Electronic Colloquium on Computational Complexity, Report No. 16 (1998)

The Shortest Vector in a Lattice is Hard to Approximate to within Some Constant. (preliminary version)

Daniele Micciancio*

MIT Laboratory for Computer Science
Cambridge, MA 02139

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 $c < \sqrt{2}$. We also give a deterministic reduction based on a number theoretic conjecture.

*email: miccianc@theory.lcs.mit.edu.

ISSN 1433-8092

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. We also give a deterministic reduction based on a reasonable number theoretic conjecture.

The first intractability results for lattice problems date back to [11] where van Emde Boas proved that the closest vector problem (CVP) is NP-hard and conjectured that the shortest vector problem (SVP) was also NP-hard.

Since then, the hardness result for CVP was considerably strenghtned: CVP was proved NP-hard to approximate within any constant factor in [3] and within a factor $2^{\lg^{(1-\epsilon)} n}$ in [6]. Despite the similarities between the two problems, progress in proving the hardness of SVP has been much slower. Even for the exact version of this problem, proving the conjectured NP-hardness remained an open problem for a long time. Finally, 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. In [5] the inapproximability factor is improved 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 was shown NP-hard to approximate 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 simpler proof and a stronger result.

The rest of the paper is organized as follows. In section 2 we formally define the approximation problems associated to SVP, CVP and a variant of the latter. In section 3 we prove that the SVP is NP-hard to approximate by reduction from the modified CVP using a technical lemma which is proved in sections 4 and 5. The proof in section 4 results in a randomized reduction. The proof in section 5 uses a number theoretic conjecture, but gives a deterministic reduction.

2 Definitions

Let $\vec{\mathbf{x}}$ be a vector in R^n. For any $p \geq 1$ let $\|\vec{\mathbf{x}}\|_p = (\sum x_i^p)^{1/p}$ be the p-norm of $\vec{\mathbf{x}}$. The results in this paper hold, with the obvious modifications, for any p-norm. However, for notational convenience we will concentrate on the euclidean norm $\|\cdot\|_2$ which we will abbreviate with $\|\cdot\|$. Moreover, in most of the proofs it will be more convenient to work with the squared norm $\|\cdot\|^2$. In order to maintain the notation uniform throughout the paper and avoid possible confusions, we will always use the squared norm $\|\vec{\mathbf{x}}\|^2$ to measure the length of a vector $\vec{\mathbf{x}}$.

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 [7].

Definition 1 (Approximate SVP) *The promise problem* $\texttt{GapSVP}_g$*, where* g *(the gap function) is a function of the dimension, is defined as follows:*

- 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* $\|V\vec{\mathbf{z}}\|^2 > gd$ *for all* $\vec{\mathbf{z}} \in Z^n \setminus \{\vec{\mathbf{0}}\}$*.*

Definition 2 (Approximate CVP) *The promise problem* $\texttt{GapCVP}_g$*, where* g *(the gap function) is a function of the dimension, is defined as follows:*

- YES *instances are triples* $(V, \vec{\mathbf{y}}, d)$ *where* $V \in Z^{k \times n}$*,* $\vec{\mathbf{y}} \in Z^k$*,* $d \in R$ *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* $V \in Z^{k \times n}$*,* $\vec{\mathbf{y}} \in Z^k$*,* $d \in R$ *and* $\|V\vec{\mathbf{z}} - \vec{\mathbf{y}}\|^2 > gd$ *for all* $\vec{\mathbf{z}} \in Z^n$*.*

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* $\texttt{GapCVP}'_g$*, where* g *(the gap function) is a function of the dimension, is defined as follows:*

- YES *instances are triples* $(V, \vec{\mathbf{y}}, d)$ *where* $V \in Z^{k \times n}$, $\vec{\mathbf{y}} \in Z^k$, $d \in R$ *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* $V \in Z^{k \times n}$, $\vec{\mathbf{y}} \in Z^k$, $d \in R$ *and* $\|V\vec{\mathbf{z}} - w\vec{\mathbf{y}}\|^2 > gd$ *for all* $\vec{\mathbf{z}} \in Z^n$ *and all* $w \in Z$.

In [3] is it proved that $\texttt{GapCVP}_c$ and its variant $\texttt{GapCVP}'_c$ are NP-hard for any constant c.

3 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 (probabilistic) polynomial time 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* $\vec{\mathbf{z}} \in Z^m$, $\|L\vec{\mathbf{z}}\|^2 > 2$.
- *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 1 *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 $\texttt{GapCVP}'_c$ to $\texttt{GapSVP}_g$ with $c = 2/\epsilon$ and $g = 2/(1 + 2\epsilon)$.

Let $(N, \vec{\mathbf{y}}, d)$ be an instance of $\texttt{GapCVP}'_c$. We define an instance (V, t) of $\texttt{GapSVP}_g$ such that if $(N, \vec{\mathbf{y}}, d)$ is a YES instance of $\texttt{GapCVP}'_c$ then (V, t) is a

YES instance of $\texttt{GapSVP}_g$, and if $(N, \vec{y}, d)$ is a NO instance of $\texttt{GapCVP}'_c$ then (V, t) is a NO instance of $\texttt{GapSVP}_g$.

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

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

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

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

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

  i.e., (V, t) is a YES instance of $\texttt{GapSVP}_g$.

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

□

4 Proof of the Technical Lemma

To prove lemma 1 we need a result from [2] and three other lemmas. Lemma 2 and Lemma 3 will also be used in the next section.

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

$$\begin{aligned}
\|L\vec{\mathbf{z}} - \vec{\mathbf{s}}\|^2 &= \|D\vec{\mathbf{z}}'\|^2 + \left(\frac{z_{m+1}}{a}\right)^2 + \beta^2\left(P\vec{\mathbf{z}}' + \frac{z_{m+1}}{b\ln b} - 1\right)^2 \\
&= 1 + \log_b\left(1 - \frac{z_{m+1}}{b}\right) + \left(\frac{z_{m+1}}{a}\right)^2 \\
&\quad + \left(\frac{\beta}{\ln b}\right)^2\left(\ln\left(1 - \frac{z_{m+1}}{b}\right) + \frac{z_{m+1}}{b}\right)^2 \\
&\leq 1 - \frac{z_{m+1}}{b\ln b} + \left(\frac{z_{m+1}}{a}\right)^2 + \left(\frac{\beta}{\ln b}\right)^2\left(\frac{z_{m+1}}{b}\right)^4 \\
&\leq 1 + \delta\left(\frac{a}{b\ln b}\right) + \delta^2 + \delta^4\left(\frac{a^2\beta}{b^2\ln b}\right)^2 < 1+\delta
\end{aligned}$$

□

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 $|\Gamma| = \binom{m}{n} > \left(\frac{m}{n}\right)^n > n^{\left(1+\frac{2}{\gamma}-\frac{\gamma}{3}\right)n}$. 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]. □

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, $\|L\vec{\mathbf{z}}\|^2 \leq 1 + \epsilon$.

5 A Deterministic Reduction

In this section we show how the proof of the technical lemma can be made deterministic using a number theoretic conjecture. The conjecture is the following.

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

We remark that altough the above conjecture is a plausible one, proving it is probably beyond the the possibilities of current mathematics.

We now show that if the above conjecture is true, then there exists a deterministic algorithm satisfying the requirements of Lemma 1. Let ϵ be a positive real between 0 and 1. Let d be such that for all large enough γ there exists a $(\log^d \gamma)$-smooth square-free integer in the interval $[\gamma, \gamma + \gamma^{\epsilon/3}]$. Let $L \in R^{(m+2) \times (m+1)}$ be the matrix defined in Lemma 2 with $b = \left(\frac{3 \cdot 4^{k^2}}{\epsilon}\right)^{6/\epsilon}$, $m = k + \log^d b$, $p_1, \ldots p_k$ distinct prime numbers of size between k and $2k$, and $p_{k+1}, \ldots, p_m$ the first $m - k$ prime numbers. Let $\vec{\mathbf{s}} \in R^{m+2}$ be the

vector defined in Lemma 3. Finally, let $C \in \{0,1\}^{k \times (m+1)}$ be the matrix $C = [I_k | 0_{k \times (m+1-k)}]$.

From Lemma 2 we know that for all non-zero $\vec{\mathbf{z}} \in Z^{m+1}$, $\|L\vec{\mathbf{z}}\|^2 \geq (2-\epsilon)$. It remains to prove that for all $\vec{\mathbf{x}} \in \{0,1\}^k$ there exists a $\vec{\mathbf{z}} \in Z^{m+1}$ such that $C\vec{\mathbf{z}} = \vec{\mathbf{x}}$ and $\|L\vec{\mathbf{z}} - \vec{\mathbf{s}}\|^2 < 1+\epsilon$. Fix some $\vec{\mathbf{x}} \in \{0,1\}^k$ and define $\alpha = \Pi_{i=1}^k p_i^{x_i}$ and $\gamma = \lfloor b/\alpha \rfloor$. Notice that $\alpha < 4^{k^2}$ and $\gamma > 4^{5k^2}$. Therefore, for all sufficiently large k, the interval $[\gamma, \gamma + \gamma^{\epsilon/3}]$ must contain a square-free $(m-k)$-smooth integer, i.e., there exists a vector $\vec{\mathbf{y}} \in \{0,1\}^{m-k}$ such that $\Pi_{i=1}^{m-k} p_{k+i}^{y_i} = \gamma + \delta$ for some $\delta < \gamma^{\epsilon/3} < b^{\epsilon/3}$. Let $g = \Pi_{i=1}^m p_i^{z_i} = \alpha(\gamma+\delta)$ and define the vector

$$\vec{\mathbf{z}} = \begin{bmatrix} \vec{\mathbf{x}} \\ \vec{\mathbf{y}} \\ b-g \end{bmatrix}.$$

$C\vec{\mathbf{z}} = \vec{\mathbf{x}}$ is obviously true. To prove $\|L\vec{\mathbf{z}} - s\|^2 < 1+\epsilon$, notice that

$$|b-g| = \alpha \left| \frac{b}{\alpha} - (\gamma+\delta) \right| = \alpha \left| \frac{b}{\alpha} - \left\lfloor \frac{b}{\alpha} \right\rfloor - \delta \right| \leq \alpha\delta < 4^{k^2} b^{\epsilon/3} = (\epsilon/3) b^{\epsilon/2}$$

and apply Lemma 3.

Theorem 2 *If Conjecture 1 holds true, than there exists a deterministic algorithm satisfying the conditions of Lemma 1.*

Corollary 1 *If Conjecture 1 holds true, than* $\texttt{GapSVP}_c$ *is NP-hard for any* $c < 2$.

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, (available at http://www.eccc.uni-trier.de/eccc/). To appear also in *Proc. 30th ACM Symp. on Theory of Computing*, 1998.

[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, 1997.

[6] I. Dinur, G. Kindler, S. Safra, "Approximating-CVP to within almost-polynomial factors is NP-hard", Manuscript, 1998.

[7] 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.

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

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

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

[11] 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.

ECCC ISSN 1433-8092
http://www.eccc.uni-trier.de/eccc
ftp://ftp.eccc.uni-trier.de/pub/eccc
ftpmail@ftp.eccc.uni-trier.de, subject 'help eccc'