LECTURE 3:
Lenstra-Lenstra-Lovász lattice basis reduction algorithm

H. Xiao NOVEMBER 2012

Recall that a full-rank *lattice* Λ is a discrete additive subgroup of $\mathbb{R}^n$ generated by all the integer combinations of n linearly independent vectors. Such a set of n vectors is called a *basis* of Λ. And Λ is usually expressed as

$$\{c_1 b_1 + \cdots + c_n b_n : c_i \in \mathbb{Z} \text{ for all } i\},$$

with the coefficients running over all integers. Given a lattice Λ, there are infinitely many different choices of lattice bases. One can obtain another lattice basis by a unimodular transformation (multiplying the basis vectors by a square matrix with integer entries and determinant plus or minus one). If we put all n basis vectors together and form an $n \times n$ matrix, the magnitude of the determinant is equal to the volume of the *fundamental parallelepiped*

$$\{x_1 b_1 + \cdots + x_n b_n : 0 \le x_i < 1 \text{ for all } i\}$$

associated with the basis. Observing that the fundamental parallelepiped of two different lattice bases have the same volume. Hence, it makes sense to define the *determinant* of a lattice as the volume of the fundamental parallelepiped of any basis.

Noticing the similarity between lattice and vector space, an orthogonal basis could be very help for investigating the property of a lattice. Not every lattice has an orthogonal basis, but a basis whose vectors are as orthogonal as possible will still preserve some good properties. A basis like that is said *nearly orthogonal*. One measure of the orthogonality of a basis is called the *orthogonality defect*, which is the ratio of the product of the Euclidean norms of the basis vectors over the determinant of the lattice $\det(\Lambda)$

$$\frac{\|b_1\| \cdot \|b_2\| \cdots \|b_n\|}{\det \Lambda}.$$

By the Hadamard inequality, the quantity is larger than or equal to one. The equality holds if and only if the basis vectors are orthogonal. To find a nearly orthogonal basis, we only need to find a basis which minimizes orthogonality defect. A classical theorem of Hermite states that for each n there exists a number $c(n)$ such that every n-dimensional lattice Λ has a basis $v_1, \ldots, v_n$ with

$$\|b_1\| \cdot \|b_2\| \cdots \|b_n\| \le c(n) \det \Lambda.$$

Hermite also showed that we can take $c(n) = (\frac{4}{3})^{n(n-1)/4}$. So once we find a basis satisfying the inequality above, we can think of this basis as an approximation of an orthogonal basis, and such a nearly orthogonal basis always exists.

In the vector space, we can always apply Gram-Schmidt process to get an orthogonal basis. The Gram-Schmidt process is initialized by setting $b_1^* = b_1$ and recursively computes

$$b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{i,j} b_j^*,$$

where $\mu_{i,j} = \frac{\langle b_i, b_j^* \rangle}{\|b_j^*\|^2}$, for $i = 2, 3, \ldots, n$. However, as the coefficients $\mu_{i,j}$ are not integral in general, the Gram-Schmidt process does not yield a lattice basis.

If we define the matrix $B = [b_1 b_2 \ldots b_n]$, the Gram-Schmidt process yields a QR-decomposition of B, where $Q = [b_1^* b_2^* \ldots b_n^*]$ and

$$R = \begin{bmatrix} 1 & \mu_{21} & \cdots & \mu_{n1} \\ 0 & 1 & \cdots & \mu_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}.$$

Observing that the coefficients $\mu_{i,j}$ would be all zero, if the basis vectors $b_1, \ldots, b_n$ were orthogonal. In this case, the orthogonality defect attains the minimum value 1. This observation motivates the idea called *size-reduction*. We can reduce $\mu_{i,j}$ by subtracting the nearest integer to $\mu_{i,j}$ to make sure $|\mu_{i,j}| \leq 1/2$. By elementary column operations one can change R into a matrix in upper-triangular form, with 1's on the diagonal, and all other entries at most $\frac{1}{2}$ in absolute value. This seems to be the best relaxation we can do.

More formally, size-reduction step can be performed:

Size Reduction
for $i = 2$ to n
  $b_i = \mu_{i,1}b_1^* + \mu_{i,2}b_2^* + \cdots + \mu_{i,i-1}b_{i-1}^* + b_i^*$
  for $j = i-1, i-2, \ldots, 1$
    $m \leftarrow$ nearest integer to $\mu_{i,j}$
    $b_i \leftarrow b_i - mb_j$
  end
end

The second idea in basis reduction is to maintain the *Lovász condition*

$$(\delta - \mu_{i+1,i}^2)\|b_i^*\|^2 \leq \|b_{i+1}^*\|^2,$$

which is designed to upper bound the orthogonality defect. By Pythagorean Theorem, the Gram-Schmidt vectors b_i^* can get shorter and shorter. This condition requires that their length can not decrease too quickly. Specifically, for any $1/4 < \delta < 1$, if we set $\alpha = 1/(\delta - \frac{1}{4})$, then Lovász condition implies

$$\|b_i^*\|^2 \leq \alpha\|b_{i+1}^*\|^2.$$

Particularly, δ is a parameter which is usually taken as $3/4$, then $\alpha = 2$. It follows that

$$\begin{aligned}
\|b_i\|^2 &= \|\mu_{i,1}b_1^* + \mu_{i,2}b_2^* + \cdots + \mu_{i,i-1}b_{i-1}^* + b_i^*\|^2 \\
&\leq \|b_i^*\|^2 + \frac{1}{4}\sum_{k=1}^{i-1}\|b_k^*\|^2 \\
&\leq \|b_i^*\|^2(1 + \frac{1}{4}\sum_{k=1}^{i-1}2^{i-k}) \\
&\leq 2^{i-1}\|b_i^*\|^2.
\end{aligned}$$

Notice that $\det\Lambda = |\det B| = |\det Q \cdot \det R| = |\det Q| = \prod_{i=1}^n \|b_i^*\|$, then consider the orthogonality defect of a basis satisfying Lovász condition,

$$\begin{aligned}
\frac{\|b_1\| \cdot \|b_2\| \cdots \|b_n\|}{\det\Lambda} &= \frac{\|b_1\| \cdot \|b_2\| \cdots \|b_n\|}{\|b_1^*\| \cdot \|b_2^*\| \cdots \|b_n^*\|} \\
&\leq \prod_{i=1}^n 2^{\frac{i-1}{2}}
\end{aligned}$$

Definition 3.1 (δ-reduced basis) *A basis $\{b_1, b_2, \ldots, b_n\}$ is a δ-reduced basis if*

- *all the non-diagonal entries of R satisfy $|\mu_{i,j}| \leq 1/2$,*
- *for any pair of consecutive vectors b_i and b_{i+1}, we have $\delta\|\pi_{S_i}(b_i)\|^2 \leq \|\pi_{S_i}(b_{i+1})\|^2$, where S_i is the orthogonal complement of span$(b_1, \ldots, b_{i-1})$, and π_{S_i} is the projection operator to S_i.*

It is fulfilled by a process resembling the Euclidean GCD algorithm: Subtract an integral multiple of the shorter vector from the longer one to get a vectors as short as possible; if the length ordering is broken, we swap the two vectors and repeat, otherwise the procedure ends (this idea is also a generation of Gauss Algorithm to higher dimensions).

References

[CW87] D. Coppersmith and S. Winograd, "Matrix multiplication via arithmetic progressions," *Proceedings of the 19th ACM Symposium on Theory of Computing*, 1987, pp. 1–6.