Gaussian distribution, Rejection sampling, Rings and Modules

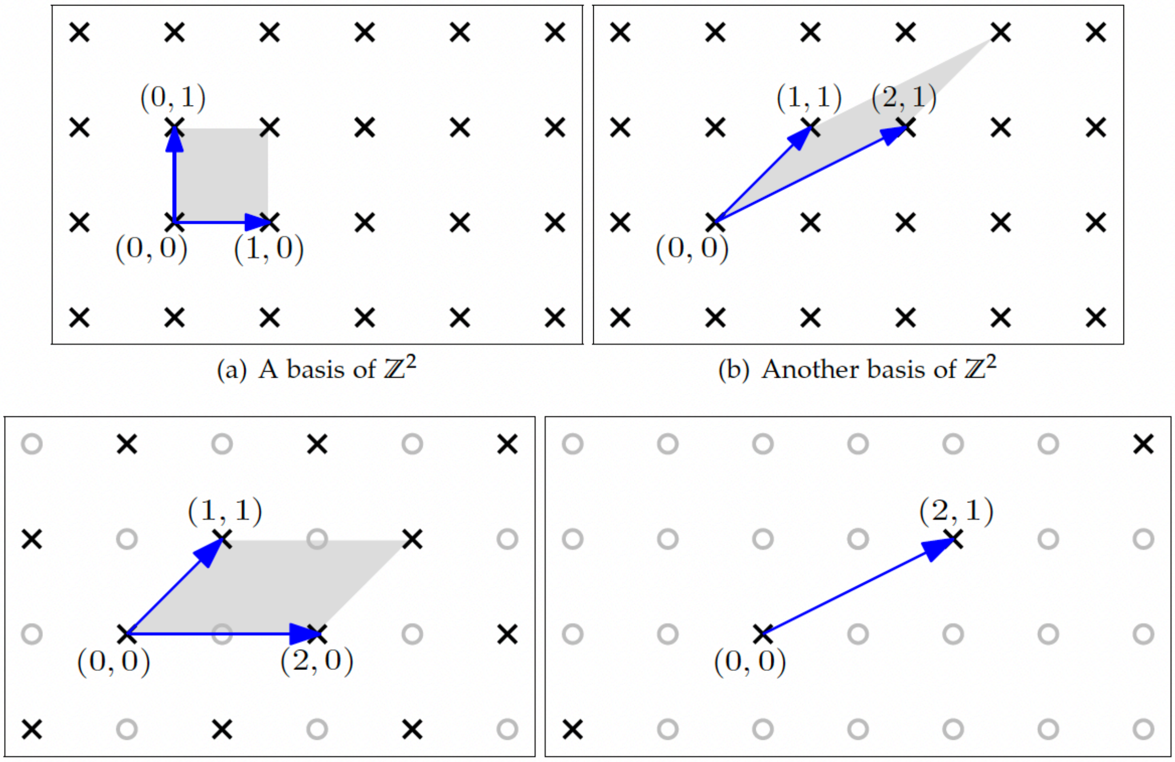
Notations

- $\mathbb{R}$, real numbers
- $\mathbb{Z}$, integers
- $\mathbb{N}$, positive integers
- $\|x\| = \sqrt{\sum_{i \in [n]} x_i^2}$, the ℓ_2 or Euclidean norm of a vector $\vec{x} \in \mathbb{R}^n$.
- $\|x\|_\infty = \mathsf{max}_{i \in n}(x_i)$, the ℓ_∞ norm of a vector $\vec{x} \in \mathbb{R}^n$.
- $\mathcal{L}$ or Λ, lattice
- $\mathcal{L}(B)$or $\Lambda(B)$, lattice generated by basis B
- $\rho(x)$, Gaussian probability density（Gaussian function）
- $D_s, \mathcal{D}_s$, (discrete or continuous) Gaussian distribution of parameter (or width) s
- $P(B)$, fundamental parallelepiped generated by B

1. Gaussian distribution

1. why do we need Gaussian distribution
2. what is it
3. how to obtain a Gaussian distribution - rejection sampling

1.1 Recall good/bad bases



(a) A basis of $\mathbb{Z}^2$

(b) Another basis of $\mathbb{Z}^2$

(c) Not a basis of $\mathbb{Z}^2$

(d) Not a full-rank lattice

Because a lattice $\mathcal{L}$ is an additive subgroup of $\mathbb{R}^n$, we have the quotient group $\mathbb{R}^n/\mathcal{L}$ of cosets

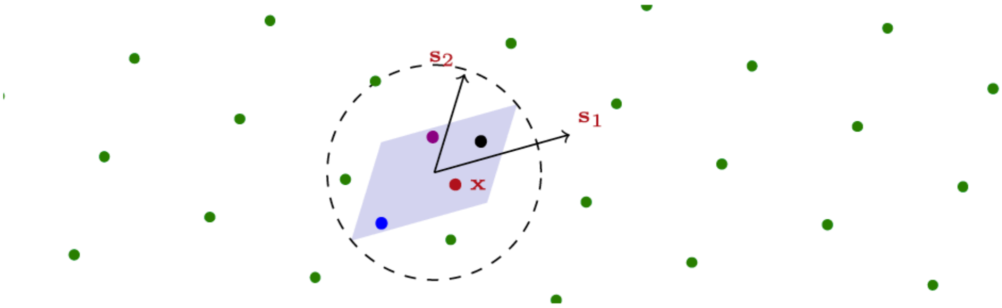
$$\mathbf{c} + \mathcal{L} = \{\mathbf{c} + \mathbf{v} : \mathbf{v} \in \mathcal{L}\}, \quad \mathbf{c} \in \mathbb{R}^n,$$

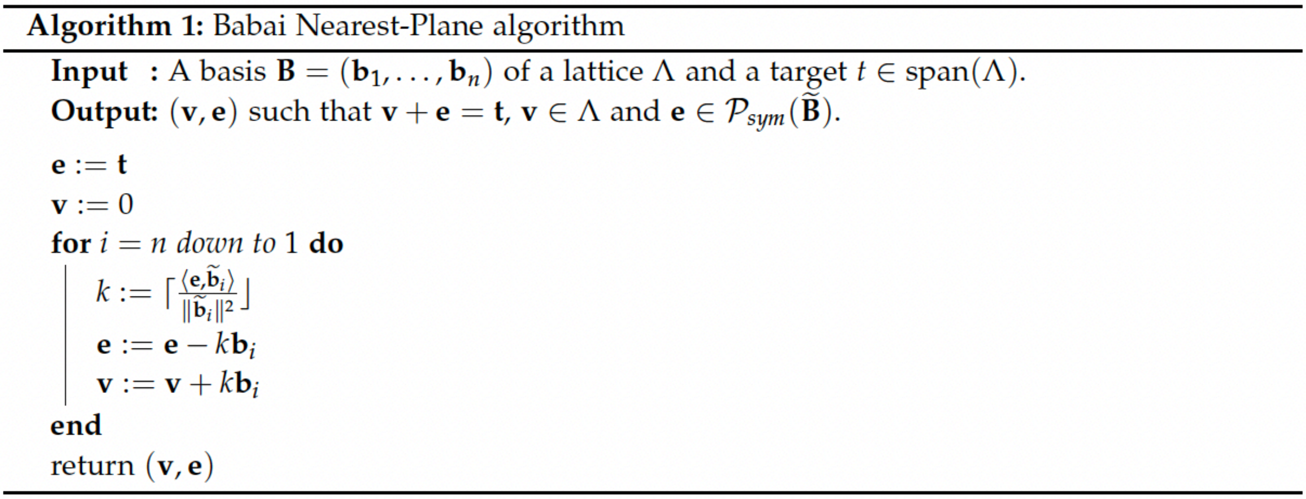
with the usual induced addition operation $(\mathbf{c}_1 + \mathcal{L}) + (\mathbf{c}_2 + \mathcal{L}) = (\mathbf{c}_1 + \mathbf{c}_2) + \mathcal{L}$. A *fundamental domain* of $\mathcal{L}$ is a set $\mathcal{F} \subset \mathbb{R}^n$ that contains exactly one representative $\bar{\mathbf{c}} \in (\mathbf{c} + \mathcal{L}) \cap \mathcal{F}$ of every coset $\mathbf{c} + \mathcal{L}$. For example, the half-open intervals $[0, 1)$ and $[-\frac{1}{2}, \frac{1}{2})$ are fundamental domains of the integer lattice $\mathbb{Z}$, where coset $c + \mathbb{Z}$ has representative $c - \lfloor c \rfloor$ and $c - \lfloor c \rceil$, respectively.

1.2 Blur

Signature Scheme [GGH'96]

- Key idea: $pk =$ "bad" basis $\mathbf{B}$ for $\mathcal{L}$, $sk =$ "short" trapdoor basis $\mathbf{S}$
- Sign: $H(\mathsf{msg}) = \mathbf{c} + \mathcal{L}$; get short $\mathbf{x} \in \mathbf{c} + \mathcal{L}$ via round-off [Babai'86]
- Verify$(\mathsf{msg}, \mathbf{x})$ check $\mathbf{x} \in H(\mathsf{msg}) = \mathbf{c} + \mathcal{L}$, and $\mathbf{x}$ short enough





Algorithm 1: Babai Nearest-Plane algorithm

Input : A basis $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of a lattice Λ and a target $t \in \text{span}(\Lambda)$.
Output: $(\mathbf{v}, \mathbf{e})$ such that $\mathbf{v} + \mathbf{e} = \mathbf{t}$, $\mathbf{v} \in \Lambda$ and $\mathbf{e} \in \mathcal{P}_{sym}(\widetilde{\mathbf{B}})$.

```
$\mathbf{e} := \mathbf{t}$
$\mathbf{v} := 0$
for $i = n$ down to $1$ do
    $k := \lceil \frac{\langle \mathbf{e}, \widetilde{\mathbf{b}}_i \rangle}{\|\widetilde{\mathbf{b}}_i\|^2} \rfloor$
    $\mathbf{e} := \mathbf{e} - k\mathbf{b}_i$
    $\mathbf{v} := \mathbf{v} + k\mathbf{b}_i$
end
return $(\mathbf{v}, \mathbf{e})$
```

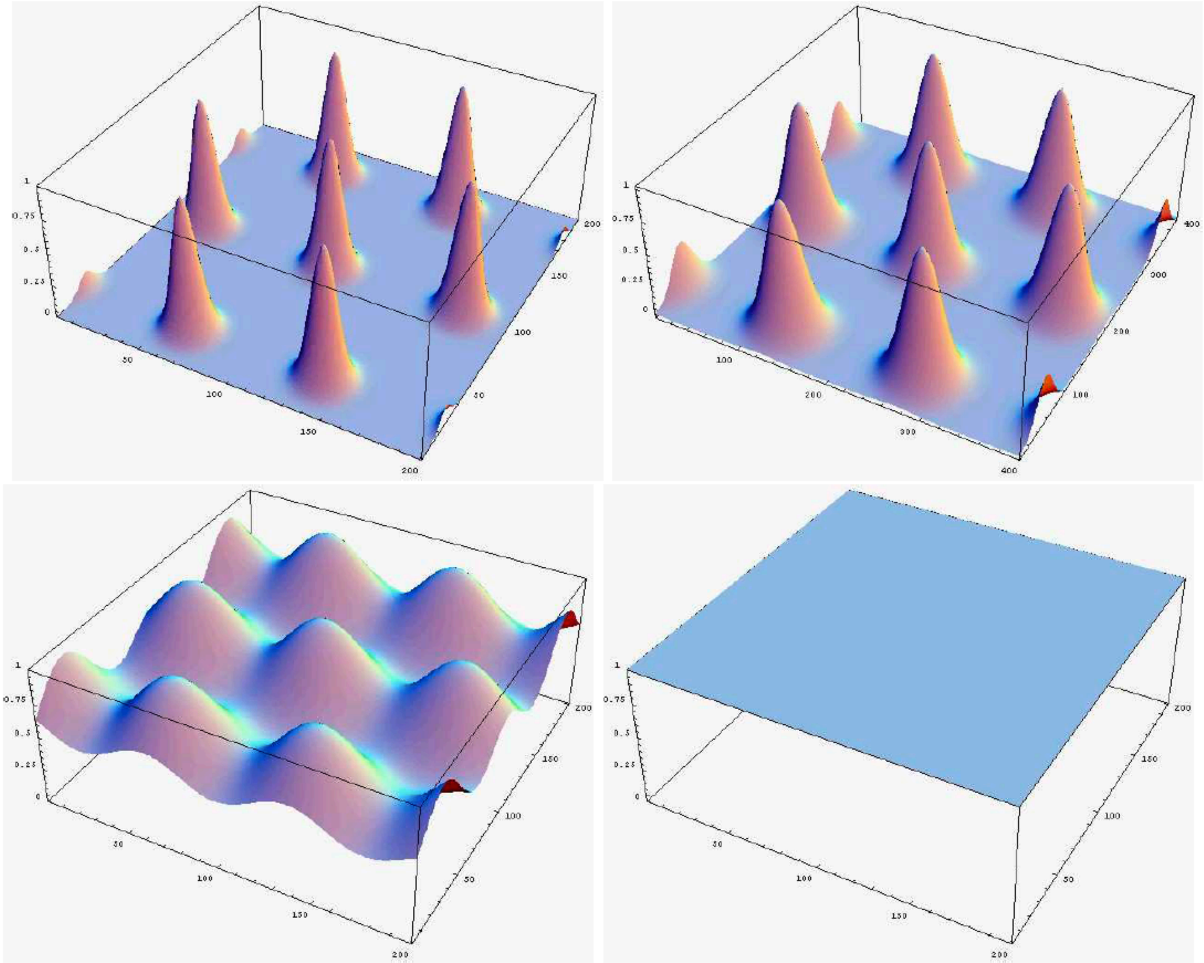
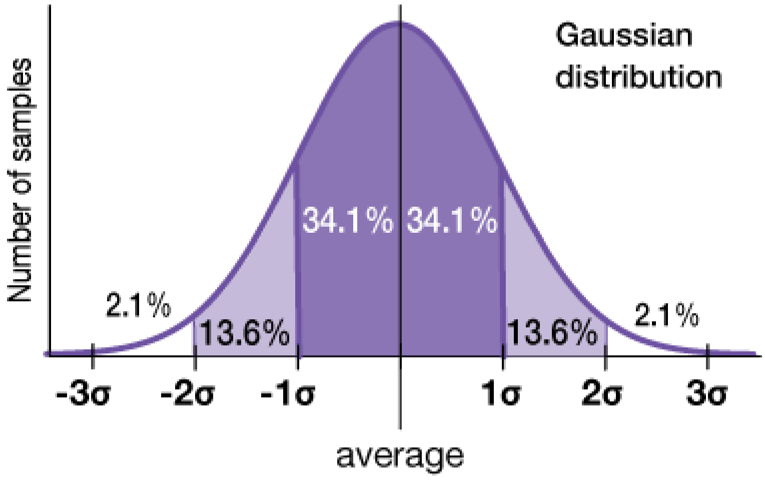


Figure 1: A lattice distribution with different amounts of Gaussian noise

1.3 Gaussian



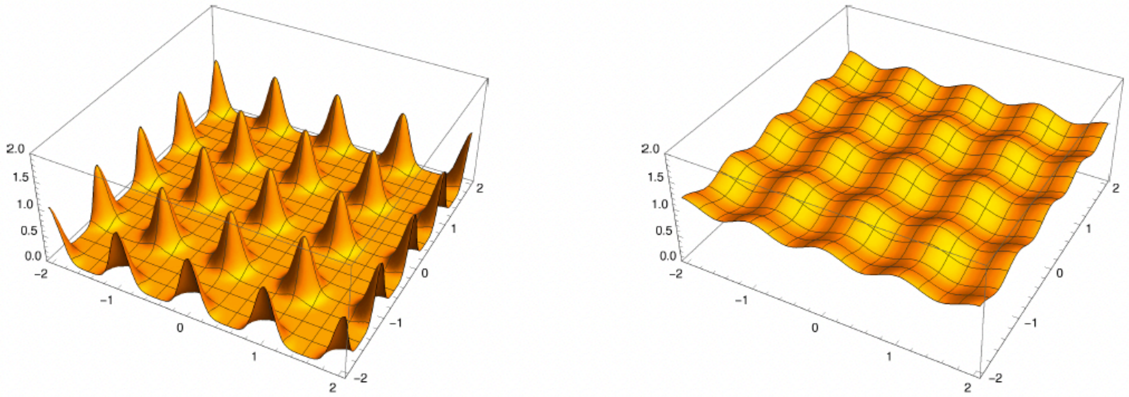
Definition 1 *We define the function* $\rho_s : \mathbb{R}^n \mapsto \mathbb{R}$ *by*

$$\rho_s(\mathbf{x}) := e^{-\pi\|\mathbf{x}/s\|^2}, \qquad s > 0,$$

and from this we define the periodic Gaussian $f_s : \mathbb{R}^n \to \mathbb{R}$ *by*

$$f_s(\mathbf{t}) := \rho_s(\mathcal{L} + \mathbf{t}) = \sum_{\mathbf{x} \in \mathcal{L}} \rho_s(\mathbf{x} + \mathbf{t}).$$

The function f approaches a constant function as $s \to \infty$, and approaches separate Gaussian densities as $s \to 0$. Later in this lecture we will formalize this notion by defining a *smoothing parameter*.



(a) Periodic Gaussian on $\mathbb{Z}^2$ for $s = 0.3$.

(b) Periodic Gaussian on $\mathbb{Z}^2$ for $s = 1$.

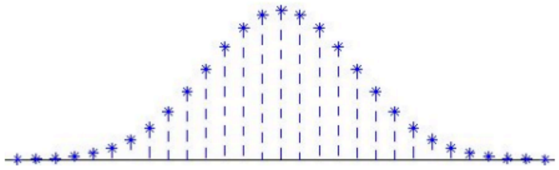


Figure 1.1: Discrete Gaussian on $\mathbb{Z}$.

Definition 1. Discrete Gaussian distribution over coset $\mathbf{c} + \mathcal{L}$ is defined as

$$D_{\mathbf{c}+\mathcal{L},s}(\mathbf{x}) = \frac{\rho_s(\mathbf{x})}{\rho_s(\mathbf{c}+\mathcal{L})} \tag{3.40}$$

for all $\mathbf{x} \in \mathbf{c} + \mathcal{L}$.

$$\Pr_{X \sim D_{\mathcal{L}+c,s}}[X = x] = \frac{\rho_s(x)}{\rho_s(c+\mathcal{L})}$$

if $x \in c + \mathcal{L}$ and 0 otherwise.

1.4 Dual lattice

DEFINITION 1 *For a full-rank lattice* Λ *we define its* dual lattice *(sometimes known as the* reciprocal lattice*)*

$$\Lambda^* = \{y \in \mathbb{R}^n \mid \forall x \in \Lambda,\ \langle x, y\rangle \in \mathbb{Z}\}.$$

In general, we define

$$\Lambda^* = \{y \in \text{span}(\Lambda) \mid \forall x \in \Lambda,\ \langle x, y\rangle \in \mathbb{Z}\}.$$

understand it: fix y or x, separated by distance $\frac{1}{\|x\|}$ or $\frac{1}{\|y\|}$.

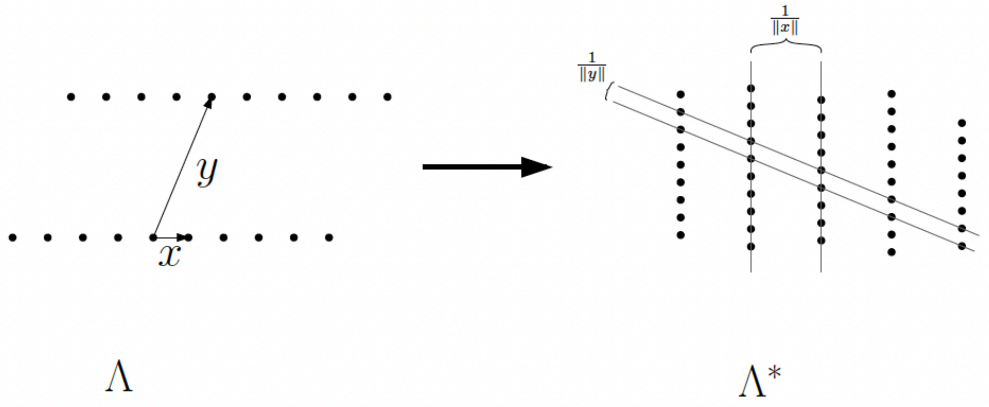
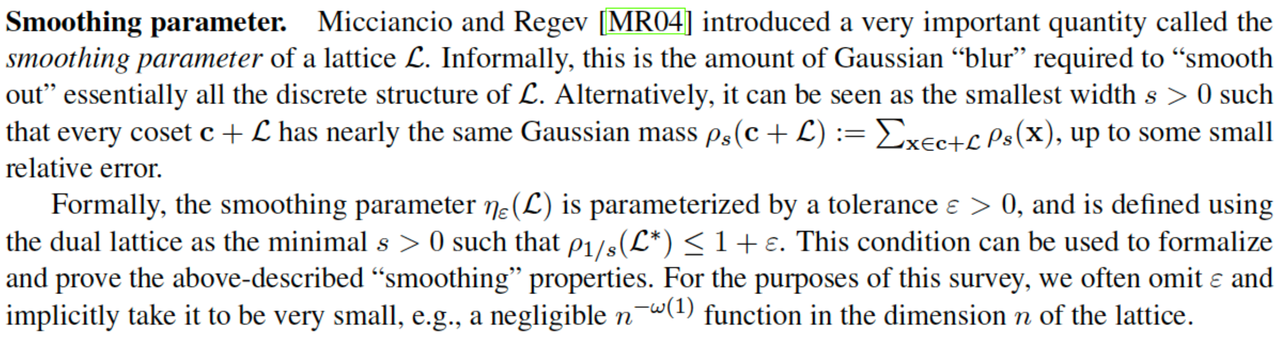


Figure 1: A lattice and its dual

its basis: For $\mathcal{L}(B)$ and $L^*(B) = L(D)$, it holds $B^\top D = I$.

1.5 Smoothing parameter

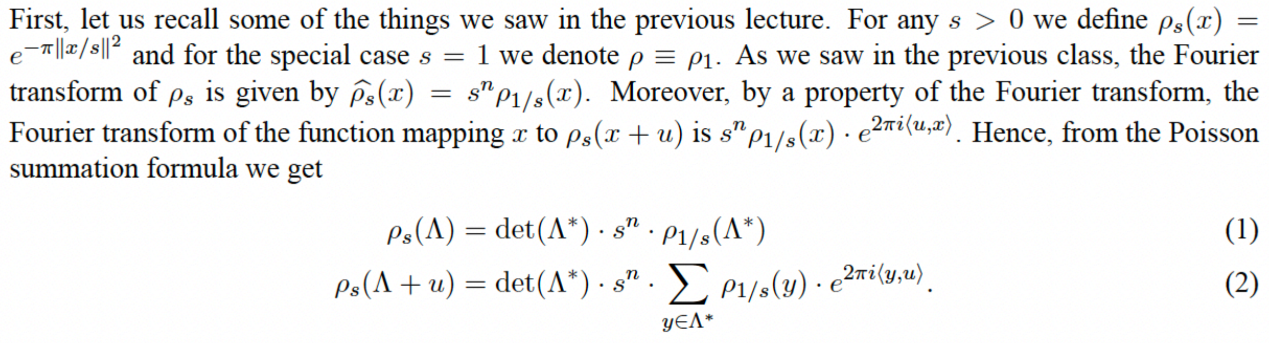


Smoothing parameter. Micciancio and Regev [MR04] introduced a very important quantity called the *smoothing parameter* of a lattice $\mathcal{L}$. Informally, this is the amount of Gaussian "blur" required to "smooth out" essentially all the discrete structure of $\mathcal{L}$. Alternatively, it can be seen as the smallest width $s > 0$ such that every coset $\mathbf{c} + \mathcal{L}$ has nearly the same Gaussian mass $\rho_s(\mathbf{c} + \mathcal{L}) := \sum_{\mathbf{x} \in \mathbf{c}+\mathcal{L}} \rho_s(\mathbf{x})$, up to some small relative error.

Formally, the smoothing parameter $\eta_\varepsilon(\mathcal{L})$ is parameterized by a tolerance $\varepsilon > 0$, and is defined using the dual lattice as the minimal $s > 0$ such that $\rho_{1/s}(\mathcal{L}^*) \leq 1 + \varepsilon$. This condition can be used to formalize and prove the above-described "smoothing" properties. For the purposes of this survey, we often omit ε and implicitly take it to be very small, e.g., a negligible $n^{-\omega(1)}$ function in the dimension n of the lattice.

Lemma 1. Let $\mathcal{L}$ be a lattice with basis B. Then the statistical distance between the uniform distribution on $P(B)$ and the distribution obtained by sampling from $\frac{\rho_s(x)}{s^n}$ and reducing the result modulo $P(B)$, or $D_{c+\mathcal{L},s}$, is at most $\frac{1}{2}\rho_{1/s}(\mathcal{L}^*)$.

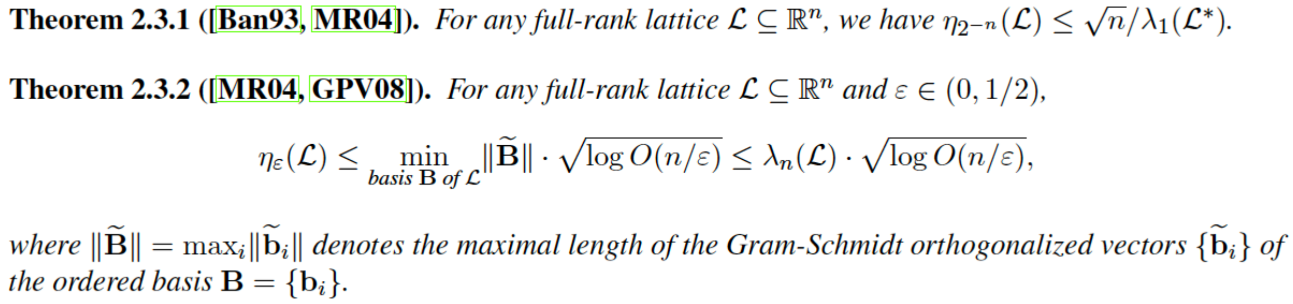
Definition 2. For any ε> 0, the smoothing parameter, denoted it by $\eta_\varepsilon(\mathcal{L})$, of $\mathcal{L}$ with parameter ε is the smallest $s > 0$ such that $\rho_{1/s}(\mathcal{L}^*/\{0\}) \leq \varepsilon$.



First, let us recall some of the things we saw in the previous lecture. For any $s > 0$ we define $\rho_s(x) = e^{-\pi\|x/s\|^2}$ and for the special case $s = 1$ we denote $\rho \equiv \rho_1$. As we saw in the previous class, the Fourier transform of ρ_s is given by $\widehat{\rho_s}(x) = s^n \rho_{1/s}(x)$. Moreover, by a property of the Fourier transform, the Fourier transform of the function mapping x to $\rho_s(x+u)$ is $s^n \rho_{1/s}(x) \cdot e^{2\pi i\langle u,x\rangle}$. Hence, from the Poisson summation formula we get

$$\rho_s(\Lambda) = \det(\Lambda^*) \cdot s^n \cdot \rho_{1/s}(\Lambda^*) \tag{1}$$

$$\rho_s(\Lambda + u) = \det(\Lambda^*) \cdot s^n \cdot \sum_{y\in\Lambda^*} \rho_{1/s}(y) \cdot e^{2\pi i\langle y,u\rangle}. \tag{2}$$



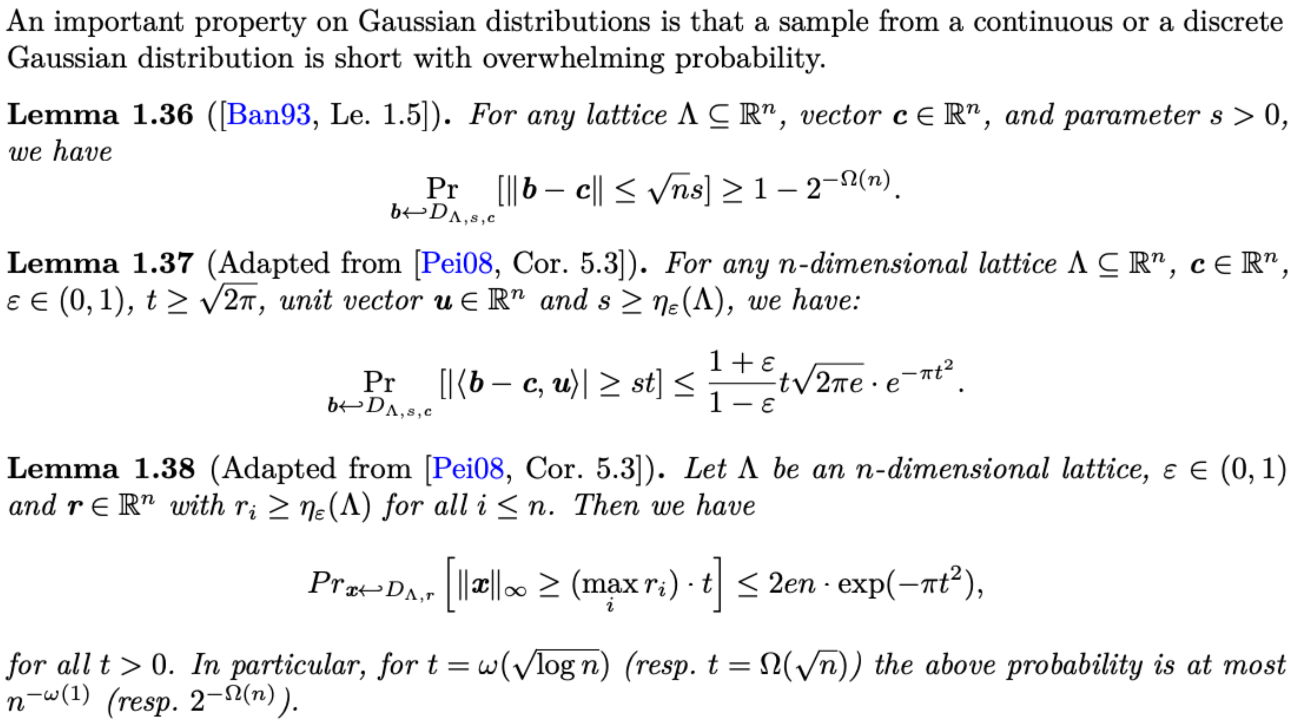
Theorem 2.3.1 ([Ban93, MR04]). *For any full-rank lattice $\mathcal{L} \subseteq \mathbb{R}^n$, we have $\eta_{2^{-n}}(\mathcal{L}) \leq \sqrt{n}/\lambda_1(\mathcal{L}^*)$.*

Theorem 2.3.2 ([MR04, GPV08]). *For any full-rank lattice $\mathcal{L} \subseteq \mathbb{R}^n$ and $\varepsilon \in (0, 1/2)$,*

$$\eta_\varepsilon(\mathcal{L}) \leq \min_{\textit{basis } \mathbf{B} \textit{ of } \mathcal{L}} \|\widetilde{\mathbf{B}}\| \cdot \sqrt{\log O(n/\varepsilon)} \leq \lambda_n(\mathcal{L}) \cdot \sqrt{\log O(n/\varepsilon)},$$

where $\|\widetilde{\mathbf{B}}\| = \max_i \|\widetilde{\mathbf{b}}_i\|$ denotes the maximal length of the Gram-Schmidt orthogonalized vectors $\{\widetilde{\mathbf{b}}_i\}$ of the ordered basis $\mathbf{B} = \{\mathbf{b}_i\}$.

Tail Bounds



An important property on Gaussian distributions is that a sample from a continuous or a discrete Gaussian distribution is short with overwhelming probability.

Lemma 1.36 ([Ban93, Le. 1.5]). *For any lattice $\Lambda \subseteq \mathbb{R}^n$, vector $\boldsymbol{c} \in \mathbb{R}^n$, and parameter $s > 0$, we have*

$$\Pr_{\boldsymbol{b} \hookleftarrow D_{\Lambda,s,\boldsymbol{c}}}[\|\boldsymbol{b} - \mathbf{c}\| \leq \sqrt{n}s] \geq 1 - 2^{-\Omega(n)}.$$

Lemma 1.37 (Adapted from [Pei08, Cor. 5.3]). *For any n-dimensional lattice $\Lambda \subseteq \mathbb{R}^n$, $\boldsymbol{c} \in \mathbb{R}^n$, $\varepsilon \in (0,1)$, $t \geq \sqrt{2\pi}$, unit vector $\boldsymbol{u} \in \mathbb{R}^n$ and $s \geq \eta_\varepsilon(\Lambda)$, we have:*

$$\Pr_{\boldsymbol{b} \hookleftarrow D_{\Lambda,s,\boldsymbol{c}}}[|\langle \boldsymbol{b} - \mathbf{c}, \boldsymbol{u} \rangle| \geq st] \leq \frac{1+\varepsilon}{1-\varepsilon} t\sqrt{2\pi e} \cdot e^{-\pi t^2}.$$

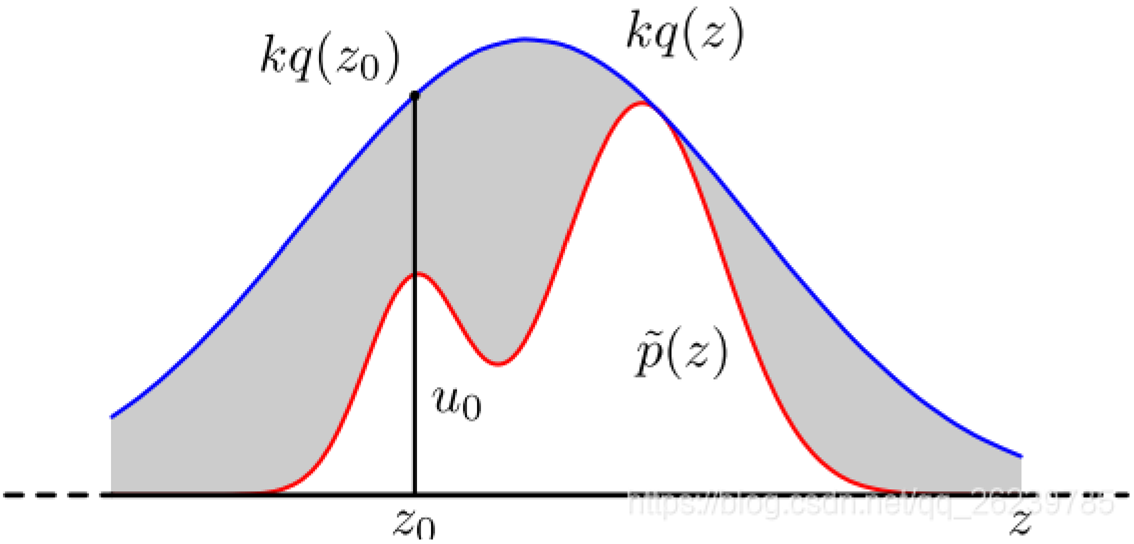
Lemma 1.38 (Adapted from [Pei08, Cor. 5.3]). *Let Λ be an n-dimensional lattice, $\varepsilon \in (0,1)$ and $\boldsymbol{r} \in \mathbb{R}^n$ with $r_i \geq \eta_\varepsilon(\Lambda)$ for all $i \leq n$. Then we have*

$$Pr_{\boldsymbol{x} \hookleftarrow D_{\Lambda,\boldsymbol{r}}}\left[\|\boldsymbol{x}\|_\infty \geq (\max_i r_i) \cdot t\right] \leq 2en \cdot \exp(-\pi t^2),$$

for all $t > 0$. In particular, for $t = \omega(\sqrt{\log n})$ (resp. $t = \Omega(\sqrt{n})$) the above probability is at most $n^{-\omega(1)}$ (resp. $2^{-\Omega(n)}$).

2. Rejection sampling

2.1 Sampling over one dimensional integer lattice



We first define the subroutine Sample$\mathbb{Z}$, which samples from the discrete Gaussian $D_{\mathbb{Z},s,c}$ over the one-dimensional integer lattice $\mathbb{Z}$. Let $t(n) \geq \omega(\sqrt{\log n})$ be some fixed function, say, $t(n) = \log n$. Sample$\mathbb{Z}$ uses rejection sampling, and works as follows: on input (s, c) and (implicitly) the security parameter n, choose an integer $x \leftarrow Z \doteq \mathbb{Z} \cap [c - s \cdot t(n), c + s \cdot t(n)]$ uniformly at random. Then with probability $\rho_s(x - c) \in (0, 1]$, output x, otherwise repeat.

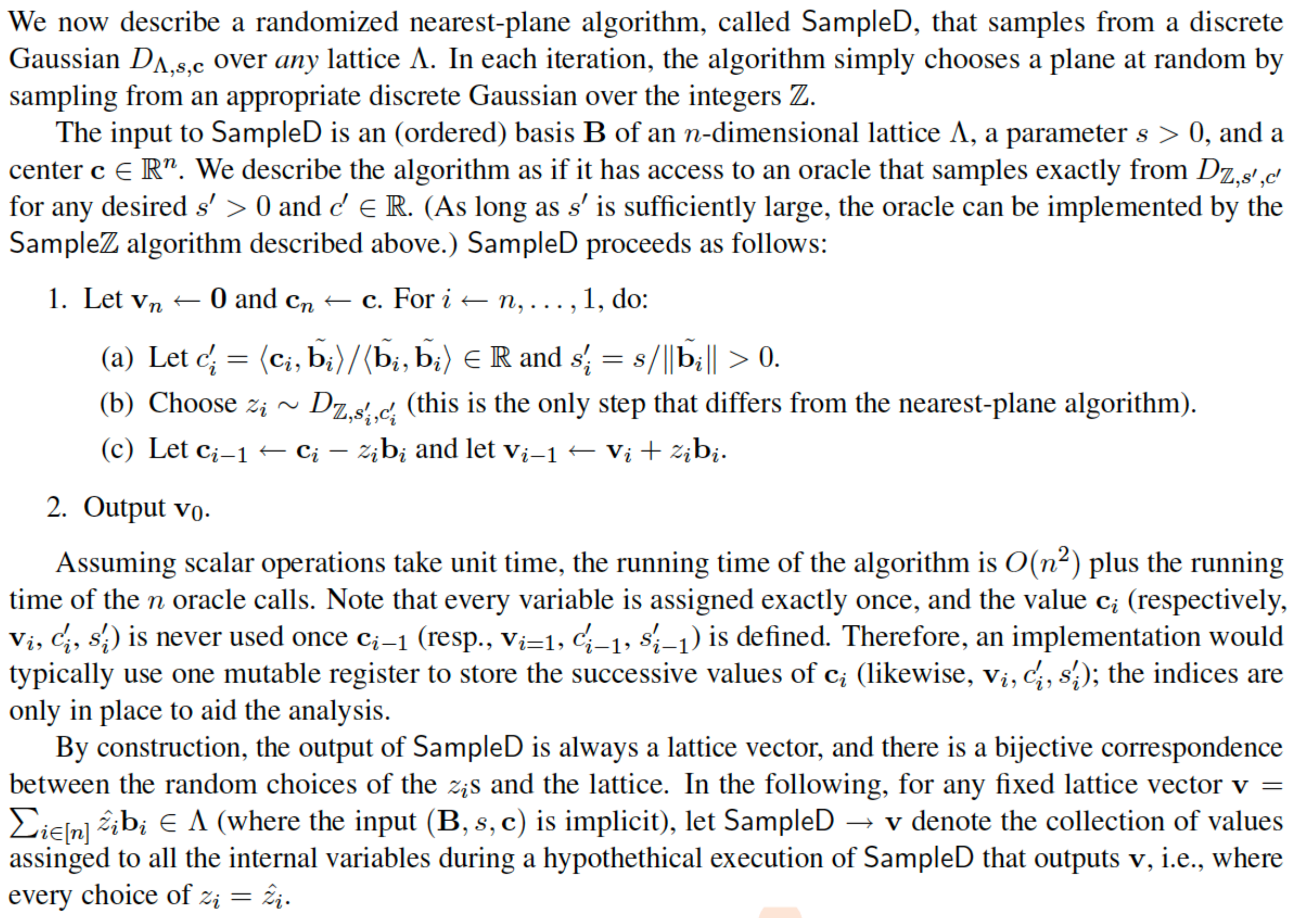
The correctness of the Sample$\mathbb{Z}$ relies on the following tail inequality on the distribution $D_{\mathbb{Z},s,c}$.

Lemma 4.2. *For any $\epsilon > 0$, any $s \geq \eta_\epsilon(\mathbb{Z})$, and any $t > 0$,*

$$\Pr_{x \sim D_{\mathbb{Z},s,c}} [|x - c| \geq t \cdot s] \leq 2e^{-\pi t^2} \cdot \tfrac{1+\epsilon}{1-\epsilon}.$$

In particular, for $\epsilon \in (0, \frac{1}{2})$ and $t \geq \omega(\sqrt{\log n})$, the probability that $|x - c| \geq t \cdot s$ is negligible.

2.2 Sampling from arbitrary lattice



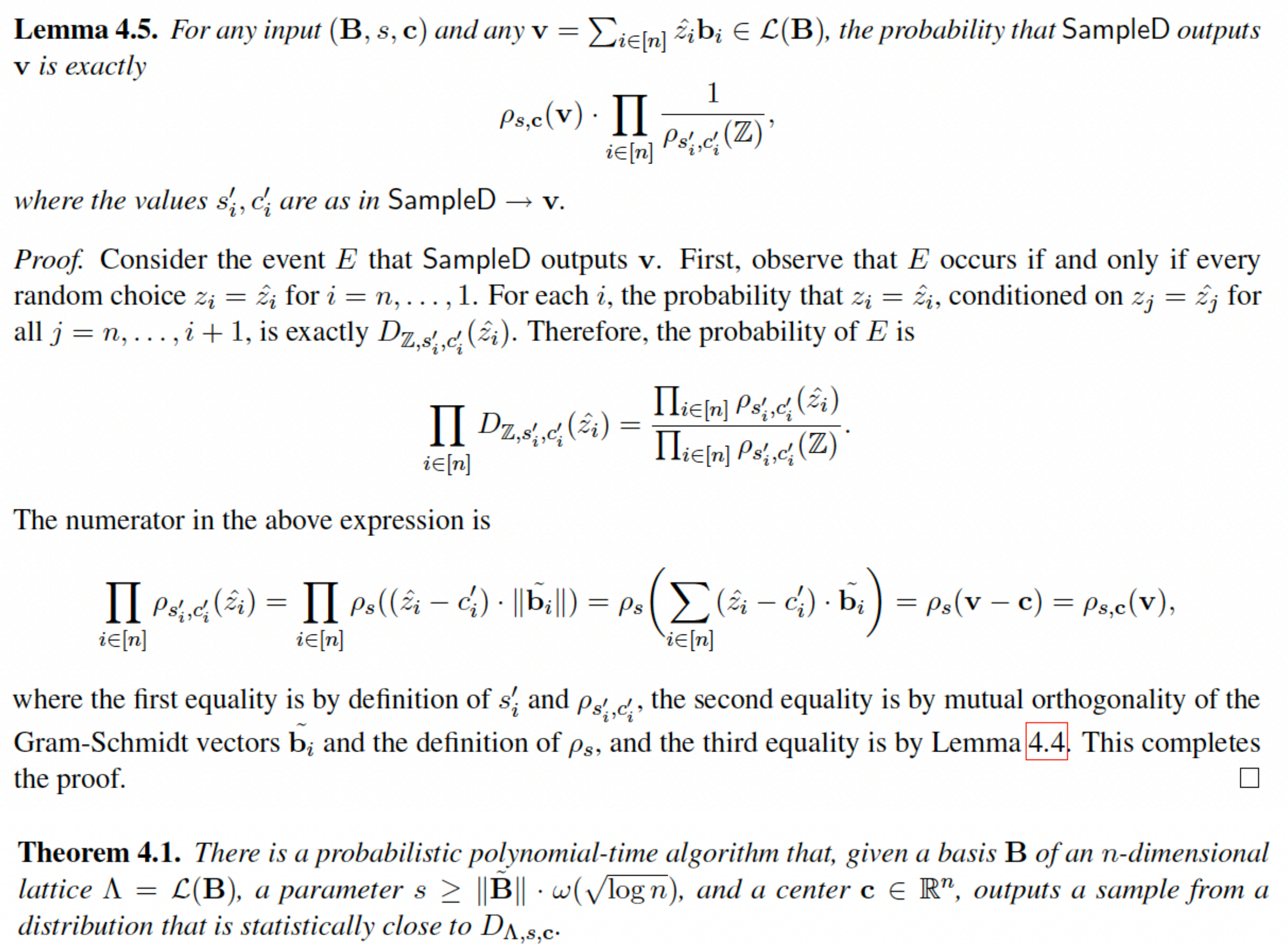
We now describe a randomized nearest-plane algorithm, called SampleD, that samples from a discrete Gaussian $D_{\Lambda,s,\mathbf{c}}$ over *any* lattice Λ. In each iteration, the algorithm simply chooses a plane at random by sampling from an appropriate discrete Gaussian over the integers $\mathbb{Z}$.

The input to SampleD is an (ordered) basis $\mathbf{B}$ of an n-dimensional lattice Λ, a parameter $s > 0$, and a center $\mathbf{c} \in \mathbb{R}^n$. We describe the algorithm as if it has access to an oracle that samples exactly from $D_{\mathbb{Z},s',c'}$ for any desired $s' > 0$ and $c' \in \mathbb{R}$. (As long as s' is sufficiently large, the oracle can be implemented by the Sample$\mathbb{Z}$ algorithm described above.) SampleD proceeds as follows:

1. Let $\mathbf{v}_n \leftarrow \mathbf{0}$ and $\mathbf{c}_n \leftarrow \mathbf{c}$. For $i \leftarrow n, \ldots, 1$, do:
   (a) Let $c'_i = \langle \mathbf{c}_i, \tilde{\mathbf{b}}_i \rangle / \langle \tilde{\mathbf{b}}_i, \tilde{\mathbf{b}}_i \rangle \in \mathbb{R}$ and $s'_i = s / \|\tilde{\mathbf{b}}_i\| > 0$.
   (b) Choose $z_i \sim D_{\mathbb{Z},s'_i,c'_i}$ (this is the only step that differs from the nearest-plane algorithm).
   (c) Let $\mathbf{c}_{i-1} \leftarrow \mathbf{c}_i - z_i \mathbf{b}_i$ and let $\mathbf{v}_{i-1} \leftarrow \mathbf{v}_i + z_i \mathbf{b}_i$.
2. Output $\mathbf{v}_0$.

Assuming scalar operations take unit time, the running time of the algorithm is $O(n^2)$ plus the running time of the n oracle calls. Note that every variable is assigned exactly once, and the value $\mathbf{c}_i$ (respectively, $\mathbf{v}_i$, c'_i, s'_i) is never used once $\mathbf{c}_{i-1}$ (resp., $\mathbf{v}_{i=1}$, c'_{i-1}, s'_{i-1}) is defined. Therefore, an implementation would typically use one mutable register to store the successive values of $\mathbf{c}_i$ (likewise, $\mathbf{v}_i$, c'_i, s'_i); the indices are only in place to aid the analysis.

By construction, the output of SampleD is always a lattice vector, and there is a bijective correspondence between the random choices of the z_is and the lattice. In the following, for any fixed lattice vector $\mathbf{v} = \sum_{i\in[n]} \hat{z}_i \mathbf{b}_i \in \Lambda$ (where the input $(\mathbf{B}, s, \mathbf{c})$ is implicit), let SampleD $\to \mathbf{v}$ denote the collection of values assinged to all the internal variables during a hypothetical execution of SampleD that outputs $\mathbf{v}$, i.e., where every choice of $z_i = \hat{z}_i$.



Lemma 4.5. *For any input* $(\mathbf{B}, s, \mathbf{c})$ *and any* $\mathbf{v} = \sum_{i\in[n]} \hat{z}_i \mathbf{b}_i \in \mathcal{L}(\mathbf{B})$, *the probability that* SampleD *outputs* $\mathbf{v}$ *is exactly*

$$\rho_{s,\mathbf{c}}(\mathbf{v}) \cdot \prod_{i\in[n]} \frac{1}{\rho_{s'_i,c'_i}(\mathbb{Z})},$$

where the values s'_i, c'_i *are as in* SampleD $\to \mathbf{v}$.

Proof. Consider the event E that SampleD outputs $\mathbf{v}$. First, observe that E occurs if and only if every random choice $z_i = \hat{z}_i$ for $i = n, \ldots, 1$. For each i, the probability that $z_i = \hat{z}_i$, conditioned on $z_j = \hat{z}_j$ for all $j = n, \ldots, i+1$, is exactly $D_{\mathbb{Z},s'_i,c'_i}(\hat{z}_i)$. Therefore, the probability of E is

$$\prod_{i\in[n]} D_{\mathbb{Z},s'_i,c'_i}(\hat{z}_i) = \frac{\prod_{i\in[n]} \rho_{s'_i,c'_i}(\hat{z}_i)}{\prod_{i\in[n]} \rho_{s'_i,c'_i}(\mathbb{Z})}.$$

The numerator in the above expression is

$$\prod_{i\in[n]} \rho_{s'_i,c'_i}(\hat{z}_i) = \prod_{i\in[n]} \rho_s((\hat{z}_i - c'_i) \cdot \|\tilde{\mathbf{b}}_i\|) = \rho_s\left(\sum_{i\in[n]} (\hat{z}_i - c'_i) \cdot \tilde{\mathbf{b}}_i\right) = \rho_s(\mathbf{v} - \mathbf{c}) = \rho_{s,\mathbf{c}}(\mathbf{v}),$$

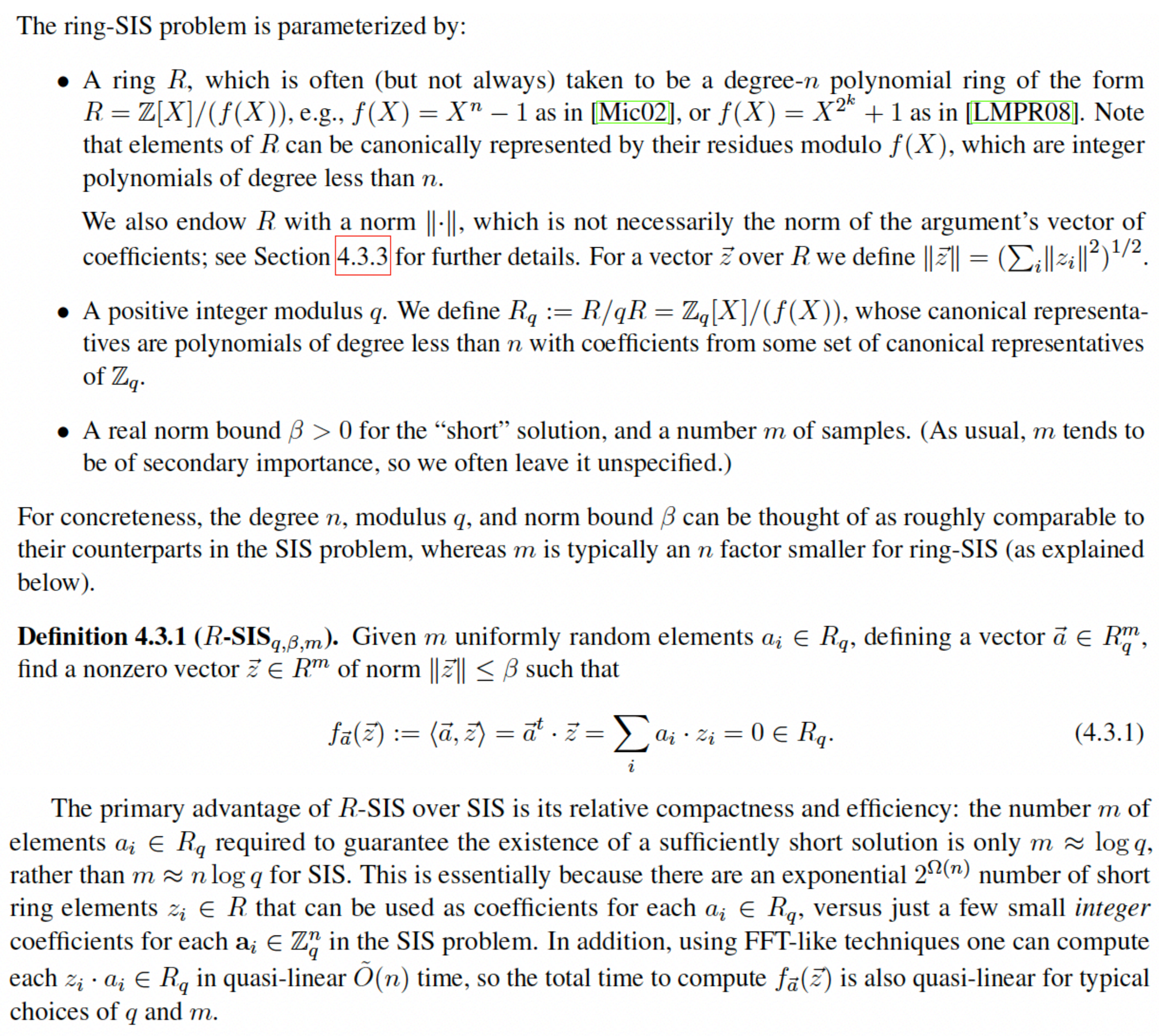
where the first equality is by definition of s'_i and $\rho_{s'_i,c'_i}$, the second equality is by mutual orthogonality of the Gram-Schmidt vectors $\tilde{\mathbf{b}}_i$ and the definition of ρ_s, and the third equality is by Lemma 4.4. This completes the proof. □

Theorem 4.1. *There is a probabilistic polynomial-time algorithm that, given a basis* $\mathbf{B}$ *of an* n*-dimensional lattice* $\Lambda = \mathcal{L}(\mathbf{B})$, *a parameter* $s \geq \|\tilde{\mathbf{B}}\| \cdot \omega(\sqrt{\log n})$, *and a center* $\mathbf{c} \in \mathbb{R}^n$, *outputs a sample from a distribution that is statistically close to* $D_{\Lambda,s,\mathbf{c}}$.

as $s \geq \|\tilde{B}\| \cdot \omega(\sqrt{\log n})$, each $s'_i = s/\|\tilde{b}_i\| \geq \omega(\sqrt{\log n})$.

3. Rings and Modules

3.1 Ring-SIS



The ring-SIS problem is parameterized by:

- A ring R, which is often (but not always) taken to be a degree-n polynomial ring of the form $R = \mathbb{Z}[X]/(f(X))$, e.g., $f(X) = X^n - 1$ as in [Mic02], or $f(X) = X^{2^k} + 1$ as in [LMPR08]. Note that elements of R can be canonically represented by their residues modulo $f(X)$, which are integer polynomials of degree less than n.

  We also endow R with a norm $\|\cdot\|$, which is not necessarily the norm of the argument's vector of coefficients; see Section 4.3.3 for further details. For a vector $\vec{z}$ over R we define $\|\vec{z}\| = (\sum_i \|z_i\|^2)^{1/2}$.

- A positive integer modulus q. We define $R_q := R/qR = \mathbb{Z}_q[X]/(f(X))$, whose canonical representatives are polynomials of degree less than n with coefficients from some set of canonical representatives of $\mathbb{Z}_q$.

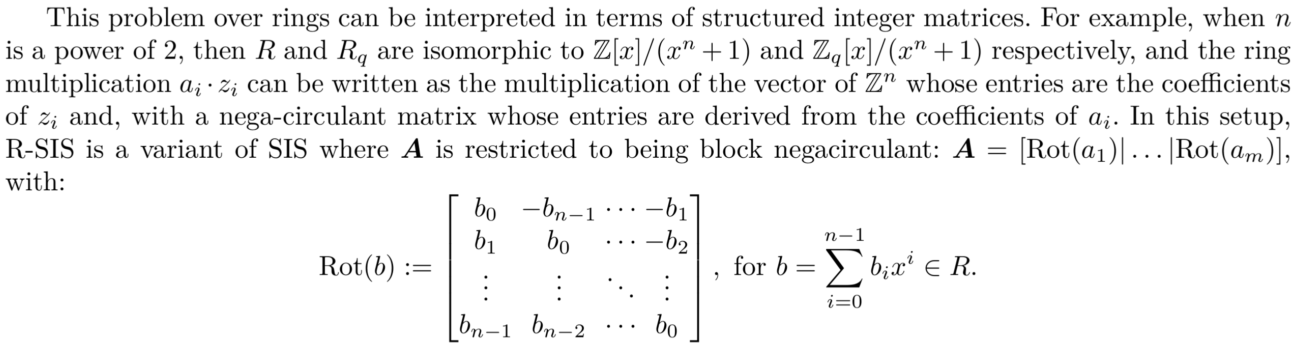
- A real norm bound $\beta > 0$ for the "short" solution, and a number m of samples. (As usual, m tends to be of secondary importance, so we often leave it unspecified.)

For concreteness, the degree n, modulus q, and norm bound β can be thought of as roughly comparable to their counterparts in the SIS problem, whereas m is typically an n factor smaller for ring-SIS (as explained below).

Definition 4.3.1 (R-**SIS**$_{q,\beta,m}$)**.** Given m uniformly random elements $a_i \in R_q$, defining a vector $\vec{a} \in R_q^m$, find a nonzero vector $\vec{z} \in R^m$ of norm $\|\vec{z}\| \leq \beta$ such that

$$f_{\vec{a}}(\vec{z}) := \langle \vec{a}, \vec{z} \rangle = \vec{a}^t \cdot \vec{z} = \sum_i a_i \cdot z_i = 0 \in R_q. \tag{4.3.1}$$

The primary advantage of R-SIS over SIS is its relative compactness and efficiency: the number m of elements $a_i \in R_q$ required to guarantee the existence of a sufficiently short solution is only $m \approx \log q$, rather than $m \approx n \log q$ for SIS. This is essentially because there are an exponential $2^{\Omega(n)}$ number of short ring elements $z_i \in R$ that can be used as coefficients for each $a_i \in R_q$, versus just a few small *integer* coefficients for each $\mathbf{a}_i \in \mathbb{Z}_q^n$ in the SIS problem. In addition, using FFT-like techniques one can compute each $z_i \cdot a_i \in R_q$ in quasi-linear $\tilde{O}(n)$ time, so the total time to compute $f_{\vec{a}}(\vec{z})$ is also quasi-linear for typical choices of q and m.



This problem over rings can be interpreted in terms of structured integer matrices. For example, when n is a power of 2, then R and R_q are isomorphic to $\mathbb{Z}[x]/(x^n+1)$ and $\mathbb{Z}_q[x]/(x^n+1)$ respectively, and the ring multiplication $a_i \cdot z_i$ can be written as the multiplication of the vector of $\mathbb{Z}^n$ whose entries are the coefficients of z_i and, with a nega-circulant matrix whose entries are derived from the coefficients of a_i. In this setup, R-SIS is a variant of SIS where $\boldsymbol{A}$ is restricted to being block negacirculant: $\boldsymbol{A} = [\mathrm{Rot}(a_1)|\ldots|\mathrm{Rot}(a_m)]$, with:

$$\mathrm{Rot}(b) := \begin{bmatrix} b_0 & -b_{n-1} & \cdots & -b_1 \\ b_1 & b_0 & \cdots & -b_2 \\ \vdots & \vdots & \ddots & \vdots \\ b_{n-1} & b_{n-2} & \cdots & b_0 \end{bmatrix}, \text{ for } b = \sum_{i=0}^{n-1} b_i x^i \in R.$$

3.2 Module-SIS

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{bmatrix} \cdot \begin{bmatrix} z_1 \\ z_2 \\ z_3 \end{bmatrix} = 0 \mod q.$$

Ideals. An (integral) *ideal* I of R is an additive subgroup of R that is closed under multiplication by every element of R. The smallest ideal of R containing the set S is denoted by (S). The quotient R/I is the set of the equivalence classes $g + I$ of R modulo I. For any nonzero ideal, the *norm* $\mathcal{N}(I)$ of the ideal is the number of elements of the quotient ring R/I. We have $\mathcal{N}((x)) = \mathcal{N}(x)$, for all $x \in K$.

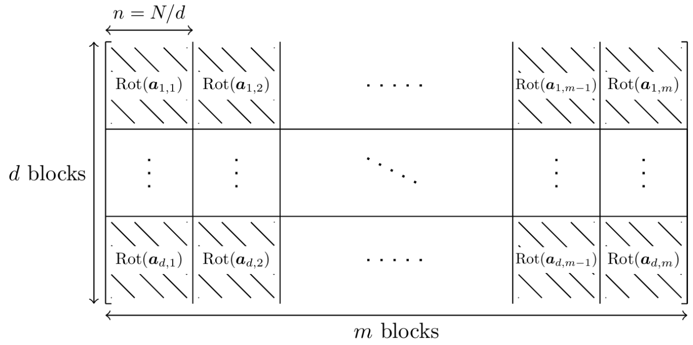
Let I and J be ideals of R. We define the *product* of two ideals by $IJ = \{\sum_i \alpha_i\beta_i : \alpha_i \in I, \beta_i \in J\}$ and their *sum* by $I + J = \{\alpha + \beta : \alpha \in I, \beta \in J\}$. An ideal $I \subsetneq R$ is *prime* if for any $ab \in I$ then $a \in I$ or $b \in I$. Every ideal of R can be represented as a unique product of prime ideals, and for a prime ideal I, the quotient ring R/I is the finite field of order $\mathcal{N}(I)$. A *fractional ideal* $I \subseteq K$ is a set such that $dI \subseteq R$ is an (integral) ideal for a nonzero $d \in R$. The *inverse* of a fractional I is defined by $I^{-1} = \{\alpha \in K : \alpha I \subseteq R\}$ and is itself a fractional ideal. We have $II^{-1} = R$. The *dual* of an ideal is defined as $I^\vee = \{x \in K : \mathrm{Tr}(xI) \subseteq \mathbb{Z}\}$. We have $I^\vee = I^{-1} \cdot R^\vee$.

Ideal and module lattices. As σ_H is an embedding from K to $\mathbb{R}^n$ and I an ideal of R, the set $\sigma_H(I)$ is a lattice. We call it ideal lattice with respect to K. To ease the presentation, we often identify I and $\sigma_H(I)$. We let Id-GIVP denote the restriction of GIVP to ideal lattices.

We define module lattices similarly. The map $(\sigma_H, \ldots, \sigma_H)$ is an embedding from K^d to $\mathbb{R}^N$, with $N = nd$, and $M \subseteq K^d$ a module of R. By abuse of notation, we also call it σ_H. The set $\sigma_H(M)$ is a module lattice. Similarly to ideal lattices, we let Mod-GIVP denote the restriction of GIVP to module lattices. Note that if M is a rank d module and if K has degree n, then the corresponding module lattice has dimension $N = nd$.

Definition 3.5. *The problem* M-SIS$_{q,m,\beta}$ *is as follows: Given* $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m \in R_q^d$ *chosen independently from the uniform distribution, find* $z_1, \ldots, z_m \in R$ *such that* $\sum_{i=1}^m \boldsymbol{a}_i \cdot z_i = 0 \bmod q$ *and* $0 < \|\boldsymbol{z}\| \leq \beta$*, where* $\boldsymbol{z} = (z_1, \ldots, z_m)^T \in R^m$.

Like R-SIS, M-SIS can be interpreted in terms of matrices. In the same setting as above for R-SIS, it consists in taking a SIS matrix $\boldsymbol{A}$ of the form:


$n = N/d$
Rot($\boldsymbol{a}_{1,1}$)
Rot($\boldsymbol{a}_{1,2}$)
.....
Rot($\boldsymbol{a}_{1,m-1}$)
Rot($\boldsymbol{a}_{1,m}$)
d blocks
Rot($\boldsymbol{a}_{d,1}$)
Rot($\boldsymbol{a}_{d,2}$)
.....
Rot($\boldsymbol{a}_{d,m-1}$)
Rot($\boldsymbol{a}_{d,m}$)
m blocks

Next time: FFT, quasi linear multiplication over rings.

------------------------- This is the end of this lecture ;) ------------------------------------