Some Mathematical Mysteries in Lattices

Chuanming Zong

Peking University

Lattice, as a basic object in Mathematics, has been studied by many prominent figures, including Gauss, Hermite, Voronio, Minkowski, Davenport, Hlawka, Rogers and many others still active today. It is one of the most important cornerstones of Geometry of Numbers, a classic branch of Number Theory. During recent decades, this pure mathematical concept has achieved remarkable applications in Cryptography, in particular its algorithm approaches. The main purpose of this talk is to demonstrate some basic mathematical problems and results (old and new) about lattices, which are probably useful in Cryptography in the future. These problems reflect some of the main interests of the mathematicians about lattices.

Before Minkowski, lattices were mainly studied through positive definitive quadratic forms. In fact, to determine the minimal value of a positive definitive quadratic form at integer points is equivalent to determine the length of the shortest vectors (except $\mathbf{o}$) of a lattice, which is also equivalent to determine the maximal density of the corresponding lattice ball packings.

It was Minkowski who first studied the density $\delta^*(C)$ of the densest lattice packings of a given centrally symmetric convex body C. In particular, he obtained the first general lower bound of $\delta^*(C)$ for n-dimensional unit ball B. In fact, to determine the density $\delta^*(C)$ is to estimate the maximal length of the shortest vectors of the lattices of determinant 1 with respect to certain metric determined by C. When C is the unit ball, the metric is just the ordinary Euclidean metric. Therefore, the shortest vector problem is a particular case of the study about $\delta^*(B)$. There are lower bound and upper bound for $\delta^*(C)$ and $\delta^*(B)$, however the asymptotic orders of both $\min \delta^*(C)$ and $\delta^*(B)$ are unknown. For lattice kissing numbers we are facing the similar situation.

The density $\theta^*(C)$ of the thinnest lattice covering of a centrally symmetric convex body C was first systematically studied by Rogers. In fact, it is equivalent to determine the minimal length of the longest distance from a point to the lattices of determinant 1 with respect to the metric determined by C. Therefore, the closest vector problem is a particular case of the study of $\theta^*(B)$. For particular object C, such as a ball in a given dimension, little is known about the exact value of $\theta^*(C)$.

Let $\gamma^*(C)$ be the smallest number that there is a lattice Λ such that $C + \Lambda$ is a packing and $\gamma^*(C)C + \Lambda$ is a covering. Equivalently, in every lattice packing $C + \Lambda$ there is a hole in which one can put a translate of $(\gamma^*(C) - 1)C$. In 1950, Rogers introduced and studied this number, in particular for the unit ball. In fact, $\gamma^*(C)$ is a bridge connecting $\delta^*(C)$ and $\theta^*(C)$. In other words, it is a

X. Wang and K. Sako (Eds.): ASIACRYPT 2012, LNCS 7658, pp. 2–3, 2012.

bridge connecting the packing radius and the covering radius of a lattice, with respect to the metric determined by C. Some results about $\gamma^*(C)$ and $\gamma^*(B)$ are known. At the same time, a number of fascinating mysteries about $\gamma^*(C)$ and their possible consequences remain unsolved.

Can you imagine that, in every three-dimensional lattice ball packing there is a straight line of infinite length which does not meet any of the balls; when n is large, in every n-dimensional lattice ball packing there is a free hyperplane of dimension more or less $n/\log n$? But, this is true!