Lattice reduction

Pierre Lairez
Outline

1. Lattice reduction
Euclidean lattices

**Definition**

An *Euclidean lattice* is a discrete subgroup of $\mathbb{R}^n$ (with its usual norm).

An *Euclidean lattice* is a group $\mathbb{Z}^n$ with a positive definite quadratic form.
**Euclidean lattices**

**Definition**

An *Euclidean lattice* is a discrete subgroup of $\mathbb{R}^n$ (with its usual norm).

An *Euclidean lattice* is a group $\mathbb{Z}^n$ with a positive definite quadratic form.

**A famous NP-hard problem**

*Input* A lattice $\Lambda \subseteq \mathbb{Z}^n$

*Output* $f \in \Lambda$ nonzero such that $\|f\| = \min \{ \|g\| \mid g \in \Lambda \text{ nonzero} \}$
### Euclidean lattices

#### Definition
An *Euclidean lattice* is a discrete subgroup of $\mathbb{R}^n$ (with its usual norm).

An *Euclidean lattice* is a group $\mathbb{Z}^n$ with a positive definite quadratic form.

#### A famous NP-hard problem

**Input** A lattice $\Lambda \subseteq \mathbb{Z}^n$

**Output** $f \in \Lambda$ nonzero such that $\|f\| = \min \{\|g\| ~|~ g \in \Lambda \text{ nonzero}\}$

#### A polynomial-time solvable problem

**Input** A lattice $\Lambda \subseteq \mathbb{Z}^n$

**Output** $f \in \Lambda$ nonzero such that $\|f\| \leq 2^{\frac{n-1}{2}} \min \{\|g\| ~|~ g \in \Lambda \text{ nonzero}\}$
Volume and \( i \)th minimum

Let \( L \) be a lattice with basis \( f_1, \ldots, f_r \).
For \( B > 0 \), let \( L_B = \langle x \in L \mid \|x\| \leq B \rangle \).

**Volume**

\[
\text{vol}(L)^2 = \det (f_i \cdot f_j)_{1 \leq i, j \leq r}
\]

**\( i \)th minimum**

\[
\lambda_k(L) = \min \{ B \mid \text{rk} L_B \geq k \} = \min \left\{ \max_{1 \leq i \leq k} \|v_i\| \mid v_1, \ldots, v_k \in L \text{ lin. indep.} \right\}.
\]
Gram–Schmidt orthogonalization

Let $f_1, \ldots, f_r \in \mathbb{Z}^n$ and let $L = \mathbb{Z}f_1 + \cdots + \mathbb{Z}f_r$ be the generated lattice.

**Gram–Schmidt basis**

$$f_i^* = f_i - \sum_{j<i} \frac{\langle f_i, f_j^* \rangle}{\|f_j^*\|^2} f_j^* \quad \in \mathbb{Q}f_1 + \cdots + \mathbb{Q}f_i$$
Gram–Schmidt orthogonalization

Let $f_1, \ldots, f_r \in \mathbb{Z}^n$ and let $L = \mathbb{Z} f_1 + \cdots + \mathbb{Z} f_r$ be the generated lattice.

**Gram–Schmidt basis**

$$f_i^* = f_i - \sum_{j<i} \frac{\langle f_i, f_j^* \rangle}{\|f_j^*\|^2} f_j^* \quad \in \mathbb{Q} f_1 + \cdots + \mathbb{Q} f_i$$

**Lemma**

$$\text{vol}(L) = \prod_{i=1}^r \|f_i^*\|$$
Lemma

For any nonzero $g \in L$, $\|g\| \geq \min \{\|f_1^*\|, \ldots, \|f_r^*\|\}$.

Proof. Write $g = \sum_{i=1}^{s} a_i f_i$, with $a_i \in \mathbb{Z}$, $1 \leq s \leq r$ and $a_s \neq 0$. In the GS basis, we have

$$g = a_s f_s^* + [... f_{s-1}^* + \cdots + [... f_1^*,$$

and in particular, $\|g\|^2 \geq a_s^2 \|f_s^*\|^2$. 
## Reduced bases I

### Definition

A basis $f_1, \ldots, f_r$ is reduced if

1. $|\mu_{ij}| \leq \frac{1}{2}$, for any $1 \leq j < i$;
2. $\|f^*_i - f^*_1\|^2 \leq 2\|f^*_i\|^2$ for any $i$.

### Lemma

Let $f_1, \ldots, f_r$ be a reduced basis.

For any nonzero $g \in L$, $\|f_1\| \leq 2\frac{r-1}{2} \|g\|$. 

---

Lattice reduction | Pierre Lairez Page 6/15
Reduced bases II

Let $\lambda_k(L) = \min \{ B \mid \text{rk} L_B \geq k \} = \min \{ \max_{1 \leq i \leq k} \| v_i \| \mid v_1, \ldots, v_k \in L \text{ lin. indep.} \}$.

Let $f_1, \ldots, f_r$ be a reduced basis.

Lemma

For any $1 \leq k \leq r$, $\min_{k \leq j \leq r} \| f_j^* \| \leq \lambda_k(L)$.

Proof. Let $v_1, \ldots, v_k \in L$ be linearly independent. Because of the linear independence, there is at least one $v_i$ which is not in $\text{Vect}(f_1, \ldots, f_{k-1})$. By a previous argument, $\| v_i \| \geq \min_{k \leq j \leq r} \| f_j^* \|$.
Lemma

For any $1 \leq k \leq r$, $\|f_k\| \leq 2^{r-1} \lambda_k(L)$.

Proof. For $k \leq j \leq r$, we have $\|f_j^*\| \geq 2^{j-k} \|f_k^*\|$. Moreover,

$$\|f_k\|^2 \leq \|f_k^*\|^2 + \sum_{j<k} \mu_{kj}^2 \|f_j^*\|^2 \leq 2^{k-1} \|f_k^*\|^2,$$

and the claim follows.
Theorem

Let $f_1, \ldots, f_r$ be a reduced basis of a lattice $L$.
For $B > 0$, let $L_B = \text{Lattice} \{ g \in L \mid \|g\| \leq B \}$.
Let $\kappa = 2^{r-\frac{1}{2}}$ and $\mu \geq \kappa$. For any $B > 0$ such that $L_B = L_{\mu B}$, there is some $k$ such that

(i) $\|f_i\| \leq \kappa B$ for all $i \leq k$ (size-reduced);

(ii) $\|f_i\| \geq \mu B$ for all $i > k$;

(iii) $f_1, \ldots, f_k$ is a basis of $L_B$. 

Reduced bases IV
Reduced bases V

**Proof.** Let $k = \text{rank}(L_B)$. By definition $\lambda_k(L) \leq B$. The hypothesis $L_B = L_{\mu B}$ means that $\lambda_{k+1}(L) > \mu B$.

For any $i \leq k$, we have

$$\|f_i\| \leq \kappa \lambda_i(L) \leq \kappa \lambda_k(L) \leq \kappa B.$$  

In particular, $f_i \in L_{\kappa B} \subseteq L_{\mu B} = L_B$, so $f_1, \ldots, f_k$ is a basis of $L_B$.

For any $j > k$, the family $f_1, \ldots, f_k, f_j$ is free, so

$$\max \{ \|f_1\|, \ldots, \|f_k\|, \|f_j\| \} \geq \lambda_{k+1}(L) > \mu B.$$  

Combining with the previous inequality, this implies that $\|f_j\| \geq \mu B$.

Reduced bases are indeed what we need!
The LLL algorithm

```python
def LLL(f1, ..., fr):
    compute the GS information (the $\|f_i^*\|^2$ and $\mu_{ij}$ coefficients)
    $i \leftarrow 2$
    while $i \leq n$:
        for $j$ from $i - 1$ to 1:
            $f_i \leftarrow f_i - \lfloor \mu_{ij} \rfloor f_j$
            update the GS information
        if $\|f_{i-1}^*\|^2 > 2\|f_i^*\|^2$:
            swap($f_{i-1}, f_i$)
            update the GS information
            $i \leftarrow \max(i - 1, 2)$
        else:
            $i \leftarrow i + 1$
    return $f_1, \ldots, f_r$
```

Lattice reduction | Pierre Lairez
Proposition

When the LLL algorithm terminates, it returns a reduced basis of the input lattice.

After the loop on line 5, it is clear that \( f_1, \ldots, f_i \) is size-reduced.
**Proposition**

When the LLL algorithm terminates, it returns a reduced basis of the input lattice.

After the loop on line 5, it is clear that $f_1, \ldots, f_i$ is size-reduced.

At the beginning of each iteration of the “while”-loop, it is also clear that $f_1, \ldots, f_{i-1}$ is reduced.

So if the algorithm terminates, it outputs a reduced basis.
Theorem (A. K. Lenstra, H. W. Lenstra, Lovász 1982)

The LLL algorithm terminates in polynomial time.

If a swap happens, let $g_1, \ldots, g_i$ denote the basis after the swap. Then $g^*_{i-1} = f^*_{i} + \mu_i$, and so

$$\|g^*_{i-1}\|_2 \leq \|f^*_{i}\|_2 + \frac{1}{4} \|f^*_{i} - f^*_{i-1}\|_2 \leq \frac{3}{4} \|f^*_{i} - f^*_{i-1}\|_2.$$ 

After the swap, $D_{i-1} = \sum_{k=1}^{i-1} \|f^*_{k}\|_2$ decreases by a factor $\frac{3}{4}$ at least. Besides, $D_j = \text{vol} (\mathbb{Z} f_1 + \cdots + \mathbb{Z} f_j)$, so $D_j$ (for $j \neq i$) remains constant. It follows that $\Delta = D_1 \cdots D_r$ is a strictly positive interger with decreases by $\frac{3}{4}$ after a swap.
Theorem (A. K. Lenstra, H. W. Lenstra, Lovász 1982)

The LLL algorithm terminates in polynomial time.

If a swap happens, let $g_1, \ldots, g_i$ denote the basis after the swap. Then

$$g^*_{i-1} = f^*_i + \mu_{i,i-1} f^*_i$$

and so

$$\|g^*_{i-1}\|^2 \leq \|f^*_i\|^2 + \frac{1}{4} \|f^*_{i-1}\|^2 \leq \frac{3}{4} \|f^*_{i-1}\|^2.$$
Theorem (A. K. Lenstra, H. W. Lenstra, Lovász 1982)

The LLL algorithm terminates in polynomial time.

If a swap happens, let $g_1, \ldots, g_i$ denote the basis after the swap. Then

$$g^*_i = f^*_i + \mu_{i,i-1} f^*_{i-1}$$

and so

$$\|g^*_i\|^2 \leq \|f^*_i\|^2 + \frac{1}{4} \|f^*_{i-1}\|^2 \leq \frac{3}{4} \|f^*_{i-1}\|^2.$$ 

After the swap, $D_{i-1} = \prod_{k=1}^{i-1} \|f^*_k\|^2$ decreases by a factor $\frac{3}{4}$ at least.
Theorem (A. K. Lenstra, H. W. Lenstra, Lovász 1982)
The LLL algorithm terminates in polynomial time.

If a swap happens, let \( g_1, \ldots, g_i \) denote the basis after the swap. Then
\[
g_{i-1}^* = f_i^* + \mu_{i,i-1}f_{i-1}^*
\]
and so
\[
\|g_{i-1}^*\|^2 \leq \|f_i^*\|^2 + \frac{1}{4} \|f_{i-1}^*\|^2 \leq \frac{3}{4} \|f_{i-1}^*\|^2.
\]

After the swap, \( D_{i-1} = \prod_{k=1}^{i-1} \|f_k^*\|^2 \) decreases by a factor \( \frac{3}{4} \) at least.
Besides, \( D_j = \text{vol} \left( \mathbb{Z}f_1 + \cdots + \mathbb{Z}f_j \right) \), so \( D_j \) (for \( j \neq i \)) remains constant. It follows that
\[
\Delta = D_1 \cdots D_r
\]
is a strictly positive integer with decreases by \( \frac{3}{4} \) after a swap.
Complexity

Let $A = \max_i \|f_i\|$.

- **Arithmetic complexity**
  The number of swaps is bounded by $\log(\Delta)/\log\left(\frac{3}{4}\right)$.
  The initial value of $\log \Delta$ is bounded by $n^2 \log A$.
Complexity

Let $A = \max_i ||f_i||$.

- Arithmetic complexity
  The number of swaps is bounded by $\log(\Delta)/\log(\frac{3}{4})$.
  The initial value of $\log \Delta$ is bounded by $n^2 \log A$. 

- Binary complexity
  Hard to do it right... Current best (of a variant of LLL) is $O(n^5 + \varepsilon \log(A) \frac{1}{1+\varepsilon})$. 

Lattice reduction | Pierre Lairez
Complexity

Let $A = \max_i \| f_i \|$.

- **Arithmetic complexity**
  The number of swaps is bounded by $\log(\Delta)/\log(\frac{3}{4})$.
  The initial value of $\log \Delta$ is bounded by $n^2 \log A$.

  We can update the GS info in $O(n^2)$ operations. The “for” loop for size reduction
  has at most one nontrivial iteration.

- **Binary complexity**
  Hard to do it right... Current best (of a variant of LLL) is $O(n^5 + \varepsilon \log(A)^{1+\varepsilon})$. 
Let $A = \max_i \|f_i\|$.

- Arithmetic complexity
  The number of swaps is bounded by $\log(\Delta)/\log\left(\frac{3}{4}\right)$.
  The initial value of $\log \Delta$ is bounded by $n^2 \log A$.

  We can update the GS info in $O(n^2)$ operations. The “for” loop for size reduction has at most one nontrivial iteration.

  How many iterations of the “while” loop?
Complexity

Let $A = \max_i \|f_i\|$.

- **Arithmetic complexity**
  The number of swaps is bounded by $\log(\Delta)/\log(\frac{3}{4})$.
  The initial value of $\log \Delta$ is bounded by $n^2 \log A$.

  We can update the GS info in $O(n^2)$ operations. The “for” loop for size reduction has at most one nontrivial iteration.

  How many iterations of the “while” loop?

  $\#\text{nonswap iter.} - \#\text{swap iter.} \leq i + 2$
Complexity

Let \( A = \max_i \| f_i \| \).

- Arithmetic complexity
  The number of swaps is bounded by \( \log(\Delta) / \log(\frac{3}{4}) \).
  The initial value of \( \log \Delta \) is bounded by \( n^2 \log A \).

We can update the GS info in \( O(n^2) \) operations. The “for” loop for size reduction has at most one nontrivial iteration.

How many iterations of the “while” loop?

\[
\#\text{nonswap iter.} - \#\text{swap iter.} \leq i + 2
\]

So at most \( O(n^2 \log A) \) iterations, and \( O(n^4 \log A) \) total iterations.
Complexity

Let $A = \max_i \|f_i\|$.

- **Arithmetic complexity**
  The number of swaps is bounded by $\log(\Delta) / \log(\frac{3}{4})$.
  The initial value of $\log \Delta$ is bounded by $n^2 \log A$.

  We can update the GS info in $O(n^2)$ operations. The “for” loop for size reduction has at most one nontrivial iteration.

  How many iterations of the “while” loop?

  \[
  \#\text{nonswap iter.} - \#\text{swap iter.} \leq i + 2
  \]

  So at most $O(n^2 \log A)$ iterations, and $O(n^4 \log A)$ total iterations.

- **Binary complexity**
  Hard to do it right... Current best (of a variant of LLL) is $O(n^{5+\varepsilon} \log(\Delta)^{1+\varepsilon})$. 
Applications of lattice reduction

• Cryptography
• Experimental mathematics
  • Disproof of Mertens’ conjecture (Odlyzko, te Riele 1985)
  • Guessing recurrence relations with little data (Kauers, Koutschan 2022)
• Integer linear programming
• ...

Lattice reduction | Pierre Lairez