# CSE206A: Lattice Algorithms and Applications
# Spring 2007, Homework 1: How good is Minkowski's bound?

Daniele Micciancio

April 12, 2007

All lattices in this assignment are assumed to have full rank. Let $V_n$ be the volume of the unit sphere in $n$-dimensional space. Minkowski's covex body theorem implies that any $n$-dimensional lattice $L$ has minimum distance at most $\lambda(L) \le (2/\sqrt[n]{V_n}) \cdot \det(L)^{1/n}$. Using $V_n > (2/\sqrt{n})^n$ as a lower bound on the volume of a sphere[1], we get that $\lambda(L) < \sqrt{n}\det(L)^{1/n}$, which is the most commonly used form of Minkowski's theorem. In this assignment, you are asked to prove that this bound is tight up to constant multiplicative factors. The problem is broken into parts, in order to guide you in your search for a solution. You are not required to follow the suggested approach. If you see a simpler proof than the one we suggest, you can organize your solution differently.

## Part 1: Finding holes in a lattice

Show that if a lattice has determinant at least $\det(L) > d^n V_n$, then there exists a point $\mathbf{x}$ at distance $d$ from the lattice, i.e., $\|\mathbf{x} - \mathbf{y}\| > d$ for all lattice vectors $\mathbf{y} \in L$. (Hint: pick a basis for the lattice and use a volume argument similar to the one from the proof of Blichfeldt theorem.)

## Part 2: Filling holes

Let $\mathbf{h}$ be a point in space furthest away from (full rank lattice) $L$, and let $\rho = \min\{\|\mathbf{h} - \mathbf{y}\| : \mathbf{y} \in L\}$ the distance to the closest lattice point. ($\rho$ is called the covering radius of the lattice, and $\mathbf{h}$ is called a deep hole.) Show that if $\mathbf{x} \in L$ is a lattice point closest to $2\mathbf{h}$, then the set $L' = L \cup (L + \mathbf{x}/2)$ is a lattice with determinant $\det(L') = \det(L)/2$ and minimum distance $\lambda(L') \ge \min\{\lambda(L), \rho/2\}$.

## Part 3: Dense lattices

Show that for any $n$ there is an $n$-dimensional (full rank) lattice such that $\lambda(L) \ge (1/(2\sqrt[n]{V_n})) \cdot \det(L)^{1/n}$. (Hint: consider the quantity $\sigma = \sup \lambda(L)^n / \det(L)$, where $L$ ranges over all $n$-dimensional lattices, assume for contradiction that $\sigma < 1/(2^n V_n)$, and apply parts 1 and 2 to a lattice $L$ satisfying $\sigma/2 < \lambda(L)/\det(L) \le \sigma$.) This proves that Minkowski's bound $\lambda(L) \le (2/\sqrt[n]{V_n}) \cdot \det(L)^{1/n}$ is tight up to a factor 4.

## Part 4: The volume of the sphere

Show that the $V_n > (2/\sqrt{n})^n$ lower bound on the volume of the sphere is also tight. Specifically, show that there is a constant $c_4$ such that $V_n \le (c_4/\sqrt{n})^n$. For this part, you may want to use the fact that for any even $n = 2k$, $V_n = \pi^{n/2}/(n/2)! = \pi^k/k!$. Conclude that Minkowki's bound $\lambda(L) \le \sqrt{n}\det(L)^{1/n}$ is tight up to constant factors.

[1] This lower bound is easily obtained by observing that the unit sphere contains the hypercube $C = \{\mathbf{x} : \|\mathbf{x}\| \le 1/\sqrt{n}\}$