SURPRISINGLY DIFFICULT LATTICE PROBLEMS

WAI LEE CHIN FEMAN

Abstract. I will give a brief description of lattices and the computational problems associated with them. A lattice is a set of vectors; the two main problems associated with lattices are: finding a lattice's shortest vector, and finding the closest vector to a target vector. As we will see, there are several different ways of formulating these problems. I will investigate the computational difficulty of various formulations, and explain reductions between computational problems. I will then sketch the proof of a very interesting combinatorial result concerning lattices.

Contents

1. Basics

A lattice is simply a linear operator whose arguments come from $\mathbb{Z}$.

Definition 1.1. A lattice basis in $\mathbb{R}^m$ is a set of n linearly independent vectors $(\mathbf{b_1}, \ldots, \mathbf{b_n}) \in \mathbb{R}^m$. If we set these vectors to be the columns of a matrix, we get a linear operator $\mathbf{B} = [\mathbf{b_1}, \ldots, \mathbf{b_n}] \in \mathbb{R}^{m\times n}$ in $\mathbb{R}^m$ where $n \leq m$

Definition 1.2. A lattice in $\mathbb{R}^m$ is defined as the set of integral combinations of its associated lattice basis.

$$L(\mathbf{B}) = \left\{ \sum_{i=1}^{n} x_i \mathbf{b_i} : x_i \in \mathbb{Z} \right\} \tag{1.3}$$

We can also think of this as $\{\mathbf{Bx} : \mathbf{x} \in \mathbb{Z}^m\}$.
It is clear that two lattice bases can describe the same lattice. Among the multiple bases describing a given lattice, some are *reduced*. The concept of a reduced basis

Date: DEADLINE AUGUST 22, 2008.

is key for solving SVP (see later) in dimensions higher than 2. See Complexity of Lattice Problems Chapter 2 Section 3.

Definition 1.4. A sublattice $\mathbf{A}$ of another lattice $\mathbf{B}$ is a lattice whose points are all contained in $\mathbf{B}$.

Definition 1.5. Given computational problems A and B, A is *reducible* to B if, having a way of instantly finding answers to arbitrary instances of B allows for some easy method of solving arbitrary instances of A. The source of information concerning B is called an "*oracle*" to B. The algorithm for using the answers of B in order to find answers to A is called the "reduction algorithm."

There are different kinds of reductions between problems. For example, solving an instance of A might require having the answer to a single instance of B or to multiple instances of B. Consider the following definition for another kind of reduction.

Definition 1.6. RUR reduction stands for "reduced unfaithful randomized" reduction; a RUR reduction consists of a reduction algorithm and a probability p, and can only reduce decisional problems to other problems. Suppose we have a decisional problem A and we have a RUR reduction from A to B. If the reduction algorithm outputs "NO," then we can be sure that the answer to A is "NO." However, if the algorithm outputs "YES," then we only know that the answer to A is "YES" with probability p. p is called the "completeness error."

1.1. **Computational problems associated with lattices.** The two problems I will discuss are SVP and CVP. Determining relatively simple pieces of information about lattices can show itself to be quite difficult. We will show that CVP is NP-hard in dimension N, and give a reduction from SVP to CVP.

Definition 1.7. The Decisional Shortest Vector Problem (SVP): An instance of SVP consists of the pair $(\mathbf{B}, r)$ where $\mathbf{B}$ is a lattice basis and r is some rational number. A solution to decisional SVP is a program which accepts such an instance and decides whether there exists some nonzero integer vector $\mathbf{x}$ satisfying $\|\mathbf{Bx}\| \leq r$ (under a fixed norm) in the given lattice.

Definition 1.8. The Search Shortest Vector Problem (SVP): An instance of search SVP consists of a lattice basis $(\mathbf{B})$. It searches the lattice associated with $(\mathbf{B})$ and returns the shortest nonzero vector in this lattice.

At this point, I should make the following remark. Given an oracle to decisional SVP, one can find the shortest vector of any lattice in polynomial time. In other words, one can reduce Search SVP to Decisional SVP.

Definition 1.9. The Promise Shortest Vector Problem$_\gamma$: An instance of the Promise SVP$_\gamma$ consists of a lattice basis and a rational number $(\mathbf{B}, \mathbf{r})$. A solution to the Promise SVP$_\gamma$ accepts an instance of the problem and outputs YES if:

$$\exists \mathbf{x} \neq 0 : \|\mathbf{Bx}\| \leq r \tag{1.10}$$

and it outputs NO if:

$$\forall \mathbf{y} \in \mathbb{Z}^m \qquad \|\mathbf{By}\| > \gamma \cdot r \tag{1.11}$$

Definition 1.12. The Promise Closest Vector Problem$_\gamma$: An instance of the Promise CVPγ consists of the triple $(\mathbf{B}, \mathbf{t}, r)$ where $\mathbf{B}$ is a lattice basis, $\mathbf{t}$ is a target vector (not necessarily in the lattice), r is a rational number. A solution to the Promise CVP$_\gamma$ accepts an instance of the problem and outputs YES if:

$$\exists \mathbf{x} : \|\mathbf{Bx} - \mathbf{t}\| \leq r \tag{1.13}$$

and it outputs NO if:

$$\forall \mathbf{y} \in \mathbb{Z}^m \qquad \|\mathbf{By} - \mathbf{t}\| > \gamma \cdot r \tag{1.14}$$

2. Closest Vector Problem

2.1. **Reduction of SVP to CVP.** There are (at least) two ways of reducing SVP to CVP. The first involves asking our CVP oracle to solve N instances of CVP, but is a deterministic reduction. The second only involves asking the CVP oracle to solve one instance of CVP, but it is an RUR reduction with completeness error of 1/2. We will begin with a lemma, which is neat enough that it provides motivation for itself.

Lemma 2.1. *Let* $\mathbf{v} = \sum_{i=1}^{n} c_i \mathbf{b_i}$ *be a shortest non-zero vector in a lattice* $\mathbf{B}$ *Then* $\exists i$ *such that* c_i *is odd.*

Proof. Assume that every c_i is even. Consider a shortest vector $\mathbf{Bv}$ in $\mathbf{L}(\mathbf{B})$. $\mathbf{Bv} = \sum_{i=1}^{n} c_i \mathbf{b_i}$. Now, consider the vector $\mathbf{v'} = (1/2)\mathbf{v} = \sum_{i=1}^{n} \frac{c_i}{2} b_i$. $\mathbf{v'}$ is clearly a vector in $\mathbf{L}(\mathbf{B})$ and it is strictly shorter than $\mathbf{v}$; this is a contradiction. □

2.2. **RUR Reduction.** In this section I will show a nondeterministic (randomized) reduction of promise SVP to promise CVP. Suppose we are working with an arbitrary lattice L. Ideally, we would like to be able to simply use our CVP oracle to check if there is a vector close to $(0, 0)$ in L. This, however, is not possible, because of the case where the lattice contains the vector $(0, 0)$. We want our oracle to check for some *nonzero* vector close to $(0, 0)$, but the CVP oracle will just see the vector $(0, 0)$ and conclude that this is the desired short vector. This is wrong.

Theorem 2.2. *For an arbitrary function* $\gamma : \mathbb{N} \to [1, \infty]$*, there is a RUR reduction from Promise SVP*$_\gamma$ *to promise CVP*$_\gamma$ *with a completeness error of at most 1/2.*

Proof. Consider an arbitrary $\mathbf{B} = [\mathbf{b_1}, \ldots, \mathbf{b_n}]$. Suppose that $(\mathbf{B}, \mathbf{r})$ is a SVP instance. We will create an instance of CVP based on $(\mathbf{B}, \mathbf{r})$. Define $\mathbf{B'} = [\mathbf{b'_1}, \ldots, \mathbf{b'_n}]$ as follows:

Let $c_1 = 1$ and for $2 \leq i \leq n$, choose $c_i \in \{0, 1\}$ at random. Now, for each i, define $\mathbf{b'_i} = \mathbf{b_i} + c_i \mathbf{b_1}$.

It remains to show that, as an instance of Promise CVP$_\gamma$, (B', b_1, r) satisfies Def. 1.6. Suppose that (B', b_1, r) does not solve to NO. This implies that,

$$\exists \mathbf{v} \in L(B') \text{ satisfying } \|\mathbf{v} - \mathbf{b_1}\| \leq \gamma(n) \cdot r. \tag{2.3}$$

Note that $L(\mathbf{B'})$ is a sublattice of $L\mathbf{B}$, and b_1 is not in $L(\mathbf{B'})$. Now consider the vector $\mathbf{v'} = \mathbf{v} - \mathbf{b_1}$. $\mathbf{v'}$ is clearly nonzero since $\mathbf{b_1}$ is not in the lattice containing v; moreover, it satisfies (2.3). These two conditions show that $(\mathbf{B}, r)$ does not solve to NO. Halfway there!

Assume, now, that $(\mathbf{B}, r)$ solves to YES. Let $\mathbf{v} = \sum_{i=1}^{n} x_i \mathbf{b_i}$ be the shortest vector in $L(\mathbf{B})$. Now, from Theorem 2.1, we know that x_j is odd for some j.

Let $\alpha = x_1 + 1 - \sum_{i>1} c_i x_i$. Now, with probabililty 1/2, α is even and therefore $\mathbf{u} = (\alpha/2)\mathbf{b_1}' + \sum_{i>1} x_i \mathbf{b_i}'$ is contained in $\mathbf{L}(\mathbf{B}')$ Now,

$$\mathbf{u} - \mathbf{b_1} = \left(\alpha \mathbf{b_1} + \sum_{i>1} x_i(\mathbf{b_i} + c_i \mathbf{b_1})\right) - \mathbf{b_1} \tag{2.4}$$

$$= (x_1 - \sum_{i>1} c_i x_i)\mathbf{b_1} + \sum_{i>1} x_i \mathbf{b_i} + \sum_{i>1} x_i c_1 \mathbf{b_1} = \mathbf{v}. \tag{2.5}$$

This shows that $(\mathbf{B}', \mathbf{b_1}, r)$ solves to YES.

□

2.3. **CVP is NP Hard.** We can show that gap CVP_γ is NP Complete by reducing the Subset Sum problem to it. It is well-known that Subset Sum is NP Hard, and so this reduction will imply that CVP is NP Hard. As we will see, given an instance I of Subset SumP, it is relatively easy to compute (in polynomial time) an instance S of Gap CVP_γ where the answer to I is yes if and only if the answer to S is yes.

Definition 2.6. An instance of the Subset Sum problem consists of a set $S = \{s_i, \ldots, s_n\}$ of integers and a target integer t. The problem consists of deciding whether there exists some vector $x = \{x_1 \ldots x_n\}$ satisfying $x_i \in \{0, 1\}, |S| = |X|$, and,

$$\sum_{i=1}^{n} (x_i \cdot s_i) = t \tag{2.7}$$

Theorem 2.8. *Subset Sum is polynomial-time reducible to gap* CVP_1 *in the* l_p *norm.*

Proof. Suppose we have an arbitrary instance of Subset Sum $S = \{s_i, \ldots, s_n\}$ and t =some integer. We will construct a new lattice basis:

$$\mathbf{b_i} = [s_i, \overbrace{0, \ldots, 0}^{i-1}, 2, \overbrace{0, \ldots, 0}^{n-i}]^T \tag{2.9}$$

and a target vector:

$$\mathbf{t} = [s, \underbrace{1, \ldots\ldots, 1}_{n}]^T \tag{2.10}$$

and finally a radius r (see (1.11)):

$$r = \sqrt[p]{n} \tag{2.11}$$

In matrix notation, the matrix representing this basis would look like,

$$B = \begin{bmatrix} a \\ 2\mathrm{I}_n \end{bmatrix} \tag{2.12}$$

Where $\mathbf{a}$ is the row vector $[a_1 \ldots a_n]$.

It remains to show that Promise CVP_1 with the aforementioned target vector and lattice basis has the answer "yes" if and only if our given instance of subset sum is solvable.

Now, assume that there exists a solution to the Subset Sum instance in consideration. If x is some vector satisfying $\sum_{i=1}^{n}(x_i \cdot s_i) = t$, then we have

$$\mathbf{Bx} - \mathbf{t} = \begin{bmatrix} \sum_{i=1}^{n}(x_i \cdot s_i) - s \\ 2x_i - 1 \\ \vdots \\ 2x_n - 1 \end{bmatrix} \tag{2.13}$$

The pth power of the l_p norm of this distance is therefore,

$$\|\mathbf{Bx} - \mathbf{t}\| = |\sum_{i=1}^{n}(x_i \cdot s_i) - s|^p + \sum_{i=1}^{n}|2x_i - 1|^p \tag{2.14}$$

Because x is a solution to the subset sum problem, (2.14) simplifies to n. Therefore, n is an upper bound on the pth power of the distance of t from $\mathbf{L}(\mathbf{B})$. So, the distance from t to $\mathbf{L}(\mathbf{B})$ is at most $\sqrt[p]{n}$. Therefore, the CVP instance consisting of $(\mathbf{B}, \mathbf{t}, \sqrt[p]{n})$ solves to YES.

Finally, assume that the CVP instance consisting of $(\mathbf{B}, \mathbf{t}, \sqrt[p]{n})$ solves to YES. Then, there exists some $\mathbf{x}$ such that, $\|\mathbf{Bx} - \mathbf{t}\| \leq \sqrt[p]{n}$. Now, as in (2.14), we have,

$$\|\mathbf{Bv} - \mathbf{t}\|^p = |\sum_{i=1}^{n}(x_i \cdot s_i) - s|^p + \sum_{i=1}^{n}|2x_i - 1|^p \tag{2.15}$$

Note that we have $\sum_{i=1}^{n}|2x_i - 1|^p \geq n$. So, because $\|\mathbf{Bx} - \mathbf{t}\|^p \leq \sqrt{n}$, the first summand in (2.14) must equal 0; we also must have $\forall i |2x_i - 1|^p = 1$. The first of these facts directly implies that $\sum i = 1^n a_i x_i = s$; the second of these facts implies that $\forall i x_i \in \{0, 1\}$. Therefore, $\mathbf{x}$ is a solution to the associated Subset Sum instance! □

3. Large Domain Theorem

3.1. Hypergraphs.

Definition 3.1. A hypergraph is a set (V, Z). As in a graph, V is a set of vertices. Instead of a set of pairs (defining edges), Z is simply a set of subsets of V.

Definition 3.2. Let $U \subseteq V$ be a set of vertices, and let $\mathbf{T} = (T_1, \ldots, T_n)$, where the T_i are subsets of V. Define the following operator,

$$\mathbf{T}(U) = (|T_1 \cap U|, \ldots, |T_n \cap U|) \tag{3.3}$$

3.2. Large Domain Theorems.

I will sketch a proof of the following theorem:

Theorem 3.4. *Let $T \in \{0, 1\}^{n \times k}$ with each entry set to 1 with probability p. Consider an arbitrary set $Z = \{z_1, \ldots, z_n\}$ with each $s_i \in \{0, 1\}^n$ containing exactly h ones. Let $|Z| > h!|k|^{\frac{4\sqrt{h}n}{\epsilon}}$. Then for any $\mathbf{x} \in \{0, 1\}^k$,*

$$Pr\{\mathbf{x} \in \mathbf{T}(\mathbf{Z})\} > 1 - 5\epsilon \tag{3.5}$$

Where $T(Z)$ represents $\{Tz : z \in Z\}$.

Remark 3.6. Note that T defines a lattice (the columns of T represent the lattice basis). Therefore, T z represents a member of the lattice defined by T.

This theorem, in addition to being really neat, is useful for proving the NP-hardness of approximating SVP.

I will prove (3.4) by sketching the proof of the following equivalent theorem:

Theorem 3.7. *Consider an arbitrary h-regular hypergraph (V, Z) of size $|Z| > h!|V|^{\frac{\sqrt{hn}}{\epsilon}}$. Define $\mathbf{T} = (T_1 \dots T_n)$, where each $T_i \subseteq V$ and each element of V is included in T_i independently with probability $p = \frac{\epsilon}{(hn)}$. Then, for any $\mathbf{x} \in \{0,1\}^n$,*

$$PR\{\mathbf{x} \in \mathbf{T}(\mathbf{Z})\} > 1 - 5\epsilon \tag{3.8}$$

.

Remark 3.9. (3.4) and (3.7) are equivalent.

Proof. Suppose we have an arbitrary operator T and set Z as defined in Thm 3.4. We can associate this pair with a hypergraph as follows:

There will be n vertices, where n is the number of rows in the matrix for T. The set of hyperedges, $\mathbf{Z}$ will be defined in the following way. We will treat each z_i as though it is a characteristic vector of a single (unique) hyperedge (if z_i has a 1 in the n^{th} place, then include the n^{th} vertex in the associated hyperedge). Notice that because each Z_i has h ones, every node in this hypergraph is connected to h other nodes.

Now, we can associate T with a set $\mathbf{T} = (T_1, \dots, T_n)$ where each T_i is the i^{th} row in the matrix representing T.

One simply needs to see that, when z is the characteristic vector of $\mathbf{z}$, we have $\mathbf{T}(\mathbf{z}) = T(z)$. This is because,

$$\mathbf{T}(\mathbf{z}) = (|T_1 \cap \mathbf{z}|, \dots, |T_n \cap \mathbf{z}|) = \sum_{i=1}^{n} z \cdot T_i e_i = T(z) \tag{3.10}$$

So, it is easy to see that, when T and Z are associated with $\mathbf{T}$ and $\mathbf{Z}$ as above, $x \in T(Z)$ iff $x \in \mathbf{T}(\mathbf{Z})$ □

As I am about to explain, (3.7) follows from the following theorem:

Theorem 3.11. *Let (V, Z) be a d-regular hypergraph. Let $T = (T_i, \dots, T_n)$ be a sequence of subsets of V, including each element of V independently with probability p. For each $x \in \{0,1\}^n$,*

$$PR_T\{x \notin T(Z)\} \leq EXP_R(e^{\theta R}) - 1 \tag{3.12}$$

Where $\theta = \frac{np}{1-p} + \frac{n}{pd^2}$ and R is the random variable defined as $|U \cap U'|$ for randomly chosen U and U'.

This inequality is interesting if and only if $EXP_R[e^{\theta R}] - 1 < 1$ (because then it gives us useful information about $PR_T\{x \notin T(Z))$. Moreover, it would be ideal if $EXP_R[e^{\theta R}]$ were very close to 1. Note that,

$$EXP_R[e^{\theta R}] = \sum_{r>0} PR_R(R = r)e^{\theta r} \tag{3.13}$$

According to (3.13), if $PR_R\{R = r\} \geq e^{-\theta r}$ more than once, we get no information about $PR_T\{x \notin T(Z)$. So, in general, we need $PR_R\{R = r\} < e^{-\theta r}$ (if we are going to get any information from the above-established inequality).

Our approach will be to look at a subgraph of (V, Z) where the expected value of R is very low. The rest of the proof of (3.10) involves removing vertices from (V, Z) until we have a subgraph, (V', Z') whose value of R is very small. The proof argues that, if $|Z|$ is very large, then it contains a subgraph where $|Z'|$ is still large and R is small. The proof proceeds to argue that, for this subgraph, $EXP_R[e^{\theta R}]$

will be very close to 1. It is clear that, if $PR_T\{x \notin T(Z'))$ is close to 0, then we also have $PR_T\{\notin T(Z))$ is also close to 0 (which is the desired result).

I will prove (3.11) in two steps. I will prove the following lemma (3.14) and its corollary (3.18). I will use the lemma and its corollary in the proof of (3.11).

Theorem 3.14. *Let* $\mathbf{x} \in \{0,1\}^n$ *and let* $\mathbf{U}, \mathbf{U}' \subset \mathbf{V}$ *be of size* d. *Let* $\mathbf{T} = (T_1 \dots T_n)$ *be defined as in (3.10), including each element of* V *with probability* p. *Then,*

$$\Phi(r) = PR_T\{\mathbf{T}U = x = \mathbf{T}U'\} \tag{3.15}$$

$$= (1-p)^{(2d-r)n}\left(\frac{pr}{1-p} + \left(\frac{p(d-r)}{1-p}\right)^2\right)^{\|x\|_1} \tag{3.16}$$

where $r = |U \cap U'|$ *and* $\|x\|_1$ *is the number of 1's in* $\mathbf{x}$

Proof. Note that the T_i's are chosen independently. Therefore,

$$PR_T\{T(U) = T(U') = x\} = \prod_{i=1}^{n} PR_{T_i}\{|T_i \cap U| = |T_i \cap U'| = x_i\}.$$

Now, it remains to prove that,

$$PR_{T_i}\{|T_i \cap U| = |T_i \cap U'|\} = (1-p)^{(2d-r)}\left(\frac{pr}{1-p} + \left(\frac{p(d-r)}{1-p}\right)^2\right)^{x_i}. \tag{3.17}$$

. Note that the $(2d-r)n$ from before has been replaced with $(2d-r)$. Now, according to (3.16), proving (3.17) gives us the desired result. It is clear that (3.17) holds trivially for the case where $x_i = 0$. The case where $x_i = 1$ is not difficult. When $x_i = 1$, $|T_i \cap U| = |T_i \cap U'| = 1$ in either of two cases. In the first case, T_i contains a single element in $U \cap U'$ and no other elements of U or U'; in the second case, T_i contains one element of U which is outside of U', and one element of U' which is outside of U. Summing these probabilities, we have:

Probability of Case 1: $|U \cap U'| \cdot p(1-p)^{|U \cup U'|-1} = (1-p)^{2d-r}\left(\frac{pr}{1-p}\right)$

Probability of Case 2: $|U \setminus U'| \cdot |U' \setminus U| \cdot p^2(1-p)^{|U \cup U'|-2} = (1-p)^{2d-r}\left(\frac{p(d-r)}{1-p}\right)^2.$

Whose sum equals, $(1-p)^{(2d-r)}\left(\frac{pr}{1-p} + \left(\frac{p(d-r)}{1-p}\right)^2\right).$

Note that in Case 1, there are $(\binom{|U \cap U'|}{1})$ sub-cases, each corresponding to a unique element of $(U \cap U')$ being equal to 1. The probability of each sub-case satisfying $x_i = 1$ is $p(1-p)^{|U \cup U'|-1}$. Case 2 works similarly.

∎

Corollary 3.18. *It immediately follows that, if* $U \subseteq V$ *and* T *is chosen as in the prececding theorem,*

$$PR_T\{T(U) = x\} = \phi(d) = (1-p)^{dn}\left(\frac{pd}{1-p}\right)^{\|x\|_1}. \tag{3.19}$$

Proof. Choose $U = U'$ in the preceding theorem. ∎

Remark 3.20. I will use $EXP_T(V)$ to refer to the expected value of a random variable V over a parameter T.

I will now give the proof of (3.11)

Proof. Let $x \in \{0,1\}^n$ be an arbitrary vector and let T be chosen as described above. Define for all $U \in Z$,

$$X_U = \begin{cases} 1 & \text{if } T(U) = x \\ 0 & \text{if } T(U) \neq x \end{cases}$$

.

Define the random variable $X = \sum_{U \in Z} X_U$.
Now, $X = 0$ iff $x \notin T(Z)$. Therefore,

$$\begin{aligned}
&PR_T\{x \notin T(Z)\} = PR_T\{X = 0\} && (3.21)\\
&\leq PR_T\{|X - EXP[X]| \geq EXP[x]\}. \text{ and by Chebyshev's inequality,} && (3.22)\\
&\leq \frac{VAR[X]}{EXP[X]^2} = \frac{EXP[(X - EXP[X])^2]}{EXP[X]^2} && (3.23)\\
&= \frac{EXP[X^2 - 2XEXP[X] + EXP[X]^2]}{EXP[X]^2} && (3.24)\\
&\text{Note that } EXP[X] \text{ is simply a constant, so we wind up with,} && (3.25)\\
&= \frac{EXP[X^2] - EXP[2X]EXP[X] + EXP[X]^2}{EXP[X]^2} && (3.26)\\
&= \frac{EXP[X^2] - EXP[2X]^2 + EXP[X]^2}{EXP[X]^2} = \frac{EXP[X^2]}{EXP[X]^2} - 1. && (3.27)
\end{aligned}$$

.

Remark 3.28. First note that (3.21) gives (3.22) because the former equation implies the latter (and so the latter occurs at least as frequently as the former).

Now, we need to calculate the expected values of $[X]$ and $[X]^2$.

$$EXP_T[X] = \sum_{U \in Z} EXP_T[X_U] = \sum_{U \in Z} PR_T T(U) = X = |Z| \cdot \Phi(d) \text{ by (3.18)} \tag{3.29}$$

and,

(3.30)

$$EXP_T[X^2] = EXP_T\left[\left(\sum_{U\in Z} X_U\right)^2\right]$$

$$= EXP_T\left[\sum_{U,U'\in Z}[X_U \cdot X'_U]\right] \tag{3.31}$$

$$= \sum_{U,U'\in Z} PR_T\{T(U) = T(U') = x\} \tag{3.32}$$

$$= \sum_{U,U'\in Z} \Phi(|U \cap U'|) \tag{3.33}$$

$$= \sum_{i=1}^{n} N\Phi(i) \text{ where } N \text{ is the number of pairs } U, U' \text{ with } |U \cap U'| = i \tag{3.34}$$

$$= |Z|^2 \cdot EXP_R[\Phi(R)], \text{ where } R \text{ is defined as above}(by(3.14) \tag{3.35}$$

Now,

(3.36)

$$PR_T\{x \notin T(Z)\} = \frac{EXP_R[\Phi(R)]}{\phi(d)^2} - 1$$

$$= EXP_R\left[(1-p)^{-nR}\left(\frac{(1-p)R}{pd^2} + \left(1 - \frac{R}{d}\right)^2\right)^{\|x\|_1}\right] - 1 \tag{3.37}$$

$$< EXP_R\left[\left(1 + \frac{p}{1-p}\right)^{nR}\left(\frac{R}{pd^2} + 1\right)^n\right] - 1 \tag{3.38}$$

$$< EXP_R\left[e^{\frac{pnR}{1-p}} e^{\frac{nR}{pd^2}}\right] - 1 \tag{3.39}$$

$$= EXP_R[e^{\theta R} - 1] \tag{3.40}$$

□

References

[1] Complexity of Lattice Problems *A Cryptographic Perspective*
by Daniele Micciancio and Shafi Goldwasser
Copyright 2002 by Kluwer Academic Publishers Boston/Dordrecht/London