Lattice reduction

Pierre Lairez
1. Lattice reduction
### Euclidean lattices

**Definition**

A lattice is a discrete subgroup of \( \mathbb{R}^n \) (often \( \mathbb{Z}^n \)).

**A famous NP-hard problem**

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

**Output** \( f \in \Lambda \) nonzero such that \( \|f\| = \min \{\|g\| \mid g \in \Lambda \) nonzero} \)

**A polynomial-time solvable problem**

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

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

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

\[ \mu_{ij} \]

**Lemma**

_for any nonzero_ \( g \in L, \|g\| \geq \min \{\|f_1^*\|, \ldots, \|f_r^*\|\} \).

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

\[ g = a_sf_s^* + [\cdots]f_{s-1}^* + \cdots + [\cdots]f_1^*, \]

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

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

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

**Lemma**

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

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

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

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

**Lemma**

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

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

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.
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 $\kappa = \frac{r-1}{2}$ and $\mu \geq \kappa$. For any $B > 0$ such that $L_B = L_\mu$, 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 $L_B$.

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

For any $i \leq k$, we have

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

In particular, \( f_i \in L_{kB} \subset L_{\mu B} = L_B \), 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(f_1, \ldots, f_r):
    compute the GS information (the $\|f_i^*\|^2$ and $\mu_{ij}$ coefficients)
    i ← 2
    while $i \leq n$:
        for $j$ from $i - 1$ to 1:
            $f_i \leftarrow f_i - \lceil \mu_{ij} \rceil f_j$
            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
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 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

$$g_{i-1}^* = f_i^* + \mu_{i,i-1} f_{i-1}^*$$

and so

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

Moreover, $\|g_i^*\| \leq \|f_{i-1}^*\|^2$

So at each swap, $D = \prod_{i=1}^{r} \|f_i^*\|^2$ decreases by a factor $\frac{3}{4}$ at least.

Besides, the classical formula for the Gram determinant yields

$$D = \det \left( \langle f_i, f_j \rangle \right) \in \mathbb{Z}.$$
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
• …