Chapter 2
Hermite’s Constant and Lattice Algorithms

Phong Q. Nguyen

Abstract We introduce lattices and survey the main provable algorithms for solving the shortest vector problem, either exactly or approximately. In doing so, we emphasize a surprising connection between lattice algorithms and the historical problem of bounding a well-known constant introduced by Hermite in 1850, which is related to sphere packings. For instance, we present the Lenstra–Lenstra–Lovász algorithm (LLL) as an (efficient) algorithmic version of Hermite’s inequality on Hermite’s constant. Similarly, we present blockwise generalizations of LLL as (more or less tight) algorithmic versions of Mordell’s inequality.

Introduction

Informally, a lattice is an infinite arrangement of points in \( \mathbb{R}^n \) spaced with sufficient regularity that one can shift any point onto any other point by some symmetry of the arrangement. The simplest example of a lattice is the hypercubic lattice \( \mathbb{Z}^n \) formed by all points with integral coordinates. Geometry of numbers [1–4] is the branch of number theory dealing with lattices (and especially their connection with convex sets), and its origins go back to two historical problems:

1. Higher-dimensional generalizations of Euclid’s algorithm. The elegance and simplicity of Euclid’s greatest common divisor algorithm motivate the search for generalizations enjoying similar properties. By trying to generalize previous work of Fermat and Euler, Lagrange [5] studied numbers that can be represented by quadratic forms at the end of the eighteenth century: given a triplet \((a, b, c) \in \mathbb{Z}^3\), identify which integers are of the form \(ax^2 + bxy + cy^2\), where \((x, y) \in \mathbb{Z}^2\). Fermat had for instance characterized numbers that are sums of two squares: \(x^2 + y^2\), where \((x, y) \in \mathbb{Z}^2\). To answer such questions, Lagrange invented a generalization [5, pages 698–700] of Euclid’s algorithm to binary quadratic forms. This algorithm is often attributed (incorrectly) to Gauss [6], and was generalized in
the nineteenth century by Hermite [7] to positive definite quadratic forms of arbitrary dimension. Let \( q(x_1, \ldots, x_n) = \sum_{1 \leq i, j \leq n} q_{i,j} x_i x_j \) be a positive definite quadratic form over \( \mathbb{R}^n \), and denote by \( \Delta(q) = \det_{1 \leq i, j \leq n} q_{i,j} \in \mathbb{R}^+ \) its discriminant. Hermite [7] used his algorithm to prove that there exist \( x_1, \ldots, x_n \in \mathbb{Z} \) such that

\[
0 < q(x_1, \ldots, x_n) \leq (4/3)^{(n-1)/2} \Delta(q)^{1/n}. \tag{2.1}
\]

If we denote by \( \|q\| \) the minimum of \( q(x_1, \ldots, x_n) \) over \( \mathbb{Z}^n \setminus \{0\} \), (2.1) shows that \( \|q\| / \Delta(q)^{1/n} \) can be upper bounded independently of \( q \). This proves the existence of Hermite’s constant \( \gamma_n \) defined as the supremum of this ratio over all positive definite quadratic forms:

\[
\gamma_n = \max_{q \text{ positive definite over } \mathbb{R}^n} \frac{\|q\|}{\Delta(q)^{1/n}}, \tag{2.2}
\]

because it turns out that the supremum is actually reached. The inequality (2.1) is equivalent to Hermite’s inequality on Hermite’s constant:

\[
\gamma_n \leq (4/3)^{(n-1)/2}, \quad n \geq 1, \tag{2.3}
\]

which can be rewritten as

\[
\gamma_n \leq \gamma_2^{n-1}, \quad n \geq 1, \tag{2.4}
\]

because Lagrange [5] showed that \( \gamma_2 = \sqrt{4/3} \). Though Hermite’s constant was historically defined in terms of positive definite quadratic forms, it can be defined equivalently using lattices, due to the classical connection between lattices and positive definite quadratic forms, which we will recall precisely in section “Quadratic Forms.”

2. Sphere packings. This famous problem [8] asks what fraction of \( \mathbb{R}^n \) can be covered by equal balls that do not intersect except along their boundaries. The problem is open as soon as \( n \geq 4 \) (see Fig. 2.1 for the densest packing for \( n = 2 \)), which suggests to study simpler problems.

![Fig. 2.1 The densest packing in dimension two: the hexagonal lattice packing](image)