Lattice reduction
Experimental mathematics

MPRI – Efficient algorithms in computer algebra

Pierre Lairez

Outline

1. Lattice reduction

2. BBP formulas

3. Disproof of Mertens' conjecture

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 $||f|| = \min\{||g|| \mid g \in \Lambda \text{ nonzero}\}$

A polynomial-time solvable problem

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

Output $f \in \Lambda$ nonzero such that $||f|| \leq 2^{\frac{n-1}{2}} \min\{||g|| \mid g \in \Lambda \text{ nonzero}\}$

Volume and ith 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

$$\mathrm{vol}(L)^2 = \det\left(f_i \cdot f_j\right)_{1 \leq i,j \leq r}$$

kth minimum

$$\begin{aligned} \lambda_k(L) &= \min\{B \mid \mathrm{rk}\, L_B \geq k\} \\ &= \min\left\{ \max_{1 \leq i \leq k} \|v_i\| \,\middle|\, v_1, \ldots, v_k \in L \text{ linearly independent} \right\}. \end{aligned}$$

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

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

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

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

Lemma

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

GSO and short vectors

Lemma

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

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

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

and in particular, $\|g\|^2 \geq a_s^2 \|f_s^*\|^2$.

Reduced bases

Definition

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

(i) $|\mu_{ij}| \leq \frac{1}{2}$, for any $1 \leq j < i$ *(size-reduced)*;

(ii) $\|f_{i-1}^*\|^2 \leq 2\|f_i^*\|^2$ for any i.

I follow Gathen, Gerhard (2013) for the definition. More commonly, condition (ii) is replaced by the stronger, with $\delta \in (\frac{1}{4}, 1)$

$$(\delta - \mu_{i,i-1}^2)\|f_{i-1}^*\|^2 \leq \|f_i^*\|^2.$$

It took 200 years to develop this definition. It's not at all clear that it's strong enough to be interesting, or weak enough for such bases to exist and be computable in polynomial time.

Reduced bases II

Lemma

Let $f_1, \ldots, f_r$ *be a reduced basis.*
For any nonzero $g \in L$, $\|f_1\| \leq 2^{\frac{r-1}{2}} \|g\|$.

Reduced bases II

Lemma

Let $f_1, \ldots, f_r$ be a reduced basis.
For any nonzero $g \in L$, $\|f_1\| \leq 2^{\frac{r-1}{2}} \|g\|$.

Proof. $\|f_i^*\| \geq 2^{\frac{i-1}{2}} \|f_1^*\|$ and $f_1^* = f_1$.

Reduced bases II

Lemma

Let $f_1, \ldots, f_r$ be a reduced basis.
For any nonzero $g \in L$, $\|f_1\| \leq 2^{\frac{r-1}{2}} \|g\|$.

Proof. $\|f_i^*\| \geq 2^{\frac{i-1}{2}} \|f_1^*\|$ and $f_1^* = f_1$.

Let $\lambda_k(L) = \min\{B \mid \mathrm{rk}\, L_B \geq k\} = \min\{\max_{1 \leq i \leq k} \|v_i\| \mid v_1, \ldots, v_k \in L$ lin. indep.$\}$.
Let $f_1, \ldots, f_r$ be a reduced basis.

Lemma

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

Reduced bases II

Lemma

Let $f_1, \dots, f_r$ be a reduced basis.
For any nonzero $g \in L$, $\|f_1\| \leq 2^{\frac{r-1}{2}} \|g\|$.

Proof. $\|f_i^*\| \geq 2^{\frac{i-1}{2}} \|f_1^*\|$ and $f_1^* = f_1$.

Let $\lambda_k(L) = \min\{B \mid \mathrm{rk}\, L_B \geq k\} = \min\{\max_{1 \leq i \leq k} \|v_i\| \mid v_1, \dots, v_k \in L$ lin. indep.$\}$.
Let $f_1, \dots, f_r$ 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 $v_1, \dots, v_k \in L$ be linearly independent. Because of the linear independence, there is at least one v_i which is not in $\mathrm{Vect}(f_1, \dots, f_{k-1})$. By a previous argument, $\|v_i\| \geq \min_{k \leq j \leq r} \|f_j^*\|$.

Reduced bases III

Lemma

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

Reduced bases III

Lemma

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

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

Reduced bases IV

Theorem

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

(i) $\|f_i\| \le \kappa B$ for all $i \le k$;

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

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

Reduced bases V

Proof. Let $k = \mathrm{rank}(L_B)$. 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

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

This proves (i).
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. This proves (iii).
For any $j > k$, the family $f_1, \ldots, f_k, f_j$ is free, so

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

Combining with the previous inequality, this implies that $\|f_j\| \geq \mu B$. This proves (ii).

Reduced bases are indeed what we need!

The LLL algorithm

```
def LLL(f_1, ..., f_r):
    compute the GS information (the ||f_i^*||^2 and μ_ij coefficients)
    i ← 2;   N_iter ← 0;   N_swap ← 0
    while i ≤ r:
        N_iter ← N_iter + 1
        for j from i − 1 to 1:
            f_i ← f_i − ⌊μ_ij⌉ 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 ← max(i − 1, 2);   N_swap ← N_swap + 1
        else:
            i ← i + 1
    return f_1, ..., f_r
```

Correction of the LLL algorithm

Proposition

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

After the loop on line 6, it is clear that $f_1, \ldots, f_i$ is size-reduced.

Correction of the LLL algorithm

Proposition

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

After the loop on line 6, it is clear that $f_1, \ldots, f_i$ is size-reduced.

At the begining 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.

Polynomial-time termination of LLL

Theorem (A. K. Lenstra, H. W. Lenstra, Lovàsz 1982)

The LLL algorithm terminates in polynomial time.

Polynomial-time termination of LLL

Theorem (A. K. Lenstra, H. W. Lenstra, Lovàsz 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

$$\|g_{i-1}^*\|^2 \leq \|f_i^*\|^2 + \frac{1}{4}\|f_{i-1}^*\|^2 \leq \frac{3}{4}\|f_{i-1}^*\|^2.$$

Polynomial-time termination of LLL

Theorem (A. K. Lenstra, H. W. Lenstra, Lovàsz 1982)

The LLL algorithm terminates in polynomial time.

If a swap happens, let $g_1, \dots, g_i$ 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.

Polynomial-time termination of LLL

Theorem (A. K. Lenstra, H. W. Lenstra, Lovàsz 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, $D_j = \mathrm{vol}\left(\mathbb{Z}f_1 + \cdots + \mathbb{Z}f_j\right)$, so D_j (for $j \neq i$) remains constant. It follows that

$$\Delta = D_1 \cdots D_r$$

is a strictly positive integer which decreases by $\frac{3}{4}$ after a swap.

Complexity

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

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

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.

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?

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? We check the following loop invariant:

$$N_{\text{iter}} \leq 2N_{\text{swap}} + i$$

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? We check the following loop invariant:

  $$N_{\text{iter}} \leq 2N_{\text{swap}} + i$$

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

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? We check the following loop invariant:

  $$N_{\text{iter}} \leq 2N_{\text{swap}} + i$$

  So at most $O(n^2 \log A)$ iterations, and $O(n^4 \log A)$ total operations.
- Binary complexity
  Hard to do it right... Current best (of a variant of LLL) is $O(n^{5+\epsilon} \log(A)^{1+\epsilon})$.

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
- ...

Outline

1. Lattice reduction

2. BBP formulas

3. Disproof of Mertens' conjecture

Outline

1. Lattice reduction

2. BBP formulas

3. Disproof of Mertens' conjecture