

---

**XIAOWEN CHANG**, McGill University

*Why is the LLL reduction useful for solving an integer least squares problem*

In some applications such as GPS and communications, there is a linear model, which involves an unknown integer parameter vector. The common method to estimate the integer parameter vector is to solve an integer least squares (ILS) problem, also referred to as a closest vector problem. A typical approach to solving an ILS problem is the so called sphere decoding, a discrete search method. To make a sphere decoder faster, the well-known Lenstra, Lenstra and Lovasz (LLL) reduction is often used as preprocessing. As a general ILS problem is NP-hard, for some applications, an approximate solution, which can be produced quickly, is computed instead. One often used approximate solution is the Babai point, the first integer point found by a typical sphere decoder. In order to verify whether an estimator is good enough for a practical use, one needs to find the probability of the estimator being equal to the true integer parameter vector, which is referred to as success probability. In addition to making the search process faster, it has been observed that the LLL reduction can also improve the success probability of the Babai point. But there has been no rigorous theory about either observation so far. In this talk we will show rigorously in theory why both are true.

This is joint work with Jinming Wen and Xiaohu Xie