(\frac{z_{m+1}}{b}\right)^4 \\
&\leq \ 1 + \delta\left(\frac{a}{b \ln b}\right) + \delta^2 + \delta^4 \left(\frac{a^2 \beta}{b^2 \ln b}\right)^2 < 1 + \delta
\end{aligned}
$$

□

Lemma 4 *For all $0 < \gamma < 1$, $\lambda > 0$ and all large enough n, if b is chosen at random from the set Γ of all products of n distinct primes less than $n^{2+2\gamma^{-1}}$, then with probability exponentially close to 1 there are at least n^n elements $g \in \Gamma$ such that $|b - g| \leq \lambda b^\gamma$.*

Proof: Let m be the number of primes less than $n^{2+2\gamma^{-1}}$. From the prime number theorem we have $m > n^{2+2\gamma^{-1}-\gamma/3}$ for all large enough n, and $|\Gamma| = \binom{m}{n} \geq \left(\frac{m}{n}\right)^n \geq n^{\left(1+\frac{2}{\gamma}-\frac{\gamma}{3}\right)n}$. Notice that $\Gamma \subseteq [0, n^{(2+2\gamma^{-1})n}]$. Divide $[0, n^{(2+2\gamma^{-1})n}]$ into $k = n^{\left(\frac{2}{\gamma}-\frac{2\gamma}{3}\right)n}$ intervals each of size $n^{\left(2+\frac{2\gamma}{3}\right)n}$. Let I_b the interval containing b. We will prove that with probability exponentially close to one $|g - b| < \lambda b^\gamma$ for all $g \in I_b$, and $|I_b \cap \Gamma| > n^n$. Let $g \in I_b$. We have $|g - b| < |I_b|$ and

$$
\begin{aligned}
\Pr(|I_b| > \lambda b^\gamma) &= \Pr\left(b < \lambda^{-\frac{1}{\gamma}} \cdot |I_b|^{\frac{1}{\gamma}}\right) \leq \frac{\lambda^{-\frac{1}{\gamma}} \cdot |I_b|^{\frac{1}{\gamma}}}{|\Gamma|} \\
&\leq \frac{\lambda^{-\frac{1}{\gamma}} \cdot n^{\left(\frac{2}{\gamma}+\frac{2}{3}\right)n}}{n^{\left(1+\frac{2}{\gamma}-\frac{\gamma}{3}\right)n}} = \lambda^{-\frac{1}{\gamma}} \cdot n^{-\left(\frac{1-\gamma}{3}\right)n}.
\end{aligned}
$$

To bound the size of $I_b \cap \Gamma$, observe that each interval I_b is chosen with probability $|I_b \cap \Gamma|/|\Gamma|$. Therefore we have

$$
\begin{aligned}
\Pr(|I_b \cap \Gamma| < n^n) &= \Pr\left(\Pr(I_b) < \frac{n^n}{|\Gamma|}\right) = k \cdot \frac{n^n}{|\Gamma|} \\
&= n^n \cdot n^{\left(\frac{2}{\gamma}-\frac{2\gamma}{3}\right)n}/|\Gamma| \leq \frac{n^{\left(1+\frac{2}{\gamma}-\frac{2\gamma}{3}\right)n}}{n^{\left(1+\frac{2}{\gamma}-\frac{\gamma}{3}\right)n}} = n^{-\left(\frac{\gamma}{3}\right)n}.
\end{aligned}
$$

□

Lemma 5 *For all* $\alpha_1, \alpha_2 > 0$*, there exists* $\delta_1, \delta_2, \delta_3 \in (0,1)$ *so that for all sufficiently large* n *the following holds: Assume that* (S, X) *is an* n*-uniform hypergraph,* $n^2 \leq |S| \leq n^{\alpha_1}$*,* $|X| \geq 2^{\alpha_2 n \lg n}$*,* $k = n^{\delta_1}$ *and* $C_1, \ldots, C_k$ *is a random sequence of pairwise disjoint subsets each with exactly* $|S|n^{-(1+\delta_2)}$ *elements, with uniform distribution on the set of all sequences with these properties. Then, with probability of at least* $1 - n^{-\delta_3}$ *the following holds: for each* $f \in \{0,1\}^k$ *there is a* $T \in X$ *so that* $f(j) = |C_j \cap T|$ *for all* j*.*

Proof: See Theorem 2.2 in [2]. $\square$

We can now prove lemma 1. Let ϵ be a positive constant less than $1/2$ and let k be a sufficiently large integer. Let $\delta_1, \delta_2, \delta_3$ be the constant defined in lemma 5 with $\alpha_1 = 2 + 4\epsilon^{-1}$ and $\alpha_2 = 1$. Let $n = k^{1/\delta_1}$. Let L be the matrix defined in lemma 2 with $p_1, \ldots, p_m$ the set of all primes less than $n^{2+4\epsilon^{-1}}$ and b chosen at random among the products of n distinct such primes.

From lemma 2 we know that $\|L\vec{\mathbf{z}}\|^2 > 2 - \epsilon$ for all non-zero $\vec{\mathbf{z}} \in Z^{m+1}$.

Let $C \in \{0,1\}^{k \times (m+1)}$ be the matrix defined by $C_{i,j} = 1$ iff $j \in C_i$, where $C_1, \ldots, C_k$ are the sets defined in lemma 5 with $S = \{p_1, \ldots, p_m\}$.

For every $\vec{\mathbf{x}} \in \{0,1\}^k$, let $f(j)$ be the function $f(j) = x_j$. Define X to be the set of all $T \subseteq S$ such that $|T| = n$ and $|b - \Pi_{t \in T} t| \leq \frac{\delta b^{\epsilon/2}}{3}$. From lemma 4 (with $\gamma = \epsilon/2$ and $\lambda = \epsilon/3$) we have $|X| \geq n^n = 2^{n \lg n}$, and from lemma 5 there exists a $T \in X$ such that $|C_j \cap T| = f(j)$ for all j. Let $\vec{\mathbf{z}}' \in \{0,1\}^m$ be the indicator vector of the set T, $g = \Pi_{t \in T} t$ and define the vector $\vec{\mathbf{z}} = [(\vec{\mathbf{z}}')^T | b - g]^T$. Notice that $|z_{m+1}| \leq \frac{\delta b^{\epsilon/2}}{3}$. We have $C\vec{\mathbf{z}} = \vec{\mathbf{x}}$, and from lemma 2, $\|L\vec{\mathbf{z}}\|^2 \leq 1 + \epsilon$.

References

[1] L. Adleman, Factoring and Lattice Reduction, *Manuscript*, 1995, cited in [2]

[2] M. Ajtai, "The Shortest Vector Problem in L_2 is NP-hard for Randomized Reductions", *Electronic Colloquium on Computational Complexity*, 1997, http://www.eccc.uni-trier.de/eccc/

[3] S. Arora, L. Babai, J. Stern, Z. Sweedyk, "The Hardness of Approximate Optima in Lattices, Codes, and Systems of Linear Equations", *Proc.*

34th Annual Symposium on Foundation of Computer Science, 1993, pp. 724-733.

[4] M. Bellare, S. Goldwasser, C. Lund, A. Russel, "Efficient Multi-Prover Interactive Proofs with Applications to Approximation Problems", In *Proc. 25th ACM Symp. on Theory of Computing*, 1993, pp. 113-131.

[5] J.Y. Cai, A. Nerurkar, "Approximating the SVP to within a factor $(1 + 1/dim^{-\epsilon})$ is NP-hard under randomized reductions", Manuscript.

[6] O. Goldreich, S. Goldwasser, "On the Limits of Non-Approximability of Lattice Problems", preliminary version in ECCC TR97-031, http://www.eccc.uni-trier.de/eccc.

[7] R.M. Karp, "Reducibility among combinatorial problems", Miller and Thatcher eds., *Complexity of Computer Computations*, 1972, Plenum Press, pp. 85-103.

[8] R. Kannan, "Minkowski's convex body theorem and integer programming", *Mathematics of Operation Research*, 12/3, 1987.

[9] C. Lund, M. Yannakakis, "On the Hardness of Approximating Minimization Problems", *Journal of the ACM*, 41(5):960-981. Prelim. version in STOC'93.

[10] P. van Emde Boas. "Another NP-complete problem and the complexity of computing short vectors in a lattice", *Tech. Report 81-04*, Math Inst. Univ. Amsterdam, 1981.