Closest Integer in Cyclotomic Number Fields
Bachelor Thesis Proposal

Léo Ducas
CWI, Amsterdam, Cryptology Group

Context and Application

A lattice is discrete subgroup of finite-dimensional euclidean vector spaces: a regular grid of points. A fundamental lattice algorithmic problem, is to determine, given a lattice a arbitrary target point in the vector space, which point of the lattice is the closest to the target. This is known as the closest vector problem (CVP). In full generality, this problem is hard: the best known algorithm require time exponential in the dimension. But for certain lattices, this task may become easy, or even trivial like with the lattice $\mathbb{Z}^n$.

Such task finds application to error correction over analog noisy channel. The discrete data to be transmitted is encoded to a lattice point and sent over the noisy channel. After reception, the decoding consist of applying the CVP algorithm, separating the data from the noise. The lattice is designed to simultaneously allow efficient decoding and maximize bandwidth.

Similar ideas have recently appeared in cryptography. An encryption scheme can be designed by making the decoding step only possible with the knowledge of a secret key: an easy to decode lattice is secretly hidden in a hard one. For efficiency reason, the hidden easy lattice is chosen with an algebraic structure, typically, the n-th cyclotomic ring $\mathcal{R}_n = \mathbb{Z}[x]/(\Phi_n(x))$ [2]. Note that the canonical inner-product of such rings is defined using the trace function: $\langle u, v\rangle = \mathrm{Tr}(u \cdot \bar{v})$.

State-of-the-art

An efficient and exact CVP algorithm for $\mathcal{R}_n$ is only known when n is a power of 2: in that case $\mathcal{R}_n$ is isometric to $\mathbb{Z}^{\varphi(n)}$. For other values of n, no dedicated algorithms are known, and cryptographers have to resort to approximate version of CVP (see decoding bases in [1]). This affect negatively the performances of cryptographic schemes.

There are other values of n for which solving exactly CVP is not so hard. In particular, when n is prime, $\mathcal{R}_n$ is a *Voronoï first-kind* lattice, that is, it admits an *obtuse super-basis*: the generating set $\{1, x, x^2, \ldots x^{n-1}\}$. This property was recently shown [3] to reduce CVP to a *min-cut* problem in a graph, allowing a solution to CVP in time $\Theta(n^4)$. This remains nevertheless too costly for a cryptographic scheme.

The project

The project for this bachelor thesis is to design fast CVP algorithm for those rings. The project includes 3 questions:

- When n is prime, because of the symmetries and the algebraic structure of $\mathcal{R}_n$ it is very plausible that a dedicated algorithm may bring down the complexity much below $\Theta(n^4)$, ideally, down to $\Theta(n \log n)$ to match the complexity of multiplication in that ring via the fast-Fourier transform.
- Once this first question is solved, a second step may be to generalize the previous algorithm to non-prime values of n.
- The project may also study the cryptographic implications of the developed algorithm, quantify precisely the gain provided by the exact CVP algorithm compared to the previous approximation algorithm.

Answering the three question would constitute a solid basis for a publication to a conference on cryptography.

References

[1] V. Lyubashevsky, C. Peikert, and O. Regev. On ideal lattices and learning with errors over rings. In *Advances in Cryptology–EUROCRYPT 2010*, pages 1–23. Springer, 2010.

[2] V. Lyubashevsky, C. Peikert, and O. Regev. A toolkit for ring-lwe cryptography. In *Advances in Cryptology–EUROCRYPT 2013*, pages 35–54. Springer, 2013.

[3] R. McKilliam and A. Grant. Finding short vectors in a lattice of voronoi's first kind. *arXiv preprint arXiv:1201.5154*, 2012.