The Discrete Gaussian Distribution

The Gaussian function of parameter $s > 0$ is defined over all $\vec{x} \in \mathbb{R}^m$ by :

$$\rho_s(\vec{x}) = e^{-\pi \frac{\|\vec{x}\|^2}{s^2}}.$$

For any countable subset $A \subseteq \mathbb{R}^m$, we denote the Gaussian mass of A by $\rho_s(A) = \sum_{\vec{x} \in A} \rho_s(\vec{x})$ when the sum converges.

1. Gaussian integrals. ($\star$)

Show that for any n-dimensional subspace E of $\mathbb{R}^m$:

$$\int_{\vec{x} \in E} \rho_s(\vec{x}) d\vec{x} = s^n.$$

2. Gaussian mass. ($\star\star$)

If L is a lattice and $\vec{x} \in \mathbb{R}^m$, show that $\rho_s(\vec{x} + L)$ is well-defined for any $s > 0$. Hint : the Gaussian heuristic holds for sufficiently large balls.

The discrete Gaussian distribution over L centered at $\vec{c} \in \mathbb{R}^m$ and width $s > 0$ is defined as follows : each vector $\vec{v} \in L$ has mass $\rho_s(\vec{v} - \vec{c})/\rho_s(L - \vec{c})$, so that the sum of all masses is 1 and the most likely lattice points are the ones closest to $\vec{c}$. If $\vec{c}$ is omitted, it means that $\vec{c} = 0$. Alternatively, this general distribution over L can be viewed as a distribution over any coset $L - \vec{c}$: each element $\vec{y} \in L - \vec{c}$ has mass $\rho_s(\vec{y})/\rho_s(L - \vec{c})$.

3. The One-Dimensional Case. ($\star$)

Show that :

---

1. *For any $s > 0$, we have : $1 \leq \rho_s(\mathbb{Z}) \leq 1 + s$.*
2. *For any $s > 0$, $0 \leq c < 1$, and any $n \geq 1$:*

$$\rho_s(\mathbb{Z}^* - c) \leq \frac{n^{n/2} s^n}{(1 - c)^n}.$$

---

4. Poisson's summation. ($\star$)

Poisson's summation transforms a sum over a lattice L into a sum over the dual lattice $L^\times$, by studying the Fourier series of a function periodic with respect to L : it shows that for all sufficiently "nice" functions f over the linear span of L,

$$\sum_{\vec{v} \in L} f(\vec{v}) = \frac{1}{\mathrm{vol} L} \sum_{\vec{w} \in L^\times} \hat{f}(\vec{w}),$$

where $\hat{f}$ is the Fourier transform of f. The Gaussian function is one such nice function, and because its Fourier transform is proportional to itself, Poisson's summation shows in particular the following fundamental equality for any n-rank lattice L and $\vec{x} \in \mathrm{span}(L)$:

$$\rho_s(\vec{x} + L) = \frac{s^n}{\mathrm{vol} L} \sum_{\vec{y} \in L^\times} \rho_{1/s}(\vec{y}) e^{2i\pi \langle \vec{y}, \vec{x} \rangle}.$$

Deduce that :

1. $\rho_s(L) = \frac{s^n}{\mathrm{vol}L}\rho_{1/s}(L^\times)$ *and* $\rho_s(L) \geq \frac{s^n}{\mathrm{vol}L}$
2. $\rho_s(L) \leq s^n\rho_1(L)$ *if* $s \geq 1$.
3. $\rho_s(\vec{x}+L) \leq \rho_s(L)$ *and* $\rho_s(L)e^{-\pi d^2/s^2} \leq \rho_s(\vec{x}+L)$ *where* $d = \min_{\vec{y}\in\vec{x}+L}\|\vec{y}\|$ *is the distance between* $-\vec{x}$ *and* L.
4. $\max_{\vec{x}\in\mathrm{span}(L)}\left|\rho_s(\vec{x}+L) - \frac{s^n}{\mathrm{vol}L}\right| = \frac{s^n\rho_{1/s}(L^\times\setminus\{0\})}{\mathrm{vol}L}$

5. The smoothing parameter. (⋆⋆)

For $\varepsilon > 0$, Micciancio and Regev introduced the *smoothing parameter* $\eta_\varepsilon(L)$ of L as the smallest $s > 0$ such that $\rho_{1/s}(L^\times \setminus \{0\}) \leq \varepsilon$. Show that :

1. *For any* $s \geq \eta_\varepsilon(L)$:

$$\max_{\vec{x}\in\mathrm{span}(L)}\left|\rho_s(\vec{x}+L) - \frac{s^n}{\mathrm{vol}L}\right| \leq \varepsilon\frac{s^n}{\mathrm{vol}L}.$$

   In particular, this shows that beyond the smoothing parameter, all Gaussian masses $\rho_s(\vec{x}+L)$ *are close to each other, independently of the shift* $\vec{x}$. *This property is crucial for the discrete Gaussian sampler of [GPV08] and for worst-case to average-case reductions.*
2. *For* $0 < \varepsilon < 1$, $\sqrt{\frac{\log(2/\varepsilon)}{\pi}} \leq \eta_\varepsilon(\mathbb{Z}) \leq \sqrt{\frac{\log(2(1+1/\varepsilon))}{\pi}}$ *and more generally* $\eta_\varepsilon(\mathbb{Z}^n) \leq \sqrt{\frac{\log(2n(1+1/\varepsilon))}{\pi}}$.
3. *For* $\varepsilon > 0$, $\eta_\varepsilon(L) \leq \lambda_n(L)\eta_\varepsilon(\mathbb{Z}^n)$. *Hint : there is a basis* $(\vec{b}_1,\ldots,\vec{b}_n)$ *of* L *such that* $\|\vec{b}_i^\star\| \leq \lambda_i(L)$.

6. Gram-Schmidt Lattices. (⋆)

Let $B = (\vec{b}_1,\ldots,\vec{b}_n)$ be a basis of a lattice L. Let L_B be the lattice spanned by the Gram-Schmidt vectors $\vec{b}_1^\star,\ldots,\vec{b}_n^\star$. Show that :

$$\rho_s(L) \leq \rho_s(L_B) = \prod_{i=1}^n \rho_s(\|\vec{b}_i^\star\|\mathbb{Z}) \leq \prod_{i=1}^n\left(1 + \frac{s}{\|\vec{b}_i^\star\|}\right).$$

7. Sublattices. (⋆)

Let L be an n-rank lattice. Let $L' \subseteq L$ be a sublattice of L such that L/L' is finite. Show that for any $s > 0$:

$$\frac{1}{[L:L']} \leq \frac{\rho_s(L')}{\rho_s(L)} \text{ and if } s \geq \eta_\varepsilon(L'), \frac{\rho_s(L')}{\rho_s(L)} \leq \frac{1}{[L:L']}(1+\varepsilon).$$

Show that if $s \geq \eta_\varepsilon(L')$ and $\vec{x} \in L$ is chosen at random from the discrete Gaussian distribution over L, then the distribution of $\vec{x}+L' \in L/L'$ is close to uniform over L/L'. This property is crucial for the SIS worst-case to average-case distribution.

8. Linear independence. ($\star\star$)

Let L be an n-rank lattice. Show that for sufficiently large s, if $\vec{v}_1, \ldots, \vec{v}_n$ are chosen independently at random from the discrete Gaussian distribution over L, then $\vec{v}_1, \ldots, \vec{v}_n$ are linearly independent with probability asymptotically close to 1 as n grows to infinity.

9. Gaussian concentration. ($\star\star\star$)

Let L be an n-rank lattice and $\vec{c}$ in the linear span of L. Let $\mathcal{B}$ be the unit ball of the linear span of L.

---

1. *Show that for all $s > 0$ and $u \geq 1/\sqrt{2\pi}$:*

$$\rho_s((L - \vec{c}) \setminus us\sqrt{n}\mathcal{B}) \leq (2\pi e u^2)^{n/2} e^{-\pi u^2 n} \rho_s(L).$$

2. *Let $d = \min_{\vec{y} \in L - \vec{c}} \|\vec{y}\|$ be the distance between $\vec{c}$ and L. Let $r > 0$ be such that $r > \sqrt{\frac{n}{2\pi}} s$, $r > d$ and $r^2 > d^2 + \frac{ns^2}{\pi} \log(\frac{2\pi d^2}{ns^2})$. When $\vec{v} \in L$ is chosen at random from the discrete Gaussian distribution over L with center $\vec{c}$ and width s, the probability that $\|\vec{v} - \vec{c}\| > r$ is :*

$$< (2e)^{n/2+1} e^{-\pi y^2/2},$$

where $y = \sqrt{r^2 - d^2}/s$. This means that most Gaussian lattice points $\vec{y}$ are within distance $O(s\sqrt{n})$ from $\vec{c}$.

For more information on the discrete Gaussian distribution, and proofs of many results, see Noah Stephens-Davidowitz's 2017 PhD Thesis : On the Gaussian Measure Over Lattices.