Complexity of Finding Lattice Isomorphisms

Léo Ducas

Bachelorseminarium AGM voorjaar 2026

Background. A lattice is a discrete subgroup of a Euclidean vector space $E = (\mathbb{R}^n, \langle\cdot,\cdot\rangle)$, say where $\langle x, y\rangle = \sum_{i=1}^n x_i y_i$ is the standard inner product. A lattice isomorphism from L to L' is isometry $O \in \mathcal{O}(E)$ such that $O \cdot L = L'$. The lattice isomorphism problem is the task of finding such an isometries between two given lattices L and L'.
More concretely, a (full-rank) lattice is given by one of its basis: $L = B \cdot \mathbb{Z}^n$ where $B \in \mathcal{GL}_n(\mathbb{R})$. Two basis B and B' generates the same lattice if and only if there exists a *unimodular* matrix $U \in \mathcal{GL}_n(\mathbb{Z})$ such that $B' = B \cdot U$. Hence, the lattice isomorphism problem is the task of finding two matrices $O \in \mathcal{O}_n(\mathbb{R})$ and $U \in \mathcal{GL}_n(\mathbb{R})$ such that:

$$B' = O \cdot B \cdot U.$$

The fastest known provable algorithm for this task [HR14] has complexity $2^{O(n \log n)}$, though in practice other approaches based are often prefered [vW23, Sec 9.5] despite a poorer provable complexity. Furthermore, the proof of [HR14] is based on a so-called isolation lemma that appears to not make much use of the available geometric information.
In a nutshell, the alternative approach instead consider the sets S, S' of all the shortest non-zero vectors of the lattices L, L'; those sets are known to have size at most $N \leq 2^{.401n+o(n)}$ [KL78]. One then choose an arbitrary ordered set $X \subset S$ of n linearly independant vectors from L, and bruteforce all such ordered sets $X' \subset S'$, and finally test wether the linear map sending X to X' is indeed an isometry.
Naively, this gives an algorithm with complexity $N^n = 2^{O(n^2)}$, but there is room for improvement. Indeed, when recursively enumerating $X' = (x'_1, \ldots, x'_n)$, we can discard many choices for x'_i using the constraints that $\langle x'_i, x'_j\rangle = \langle x_i, x_j\rangle$ based on choices already made for x'_j, for $j < i$. Secondly, we can choose the set X wisely, so that those constraints to bound the set of valid choices at each level of the enumeration.

Goals. Potential goals for a thesis on this general topic could be:

- Revisit the algorithm of [HR14], determine the hidden constant in the $O(n \log n)$, and attempt to improve it.
- Explore and optimize the complexity of the alternative approach, in particular by making use of bounds on spherical codes such as [KL78, Tao13].

References

[HR14] Ishay Haviv and Oded Regev. On the lattice isomorphism problem. In *Proceedings of the twenty-fifth annual ACM-SIAM symposium on Discrete algorithms*, pages 391–404. SIAM, 2014. https://arxiv.org/abs/1311.0366.

[KL78] Grigorii Anatol'evich Kabatiansky and Vladimir Iosifovich Levenshtein. On bounds for packings on a sphere and in space. *Problemy peredachi informatsii*, 14(1):3–25, 1978.

[Tao13] Terence Tao, 2013. https://terrytao.wordpress.com/2013/07/18/a-cheap-version-of-the-kabatjanskii-levenstein-bound-for-almost-orthogonal-vectors/.

[vW23] Wessel van Woerden. *Lattice cryptography: from cryptanalysis to New Foundations.* PhD thesis, Leiden University, 2023. https://scholarlypublications.universiteitleiden.nl/access/item%3A3564772/download.