Algorithmic Geometry of Numbers: LLL and BKZ

Léo Ducas

CWI, Amsterdam, The Netherlands

HEAT Summer-School on FHE and MLM
A gift from Johannes Kepler to Matthäus Wacker von Wackenfels

New year of 1611:
A gift from Johannes Kepler to Matthäus Wacker von Wackenfels

New year of 1611:
A fruitful contemplation

Figure: *Strena, De Nive Sexangula* (A new year gift: on the sexangular snow)

http://www.franceinter.fr/player/reecouter?play=798226
A famous Conjecture

Figure: The close packing conjecture

Arrangement $B$ is the most compact arrangement.
A proof in dimension 2?

Let us restrict our attention to “regular arrangement”: lattices. What do we mean by compact?
A proof in dimension 2?

Let us restrict our attention to “regular arrangement”: lattices. What do we mean by compact?

Definition (Packing density)

Let $\Lambda$ be a lattice lattice, $\mathcal{F}$ a fundamental domain of $\Lambda$, and $\lambda_1$ the length of the shortest non-zero vector. The packing density is defined by:

$$\rho(\Lambda) = \frac{\text{Vol}(\frac{\lambda_1}{2} \cdot B)}{\text{Vol}(\mathcal{F})}.$$
A proof in dimension 2?

Let us restrict our attention to “regular arrangement”: lattices. What do we mean by compact?

**Definition (Packing density)**

Let Λ be a lattice lattice, \( \mathcal{F} \) a fundamental domain of Λ, and \( \lambda_1 \) the length of the shortest non-zero vector. The packing density is defined by:

\[
\rho(\Lambda) = \frac{\text{Vol}(\frac{\lambda_1}{2} \cdot B)}{\text{Vol}(\mathcal{F})}.
\]

**Figure : Fundamental domains**
Lemma

Let $\Lambda$ be a lattice. Assume, wlog. that $\mathbf{v} = (1, 0)$ is a shortest vector. Then, there exists a basis $\mathbf{v}, \mathbf{w}$ that:

- $\|\mathbf{w}\| \geq 1$
- $\mathbf{w} = (x, y)$ where $|x| \leq 1/2$
Lemma

Let $\Lambda$ be a lattice. Assume, wlog. that $\mathbf{v} = (1, 0)$ is a shortest vector. Then, there exists a basis $\mathbf{v}, \mathbf{w}$ that:

- $\|\mathbf{w}\| \geq 1$
- $\mathbf{w} = (x, y)$ where $|x| \leq 1/2$
We had \( \mathbf{v} = (1, 0) \), \( \mathbf{w} = (x, y) \) with \( \| \mathbf{w} \| \geq 1 \), and \( |x| \leq 1/2 \). Hence:

\[
|y| \geq \sqrt{3}/4.
\]

A fundamental domain is given by the parallelepiped:

\[
\begin{pmatrix} \mathbf{v} \\ \mathbf{w} \end{pmatrix} \cdot \left[ -\frac{1}{2}, \frac{1}{2} \right]^2
\]

Its volume is:

\[
\det \begin{pmatrix} \mathbf{v} \\ \mathbf{w} \end{pmatrix} = \det \begin{pmatrix} 1 & 0 \\ x & y \end{pmatrix} = y \geq \sqrt{3}/4.
\]

This gives:

\[
\rho(\Lambda) \leq \frac{\pi \cdot (1/2)^2}{\sqrt{3}/4} = \frac{\pi}{2\sqrt{3}} \approx 0.9068997.
\]
Optimal packing in dimension 2

This bound is reached by the hexagonal lattice packing:
Optimal packing in dimension 2

This bound is reached by the hexagonal lattice packing:

This is well-known since [Bees, $2 \cdot 10^9$ BC] (proof by trial-and-error)
Overview

1. Introduction

2. Hermite reduction, and the LLL algorithm

3. BKZ, and security estimate for lattice based cryptography

4. Conclusion
Gram-Schmidt Orthogonalization

Orthogonal projection on the direction of $\mathbf{u}$:

$$\pi_{\mathbf{u}} (\mathbf{v}) = \frac{\langle \mathbf{u}, \mathbf{v} \rangle}{\langle \mathbf{u}, \mathbf{u} \rangle} \mathbf{u}.$$ 

Gram Schmidt Process:

$$\begin{align*}
\mathbf{b}_1^* &= \mathbf{b}_1 = \pi_0 (\mathbf{b}_1) \\
\mathbf{b}_2^* &= \mathbf{b}_2 - \pi_{\mathbf{b}_1^*} (\mathbf{b}_2) = \pi_1 (\mathbf{b}_2) \\
\mathbf{b}_3^* &= \mathbf{b}_3 - \pi_{\mathbf{b}_1^*} (\mathbf{b}_3) - \pi_{\mathbf{b}_2^*} (\mathbf{b}_3) = \pi_2 (\mathbf{b}_3) \\
&\vdots \\
\mathbf{b}_k^* &= \mathbf{b}_k - \sum_{j=1}^{k-1} \pi_{\mathbf{b}_j^*} (\mathbf{b}_k) = \pi_{k-1} (\mathbf{b}_k)
\end{align*}$$
Gram-Schmidt basis and Volume

- For any basis $\mathbf{B}$ of $\Lambda$, $\mathcal{P}(\mathbf{B})$ is a fundamental domain of $\Lambda$, and so is $\mathcal{P}(\mathbf{B}^*)$.
- The volume of the fundamental domain is independent of the choice of the basis:

$$\text{Vol}(\Lambda) \triangleq \text{Vol}(\mathcal{P}(\mathbf{B}^*)) = \prod \|b_i^*\|$$
Reduced basis of 2-dimensional lattice

Let us re-express reduction in dimension 2 in Gram-Schmidt terms:

**Definition (Simplified)**

A basis \((b_1, b_2)\) of \(\Lambda\) is said reduced if

\[
\frac{\|b_1\|}{\|b_2^*\|} \leq \sqrt{\frac{4}{3}}
\]

Such bases always exist.
Reduced basis of $n$-dimensional lattice

**Definition (Hermite)**

Let $B = (b_1, b_2, \ldots, b_n)$ be a basis of $\Lambda$. Set $\Lambda_i = \pi_i^\perp(L(b_i, b_{i+1}))$.

The basis $B$ is said reduced if, for all $i$,

$$\pi_i^\perp(b_i), \pi_i^\perp(b_{i+1})$$

is a reduced of $\Lambda_i$.

In particular:

$$\frac{\|b_i^*\|}{\|b_{i+1}^*\|} \leq \sqrt{\frac{4}{3}} \quad \text{and}$$

$$\|b_0\| \leq \left(\frac{4}{3}\right)^{n/4} \cdot \text{Vol}(\Lambda)^{1/n}.$$
Reduction basis of $n$-dimensional lattice

**Definition (Hermite)**

Let $\mathbf{B} = (\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n)$ be a basis of $\Lambda$. Set $\Lambda_i = \pi_i(\mathcal{L}(\mathbf{b}_i, \mathbf{b}_{i+1}))$. The basis $\mathbf{B}$ is said reduced if, for all $i$,

$$\pi_i(\mathbf{b}_i), \pi_i(\mathbf{b}_{i+1})$$

is a reduced of $\Lambda_i$.

In particular:

$$\frac{\|\mathbf{b}_i^*\|}{\|\mathbf{b}_{i+1}^*\|} \leq \sqrt{\frac{4}{3}}$$

and

$$\|\mathbf{b}_0\| \leq \left(\frac{4}{3}\right)^{n/4} \cdot \text{Vol}(\Lambda)^{1/n}.$$

**Theorem**

*Such bases always exist.*

Proof by animation.
Existence of Hermite-reduced basis

- Define a potential $P = \sum (n - i) \log \| b_i^* \|
- Prove that the potential strictly decrease at each step
- Prove that there are only finitely bases that can be visited during this process (discreteness of the lattice and bound on the norms)
Existence of Hermite-reduced basis

- Define a potential \( P = \sum (n - i) \log \|b_i^*\| \)
- Prove that the potential strictly decrease at each step
- Prove that there are only finitely bases that can be visited during this process (discreteness of the lattice and bound on the norms)

This proof is an algorithm!
Existence of Hermite-reduced basis

- Define a potential \( P = \sum (n - i) \log \| b_i^* \| \)
- Prove that the potential strictly decrease at each step
- Prove that there are only finitely bases that can be visited during this process (discreteness of the lattice and bound on the norms)

This proof is an algorithm!
But it may require super-exponentially many step...
**Idea:** Relax the constraint so that each step improves the potential $P$ by a non-negligible term $\epsilon > 0$.

**Theorem (LenstraLenstraLovasz82)**

*For any $\epsilon$, there exists a deterministic polynomial time algorithm, the basis of a lattice can be reduced so that:*

\[
\frac{\|b_i^*\|}{\|b_{i+1}^*\|} \leq \sqrt{\frac{4}{3}} + \epsilon.
\]

Must-read: [The LLL Algorithm, NguyenVallée].
The analysis guarantee that:

$$\frac{\|b_i\|}{\|b_{i+1}\|} \leq \sqrt{\frac{4}{3}} + \epsilon \approx 1.15.$$
LLL in practice

The analysis guarantee that:

$$\frac{\|b_i^*\|}{\|b_{i+1}^*\|} \leq \sqrt{\frac{4}{3}} + \epsilon \approx 1.15.$$ 

In practice

$$\frac{\|b_i^*\|}{\|b_{i+1}^*\|} \approx 1.04.$$
The analysis guarantee that:

\[
\frac{\|b_i^*\|}{\|b_{i+1}^*\|} \leq \sqrt{\frac{4}{3}} + \epsilon \approx 1.15.
\]

In practice

\[
\frac{\|b_i^*\|}{\|b_{i+1}^*\|} \approx 1.04.
\]

P. Nguyen: “I hope I’ll get to learn why before I die!”
Overview

1. Introduction

2. Hermite reduction, and the LLL algorithm

3. BKZ, and security estimate for lattice based cryptography

4. Conclusion
The BKZ algorithm

Idea: [SchnorrEuchner,1994] find the shortest vector in projected sub-lattices of dimension $b > 2$ as a sub-routine.

Theorem (HanrotPujolStehlé)

The BKZ$_b$ algorithm runs in time $\text{poly}(n) \cdot \text{SVP}(b)$. 

▶ Theoretical upper-bounds involving Rankin's constant

▶ Heuristically and experimentally, BKZ behave much better
The BKZ algorithm

Idea: [SchnorrEuchner,1994] find the shortest vector in projected sub-lattices of dimension $b > 2$ as a sub-routine.

Theorem (HanrotPujolSthélé)

The BKZ$_b$ algorithm runs in time $\text{poly}(n) \cdot \text{SVP}(b)$.

How short of a vector does BKZ$_b$ finds?

- Theoretical upper-bounds involving Rankin’s constant
- Heuristically and experimentally, BKZ behave much better
The root hermite factor (heuristic)

In practice, BKZ\(_b\) produces a vector of size:

\[ \delta_b^n \cdot \text{Vol}(\Lambda)^{1/n}. \]

The gaussian heuristic predicts that the root Hermite factor \( \delta_b \) is about:

\[ \delta_b = (b/2\pi e)^{1/2b}. \]
The root hermite factor (heuristic)

In practice, BKZ\textsubscript{b} produces a vector of size:

\[ \delta^n_b \cdot \text{Vol}(\Lambda)^{1/n}. \]

The gaussian heuristic predicts that the root Hermite factor \( \delta_b \) is about:

\[ \delta_b = \left(\frac{b}{2\pi e}\right)^{1/2^b}. \]

Figure: Heuristic Root Hermite factor \( \delta_b \)
The root hermite factor (a better heuristic?)

This heuristic seems accurate for $b > 45$, but below that, is completely absurd! Find out a better one!
No good close formula—even abstracting out the cost of $\text{SVP}(b)$.

Very complete survey on the state of the art, and prediction scripts in [AlbrechtPlayerScott2015].

**A gold mine:** Thesis of [Chen2013] (a.k.a. full version of BKZ 2.0)!
Reproducing and sharing code for some of those technique would be very valuble (and should be rewarded...)

---

Léo Ducas  (CWI, Amsterdam)  
LLL and BKZ  
HEAT, October 2015  
21 / 28
Run-time of SVP

- Enumeration [Kannan, FinckePost] with pruning [GamaNguyenRegev]: Super-exponential, ugly, hard to optimize, performance hard to predict, but still the best algorithm
- Sieving [MicciancioVoulgaris] with NNS techniques [Laarhoven, ...]: neat, clean, exponential run-time with known constant...
Run-time of SVP

- **Enumeration** [Kannan, FinckePost] with pruning [GamaNguyenRegev]: Super-exponential, ugly, hard to optimize, performance hard to predict, but still the best algorithm
- **Sieving** [MicciancioVoulgaris] with NNS techniques [Laarhoven, ...]: neat, clean, exponential run-time with known constant... and catching up!

**Hot topic:**
Get sieving to beat enumeration in practice.
My grain of salt:

- Simplify all hard to predict terms to the advantage of the attacker (he could come up with heuristic tricks)
- Make a clear distinction between \textit{best-known attack} and \textit{security claim} (help the cryptanalyst getting there hard work published)
Lower bounds for the designer

My grain of salt:

- Simplify all hard to predict terms to the advantage of the attacker (he could come up with heuristic tricks)
- Make a clear distinction between best-known attack and security claim (help the cryptanalyst getting there hard work published)

Sieve-BKZ cost (using [BeckerD.GamaLaarhoven] for sieving):

\[ \text{poly}(n) \cdot 2^{0.292b + o(b)} \]

Lower bound for the designer:

\[ 2^{0.292b} \quad \text{(paranoïacs may use } 2^{0.215b}) \].
Lower bounds for the designer

My grain of salt:

- Simplify all hard to predict terms to the advantage of the attacker (he could come up with heuristic tricks)
- Make a clear distinction between *best-known attack* and *security claim* (help the cryptanalyst getting there hard work published)

Sieve-BKZ cost (using [BeckerD.GamaLaarhoven] for sieving):

\[ \text{poly}(n) \cdot 2^{0.292b + o(b)} \]

Lower bound for the designer:

\[ 2^{0.292b} \quad \text{(paranoiacs may use} \quad 2^{0.215b}). \]

This lower bounds also applies to enumeration with sieving for \( b > 150 \)!
Overview

1. Introduction
2. Hermite reduction, and the LLL algorithm
3. BKZ, and security estimate for lattice based cryptography
4. Conclusion
The killer instinct ?

Figure: Cryptanalysis (according to certain view)
Figure: Cryptanalysis (according to certain view)
A game (a very serious one!)

**Figure**: Cryptanalysis (according my view)
The cat and mouse game

The **cat and mouse game** is essential in determining what is secure and what is not, and is an amazing catalyst for crypto, math, and algorithmic.

**The rules:**

**Mouse:** Meaningful and compact problems, or the cat may not even bother

**Cat:** Reproducible claims, code-sharing, work as a community toward a *unified lattice cryptanalysis playground*
The cat and mouse game

The cat and mouse game is essential in determining what is secure and what is not, and is an amazing catalyst for crypto, math, and algorithmic.

The rules:

Mouse: Meaningful and compact problems, or the cat may not even bother

Cat: Reproducible claims, code-sharing, work as a community toward a unified lattice cryptanalysis playground

Problem:

In lattice-based crypto, we don’t have enough cats!
The cat and mouse game

The **cat and mouse game** is essential in determining what is secure and what is not, and is an amazing catalyst for crypto, math, and algorithmic.

**The rules:**

**Mouse:** Meaningful and compact problems, or the cat may not even bother

**Cat:** Reproducible claims, code-sharing, work as a community toward a *unified lattice cryptanalysis playground*

**Problem:**

In lattice-based crypto, we don’t have enough cats!

**Solution:**

Feed your cats (achievable concrete targets)!

**Solution:**

Become a cat!
Thank you!