CS 354: Unfulfilled Algorithmic Fantasies May 13, 2019

Lecture 13: Reduction of approximate SVP to average SIS

Lecturer: Aviad Rubinstein *Scribe: Guillermo Angeris*

1 Lattices and definitions

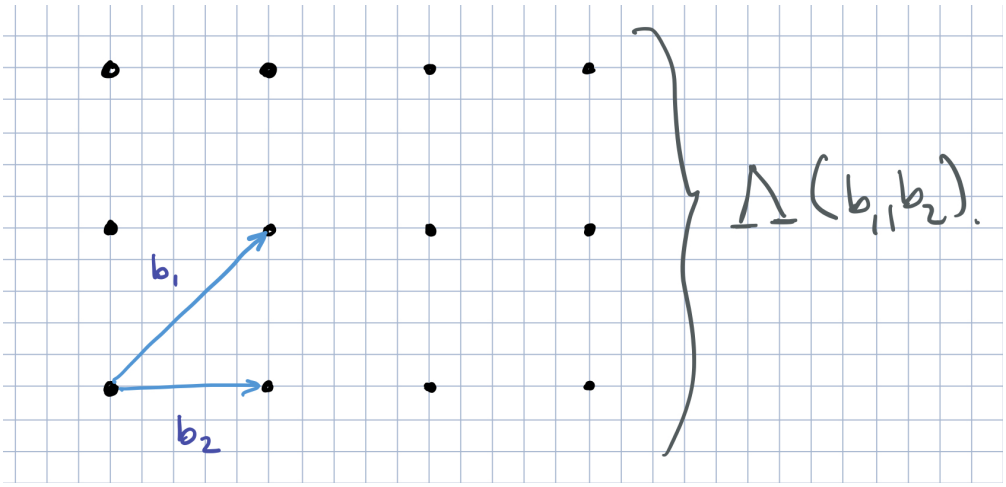

Figure 1: A simple 2D lattice with basis vectors b_1 and b_2.

A *lattice* $\Lambda(b_1, \ldots, b_n)$ is defined as the set of all integral combinations of the basis vectors $b_1, \ldots, b_n$. In other words,

$$\Lambda(b_1, \ldots, b_n) = \left\{ \sum_i b_i c_i \mid c \in \mathbb{Z}^n \right\}$$

see figure 1.

Shortest vector problem (SVP). The *SVP* is to find $x \in \Lambda(b_1, \ldots, b_n) - \{0\}$ such that $\|x\|$ is smallest. Note that this can be in any metric. The only known algorithms are all in exponential time.

Shortest independent vector problem (SIVP). In the SIVP, we seek to minimize the length of the longest vector in the basis. In other words, we seek to find a new basis which yields the same lattice, but minimizes the length of the longest vector.

Dual lattice. We define the *dual lattice* Λ^* of lattice Λ, as the set of vectors whose inner product yields an integer for all points in the lattice. That is,

$$\Lambda^* = \{y \in \mathbf{R}^n \mid x^T y \in \mathbb{Z} \quad \forall x \in \Lambda\}$$

This definition, while not necessarily extremely intuitive, yields a neat, if somewhat technical, theorem by [2] (the proof is based on some results in harmonic analysis). In particular, we have that $1 \leq \mathrm{SVP}(\Lambda) \cdot \mathrm{SIVP}(\Lambda^*) \leq Cn$. As a side note, this definition makes some intuitive sense as the reciprocal lattice can be seen as a "stretched out" (or shrunk, correspondingly) version of the original lattice.

The bound is also essentially tight as stated, up to constants. [3, Theorem 2.5]

Short integer solution (SIS). The SIS is the problem defined as finding some $y \in \{-1, 0, 1\}^n - \{0\}$ with $Ay \equiv 0 \mod q$, for a given $A \in \mathbb{Z}_q^{n \times m}$ and $m \geq n \log q$, to guarantee existence of a solution.

2 Construction and proof sketch

2.1 Theorem statement

We focus on the outline of a proof of the following theorem.

Theorem 2.1. *If finding a* $\mathrm{poly}(n)$ *approximation of* SVP *is hard in the worst case, then the average case complexity (over uniformly sampled matrices) of* SVP *is hard [1], which immediately implies that the average case complexity of* SIS *is hard [4].*

This is a little surprising and worth reiterating—we are saying that, if we can solve SIS efficiently for a uniformly random matrix for, then somehow we can solve the problem approximately for the worst case. This is a reduction that is quite different from most others that we have seen in class.

The usefulness of these problems comes from the fact that they are believed to be hard even for quantum computers, and so could form the basis of quantum-resistant crypto.

2.2 Proof sketch

Step 1. Sample points x_i from the ball (*e.g.*, via a Gaussian) around the origin with radius $R \leq \mathrm{poly}(n) \cdot \mathrm{SIVP}$

Step 2. Let $y_i = x_i$ 'modulo the parallelepiped' (see Figure 2). We can transfer all points by adding or subtracting vectors from the lattice until they land into the unit cell (that we can do this efficiently should also be clear).

Step 3. Fourier analysis (Lemma, skipped). Look at the distribution of y_i (call it P), it can be compared to the uniform distribution over the parallelepiped (call it Q). It turns out that, $\|P - Q\|_{\mathrm{TV}} \leq 2^{-n}$.

Note that we picked the SIVP rather than the SVP. In this case, the smallest basis is completely contained in the ball several times, which means that we're essentially guaranteed to be uniform over the entire parallelepiped.

Step 4. Now, we take the minimal basis and round the y_i to the smallest z_i which is representable in the small basis. In other words, we round y_i down (see Figure 3),

$$z_i = \frac{B\lfloor qB^{-1}y_i \rfloor}{q},$$

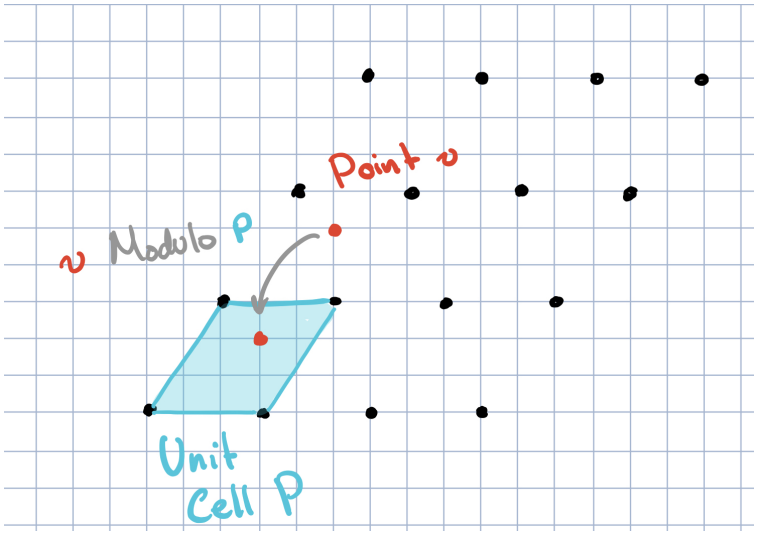

Figure 2: An example showing a point $v \in \Lambda$ modulo the parallelepiped P.

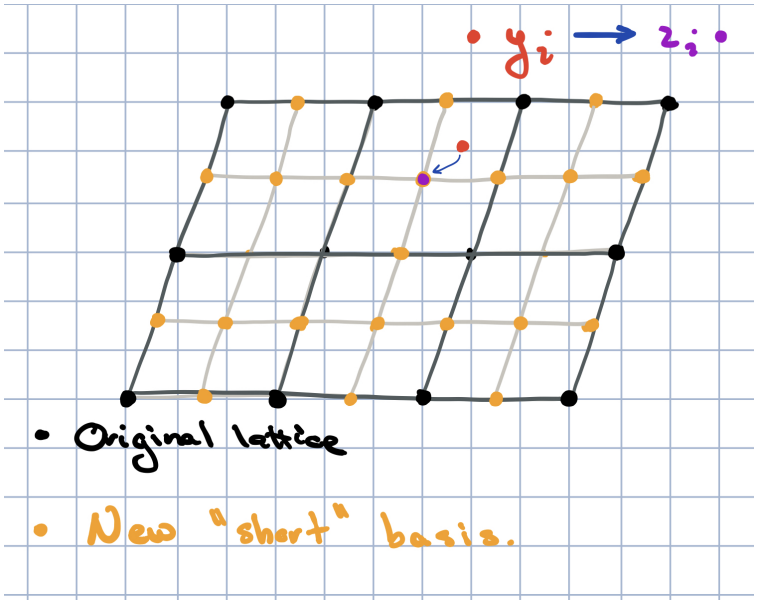

Figure 3: An example showing a point $y_i \in \mathbf{R}^n$ rounded to the (new) short lattice, resulting in a vector z_i.

and we get the corresponding indices in the parallelepiped,

$$a_i = \lfloor qB^{-1}y \rfloor \in \mathbb{Z}_q^n.$$

So now, we have a bunch of a_is which are roughly uniformly distributed among the unit cell—this means we can use out average case SIS oracle on the constructed A, to get

$$b \leftarrow SIS(a_1, \ldots, a_n) \in \{-1, 0, 1\}^n.$$

All that remains (modulo some cheating) is to construct a required solution.

Step 5. Set

$$v = \sum_i b_i(x_i - y_i + z_i).$$

We will prove that this v actually lies in the lattice and that it is small.

Note (a) that $z_i - y_i \in \Lambda$ (exercise for the reader), while we have (b) that

$$\sum_i b_i z_i = B\left(\sum_i \frac{b_i a_i}{q}\right),$$

while we have that, by definition of b as the solution to SIS, $\sum_i b_i a_i \equiv 0 \mod q$. This immediately implies that $\sum_i b_i z_i \in \Lambda$, as required.

Now that we know v is in the lattice, we have to verify that v is small.

First, since we sampled from the ball, we know that $\|x_i\| \leq \text{poly}(n)\text{SIVP}(\Lambda)$, by definition. Now

$$y_i - z_i \leq \frac{\|\text{input basis vector}\|}{q} \leq \text{SIVP}(\Lambda)$$

So, we can take $q = 2^n$ (as we have a poly-time approximation algorithm within exponential factors), which will immediately imply that

$$v = \sum_i b_i(x_i - y_i + z_i) \lesssim \text{poly}(n)\text{SIVP}(\Lambda)$$

All that remains is to show that the vector v is nonzero, which follows with high probability from the following lemma:

Lemma 2.2. *For any $y \in P$ where P is a parallelpiped and any $(n-1)$-dimensional hyperplane H, we have that*

$$\mathbb{P}_{x \in \text{ball}}[x \in H \mid x \equiv y \bmod P] < .9.$$

This proves the final claim as we can repeat the construction enough times to give a good result with high probability.

References

[1] M. Ajtai. Generating hard instances of lattice problems (extended abstract). In *Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing*, STOC '96, pages 99–108, New York, NY, USA, 1996. ACM.

[2] W. Banaszczyk. New bounds in some transference theorems in the geometry of numbers. *Mathematische Annalen*, 296(1):625–635, Dec 1993.

[3] Jin-Yi Cai. A relation of primal-dual lattices and the complexity of shortest lattice vector problem. *Theoretical Computer Science*, 207(1):105 – 116, 1998.

[4] Shai Halevi Oded Goldreich, Shafi Goldwasser. Collision-free hashing from lattice problems. Cryptology ePrint Archive, Report 1996/009, 1996.