# Density of Ideal Lattices

## - Preliminary Draft -

Johannes Buchmann and Richard Lindner

Technische Universität Darmstadt, Department of Computer Science
Hochschulstraße 10, 64289 Darmstadt, Germany
buchmann,rlindner@cdc.informatik.tu-darmstadt.de

**Abstract.** The security of many *efficient* cryptographic constructions, e.g. collision-resistant hash functions, digital signatures, and identification schemes, has been proven assuming the hardness of *worst-case* computational problems in ideal lattices. These lattices correspond to ideals in the ring $\mathbb{Z}[\zeta]$, where $\zeta$ is some fixed algebraic integer.
In this paper we show that the density of $n$-dimensional ideal lattices with determinant $\leq b$ among all lattices under the same bound is in $O(b^{1-n})$. So for lattices of dimension $> 1$ with bounded determinant, the subclass of ideal lattices is always vanishingly small.

**Keywords:** post-quantum cryptography, provable security, ideal lattices.

## 1 Introduction

Following the seminal result of Ajtai from 1996, where he showed a worst-case to average-case reduction for computational problems in lattices[1], the security of many lattice-based cryptographic schemes was proven assuming the hardness of these worst-case problems, e.g. [4,6,3,9].

Using similar methods, Lyubashevsky and Micciancio found in 2006, that a worst-case to average-case reduction exists for a different class of lattices, namely lattices corresponding to ideals in the ring $\mathbb{Z}[\zeta]$, where $\zeta$ is some algebraic integer that is fix for the reduction. The additional structure of these lattices allows the cryptographic schemes which use them to be much more efficient and require smaller keys. In each case, the change for keysizes and trapdoor evaluation time is from $\tilde{O}(n^2)$ for general lattices to $\tilde{O}(n)$ for ideal lattices. Again, many cryptographic schemes were proven secure assuming the hardness of worst-case problems in ideal lattices, see [5,6,7].

For all these schemes, the authors recommended to use rings $\mathbb{Z}[\zeta]$, that are equal to the ring of algebraic integers of a number field, because the connection to worst-case problems is tightest in these cases. So, we will only consider ideal lattices corresponding to ideals in the ring of integers of a number field.

Until today, there has been no in depth work on the relationship of the hardness for these two worst-case problems which have become the basis of security

Dagstuhl Seminar Proceedings 09221
Algorithms and Number Theory
http://drops.dagstuhl.de/opus/volltexte/2009/2125

for so many schemes. We give an indication that worst-case computational problems in ideal lattices are potentially much simpler. We show that the number of $n$-dimensional lattices with bounded determinant $\leq b$, is $\Omega(b^n)$ as $b$ goes to infinity. In comparison, the number of ideal lattices under the same constraints is only $O(b)$, a vanishingly small quantity.

## 2 Preliminaries

A lattice $L$ is a discrete, additive subgroup of $\mathbb{R}^n$. It can always be described as $L = \{\sum_{i=1}^{d} x_i \, \mathbf{b}_i \, : \, x_i \in \mathbb{Z}\}$, where $\mathbf{b}_1, \ldots, \mathbf{b}_d \in \mathbb{R}^n$ are linearly independent. The matrix $\mathbf{B} = [\mathbf{b}_1, \ldots, \mathbf{b}_d]$ is a *basis* of $L$. The number of vectors in the basis is the *dimension*, or *rank* of the lattice $\dim(L) = d$. The *fundamental parallelepiped* spanned by the basis is $\mathcal{P}(\mathbf{B}) = \mathbf{B}[0,1]^d$, so it consists of all linear combinations of basis vectors with coefficients between 0 and 1. The *determinant* of a lattice is the volume of the fundamental parallelepiped, i.e. $\det(L) = \sqrt{\det(\mathbf{B}^T\mathbf{B})}$. This value is independent of the choice of basis.

For any integral lattice $L$ of full-rank, there exists a *unique* basis $\mathbf{B}$ such that

$$b_{i,j} = 0 \text{ for } i < j, \quad b_{i,i} > 0 \text{ for } 1 \leq i \leq n, \quad b_{i,i} > b_{i,j} \geq 0 \text{ for } 1 \leq j < i \leq n.$$

This basis is in Hermite Normal Form, $\mathbf{B} = \mathrm{HNF}(L)$.

Throughout this paper $K = \mathbb{Q}(\zeta)$ will always be a number field of *degree* $\deg(K) = [K : \mathbb{Q}] = n$, i.e. there is a monic, irreducible polynomial $f \in \mathbb{Q}[x]$ of that degree with $f(\zeta) = 0$.

**Definition 1.** *An order $\mathcal{O}$ in $K$ is a subring of $K$ which is a free $\mathbb{Z}$-module of rank $n = \deg(K)$.*

The integral combinations of powers of $\zeta$ form an order $\mathbb{Z}[\zeta] = [1, \zeta, \ldots, \zeta^{n-1}]\mathbb{Z}^n$. Another order, the *ring of integers* in $K$, is

$$\mathcal{O}_K = \{\alpha \in K : \exists \text{ monic } f \in \mathbb{Z}[x], f(\alpha) = 0\}.$$

This order is maximal in the sense that it contains *all* other orders. By definition, there exist $\beta_1, \ldots, \beta_n \in \mathcal{O}_K$ such that $\mathcal{O}_K = [\beta_1, \ldots, \beta_n]\mathbb{Z}^n$.

We can embedded $K$ into rational vectorspace via the *coefficients*

$$\sigma \colon K \longrightarrow \mathbb{Q}^n : a_0 + a_1\zeta + \cdots + a_{n-1}\zeta^{n-1} \longmapsto (a_0, a_1, \ldots, a_{n-1})^T = \mathbf{a}.$$

**Definition 2.** *Let $\mathcal{O}$ be an order in $K$. An $\mathcal{O}$-*ideal lattice *is a lattice $L \subseteq \mathbb{Z}^n$ such that $L = \sigma(\mathfrak{i})$ for some ideal $\mathfrak{i} \subseteq \mathcal{O}$.*

In the special case $\mathcal{O} = \mathbb{Z}[\zeta]$ this matches the definition of Lyubashevsky and Micciancio in [5].

We will often use the embedding $\sigma$ implicitly and write, for example, $\det(\mathfrak{i})$ instead of $\det(\sigma(\mathfrak{i}))$. The *norm* of an ideal $\mathfrak{i}$ in $\mathcal{O}$ is $N(\mathfrak{i}) = |\mathcal{O} \,/\, \mathfrak{i}|$. This is related to the determinant of the corresponding ideal lattice

$$N(\mathfrak{i}) = \det(\mathfrak{i}) \cdot \det(\mathcal{O}). \tag{1}$$

For the case $\mathcal{O} = \mathcal{O}_K$ this is the *field norm*.

Conforming with notations in previous works, we will write vectors and matrices in boldface. We will also use greek letters for elements of $K$ and (fractional) ideals of $\mathcal{O}_K$ will be set in fraktur.

## 3 Density of ideal lattices

*General lattices.* For integers $n, b > 0$, let all full-rank sublattices of $\mathbb{Z}^n$ with determinant $\leq b$ be

$$L_n(b) = \{L \subseteq \mathbb{Z}^n : 0 < \det(L) \leq b\}, \qquad l_n(b) = |L_n(b)|.$$

In 1968 Schmidt showed in [10] that as $b$ tends to infinity $l_n(b) \in O(b^n)$. We will use a similar methodology to derive a *lower* bound.

**Theorem 1.** *For integers $n, b > 0$, we have $l_n(b) \geq b^n/n$.*

*Proof.* Let $L'_n(d) = \{L \subseteq \mathbb{Z}^n : \det(L) = d\}, l'_n(d) = |L'_n(d)|$. We start by showing

$$l'_n(1) = l'_1(d) = 1, \tag{2}$$

$$l'_n(d) = \sum_{c|d} c^{n-1}\, l'_{n-1}(d/c). \tag{3}$$

It suffices to count the number of possible lattice bases in HNF, because this form is unique for each lattice. Equations (2) are an immediate consequence.

Now, let $L \in L'_n(d)$, $\mathbf{B} = \mathrm{HNF}(L)$, and $c = b_{n,n}$. Consider the last row of $\mathbf{B}$. We know $c \mid d$ and $0 \leq b_{n,i} < c$ for $i = 1, \ldots, n-1$. These are $\sum_{c|d} c^{n-1}$ possible rows. The remaining upper left $(n-1) \times (n-1)$ submatrix of $\mathbf{B}$ could be the HNF of *any* lattice in $L'_{n-1}(d/c)$, which shows Equation (3).

We can now show the claim

$$l_n(b) = \sum_{d=1}^{b} l'_n(d) = \sum_{d=1}^{b} \sum_{c|d} c^{n-1} l'_{n-1}(d/c) \geq \sum_{d=1}^{b} d^{n-1} \geq \int_0^b d^{n-1}\,\mathrm{d}d \geq b^n/n.$$

$\square$

*Remark 1.* Note that, during the proof we counted lattices whose Hermite normal form differs from the identity matrix only in the last row and we found there are at least $\Omega(b^n)$ of those. Since Schmidt showed in [10], that $O(b^n)$ is also an upper bound on the number of $n$-dimensional lattices with determinant $\leq b$, it follows that lattices with this special Hermite normal form are a *dense* subset of all lattices. This was shown less elementary by Goldstein and Mayer [2].

*Ideal lattices.* Let $\mathcal{O}$ be an order in some number field $K$ of degree $n$. For integers $b > 0$, let the set of all *$\mathcal{O}$-ideal lattices* with determinant $\leq b$ be

$$I_n^{\mathcal{O}}(b) = \{L \subseteq \mathbb{Z}^n : L \text{ is } \mathcal{O}\text{-ideal lattice}, 0 < \det(L) \leq b\}, \quad i_n^{\mathcal{O}}(b) = |I_n^{\mathcal{O}}(b)|.$$

We adapt an old result of Dedekind and Weber, which was recently made more precise by Murty and Van Order [8].

**Theorem 2.** *Let $K$ be a number field of degree $n$, then for integers $b > 0$*

$$i_n^{\mathcal{O}_K}(b) \leq h_K(2c_K b^{1/n} + 1)^n/(w \det(\mathcal{O}_K)),$$

*where $h_K$ is the number of ideal classes, $w$ is the number of roots of unity in $K$, and $c_K$ is another real constant depending only on $K$.*

*Proof.* Let $\mathcal{C}$ be some ideal class in $\mathcal{O}_K$,

$$I_n^{\mathcal{C}}(b) = \{\mathfrak{a} \in \mathcal{C} : 0 < N(\mathfrak{a}) \leq b\}, \qquad i_n^{\mathcal{C}}(b) = |I_n^{\mathcal{C}}(b)|.$$

We start by showing for any ideal $\mathfrak{b} \in \mathcal{C}^{-1}$, $i_n^{\mathcal{C}}(b) = |\mathfrak{b} I_n^{\mathcal{C}}(b)|$. Obviously, $\geq$ holds and we also have $|\mathfrak{b} I_n^{\mathcal{C}}(b)| \geq |(\mathfrak{b}^{-1})\mathfrak{b} I_n^{\mathcal{C}}(b)| = |I_n^{\mathcal{C}}(b)|$, which gives us $\leq$. Note that

$$\mathfrak{b} I_n^{\mathcal{C}}(b) = \{\langle \alpha \rangle \subseteq \mathfrak{b} : 0 < N(\alpha) \leq bN(\mathfrak{b})\},$$

so in order to count ideals in $\mathcal{C}$ it suffices to count principal ideals in $\mathfrak{b}$.

The span of two elements is equal if and only if they differ by a ring unit, $\langle \alpha \rangle = \langle \alpha' \rangle \iff$ there exists a unit $\epsilon \in \mathcal{O}_K$, such that $\alpha' = \epsilon\alpha$.

Let $(r_1, r_2)$ be the signature of $K$ and $r = r_1 + r_2 - 1$. Dirichlet proved the following classification. There exist fundamental units $\epsilon_1, \dots, \epsilon_r \in \mathcal{O}_K$, such that $\epsilon$ is a unit in $\mathcal{O}_K$ if and only if $\epsilon = \zeta\epsilon_1^{n_1} \cdots \epsilon_r^{n_r}$, where $\zeta \in K$ is a root of unity, and $n_1, \dots, n_r \in \mathbb{Z}$. Recall, that the total number of roots of unity in $K$ is $w$.

We continue by showing that for each principal ideal $\langle \alpha \rangle \in \mathfrak{b} I_n^{\mathcal{C}}(b)$ there exist $w$ many reals $0 \leq c_1, \dots, c_r < 1$ such that

$$\sum_{j=1}^{r} c_j \log |\epsilon_j^{(i)}| = \log(|\alpha^{(i)}| N(\alpha)^{-1/n}) \qquad \text{for } 1 \leq i \leq n. \tag{4}$$

Note that the $r \times r$ matrix $(\log |\epsilon_j^{(i)}|)_{1 \leq i,j \leq r}$ is non-singular, so for each $\alpha \in \mathfrak{b}$ there exist (unrestricted) reals $c_1, \dots, c_r$ such that (4) holds for $1 \leq i \leq r$. Let $\alpha' = \epsilon\alpha$ for some unit $\epsilon$, then we have

$$\log(|\alpha'^{(i)}| N(\alpha')^{-1/n}) = \sum_{j=1}^{r} n_j \log |\epsilon_j^{(i)}| + \log(|\alpha^{(i)}| N(\alpha)^{-1/n}) = \sum_{j=1}^{r} (n_j + c_j) \log |\epsilon_j^{(i)}|.$$

So, by Dirichlet's classification, restricting the reals to $0 \leq c_1, \dots, c_r < 1$ leaves only $w$ many for each principal ideal. For the rest, fix any of the $w$ many.

For $r + 1 < i \leq n$, we have $|(\cdot)^{(i)}| = |\overline{(\cdot)}^{(i-r_2)}| = |(\cdot)^{(i-r_2)}|$, so Equation (4) holds for these.

Since $N(\alpha) = \prod_{i=1}^n |\alpha^{(i)}|$ and $1 = N(\epsilon_j) = \prod_{i=1}^n |\epsilon_j^{(i)}|$ for $1 \leq j \leq r$, we get

$$\sum_{i=1}^n \sum_{j=1}^r c_j \log |\epsilon_j^{(i)}| = \sum_{j=1}^r c_j \left( \sum_{i=1}^n \log |\epsilon_j^{(i)}| \right) = 0 = \sum_{i=1}^n \log(|\alpha^{(i)}| N(\alpha)^{-1/n}).$$

We already knew that the summands of the left- and rightmost sum are equal for $i \neq r+1$, so this equality gives us the final case $i = r+1$ for Equation (4).

Finally, we prove the theorem. Let $h_K$ be the number of ideal classes,

$$i_n^{\mathcal{O}_K}(b) \leq h_K \max_{\mathcal{C}} \{ i_n^{\mathcal{C}}(b) \} / \det(\mathcal{O}_K).$$

Let $\beta_1, \ldots, \beta_n$ be an integral basis of $\mathcal{O}_K$. For each principal ideal in $\mathfrak{b} I_n^{\mathcal{C}}(b)$, there are $w$ many $\alpha$s subject to Equation (4). For each of these $\alpha$, there exist unique integers $x_1, \ldots, x_n$ such that $\alpha = x_1\beta_1 + \cdots x_n\beta_n$. We will show that the total number of these integers, and thus $i_n^{\mathcal{C}}(b)$ is bounded.

The $\beta$s form a basis, so the matrix $\mathbf{B} = (\beta_j^{(i)})_{1 \leq i,j \leq n}$ is invertible and

$$\|(x_i)_{1 \leq i \leq n}\|_\infty \leq \|\mathbf{B}^{-1}\|_\infty \; \|(\alpha^{(i)})_{1 \leq i \leq n}\|_\infty.$$

Let $m_\epsilon = \max\{\log |\epsilon_j^{(i)}| : 1 \leq i, j \leq r\}$, by Equation (4) we know

$$\|(\alpha^{(i)})_{1 \leq i \leq n}\|_\infty \leq \exp(rm_\epsilon) |N(\alpha)^{1/n}| \leq \exp(rm_\epsilon)(bN(\mathfrak{b}))^{1/n}.$$

Minkowski showed that an ideal $\mathfrak{b}$ in class $\mathcal{C}^{-1}$ can always be chosen such that

$$N(\mathfrak{b}) \leq (4/\pi)^{r_2} n! \sqrt{|d_K|}/n^n,$$

where $d_K$ is the discriminant of $K$. Altogether, we have

$$\|(x_i)_{1 \leq i \leq n}\|_\infty \leq \underbrace{(4/\pi)^{r_2/n} \|\mathbf{B}^{-1}\|_\infty \exp(rm_\epsilon)(n! \sqrt{|d_K|}/n^n)^{1/n}}_{=c_K} \cdot b^{1/n}.$$

Since all possible $x_1, \ldots, x_n$ are bounded in this way, the total number of $\alpha$s subject to Equation (4) is $(2c_K + 1)^n$. As we know there exist at most $w$ many of these $\alpha$ for every principal ideal in $\mathfrak{b} I_n^{\mathcal{C}}(b)$, we get

$$i_n^{\mathcal{C}}(b) \leq (2c_K b^{1/n} + 1)^n / w,$$

which completes the proof. □

*Density.*

**Corollary 1.** *For integers $n, b > 0$, as $b \to \infty$*

$$i_n^{\mathcal{O}_K}(b)/l_n(b) \in O(b^{1-n}).$$

So the ratio vanishes for all $n > 1$.

## References


1. Miklós Ajtai. Generating hard instances of lattice problems (extended abstract). In *Proceedings of the Annual Symposium on the Theory of Computing (STOC) 1996*, pages 99–108. ACM Press, 1996.
2. Andrew Mayer Daniel Goldstein. On the equidistribution of hecke points. *Forum Mathematicum 2003, 15:2*, pages 165–189, 2003.
3. Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the Annual Symposium on the Theory of Computing (STOC) 2008*, pages 197–206. ACM Press, 2008.
4. Oded Goldreich, Shafi Goldwasser, and Shai Halevi. Collision-free hashing from lattice problems. *Electronic Colloquium on Computational Complexity (ECCC)*, 3(42), 1996.
5. Vadim Lyubashevsky and Daniele Micciancio. Generalized compact knapsacks are collision resistant. In *International Colloquium on Automata, Languages and Programming (ICALP) 2006*, Lecture Notes in Computer Science, pages 144–155. Springer-Verlag, 2006.
6. Vadim Lyubashevsky and Daniele Micciancio. Asymptotically efficient lattice-based digital signatures. In *Theory of Cryptography Conference (TCC) 2008*, Lecture Notes in Computer Science, pages 37–54. Springer-Verlag, 2008.
7. Vadim Lyubashevsky, Daniele Micciancio, Chris Peikert, and Alon Rosen. SWIFFT: A modest proposal for FFT hashing. In *Fast Software Encryption (FSE) 2008*, Lecture Notes in Computer Science, pages 54–72. Springer-Verlag, 2008.
8. Maruti Ram Murty and Jeanine Van Order. Counting integral ideals in a number field. *Expositiones Mathematicae*, 25(1):53–66, 2007.
9. Chris Peikert. Public-key cryptosystems from the worst-case shortest vector problem: extended abstract. In Michael Mitzenmacher, editor, *STOC*, pages 333–342. ACM, 2009.
10. Wolfgang M. Schmidt. Asymptotic formulae for point lattices of bounded determinant and subspaces of bounded height. *Duke Mathematical Journal*, 35(2):327–339, 1968.