Mastermath, Spring 2018 | **Lecturers: D. Dadush, L. Ducas**
Intro to Lattice Algs & Crypto | **Lecture 7** | **Scribe: S. Huiberts**

Periodic Gaussian, Discrete Gaussian and Transference

In this lecture, we look at the Periodic and Discrete Gaussian functions and study them through Fourier-analytic methods. We prove a tail bound for the Discrete Gaussian, which we use to prove a stronger transference result.

1 The Periodic Gaussian

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

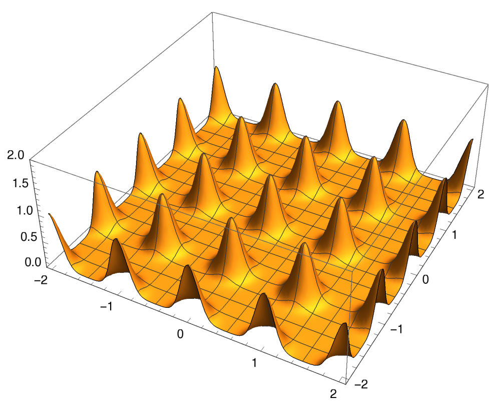
$$\rho_s(\mathbf{x}) := e^{-\pi\|\mathbf{x}/s\|^2}, \qquad s > 0,$$

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

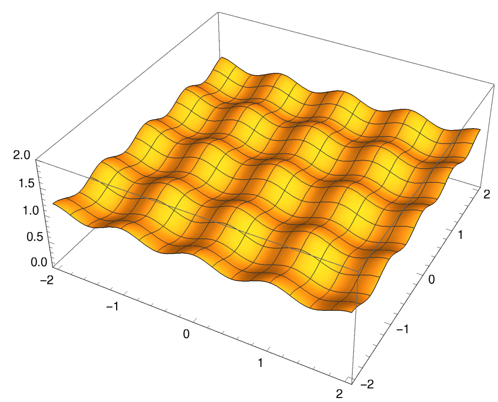
$$f_s(\mathbf{t}) := \rho_s(\mathcal{L} + \mathbf{t}) = \sum_{\mathbf{x} \in \mathcal{L}} \rho_s(\mathbf{x} + \mathbf{t}).$$

We write $\rho := \rho_1$.

The function f_s 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 $s = 1$.

Proposition 2 *The functions ρ_s satisfy the following properties.*

1. $\int_{\mathbb{R}^n} \rho_s(\mathbf{x}) \mathrm{d}\mathbf{x} = s^n$.
2. $\widehat{\rho_s}(\mathbf{y}) = s^n \rho_{1/s}(\mathbf{y})$.

Proof: We prove both properties for $s = 1$. The general cases follow by a change of variables. The first property is proven by switching the product and integration:

$$\int_{\mathbb{R}^n} \rho(\mathbf{x}) \mathrm{d}\mathbf{x} = \int_{\mathbb{R}^n} \prod_{i=1}^{n} e^{-\pi x_i^2} \mathrm{d}\mathbf{x} = \prod_{i=1}^{n} \int_{-\infty}^{\infty} e^{-\pi x_i^2} \mathrm{d}x_i = 1.$$

The equality $\int_{-\infty}^{\infty} e^{-\pi x_i^2} \mathrm{d}x_i = 1$ is the standard Gaussian integral.

Observe that we can also integrate every variable separately to prove the second property.

$$\widehat{\rho}(\mathbf{y}) = \int_{\mathbb{R}^n} e^{-\pi\|\mathbf{x}\|^2} e^{-2\pi i\langle \mathbf{y},\mathbf{x}\rangle} \mathrm{d}\mathbf{x} = \prod_{j=1}^{n} \int_{-\infty}^{\infty} e^{-\pi x_j^2 - 2\pi i y_j x_j} \mathrm{d}x_j$$

We complete the square and get $\int_{-\infty}^{\infty} e^{-\pi x_j^2 - 2\pi i y_j x_j} \mathrm{d}x_j = e^{-\pi y_j^2} \int_{-\infty}^{\infty} e^{-\pi(x_j + i y_j)^2} \mathrm{d}x_j$. We argue that the integral $\int_{-\infty}^{\infty} e^{-\pi(x_j+iy_j)^2} \mathrm{d}x_j$ is the same for every value of y_j, which we show by differentiation.

$$\begin{aligned} \frac{\mathrm{d}}{\mathrm{d}y_j} \int_{-\infty}^{\infty} e^{-\pi(x_j+iy_j)^2} \mathrm{d}x_j &= \int_{-\infty}^{\infty} (2ix_j - 2iy_j) e^{-\pi(x_j+iy_j)^2} \mathrm{d}x_j \\ &= 2i[e^{-\pi(x_j+iy_j)^2}]_{x_j=-\infty}^{\infty} \\ &= 0. \end{aligned}$$

The derivative equals 0 for all values of y_j, hence the integral does not depend on y_j and $\int_{-\infty}^{\infty} e^{-\pi(x_j+iy_j)^2} \mathrm{d}x_j = \int_{-\infty}^{\infty} e^{-\pi x_j^2} \mathrm{d}x_j = 1$. □

Lemma 3 (Properties of the periodic Gaussian) *For a full-rank lattice $\mathcal{L} \subset \mathbb{R}^n$ and $s > 0$, the periodic Gaussian f_s satisfies*

1. *$f_s(\mathbf{t})$ is maximized when $\mathbf{t} \in \mathcal{L}$.*
2. *$f_s(\mathbf{t}) \geq f_s(\mathbf{0}) e^{-\pi\|\mathbf{t}/s\|^2}$ for all $\mathbf{t} \in \mathbb{R}^n$.*

Proof: The function ρ_s satisfies all conditions for the Poisson summation formula: it is continuous, and satisfies $|\rho_s(\mathbf{x})| \leq \frac{C}{(\|\mathbf{x}\|+1)^{n+\delta}}$ for some $C, \delta > 0$. In particular, $\rho(\mathbf{x}) \geq 0$, and

$$\rho(\mathbf{x}) \leq e^{-\|\mathbf{x}\|^2} \leq C e^{-(n+\delta)\|\mathbf{x}\|} \leq \frac{C}{(1 + \|\mathbf{x}\|)^{(n+\delta)}},$$

for $C = e^{(n+\delta)^2}$ and any $\delta > 0$. The second inequality follows from $a \cdot b \leq a^2 + b^2$, and the last inequality stems from the fact that $1 + a \leq e^a$.

As ρ_s satisfies all necessary conditions, we can use the Poisson summation formula:

$$\begin{aligned} \rho_s(\mathcal{L} + \mathbf{t}) &= \frac{1}{\det(\mathcal{L})} \sum_{\mathbf{y} \in \mathcal{L}^*} e^{2\pi i\langle \mathbf{y},\mathbf{t}\rangle} \widehat{\rho_s}(\mathbf{y}) \\ &= \frac{s^n}{\det(\mathcal{L})} \sum_{\mathbf{y} \in \mathcal{L}^*} e^{2\pi i\langle \mathbf{y},\mathbf{t}\rangle} \rho_{1/s}(\mathbf{y}). \end{aligned}$$

We know that ρ_s is real-valued, so it makes sense to upper bound the above sum. The function $\rho_{1/s}$ is non-negative everywhere, so we can upper bound the summation by the triangle inequality as

$$\sum_{\mathbf{y} \in \mathcal{L}^*} e^{2\pi i\langle \mathbf{y},\mathbf{t}\rangle} \rho_{1/s}(\mathbf{y}) \leq |\sum_{\mathbf{y} \in \mathcal{L}^*} e^{2\pi i\langle \mathbf{y},\mathbf{t}\rangle} \rho_{1/s}(\mathbf{y})| \leq \sum_{\mathbf{y} \in \mathcal{L}^*} |e^{2\pi i\langle \mathbf{y},\mathbf{t}\rangle}| \rho_{1/s}(\mathbf{y}).$$

For $\mathbf{t} \in \mathcal{L}$ we have $e^{2\pi i\langle \mathbf{y},\mathbf{t}\rangle} = 1$, which makes both inequalities tight. Hence ρ_s attains its maximal value at points $\mathbf{t} \in \mathcal{L}$.

For the second statement, we have

$$\begin{aligned}
f_s(\mathbf{t}) &= \sum_{\mathbf{x}\in\mathcal{L}} e^{-\pi\|\frac{\mathbf{x}+\mathbf{t}}{s}\|^2} \\
&= \sum_{\mathbf{x}\in\mathcal{L}} \frac{1}{2}(e^{-\pi\|\frac{\mathbf{x}+\mathbf{t}}{s}\|^2} + e^{-\pi\|\frac{\mathbf{t}-\mathbf{x}}{s}\|^2}) \\
&= \sum_{\mathbf{x}\in\mathcal{L}} e^{-\pi\|\mathbf{t}/s\|^2} e^{-\pi\|\mathbf{x}/s\|^2} (\frac{1}{2}e^{-2\pi\langle\mathbf{x},\mathbf{t}\rangle/s^2} + \frac{1}{2}e^{2\pi\langle\mathbf{x},\mathbf{t}\rangle/s^2}).
\end{aligned}$$

By convexity, $\frac{1}{2}e^{-2\pi\langle\mathbf{x},\mathbf{t}\rangle/s^2} + \frac{1}{2}e^{2\pi\langle\mathbf{x},\mathbf{t}\rangle/s^2} \geq 1$. □

DEFINITION 4 *For a full-rank lattice $\mathcal{L} \subset \mathbb{R}^n$ and $\varepsilon > 0$, the smoothing parameter $\eta_\varepsilon(\mathcal{L})$ is the number $s > 0$ such that $\rho_{1/s}(\mathcal{L}^*) = 1 + \varepsilon$.*

As a function of s, $\rho_{1/s}(\mathcal{L}^*)$ is strictly decreasing, going to 0 as $s \to \infty$ and going to ∞ as $s \to 0$. Because of this, $\eta_\varepsilon(\mathcal{L})$ is well-defined: it exists and is unique. The following lemma justifies why we call $\eta_\varepsilon(\mathcal{L})$ the smoothing parameter.

LEMMA 5 *For $\mathcal{L} \subset \mathbb{R}^n$ a lattice and $s \geq \eta_\varepsilon(\mathcal{L})$, we have*

$$(1-\varepsilon)\frac{s^n}{\det(\mathcal{L})} \leq \rho_s(\mathcal{L}+t) \leq (1+\varepsilon)\frac{s^n}{\det(\mathcal{L})}.$$

PROOF: Using the Poisson summation formula we get

$$\begin{aligned}
\rho_s(\mathcal{L}+\mathbf{t}) &= \frac{s^n}{\det(\mathcal{L})} \sum_{\mathbf{y}\in\mathcal{L}^*} e^{2\pi i\langle\mathbf{y},\mathbf{t}\rangle} e^{-\pi\|s\mathbf{y}\|^2} \\
&= \frac{s^n}{\det(\mathcal{L})} \left(1 + \sum_{\mathbf{y}\in\mathcal{L}^*\setminus\{\mathbf{0}\}} e^{2\pi i\langle\mathbf{y},\mathbf{t}\rangle} e^{-\pi\|s\mathbf{y}\|^2}\right).
\end{aligned}$$

It suffices if we can bound the summation in absolute value by ε. By the triangle inequality, $|\sum_{\mathbf{y}\in\mathcal{L}^*\setminus\{\mathbf{0}\}} e^{2\pi i\langle\mathbf{y},\mathbf{t}\rangle} e^{-\pi\|s\mathbf{y}\|^2}| \leq \sum_{\mathbf{y}\in\mathcal{L}^*\setminus\{\mathbf{0}\}} |e^{2\pi i\langle\mathbf{y},\mathbf{t}\rangle}| e^{-\pi\|s\mathbf{y}\|^2}$. We know that $|e^{2\pi i\langle\mathbf{y},\mathbf{t}\rangle}| \leq 1$, so the last sum is bounded by $\rho_{1/s}(\mathcal{L}^*\setminus\{\mathbf{0}\})$. Now recall that $\rho_{1/s}(\mathcal{L}^*\setminus\{\mathbf{0}\}) \leq \varepsilon$ by our assumption that $s \geq \eta_\varepsilon(\mathcal{L})$. This implies

$$\rho_s(\mathcal{L}+\mathbf{t}) \in [1-\varepsilon, 1+\varepsilon]\frac{s^n}{\det(\mathcal{L})}.$$

□

For some basic intuition, we provide the next two lemmas on the behavior of $\eta_\varepsilon(\mathcal{L})$

LEMMA 6 *For $\mathcal{L} \subset \mathbb{R}^n$ a full-rank lattice, $\eta_{1/2}(\mathcal{L}) \geq \frac{1}{2\lambda_1(\mathcal{L}^*)}$.*

PROOF: Let $s = \frac{1}{2\lambda_1(\mathcal{L}^*)}$. It suffices to show that $\rho_{1/s}(\mathcal{L}^*) \geq 3/2$. Let $\mathbf{x} \in \mathcal{L}^*$ have $\|\mathbf{x}\| = \lambda_1(\mathcal{L}^*)$. We have

$$\rho_{1/s}(\mathcal{L}^*) > 1 + \rho_{1/s}(\mathbf{x}) + \rho_{1/s}(-\mathbf{x}) = 1 + 2\cdot e^{-\pi\|s\mathbf{x}\|^2} > \frac{3}{2},$$

as needed. □

The function $\rho_s(\mathcal{L}\setminus\{\mathbf{0}\})$ decays quickly as s grows. This is reflected in the smoothing parameter for different values of ε, which are not too far off from each other.

Lemma 7 *For any full-rank lattice $\mathcal{L} \subset \mathbb{R}^n$, $\varepsilon \in (0,1)$, and $k > 1$, we have $\eta_\varepsilon(\mathcal{L}) < \eta_{\varepsilon^{k^2}}(\mathcal{L}) < k\eta_\varepsilon(\mathcal{L})$.*

Proof: The first inequality holds because $\rho_{1/s}(\mathcal{L}^*)$ is strictly decreasing in s. Now suppose without loss of generality that $\eta_\varepsilon(\mathcal{L}) = 1$. Then,

$$\rho_{1/k\eta_\varepsilon(\mathcal{L})}(\mathcal{L}^* \backslash \{\mathbf{0}\}) = \sum_{\mathbf{y} \in \mathcal{L}^* \backslash \{\mathbf{0}\}} \rho_{\eta_\varepsilon(\mathcal{L})}(\mathbf{y})^{k^2} < \left(\sum_{\mathbf{y} \in \mathcal{L}^* \backslash \{\mathbf{0}\}} \rho_{\eta_\varepsilon(\mathcal{L})}(\mathbf{y}) \right)^{k^2} = \varepsilon^{k^2},$$

so $k\eta_\varepsilon(\mathcal{L}) > \eta_{\varepsilon^{k^2}}(\mathcal{L})$ as needed. □

Proposition 8 *For a full-rank lattice $\mathcal{L} \subset \mathbb{R}^n$ and any $\mathbf{t} \in \mathbb{R}^n, s > 0, \alpha \geq 1$ we have*

$$\rho_{\alpha s}(\mathcal{L} + \mathbf{t}) \leq \alpha^n \rho_s(\mathcal{L}).$$

Proof: We recall that by Lemma 3, $\rho_{\alpha s}(\mathcal{L} + \mathbf{t}) \leq \rho_{\alpha s}(\mathcal{L})$. From here, we derive the result using the Poisson summation formula:

$$\begin{aligned} \rho_{\alpha s}(\mathcal{L}) &= \frac{(\alpha s)^n}{\det(\mathcal{L})} \rho_{1/(\alpha s)}(\mathcal{L}^*) \\ &\leq \alpha^n \frac{s^n}{\det(\mathcal{L})} \rho_{1/s}(\mathcal{L}^*) \\ &= \alpha^n \rho_s(\mathcal{L}). \end{aligned}$$

□

2 The Discrete Gaussian

In this section we define the discrete Gaussian distribution. For the discrete Gaussian we can prove similar tail bounds as for the regular Gaussian. At the end of this section, we use these tail bound to get a stronger transference result.

Definition 9 *For a full-rank lattice $\mathcal{L} \subset \mathbb{R}^n$, $s > 0$ and $\mathbf{t} \in \mathbb{R}^n$, the discrete Gaussian distribution $D_{\mathcal{L}+\mathbf{t},s}$ has probability mass function $\Pr_{\mathbf{X} \sim D_{\mathcal{L}+\mathbf{t},s}}[\mathbf{X} = \mathbf{x}] = \frac{\rho_s(\mathbf{x})}{\rho_s(\mathcal{L}+\mathbf{t})}$ if $\mathbf{x} \in \mathcal{L} + \mathbf{t}$ and 0 otherwise.*

To prove a strong tail bound on the norm of $\mathbf{X} \sim D_{\mathcal{L}+\mathbf{t},s}$, we use the following general bound for non-negative random variables.

Lemma 10 *For any random variable X on $\mathbb{R}_+$ we have the following tail estimate for all $t, \lambda > 0$:*

$$\Pr[X \geq t] \leq \frac{\mathbb{E}[e^{\lambda X^2}]}{e^{\lambda t^2}}.$$

Proof: By monotonicity we have the following equalities of probabilities:

$$\Pr[X \geq t] = \Pr[X^2 \geq t^2] = \Pr[\lambda X^2 \geq \lambda t^2] = \Pr[e^{\lambda X^2} \geq e^{\lambda t^2}].$$

Recall Markov's inequality: for $s > 0$ and a random variable Y on $\mathbb{R}_+$ we have $\Pr[Y \geq s] \leq \frac{\mathbb{E}[Y]}{s}$. This is because $\mathbb{E}[Y] = \mathbb{E}[Y | Y \geq s] \Pr[Y \geq s] + \mathbb{E}[Y | Y < s] \Pr[Y < s] \geq s \Pr[Y \geq s]$. The result immediately follows. □

LEMMA 11 *Let $\mathcal{L} \subset \mathbb{R}^n$ be a full-rank lattice and $\mathbf{t} \in \mathbb{R}^n$. For any $\alpha < 1$ and $\mathbf{X} \sim D_{\mathcal{L}+\mathbf{t}}$,*

$$\mathbb{E}[e^{\alpha\pi\|\mathbf{X}\|^2}] \leq \frac{1}{\sqrt{1-\alpha}^n} \cdot \frac{\rho(\mathcal{L})}{\rho(\mathcal{L}+\mathbf{t})}.$$

PROOF: We rewrite the expectation by writing out the summation defining it.

$$\begin{aligned}\mathbb{E}[e^{\alpha\pi\|\mathbf{X}\|^2}] &= \frac{\sum_{\mathbf{x}\in\mathcal{L}+\mathbf{t}} e^{\alpha\pi\|\mathbf{x}\|^2} e^{-\pi\|\mathbf{x}\|^2}}{\rho(\mathcal{L}+\mathbf{t})} \\ &= \frac{\rho_{1/\sqrt{1-\alpha}}(\mathcal{L}+\mathbf{t})}{\rho(\mathcal{L}+\mathbf{t})}\end{aligned}$$

By Proposition 8, $\rho_{1/\sqrt{1-\alpha}}(\mathcal{L}+\mathbf{t}) \leq \frac{1}{\sqrt{1-\alpha}^n} \frac{\rho(\mathcal{L})}{\rho(\mathcal{L}+\mathbf{t})}$ as needed. □

THEOREM 12 *For $\mathcal{L} \subset \mathbb{R}^n$ a full-rank lattice, $r \geq 1, s > 0$ and $\mathbf{X} \sim D_{\mathcal{L}+\mathbf{t},s}$, we have*

$$\Pr\left[\|\mathbf{X}\| > rs\sqrt{\frac{n}{2\pi}}\right] \leq \frac{\rho_s(\mathcal{L})}{\rho_s(\mathcal{L}+\mathbf{t})} r^n e^{-\frac{n}{2}(r^2-1)} \leq \frac{\rho_s(\mathcal{L})}{\rho_s(\mathcal{L}+\mathbf{t})} e^{-\frac{n}{2}(r-1)^2}.$$

PROOF: We prove this inequality using Lemma 10, which holds for all $\alpha > 0$, and Lemma 11, which holds for $\alpha < 1$.

$$\begin{aligned}\Pr[\|\mathbf{X}\| > rs\sqrt{\frac{n}{2\pi}}] &\leq \min_{0<\alpha<1} \frac{\mathbb{E}[e^{\alpha\pi\|\mathbf{X}\|^2}]}{e^{\alpha n r^2/2}} \\ &\leq \min_{0<\alpha<1} \frac{1}{\sqrt{1-\alpha}^n} \frac{\rho(\mathcal{L})}{\rho(\mathcal{L}+\mathbf{t})} e^{-\alpha n r^2/2}.\end{aligned}$$

We can minimize the last expression by differentiating with respect to α. Doing so, we find that $\alpha = 1 - \frac{1}{r^2}$ minimizes the right-hand side. We fill this in and find

$$\begin{aligned}\Pr[\|\mathbf{X}\| > rs\sqrt{\frac{n}{2\pi}}] &\leq \frac{\rho_s(\mathcal{L})}{\rho_s(\mathcal{L}+\mathbf{t})} r^n e^{-\frac{n}{2}(r^2-1)} \\ &\leq \frac{\rho_s(\mathcal{L})}{\rho_s(\mathcal{L}+\mathbf{t})} e^{-\frac{n}{2}(r-1)^2}.\end{aligned}$$

We used on the last line that $0 \leq \ln(r) \leq r-1$ for all $r \geq 1$. □

COROLLARY 13 *For any full-rank lattice $\mathcal{L} \subset \mathbb{R}^n$, $\mathbf{t} \in \mathbb{R}^n$ and $s > 0$, we have that*

$$\Pr_{\mathbf{X}\sim D_{\mathcal{L}+\mathbf{t},s}}[\|\mathbf{X}\| \geq s\sqrt{n}] \leq \frac{\rho_s(\mathcal{L})}{\rho_s(\mathcal{L}+\mathbf{t})} 4^{-n}.$$

Consequently, $\rho(\mathcal{L}+\mathbf{t} \backslash \sqrt{n}\mathcal{B}_2^n) \leq 4^{-n}\rho(\mathcal{L})$.

PROOF: We apply the stronger bound in Theorem 12 with $r = \sqrt{2\pi}$. The corollary follows because $-(2\pi-1)/2 + \ln(\sqrt{2\pi}) < -\ln(4)$. We observe that $\Pr_{\mathbf{X}\sim D_{\mathcal{L}+\mathbf{t},s}}[\|\mathbf{X}\| \geq s\sqrt{n}] = \frac{\rho(\mathcal{L}+\mathbf{t}\backslash\sqrt{n}\mathcal{B}_2^n)}{\rho(\mathcal{L}+\mathbf{t})}$ to conclude the final result. □

Now we have all tools we need to prove strong transference theorems.

THEOREM 14 *For any full-rank lattice $\mathcal{L} \subset \mathbb{R}^n$, the following inequalities hold:*

1. $\frac{\sqrt{n}}{2\lambda_1(\mathcal{L}^*)} \leq \eta_{\frac{2}{4^n}}(\mathcal{L}) \leq \frac{\sqrt{n}}{\lambda_1(\mathcal{L}^*)}$.
2. $\frac{1}{2}\eta_{1/2}(\mathcal{L}) \leq \mu(\mathcal{L}) \leq \sqrt{n}\eta_{1/2}(\mathcal{L})$.

PROOF OF 1: We abbreviate $s = \frac{\sqrt{n}}{\lambda_1(\mathcal{L}^*)}$. For the lower bound, let $\mathbf{x} \in \mathcal{L}$ be such that $\|\mathbf{x}\| = \lambda_1(\mathcal{L})$. We have that

$$\rho_{2/s}(\mathcal{L}\backslash\{\mathbf{0}\}) > \rho_{2/s}(\mathbf{x}) + \rho_{2/s}(-\mathbf{x}) = 2 \cdot e^{-\pi(s\lambda_1(\mathcal{L})/2)^2} > 2 \cdot 4^{-n},$$

as needed.

For the upper bound, we use the tail bound on the discrete Gaussian to bound the probability mass at distance $\lambda_1(\mathcal{L}^*)$ from the center of the distribution $D_{\mathcal{L}^*,1/s}$, which will allow for a bound on $\rho_s(\mathcal{L}^*)$. Using that $\lambda_1(\mathcal{L}^*) = \frac{1}{s}\sqrt{n}$ and applying Corollary 13,

$$\Pr_{\mathbf{X}\sim D_{\mathcal{L}^*,1/s}}[\|\mathbf{X}\| \geq \lambda_1(\mathcal{L}^*)] \leq 4^{-n}.$$

Observe that

$$\Pr_{\mathbf{X}\sim D_{\mathcal{L}^*,1/s}}[\|\mathbf{X}\| \geq \lambda_1(\mathcal{L}^*)] = \frac{\rho_{1/s}(\mathcal{L}^*\backslash\{\mathbf{0}\})}{\rho_{1/s}(\mathcal{L}^*)} = \frac{\rho_{1/s}(\mathcal{L}^*) - 1}{\rho_{1/s}(\mathcal{L}^*)}.$$

It therefore follows that $\rho_{1/s}(\mathcal{L}^*) \leq \frac{1}{1-4^{-n}} \leq 1 + 2 \cdot 4^{-n}$, so $s \geq \eta_{2\cdot 4^{-n}}(\mathcal{L})$. □

PROOF OF 2: Let $s = \eta_{1/2}(\mathcal{L})$. First we prove the upper bound. We fix some $\mathbf{t} \in \mathbb{R}^n$. Lattice points in $\mathcal{L}$ close to a vector $\mathbf{t}$ correspond to short vectors in the set $\mathcal{L} - \mathbf{t}$. We show that such short vectors exist through a probabilistic argument. We will prove that for $\mathbf{X} \sim D_{\mathcal{L}-\mathbf{t},s}$ we have $\Pr_{\mathbf{X}\sim D_{\mathcal{L}-\mathbf{t},s}}[\|\mathbf{X}\| < s\sqrt{n}] > 0$. Using the tail bound on the discrete Gaussian and Lemma 5 we have

$$\begin{aligned}
\Pr_{\mathbf{X}\sim D_{\mathcal{L}-\mathbf{t},s}}[\|\mathbf{X}\| \geq s\sqrt{n}] &\leq \frac{\rho_s(\mathcal{L})}{\rho_s(\mathcal{L}+\mathbf{t})}4^{-n} \\
&\leq \frac{(1+\frac{1}{2})s^n/\det(\mathcal{L})}{(1-\frac{1}{2})s^n/\det(\mathcal{L})}4^{-n} \\
&= 3 \cdot 4^{-n} < 1.
\end{aligned}$$

So with non-zero probability, $\|\mathbf{X}\| < s\sqrt{n}$, which is equivalent to the lattice point $\mathbf{X} + \mathbf{t}$ having distance less than $s\sqrt{n}$ from $\mathbf{t}$. As such a nearby lattice point exists for any choice of $\mathbf{t}$, we have a bound on the covering radius $\mu(\mathcal{L}) \leq \sqrt{n}\eta_{1/2}(\mathcal{L})$.

For the lower bound, choose $\mathbf{t} \in \mathbb{R}^n$ such that $\rho_s(\mathcal{L}+\mathbf{t}) \leq \frac{s^n}{\det(\mathcal{L})}$ and $\|\mathbf{t}\| \leq \mu(\mathcal{L})$. Such $\mathbf{t}$ exists, because for D a fundamental domain of $\mathcal{L}$, $\int_D \rho_s(\mathcal{L}+\mathbf{x})\mathrm{d}\mathbf{x} = \frac{s^n}{\det(\mathcal{L})}$. Furthermore, the upper bound of Lemma 5 is tight for $\rho_s(\mathcal{L}) = \frac{3s^n}{2\det(\mathcal{L})}$. Appealing to Lemma 3,

$$\frac{2}{3} = \frac{\rho_s(\mathcal{L}+\mathbf{t})}{\rho_s(\mathcal{L})} \geq e^{-\pi\|\mathbf{t}/s\|^2}.$$

Taking logarithms lets us deduce the result. □

COROLLARY 15 *For a full-rank lattice $\mathcal{L} \subset \mathbb{R}^n$, $\mu(\mathcal{L})\lambda_1(\mathcal{L}^*) \leq n$.*

Proof: We know that $\eta_{1/2}(\mathcal{L}) \leq \eta_{\frac{2}{4^n}}(\mathcal{L})$, which implies that

$$\mu(\mathcal{L}) \leq \sqrt{n}\eta_{1/2}(\mathcal{L}) \leq \sqrt{n}\eta_{\frac{2}{4^n}}(\mathcal{L}) \leq \frac{n}{\lambda_1(\mathcal{L}^*)}.$$

□