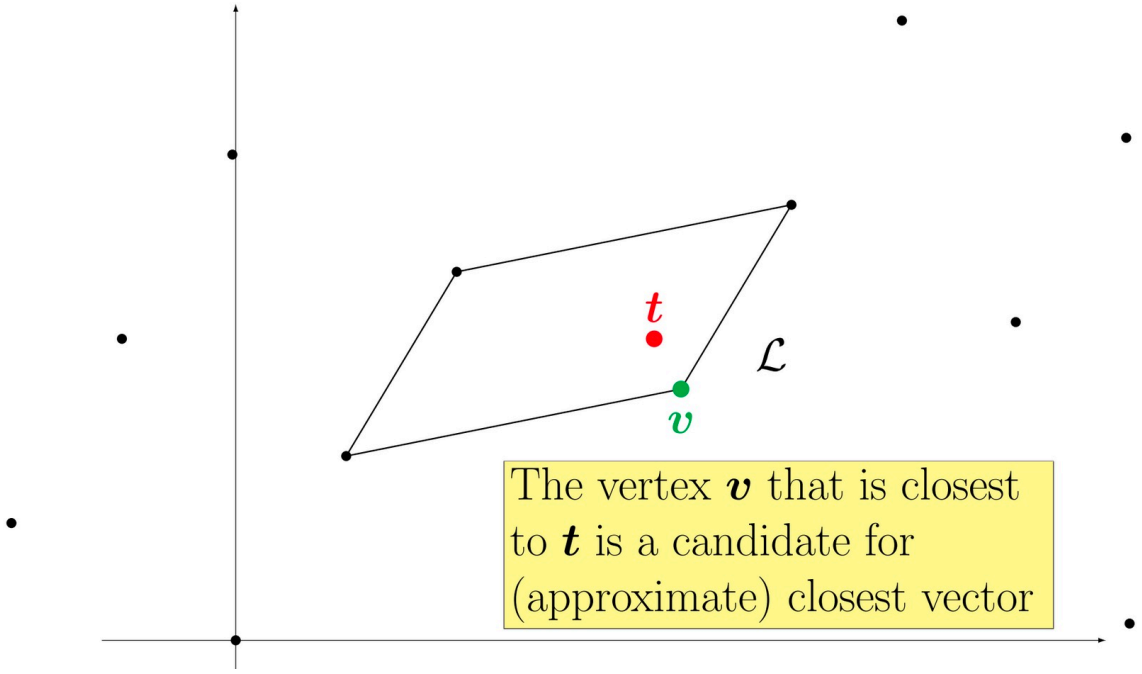
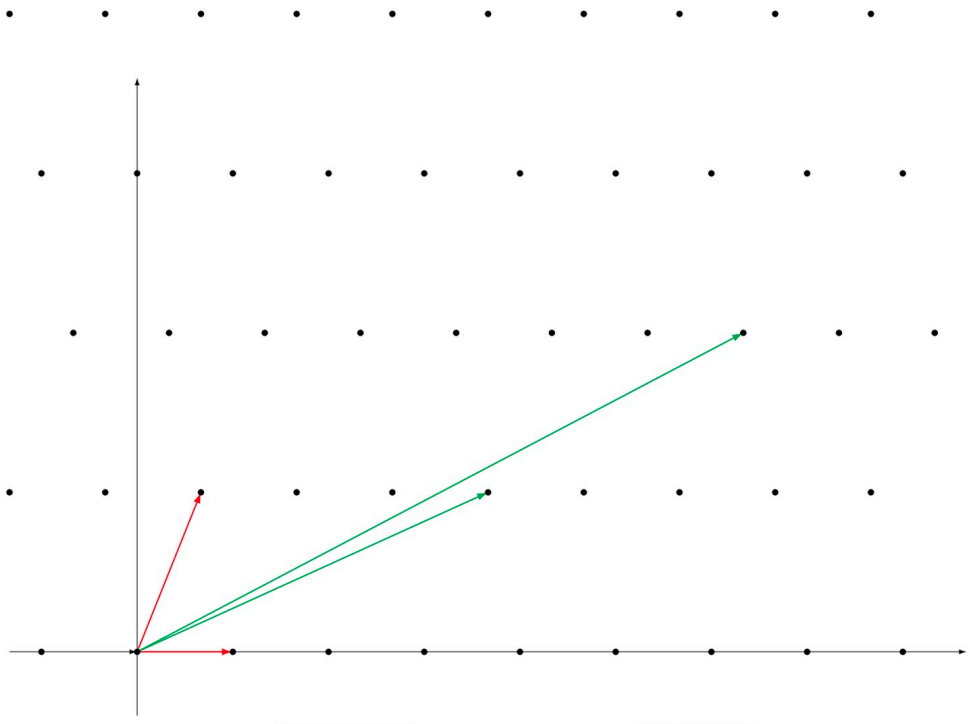
Using a Basis to Try to Solve the Closest Vector Problem

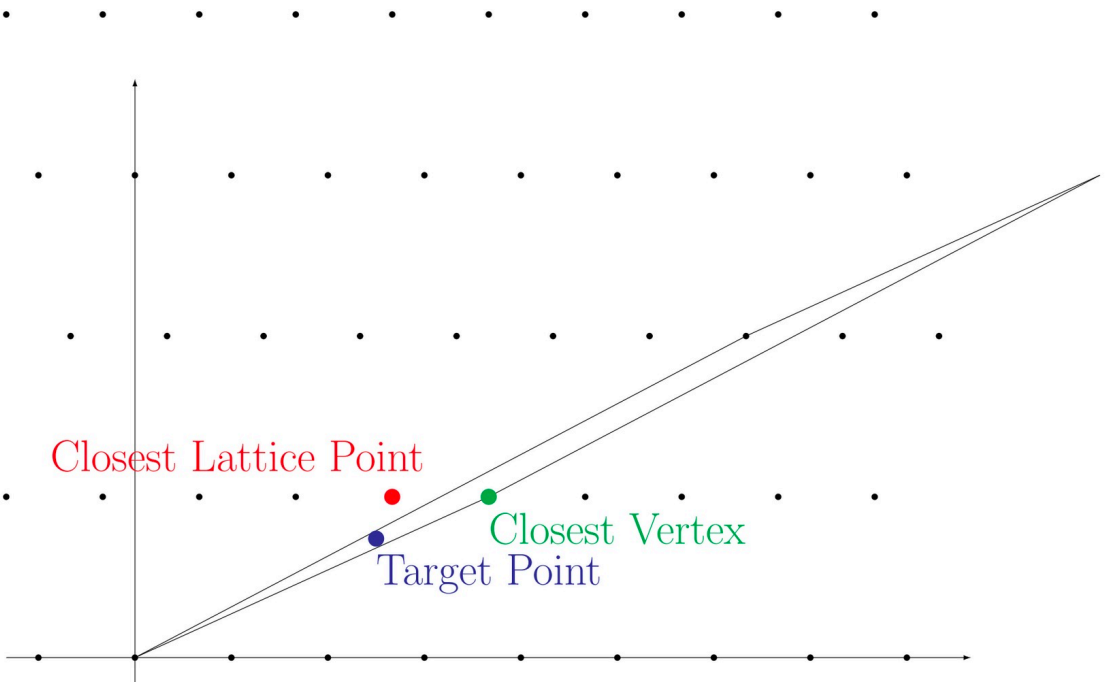


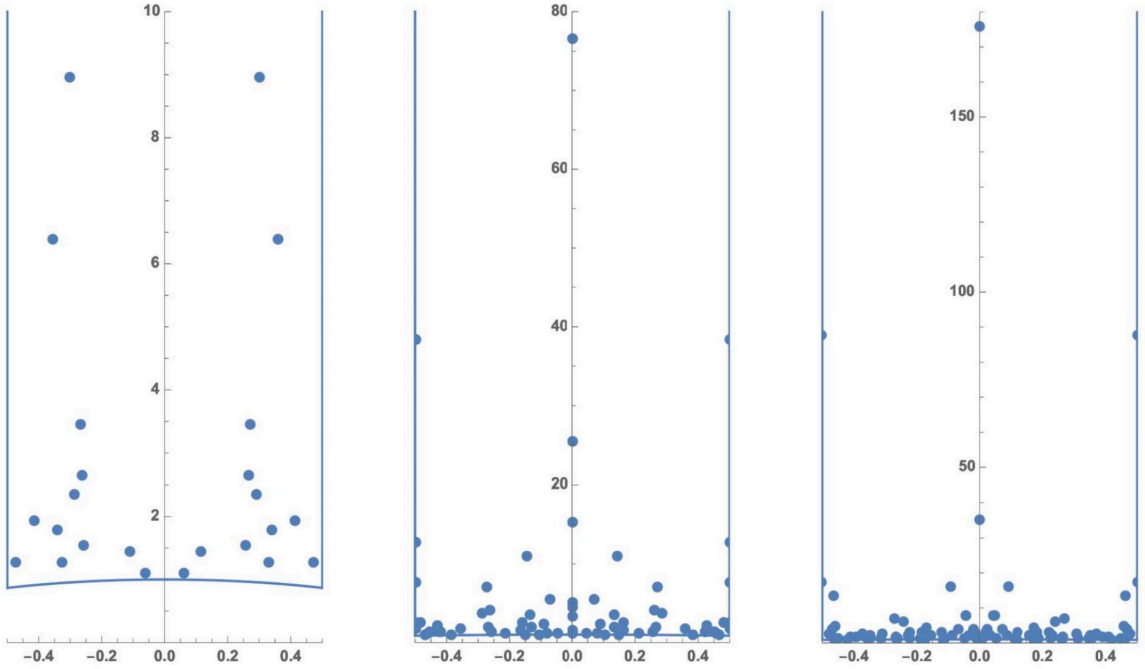
Good and Bad Bases

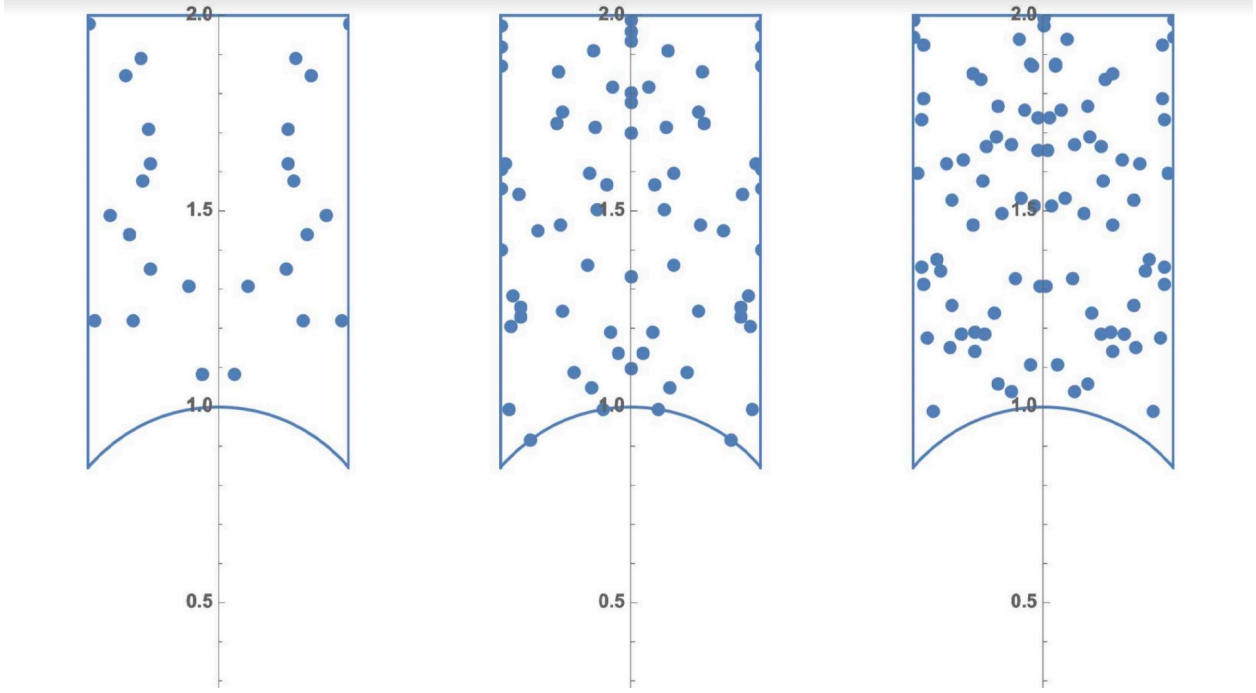


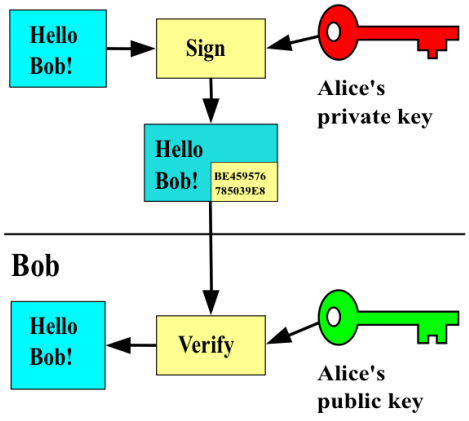
A "good" basis and a "bad" basis

Closest Vertex Method Using Bad Basis






2.0
1.5
1.0
0.5
2.0
1.5
1.0
0.5
2.0
1.5
1.0
0.5


Alice
Hello Bob!
Sign
Alice's private key
Hello Bob!
BE459576 785039E8
Bob
Hello Bob!
Verify
Alice's public key

Geometry of Numbers Lecture 12

Lattices and computer science.

For a computer scientist, a lattice is a sublattice of $\mathbb{Z}^n$. Take $v_1, \dots, v_n \in \mathbb{Z}^n$, $L = \text{span}_{\mathbb{Z}}(v_1, \dots, v_n)$.

Some (easy) computational problems

1. Given $v_1, \dots, v_n \in \mathbb{Z}^n$, and $u \in \mathbb{Z}^n$, does $u \in L = \text{span}_{\mathbb{Z}}(v_j)$?

   Solve the equations $\sum a_i v_j = u$

   (n equations with n variables $a_1, \dots, a_n$)

   If $a_i \in \mathbb{Z}$, $i = 1, \dots, n$ then yes.

2. Given $L = \text{span}_{\mathbb{Z}}(v_1, \dots, v_n)$, let $P = \{\sum c_i v_i : c_i \in [0,1)\}$ (fundamental parallelepiped).

   Given $y \in \mathbb{R}^n$, find $u \in L$ s.t. $y - u \in P$.

   Write $y = \sum a_i v_i$, $a_i \in \mathbb{R}$

Take $u = \sum_{i=1}^{n} \lfloor a_i \rceil v_i$.

Harder problems

3. SVP - shortest vector problem.

Given $v_1, \dots, v_n \in \mathbb{Z}^n$ find $v \in L = \text{span}_{\mathbb{Z}}(v_j)$

s.t. $\|v\| = \lambda_1(L)$.

3a Find $\lambda_1(L)$.

3b. For fixed $r > 1$, find $v \in L$ s.t. $\|v\| \leq r\lambda_1(L)$.

(can be hard or easy depending on r)

3c. For fixed $r > 1$, decide whether $\lambda_1(L) \leq r$.

4. CVP - closest vector problem.

Given $v_1, \dots, v_n \in \mathbb{Z}^n$, and $y \in \mathbb{R}^n$ find

$u \in L = \text{span}_{\mathbb{Z}}(v_j)$ s.t.

$\|y - u\| = \min\{\|y - v\| : v \in L\}$.

(4a) Find $\text{dist}(y, L)$.

(4b) For fixed $r > 1$, find $u \in L$ s.t.

· $\|y-u\| \leq r \cdot dist(y,L)$.

(NC) For fixed $r>1$, decide whether $d(y,L) \leq r$.

Sample application - digital signature (following Silverman)

Goal Find a protocol making it impossible for someone other than Alice to authenticate Alice's document, and making it possible for anyone to convince themselves of this.

Basic structure of a solution Find a math. problem that is hard to solve in general, easy to solve with some extra information, easy to check that a solution is correct. The extra info becomes Alice's private key. The document to be signed generates an instance of the hard problem. Alice solves the hard

problem and transmits the solution, along with the document.

Example (Rivest-Shamir-Adelman '77 following Diffie and Hellman '76)

Hard problem: Given two large primes p, q, factor $N = pq$.

Lattice based problem (Silverman et al).

Use (4b) Given $v_1, \dots, v_n \in \mathbb{Z}^n$, $r > 1$.

Given $y \in \mathbb{R}^n$, find $u \in L = \text{span}_{\mathbb{Z}}(v_i)$

s.t. $\|y - u\| < r \, \text{dist}(y, L)$.

Facts: $\exists r$ s.t. for typical L,

(i) $\forall y \in \mathbb{R}^n$, $\text{dist}(y, L) < r$.

(i.e. covering radius of L is $< r$).

(ii) Given $y \in \mathbb{R}^n$, it is hard to find $u \in L$

s.t. $\|y - u\| < r$.

(iii) Given an "efficient basis" (e.g. KZ-reduced basis) of L, it is easy to find $u \in L$ s.t. $\|y - u\| \leq r$.

Private key will be the reduced basis.
The public information will be L, r.

Recent developments have made lattice based cryptography interesting for many scientists.

1. hard on average (Ajtai-Dwork '97).
   On average - w.r.t. Haar-Siegel measure.
2. not susceptible (?) to quantum computer attack - "post-quantum cryptography".

Some algorithms

LLL algorithm (after A. Lenstra, H. Lenstra, and L. Lovasz '82)

computes a "somewhat efficient" basis and an

"almost shortest" vector, of a given lattice, efficiently.

Imprecisely: there are factors $\delta, \delta' < 1$ (depend on n and on the runtime) so that given L, algorithm computes a basis $b_1, \dots, b_n$ s.t. $L = \text{span}_{\mathbb{Z}}(b_j)$, with

$\delta \|b_1\| \leq \lambda_1(L)$

$\delta' \|u_i\| \leq \|b_i\| \leq \frac{1}{\delta'} \|u_i\|$, where $u_1, \dots, u_n$ is a KZ-reduced basis for L.

Gram-Schmidt orthogonalization

$\langle \cdot, \cdot \rangle$ is the standard inner product on $\mathbb{R}^n$.

Given $b_1, \dots, b_n$ a basis of $\mathbb{R}^n$, define $\tilde{b}_1 = b_1$, and inductively, $\tilde{b}_i = b_i - \sum_{j=1}^{i-1} \mu_{ij} \tilde{b}_j$

where $\mu_{ij} = \frac{\langle b_i, \tilde{b}_j \rangle}{\langle \tilde{b}_j, \tilde{b}_j \rangle}$

$\tilde{b}_i = b_i - \mu_{ij} \tilde{b}_j$ is proj. of b_i onto $(\tilde{b}_j)^{\perp}$.

i.e. $\tilde{b}_i$ is the projection of b_i onto $\text{span}(\tilde{b}_1,\dots,\tilde{b}_{i-1})^{\perp}$

Then: * $\tilde{b}_i$ are orthogonal

* For each i, $\text{span}_{\mathbb{R}}(b_1,\dots,b_i) = \text{span}_{\mathbb{R}}(\tilde{b}_1,\dots,\tilde{b}_i)$
* $\tilde{b}_i$ is projection of b_i onto $\text{span}(\quad)^{\perp}$
* these properties determine $\tilde{b}_1,\dots,\tilde{b}_n$.

Def: Given $\delta \in (0,1)$, a basis $B=(b_1,\dots,b_n)$ is said to be δ-LLL reduced if:

(i) $\forall\, 1 \le j < i \le n$, $\quad |\mu_{i,j}| \le \frac{1}{2}$.

(ii) $\forall i \quad \delta \|\tilde{b}_i\|^2 \le \|\mu_{i+1,i}\tilde{b}_i + \tilde{b}_{i+1}\|^2$!

Note: (ii) $\iff \delta\|\tilde{b}_i\|^2 \le \mu_{i+1,i}^2\|\tilde{b}_i\|^2 + \|\tilde{b}_{i+1}\|^2$

$$\Rightarrow \|\tilde{b}_{i+1}\|^2 \ge (\delta-\mu_{i+1,i}^2)\|\tilde{b}_i\|^2 \underset{\text{use (i)}}{\ge} (\delta-\tfrac{1}{4})\|\tilde{b}_i\|^2$$

"$\tilde{b}_{i+1}$ not much shorter than $\tilde{b}_i$".

(i) is called Lovasz condition, it can be thought

of as saying that for every $i<j$, b_i, b_j are close to orthogonal.

To understand this definition, let $c_i = \frac{\tilde{b}_i}{\|\tilde{b}_i\|}$.

(orthonormal basis coming from Gram-Schmidt).

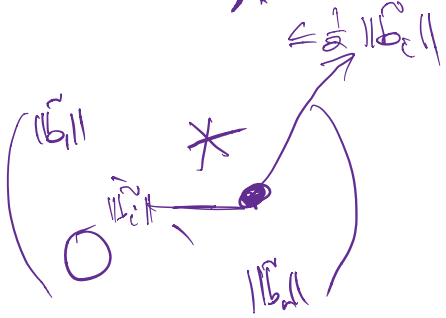
Then we have:

$b_1 = \tilde{b}_1 = \|\tilde{b}_1\| c_1$

$b_2 = \|\tilde{b}_2\| (c_2 + \mu_{2,1} c_1)$

$\vdots$

$b_n = \|\tilde{b}_n\| (c_n + \mu_{n,n-1} c_{n-1} + \cdots + \mu_{n,1} c_1)$, $|\mu_{ij}| \le \frac{1}{2}$.



Also, each 2×2 block $\begin{pmatrix} \|\tilde{b}_i\| & \|\tilde{b}_i\|\mu_{i+1,i} \\ 0 & \|\tilde{b}_{i+1}\| \end{pmatrix}$

has 2^{nd} column almost as large as 1^{st} column.

<u>Claim</u> If $b_1, \ldots, b_n$ is δ-LLL reduced, $\delta \in (\frac{1}{4}, 1)$, then

$\|b_1\| \le \left(\frac{2}{\sqrt{4\delta - 1}}\right)^{n-1} \lambda_1(L)$, where $L = \mathrm{span}_{\mathbb{Z}}(b_j)$.

(For $\delta = \frac{3}{4}$, and then const becomes $2^{\frac{n-1}{2}}$).

Pf: First we claim $\lambda_1(L) \geq \min_i \|b_i^*\|$ (*)

(for this we won't is δ-LLL reduced).

Let $u \in L \setminus \{0\}$, $u = \sum_{i=1}^{n} \alpha_i b_i$, $\alpha_i \in \mathbb{Z}$ not all 0.

Let i_0 be the last index with $\alpha_i \neq 0$.

$$u = \sum_{i=1}^{i_0} \alpha_i b_i \qquad \alpha_{i_0} \in \mathbb{Z} \setminus \{0\}.$$

$$|\langle u, b_{i_0}^* \rangle| = \left|\left\langle \sum_{i=1}^{i_0} \alpha_i b_i, b_{i_0}^* \right\rangle\right| = |\alpha_{i_0}| |\langle b_{i_0}, b_{i_0}^* \rangle|$$

($\langle b_i, b_{i_0}^* \rangle = 0$ for $i < i_0$)

$$= |\alpha_{i_0}| |\langle b_{i_0}^*, b_{i_0}^* \rangle| = |\alpha_{i_0}| \|b_{i_0}^*\|^2 \geq \|b_{i_0}^*\|^2$$

($\langle b_{i_0} - b_{i_0}^*, b_{i_0}^* \rangle = 0$; $\alpha_{i_0} \in \mathbb{Z} \setminus \{0\}$)

$$|\langle u, b_{i_0}^* \rangle| \leq \|u\| \|b_{i_0}^*\|$$

$$\Rightarrow \|u\| \|b_{i_0}^*\| \geq \|b_{i_0}^*\|^2 \Rightarrow \|u\| \geq \|b_{i_0}^*\| \geq \min_i \|b_i^*\|.$$

This proves (*).

Also, $\|\tilde{b}_n\|^2 \underset{(ii)}{\geq} (\delta - \frac{1}{4})\|\tilde{b}_{n-1}\|^2 \geq \cdots \geq (\delta - \frac{1}{4})^{n-1}\|\tilde{b}_1\|^2$

$= (\delta - \frac{1}{4})^{n-1}\|b_1\|^2$

For each i, $\|\tilde{b}_i\| \geq (\delta - \frac{1}{4})^{\frac{-n-1}{2}}\|b_1\| = \left(\frac{\sqrt{4\delta - 1}}{2}\right)^{n-1}\|b_1\|$

Combining with (*), we get the Lemma.

The LLL-algorithm takes a basis and transforms it into a δ-LLL reduced basis. As a solution to SVP, it returns b_1.

The algorithm

Input: $b_1, \ldots, b_n \in \mathbb{Z}^n$

Output: δ-LLL reduced basis for $L = \text{span}_{\mathbb{Z}}(b_j)$.

Start: Compute $\tilde{b}_1, \ldots, \tilde{b}_n$.

Reduction step:

For $i = 2$ to n

For $j = i-1$ to 1

$b_i \leftarrow b_i - c_{ij} b_j$, where

c_{ij} = the nearest integer to

$$\frac{\langle b_i, \tilde{b}_j \rangle}{\langle \tilde{b}_j, \tilde{b}_j \rangle}$$

Swap step

If there is an i for which

$$\delta \|\tilde{b}_i\|^2 > \|\mu_{i+1,i}\tilde{b}_i + \tilde{b}_{i+1}\|^2,$$

then $b_i \leftrightarrow b_{i+1}$ (swap these two vectors)

and return to start.

Otherwise step. Output $b_1, \ldots, b_n$.

Assume the algorithm stops, in other words, in swap step, at some point, for all i, Condition (ii) holds. Let's check that (i) also holds.

Note that during reduction step, we do not

change $\tilde{b}_1, \tilde{b}_2, \ldots, \tilde{b}_n$. This uses the characterization of $\tilde{b}_1, \ldots \tilde{b}_n$ and the fact that in the reduction step, inside loop, j goes down. The μ_{ij} satisfy $|\mu_{ij}| \leq \frac{1}{2}$ after step j in the inside loop, and after that they are not changed (when continuing in the inside loop or in updating $\tilde{c}$).

So when reduction step is done $|\mu_{ij}| \leq \frac{1}{2}$ for all $j < i$.

We will show that indeed, algorithm stops (in fact it stops quickly, i.e. polynomially in $\max\{n, \log \max_i \|b_i\|\}$).

Def Given a basis $B = (b_1, \ldots b_n)$ of $L = \text{span}_{\mathbb{Z}}(b_j)$ the potential of B is $D_B = \prod_{i=1}^{n} \|\tilde{b}_i\|^{n-i+1}$

$$= \prod_{i=1}^{n} \left(\|\tilde{b}_1\| \cdot \ldots \cdot \|\tilde{b}_i\| \right) = \prod_{i=1}^{n} \|b_1 \wedge \ldots \wedge b_i\| =$$

$$= \prod_{i=1}^{n} \operatorname{covol}\left(\operatorname{span}_{\mathbb{Z}}(b_1, \dots, b_i)\right).$$

$$= \prod_{i=1}^{n} D_{B,i}$$

↑ notation

Let $B' = (b_1', \dots, b_n')$ be the basis obtained from B after one iteration of the algorithm.

During the reduction, Gram-Schmidt orthogonal basis is not changed, so none of the $D_{B,i}$ is changed. In the swap step, let i be such that b_i is swapped with b_{i+1}, then for $k \neq i$, $\operatorname{span}_{\mathbb{Z}}(b_1, \dots, b_k) = \operatorname{span}(b_1', \dots, b_k')$

So $D_{B,k} = D_{B',k}$ for $k \neq i$.

Set $\Lambda_i = \operatorname{span}_{\mathbb{Z}}(b_1, \dots, b_i)$,

$\Lambda_i' = \operatorname{span}_{\mathbb{Z}}(b_1', \dots, b_i')$

ex.

$$\frac{D_{B',i}}{D_{B,i}} = \frac{\text{covol}(\Lambda_i')}{\text{covol}(\Lambda_i)} = \frac{\prod_{j=1}^{i-1} \|\tilde{b}_j\| \cdot \|\mu_{i+1,i}\tilde{b}_i + \tilde{b}_{i+1}\|}{\prod_{j=1}^{i} \|\tilde{b}_j\|}$$

$$= \frac{\|\mu_{i+1,i}\tilde{b}_i + \tilde{b}_{i+1}\|}{\|\tilde{b}_i\|} \leq \sqrt{\delta}^{\,i-1}$$

↑ cond'n for swap step.

So in every iteration, quantity D_B decreases by a multiplicative factor $\leq \sqrt{\delta} < 1$.

$D_B \in \mathbb{N}$, since they are products of covolumes of integer lattices. So process terminates.

Simulating Haar-Siegel measure

Recall: $m_{\mathcal{X}_n}(A) = m_{SL_n(\mathbb{R})}(\Omega \cap \pi^{-1}(A))$

where $\pi : SL_n(\mathbb{R}) \longrightarrow SL_n(\mathbb{R})/SL_n(\mathbb{Z}) = \mathcal{X}_n$.

Ω is a fundamental domain.

$\forall L = g\mathbb{Z}^n \quad (g \in SL_n(\mathbb{R}))$

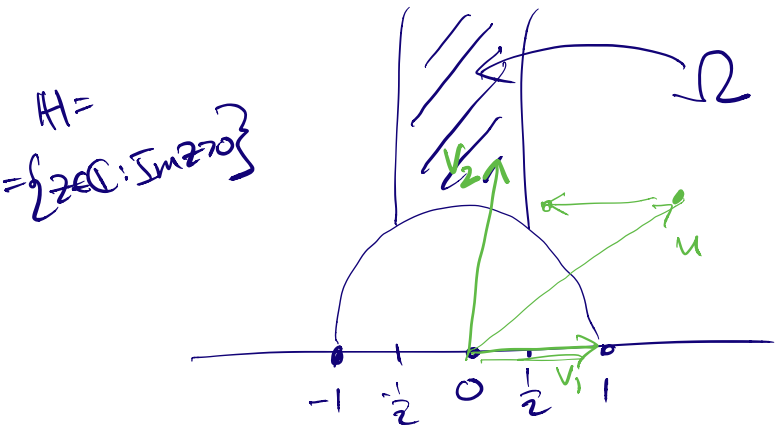
$= \mathrm{span}_{\mathbb{Z}}(v_1, \dots, v_n), \quad \begin{pmatrix} | & & | \\ v_1 & \cdots & v_n \\ | & & | \end{pmatrix} = g$

$\exists \gamma \in SL_n(\mathbb{Z})$, s.t. $g\gamma \in \Omega \iff$

L contains a basis $u_1, \dots, u_n$ s.t.

$g' = \begin{pmatrix} | & & | \\ u_1 & \cdots & u_n \\ | & & | \end{pmatrix}$, then $g' = g\gamma$, and $g' \in \Omega$.

Ex Ω can be chosen using the picture



Given L, let v_1 s.t. $\|v_1\| = \lambda_1(L)$.

Rotate and rescale L so that $v_1 = e_1$

claim (ex). v_2, the shortest vector s.t.

$L = \mathrm{span}_{\mathbb{Z}}(v_1, v_2)$, is in $\mathcal{L}$.

In $n=2$, $m_{\mathbb{Z}^n}$ corresponds to the volume of hyperbolic metric on $\mathbb{H}$.

We would like to simulate $m_{\mathbb{Z}^n}$ on a computer. What does this mean?

Recall (Riesz rep'n thm)

$(X, \mathcal{B})$ is a lcsc space with Borel σ-alg.

A Radon measure μ on $(X, \mathcal{B})$ is equiv to a cont. pos. lin. functional on $C_c(X)$

$$f \longmapsto \int_X f \, d\mu .$$

We say $\mu_j \xrightarrow[j\to\infty]{} \mu$ if $\forall f \in C_c(X)$

$$\int_X f \, d\mu_j \xrightarrow[j\to\infty]{} \int_X f \, d\mu .$$

Can define a metric on $\{$Radon meas. on $(X, \mathcal{B})\}$ $= \mathcal{M}(X)$

which turns this notion into convergence w.r.t.

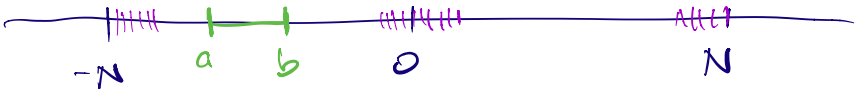
this metric. With this metric, $\mathcal{U}(X)$ is a complete separable metric space.

This is the weak-$*$ topology.

Example (more details next week).

$X = \mathbb{R}$

$$\nu_N = \frac{1}{N} \sum_{x \in \{-N, -N+\frac{1}{N}, \dots, N-\frac{1}{N}, N\}} \delta_x .$$



$\nu_N \longrightarrow \mathrm{Vol}.$

Reformulation of the problem

Want μ_j defined on $\mathcal{X}_n$, which we can simulate on a computer,

s.t. $\mu_j \xrightarrow[j \to \infty]{} m_{\mathcal{X}_n}$.

We want a rate bound, i.e., for a given test function f (perhaps with nice

properties) want a rate in the convergence

$$\left| \int_{\mathcal{X}_n} f d\mu_j - \int_{\mathcal{X}_n} f dm_{\mathcal{X}_n} \right| < E_j \longrightarrow 0$$

(want explicit E_j depending on f).

Two such constructions

@ Hecke correspondence

Let $L_0 \in \mathcal{X}_n$, let p be a prime.

$L' \in \mathcal{X}_n$ is called a p-Hecke friend of L_0

if $\exists\, L_1 \subset L_0$, $[L_1 : L_0] = p$ s.t.

$L' = p^{-\frac{1}{n}} L_1$.

(L' is the covolume one rescaling of L_1).

Let $N_p = \#\{$p-Hecke friends of $L_0\}$

Define $\nu_p = \frac{1}{N_p} \sum_{\substack{L' \text{ a p-Hecke} \\ \text{friend of } L_0}} \delta_{L'}$.

Then $\nu_p \xrightarrow[\substack{p \to \infty \\ p \text{ prime}}]{} m_{\mathcal{X}_n}$.