Kissing Number of Craig's Lattice and Spherical Decoding

Léo Ducas

Bachelorseminarium AGM voorjaar 2025

Craig's Lattices. We propose to study a family of euclidean lattices known as Craig's Lattices and denoted A_{n-1}^k ($n \geq 3$, $k \geq 1$), also called "repeated difference lattices". While there definition is rather simple, they are known to provide near-optimal lattice packing. Indeed, define the $n \times n$ circulant matrix (zero-entries left blank)

$$B_{n-1} = \begin{bmatrix} 1 & & & & -1 \\ -1 & 1 & & & \\ & -1 & 1 & & \\ & & \ddots & \ddots & \\ & & & -1 & 1 \end{bmatrix} \tag{1}$$

and consider A_{n-1}^k the lattice generated by the columns of B_{n-1}^k. Alternatively, one may think of A_n^k is the ideal generated by $(1-X)$ in the ring $\mathbb{Z}[X]/(1-X^n)$. This lattices has dimension $n-1$, and determinant $n^{k/2}$. For n prime and $k \leq 1$ one can show [CS13, Chap. 8, §6] a lower bound on its *minimal distance*[1] namely:

$$\lambda_1(A_{n-1}^k) \geq \sqrt{2k}.$$

This lower bound can be compared to Minkowski upper bound $\frac{\lambda_1(L)}{\det(L)^{1/n}} \leq \sqrt{\frac{2n}{\pi e}} + o(\sqrt{n})$, and choosing $k = \lfloor n/\ln n \rfloor$ we note a gap of only $O(\ln n)$ between this lower and upper bounds. In other terms, these rather simply defined lattices are not that far from providing optimal minimal distances. This property is not only of pure mathematical interest, but has potential application in information theory and cryptography.

Some experimental conjectures. One may wonder whether this bound $\lambda_1(A_{n-1}^k) \geq \sqrt{2k}$ is actually reached, and by how many vectors. For $k = 1$, the answer is easy and well documented ($A_{n-1} = A_{n-1}^1$ is known as a so-called "root lattice"): $\lambda_1(A_n^1) = \sqrt{2}$, and its *kissing number*[2] is $\kappa(A_{n-1}^1) = n(n-1)$.

Not much more appears to be known for $k \geq 2$, except for rather specific cases: $\lambda_1(A_{n-1}^k) = \sqrt{2k}$ is already known if k divides $(n-1)$, or if $k = \frac{1}{4}(p+1)$ with $k \equiv 3 \bmod 4$ [BB92, Prop 4.1]. But experimentally, it seems that more could be said. Indeed, for parameters where we could brute-force the enumeration of short vectors on a computer (say, $n \leq 200, k \leq 7$) we remark that:

[1] i.e. the quantity $\lambda_1(L) := \min_{x \in L \setminus \{0\}} \|x\|$, where $\|\cdot\|$ denotes the standard euclidean norm of $\mathbb{R}^n$.

[2] i.e. the quantity $\kappa(L) := |\{x \in L \mid \|x\| = \lambda_1(L)\}|$

- For $k = 2$ and any $n \geq 5$ (including composite n), $\lambda_1(A^2_{n-1}) = 2$ and

$$\kappa(A^2_{n-1}) = \begin{cases} n(n-1)(n-3)/4 & \text{if } n \text{ is odd} \\ n(n-2)(n-4)/4 & \text{if } n \text{ is even.} \end{cases}$$

  Perhaps interestingly, this match a known integer sequence, namely the number of obtuse triangles made from vertices of a regular n-gon [`https://oeis.org/A060423`].

- For any fixed k, and for large enough primes n, $\lambda_1(A^k_{n-1}) = \sqrt{2k}$ and

$$\kappa(A^k_{n-1}) \sim \binom{n}{k}^2 \cdot n^{1-k} \quad \text{as } n \to \infty$$

Problem 1: Prove, or disprove the above conjectures, even partially.

Spherical Codes and Decoding. A spherical code with parameters (n, N, α) is a finite subset C of the Euclidean sphere $\mathcal{S}^{d-1}$ of $\mathbb{R}^d$ such that any distinct points $c, c' \in C$ satisfy $\langle c, c' \rangle \leq \cos\alpha$. In other terms, the angles between any two points of C are at least α.
By intersecting a (re-scaled) lattice $L \subset \mathbb{R}^n$ with the sphere, one obtain a spherical code $C(L) = \frac{1}{\lambda_1(L)} L \cap \mathcal{S}^{n-1}$ with parameters $(n, \kappa(L), \pi/3)$.
The list decoding problem for a code C and angle β and target $t \in \mathcal{S}^{n-1}$ is the algorithmic task of finding all codewords close to t; i.e. computing the set $\{c \in C \mid \langle c, t \rangle \geq \cos\beta\}$. Note that if $\beta \leq \alpha/2$, there is at most one solution, in which case the problem is called unique decoding.
Generically, this problem can be solved in time $O(n \cdot N)$ by brute-force, that is by computing the N inner products and testing the inequality. But we hope to do better for well structured spherical codes. For example, the spherical code $C(A^1_{n-1})$ has $N = n(n-1)$ many elements, and for any $\beta < \pi/6$ the unique decoding problem can be solved in time $O(n)$ instead of the brute-forcing time $O(n^3)$. Indeed, one may simply find the index i (resp j) of the minimal (resp. maximal) coordinate of t, leading to the single candidate solution $c = \frac{1}{\sqrt{2}}(e_i - e_j)$.

Problem 2: Invent and analyze algorithms faster than brute-force for decoding the spherical code $C(A^k_n)$ for $k > 1$. Precomputation that depends only on n, k, β but not on t is allowed.

References

[BB92] Christine Bachoc and Christian Batut. "Etude algorithmique de réseaux construits avec la forme trace". In: *Experimental Mathematics* 1.3 (1992), pp. 183–190.

[CS13] John Horton Conway and Neil James Alexander Sloane. *Sphere packings, lattices and groups*. Vol. 290. Springer Science & Business Media, 2013.