

HOMEWORK 3

Instructor: Daniele Micciancio

UCSD CSE

Lattices with large minimum distance λ_1 make good error correcting codes, or lattice packings. Lattices with small covering radius μ make good quantizers, which can be used to approximate arbitrary points in space with small distortion. The lattice families D_n and D_n^* defined below contain the best (known) lattice codes and lattice quantizers in low dimension. Specifically, D_3, D_4, D_5 are (provably) the best possible lattice codes in dimension 3, 4, 5, and D_3^*, D_4^*, D_5^* are the best (known) quantizers. Moreover, $D_4 \cong D_4^*$ are essentially the same lattice, making D_4 simultaneously a good code and good quantizer in dimension 4, and $E_8 \cong E_8^*$ (the best lattice packing and quantizer in dimension 8) is easily obtained from D_8 . In 2022, Maryna Viazovska received the Fields medal for proving that E_8 is the best way to pack spheres in 8-dimensional space (even among packings that are not lattices.) In this homework, we explore efficient decoding algorithms for these lattices.

1 Decoding D_n

Let $D_n = \{x \in \mathbb{Z}^n : \sum_i x_i \equiv 0 \pmod{2}\}$ be the lattice containing all n -dimensional integer vectors such that the sum of the coordinates is even.

Part a) Give a polynomial time CVP algorithm for D_n that on input an arbitrary point $y \in \mathbb{R}^n$, returns the lattice point $x \in D_n$ closest to y . Prove (at least informally) that your algorithm is correct, and analyze its running time. [Hint: round each coordinate of y to the closest integer, and then determine how to modify the resulting integer vector so that it belongs to D_n]

Part b) Use your solution to (a) to determine the covering radius μ of D_n . Prove that your answer is correct by showing that your CVP algorithm always returns a lattice point within distance μ from D_n , and find a point at distance μ from the lattice.

2 Decoding D_n^*

Let D_n^* be the dual of the lattice defined in Problem 1. (In class, we have used notation $\hat{L}$ for the dual of a lattice, to avoid confusion with Gram-Schmidt orthogonalization. Here we write D_n^* because this is the notation most commonly used for this specific family of lattices.

Part a) Give a polynomial time CVP algorithm for D_n^* that on input an arbitrary point $y \in \mathbb{R}^n$, returns the lattice point $x \in D_n^*$ closest to y . Prove (at least informally) that your algorithm is correct, and analyze its running time. [Hint: express D_n^* as the union of two shifted copies of $\mathbb{Z}^n$.]

Part b) Use your solution to (a) to determine the covering radius μ of D_n^* . Prove that your answer is correct by showing that your CVP algorithm always returns a lattice point within distance μ from D_n^* , and find a point at distance μ from the lattice.