About geometry, closest vector and shadow simplex

M1 internship report

Arthur Rousseau
Under the direction of Daniel Dadush

1 Introduction

This report is the result of a five months internship at the Centrum Wiskunde & Informatica in Amsterdam, Netherlands. During this internship, we studied two optimization problem : the Closest Vector Problem with Pre-processing and the shadow simplex method for linear programing.

The Closest Vector Problem (CVP) consists, given a lattice and a target, in finding the vector of the lattice that is the closest to the target. This problem is NP-hard, and it is also considered hard to solve for a quantum computer, which makes it a good problem to create post-quantum cryptographic systems, even in its decisional form or for polynomial approximations. The fastest known algorithm for this problem has complexity $2^{n+o(n)}$ in time and space and was developed by Aggarwal, Dadush, Regev, and Stephens-Davidowitz in 2015 [1][2]. This algorithm was simplified in 2017 by Aggarwal and Stephens-Davidowitz [3], without changing the complexity. Both those algorithms use discrete gaussian sampling methods.
The problem that we are studying is slightly different : we are allowed, before solving the problem and being given only the lattice, to do a pre-processing with a huge computing power. To avoid the possibility of computing and storing the solution of the problem for any point in space, the result of the pre-processing has to be bounded in size, often by $O(2^n)$. Then we are given a target and have to solve CVP, using the pre-processed data. The newly defined problem is called Closest Vector Problem with Pre-processing (CVPP). To solve this problem, a classical method is to pre-process the Voronoi cell – the set of all points closer to $\mathbf{0}$ than to any other point of the lattice – and then use it to solve CVP. The Voronoi cell can be stored using $O(2^n)$ bits and a basis of $\mathcal{L}$, by storing the at most $2(2^n - 1)$ inequalities defining it. By translating the Voronoi cell with the points of the lattice, we get a tiling of $\mathbb{R}^n$. Then, a point of the lattice is a closest vector if the target is inside the Voronoi cell around this point. The goal is to move from a Voronoi cell to an adjacent one, improving the distance to the target, until we get into the good cell. The complexity of such an algorithm is proportional to the number of Voronoi cells crossed, which we are therefore trying to minimize.
The first algorithm using Voronoi cell is the Iterative Slicer [4] developed in 2009 by Sommer, Feder & Shalvi. They proved termination, but with no guarantee on the number of cells crossed. In 2010, Micciancio & Voulgaris developed the straight line algorithm [5]. It consists in drawing the straight line from $\mathbf{0}$ to the target, and then go through the Voronoi cells crossed by this line. Micciancio & Voulgaris proved a $O(2^n)$ bound on the number

of cells crossed, for a algorithm with total computing time $\tilde{O}(4^n)$. This $O(2^n)$ bound is however a worst case in the analysis, but no example are known where this bound is tight. In fact, the number of Voronoi cells crossed seems much lower for most straight lines. Dadush & Bonifas therefore developed in 2014 a randomized straight line algorithm [6]. The idea is that instead of going directly from $\mathbf{0}$ to the target, we first we move to a random point not far from $\mathbf{0}$, then we follow the straight line parallel to the one from $\mathbf{0}$ to the target and finally go back to the target. Doing so, we can avoid the potentially bad cases of the analysis of Micciancio & Voulgaris. Dadush & Bonifas found a weakly polynomial bound for the number of cells crossed, depending on a bit length bound for the target and the lattice.
During the internship, the first goal was to try to get rid of this bit length bound, to get a strongly polynomial bound on the number of cells crossed. Therefore, lots of different geometrical results will be found in this report, following our attempts.

Linear programing is a classical optimization problem which consists in maximizing an n-dimensional linear function over a set (polyhedron) defined by m linear constraints. To do so, a classical method is the simplex method, which consists in moving iteratively among the vertices, improving the linear function at each step. A simplex algorithm provides a way of moving from a vertex to an other. For a long time, the Hirsch conjecture postulated that the diameter of a polyhedron was bounded by $m - n$. This conjecture was disproved in 2012 by Santos [7]. The polynomial Hirsch conjecture postulates that there is a polynomial bound in n, m for the diameter of a polyhedron. This problem is still open, the best bound today being quasi-polynomial. Polynomial bounds have been proven for special cases of polytopes (bounded polyhedra) like 0/1 polytopes [8] or transportation polytopes [9].
However, for the simplex method, it is not enough to bound the diameter of a polyhedron, because an efficient simplex algorithm should be provided. The simplex algorithm we are going to study is the shadow simplex algorithm. It consists in moving among the cones generated by the vertices instead of the vertices themselves. As most simplex algorithm, some bad-conditioned setups give way to exponential-length path [10].
To avoid such cases, some hypothesis can be made on the polyhedron. For example, if all subdeterminants of the constraint matrix are bounded by Δ, Brunsch & Röglin [11] built a path between any two vertices of length $O(m\Delta^4 n^4)$. An other property we can use is the δ-distance property, which measures, for a family of linearly independent constraints, the distance between a constraint and the hyperplane generated by the other. Brunsch & Röglin gave a $O(mn^2/\delta^2)$ bound using this parameter. In 2013, Eisenbrand & Vempala proved a polynomial bound in $n, 1/\delta$, getting rid of the dependency in m. This bound was improved by Dadush & Hähnle in 2014, who proved an expected $O\left(\frac{n^3}{\delta}\ln\left(\frac{n}{\delta}\right)\right)$ bound on the number of shadow simplex pivots. However, the algorithm of Dadush & Hähnle requires knowledge of δ. We will be working on the method they used to get rid of this knowledge.

2 Notation, definitions and classical results

Denote by $\mathbb{R}_+$ the set of nonnegative real numbers. Denote by $(\mathbf{e}_i)_{1\leqslant i\leqslant n}$ the canonical basis of $\mathbb{R}^n$. For $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, let $\langle \mathbf{x}, \mathbf{y}\rangle = \sum_{i=1}^{n} x_i y_i$ denote the inner product in $\mathbb{R}^n$. Let $\|\mathbf{x}\| = \|\mathbf{x}\|_2 = \langle \mathbf{x}, \mathbf{x}\rangle$, $\|\mathbf{x}\|_1 = \sum_{i=1}^{n} |x_i|$ and $\|\mathbf{x}\|_\infty = \max_{1\leqslant i\leqslant n} |x_i|$ denote respectively the euclidean, L^1 and L^∞ norms. Let $\mathcal{B}_2^n = \{\mathbf{x} \in \mathbb{R}^n : \|\mathbf{x}\| \leqslant 1\}$ and $\mathbb{S}^{n-1} = \partial\mathcal{B}_2^n$ denote the euclidean unit ball and sphere in $\mathbb{R}^n$. We denote the linear span of a set $A \in \mathbb{R}^n$ by $\mathrm{Span}(A)$. We write $[\mathbf{x}, \mathbf{y}] = \{\lambda\mathbf{x} + (1-\lambda)\mathbf{y} : \lambda \in [0, 1]\}$ the line segment between $\mathbf{x}$ and $\mathbf{y}$. We denote by $\mathrm{Vol}(A)$ the Lebesgue measure of a set $A \subset \mathbb{R}^n$. For a set $F \subset \mathbb{R}^n$, we denote by $\mathrm{conv}(F)$ its convex hull. For $H \subset \mathbb{R}^n$, define $H^\perp$ the set of all vectors orthogonal to all elements of H. For simplicity, for a family $\mathbf{a}_1, \cdots, \mathbf{a}_k$ of vectors, we write $\{\mathbf{a}_1, \cdots, \mathbf{a}_k\}^\perp = (\mathbf{a}_1, \cdots, \mathbf{a}_k)^\perp$.
Let X be a random variable distributed on $\mathbb{R}^n$. We say that X follows an exponential distribution of parameter

$\lambda > 0$ on $\mathbb{R}^n$ if X has probability density function proportional to $\mathbf{x} \mapsto e^{-\lambda\|\mathbf{x}\|}$, and we write $X \sim \mathrm{Exp}_{\mathbb{R}^n}(\lambda)$.

Definition 1 (Lattice)**.** A *lattice* $\mathcal{L}$ is a discrete subgroup of $\mathbb{R}^n$. $\mathcal{L}$ is said to be *d-dimensional* if $\dim(\mathrm{Span}(\mathcal{L})) = d$. $\mathcal{B} = (\mathbf{b}_1, \cdots, \mathbf{b}_d) \in \mathbb{R}^{n\times d}$ is said to be a *basis* of a d-dimensional lattice $\mathcal{L}$ if $\mathcal{L} = \mathcal{B}\mathbb{Z}^n$.
Denote the minimum distance of $\mathcal{L}$ as $\lambda_1(\mathcal{L}) = \inf_{\mathbf{x}\in\mathcal{L}\setminus\{\mathbf{0}\}} \|\mathbf{x}\| = \inf_{\mathbf{x}\neq\mathbf{y}\in\mathcal{L}} \|\mathbf{x}-\mathbf{y}\|$. Denote the distance of a point $\mathbf{t} \in \mathbb{R}^n$ to the lattice by $\mathrm{d}(\mathcal{L}, \mathbf{t}) = \inf_{\mathbf{x}\in\mathcal{L}} \|\mathbf{x}-\mathbf{t}\|$ and the covering radius of $\mathcal{L}$ as $\mu(\mathcal{L}) = \sup_{\mathbf{t}\in\mathbb{R}^n} \mathrm{d}(\mathcal{L}, \mathbf{t})$.

Proposition 1. Let $\mathcal{L}$ be a lattice, then there exist $\mathbf{x} \in \mathcal{L}, \mathbf{t} \in \mathbb{R}^n$ such that $\lambda_1(\mathcal{L}) = \|\mathbf{x}\|$, $\mu(\mathcal{L}) = \mathrm{d}(\mathcal{L}, \mathbf{t})$.

Proposition 2. For two bases $\mathcal{B}, \mathcal{B}'$ of $\mathcal{L}$, define $|\det(\mathcal{B})| = \sqrt{\det(\mathcal{B}^\perp\mathcal{B})}$. Then $|\det\mathcal{B}| = |\det(\mathcal{B}')|$. We note $\det(\mathcal{L})$ the common absolute value of all determinant of basis of $\mathcal{L}$.

Theorem 1 (Minkowski's first theorem)**.** *Let $\mathcal{L}$ be an n-dimensional lattice. Then $\lambda_1(\mathcal{L}) \leqslant \sqrt{n}(\det(\mathcal{L}))^{1/n}$.*

Definition 2 (Closest vector problem)**.** The closest vector problem (CVP) consists, given an n-dimensional lattice $\mathcal{L}$ and a target $\mathbf{t} \in \mathbb{R}^n$, in finding a point $\mathbf{v}^* \in \mathcal{L}$ so that

$$\|\mathbf{t} - \mathbf{v}^*\| = \min_{\mathbf{v}\in\mathcal{L}} \|\mathbf{t} - \mathbf{v}\|.$$

Definition 3 (Voronoi cell)**.** Let $\mathcal{L}$ be a lattice, we define the *Voronoi cell* of $\mathcal{L}$ as

$$\mathcal{V}(\mathcal{L}) = \{\mathbf{x} \in \mathbb{R}^n : \forall \mathbf{y} \in \mathcal{L}, \|\mathbf{x}\| \leqslant \|\mathbf{x}-\mathbf{y}\|\} = \{\mathbf{x} \in \mathbb{R}^n : \forall \mathbf{y} \in \mathcal{L}, \langle\mathbf{x}, \mathbf{y}\rangle \leqslant \langle\mathbf{y}, \mathbf{y}\rangle\}.$$

$\mathcal{V}(\mathcal{L})$ is the set of points that are closer to $\mathbf{0}$ than to any other point of the lattice.
For $\mathbf{y} \in \mathcal{L}$, let $H_{\mathbf{y}} = \{\mathbf{x} \in \mathbb{R}^n : \|\mathbf{x}\| \leqslant \|\mathbf{x}-\mathbf{y}\|\}$. Then $\mathcal{V}(\mathcal{L}) = \bigcap_{\mathbf{y}\in\mathcal{L}} H_{\mathbf{y}}$. We define $VR \subset \mathcal{L}$ the set of *Voronoi relevant vectors* of the lattice as the smallest set of points of the lattice such that $\mathcal{V}(\mathcal{L}) = \bigcap_{\mathbf{y}\in VR} H_{\mathbf{y}}$.
Two vectors of $\mathcal{L}$ are said to be *adjacent* if their difference is in VR.

For proofs of basic lattice results and more, see [12].

Proposition 3. Let $\mathcal{L}$ be a lattice and $\mathbf{x}$ be a Voronoi relevant vector. Then $\|\mathbf{x}\| \leqslant 2\mu(\mathcal{L})$.

Proposition 4. Let $\mathcal{L}$ be a lattice. Then $\mathbf{v} \in VR$ if and only if for all $\mathbf{w} \in \mathcal{L}\setminus\{\mathbf{0}, -\mathbf{v}\}$, $\|\mathbf{v} + 2\mathbf{w}\| > \|\mathbf{v}\|$.

Definition 4 (Voronoi norm)**.** Let $\mathcal{L}$ be a lattice and $\mathbf{x} \in \mathbb{R}^n$. We define the *Voronoi norm* of $\mathbf{x}$ by :

$$\|\mathbf{x}\|_{\mathcal{V}(\mathcal{L})} = \inf\{s \geqslant 0 : \mathbf{x} \in s\mathcal{V}(\mathcal{L})\}.$$

It is a norm.

Proposition 5. Let $\mathcal{L}$ be an n-lattice and $\mathbf{v}_1, \cdots, \mathbf{v}_k \in \mathcal{L}$. Denote by π the orthogonal projector onto $(\mathbf{v}_1, \cdots, \mathbf{v}_k)^\perp$. Then $\pi(\mathcal{L})$ is a lattice, and its dimension is $n - \dim(\mathrm{Span}(\mathbf{v}_1, \cdots, \mathbf{v}_k))$.

Definition 5 (Cosets)**.** For $\mathbf{u}, \mathbf{v} \in \mathcal{L}$, let us define

$$\mathbf{u} \equiv \mathbf{v}(\bmod 2\mathcal{L}) \text{ is and only if } \mathbf{u} - \mathbf{v} \in 2\mathcal{L}.$$

This is clearly an equivalence relation. The equivalence classes are called the *cosets* of $\mathcal{L}$. By taking a basis $(\mathbf{v}_1, \cdots, \mathbf{v}_n)$ of $\mathcal{L}$, every coset is represented by a unique $\sum_{i=1}^{n} \varepsilon_i\mathbf{v}_i$ for some $\varepsilon_1, \cdots, \varepsilon_n \in \{0, 1\}$, which proves that there are exactly 2^n cosets.

Definition 6 (Cone)**.** A *cone* is a subset $C \subset \mathbb{R}^n$ so that $\mathbf{0} \in C$ and $\forall \mathbf{x}, \mathbf{y} \in C, \lambda \in \mathbb{R}_+$, $\mathbf{x} + \mathbf{y}, \lambda\mathbf{x} \in C$.
For $\mathbf{a}_1, \cdots, \mathbf{a}_k \in \mathbb{R}^n$, define $\mathrm{cone}(\mathbf{a}_1, \cdots, \mathbf{a}_k) = \left\{\sum_{i=1}^{k} \lambda_i\mathbf{a}_i : \lambda_1, \cdots, \lambda_k \in \mathbb{R}_+\right\}$ the cone they generate.
A cone is said *polyhedral* if it is finitely generated, and *simplicial* if the generators are linearly independent.

Definition 7 (τ-wideness & δ-distance)**.** We say that :

- a cone C is τ-*wide* if there exists a unit vector $\mathbf{x} \in C$ such that $\mathbf{x} + \tau\mathcal{B}_2^n \subset C$, which means that C contains a ball of radius τ centered on a unit vector.
- a set of linearly independent vectors $\mathbf{a}_1, \cdots, \mathbf{a}_k$ satisfies the δ-*distance property* if for every $i \in [\![1, k]\!]$, $\mathbf{a}_i$ is at distance at least $\delta\|\mathbf{a}_i\|$ of $\mathrm{Span}(\{\mathbf{a}_j : j \in [\![1, k]\!] \backslash \{i\}\})$. More generally, a set of vectors satisfy the δ-distance property if every subset of independent vector does.
- a simplicial cone $\mathrm{cone}(\mathbf{a}_1, \cdots, \mathbf{a}_k)$ satisfies the δ-*distance property* if the set of its generators satisfies it.

Definition 8 (Polyhedron & normal cones)**.** A *polyhedron* is a subset $P = \{\mathbf{x} \in \mathbb{R}^n A\mathbf{x} \leqslant \mathbf{b}\}$ of $\mathbb{R}^n$ for some $A \in \mathbb{R}^{m \times n}$ and $\mathbf{b} \in \mathbb{R}^m$. The rows of A are called the *constraints* of the polyhedron. A polyhedron is *pointed* if A has full column rank, in what case P has *vertices* (a point of $\mathbb{R}^n$ where n linearly independent constraints are tight). For such a vertex $\mathbf{v}$, the *normal cone* $N_\mathbf{v}$ of P at $\mathbf{v}$ is the cone generated by the tight constraints at $\mathbf{v}$. A polyhedron is *simple* if all its normal cones are simplicial, is τ-*wide* if all its normal cones are τ-wide and satisfies the *local* δ-*distance property* if all its normal cones satisfy the δ-distance property. A polyhedron satisfies the *global* δ-*distance property* if its constraints satisfy the δ-distance property. A *polytope* is a bounded polyhedron. A d-dimensional face of a polyhedron is a subset of the polyhedron where the tight constraints are $n - d$-dimensional. A vertex, an edge, a ridge and a facet are respectively 0-dimensional, 1-dimensional, $(n-2)$-dimensional and $(n-1)$-dimensional faces.

For the proofs of the three following lemmas, see [13], lemmas 5, 16 and 19.

Lemma 1. Let $C = \mathrm{cone}(\mathbf{a}_1, \cdots, \mathbf{a}_n)$ be a simplicial cone. If C satisfies the δ-distance property for some $\delta > 0$, then C is $\dfrac{\delta}{n}$-wide. Furthermore, for $\mathbf{c} = \dfrac{1}{n}\displaystyle\sum_{i=1}^{n} \frac{\mathbf{a}_i}{\|\mathbf{a}_i\|}$, $\mathbf{c} + \dfrac{\delta}{n}\mathcal{B}_n^2 \subset C$.

Lemma 2 (δ-distance lower bound)**.** Let $\mathbf{a}_1, \cdots, \mathbf{a}_m \in \mathbb{S}^{n-1}$. The following are equivalent :

1. $\mathbf{a}_1, \cdots, \mathbf{a}_m$ satisfy the δ-distance property.
2. For every subset $(\mathbf{a}_i)_{i \in I}$ of independent vectors, for every $(\lambda_i)_{i \in I} \in \mathbb{R}^I$, $\left\| \displaystyle\sum_{i \in I} \lambda_i \mathbf{a}_i \right\| \geqslant \delta \max_{i \in I} |\lambda_i|$.

Lemma 3. Let $\mathbf{a}_1, \cdots, \mathbf{a}_k$ be independent vectors satisfying the δ-distance property and π be the orthogonal projector onto $\mathbf{a}_k^\perp$. Then $\pi(\mathbf{a}_1), \cdots, \pi(\mathbf{a}_{k-1})$ satisfy the δ-distance property.

Definition 9 (Linear program)**.** Let $n, m \in \mathbb{N}^*$. A linear program of size (n, m) is an optimization problem defined by a pointed polyhedron $P = \{\mathbf{x} \in \mathbb{R}^n A\mathbf{x} \leqslant \mathbf{b}\}$ for some $A \in \mathbb{R}^{m \times n}$ and $\mathbf{b} \in \mathbb{R}^m$ and an optimization direction $\mathbf{c} \in \mathbb{R}^n$. The linear program consists in finding

$$\max_{\mathbf{x} \in P} \mathbf{c}^\perp \mathbf{x}$$

and the value of $\mathbf{x}$ for which this value is attained.

3 Lattices and Voronoi cells

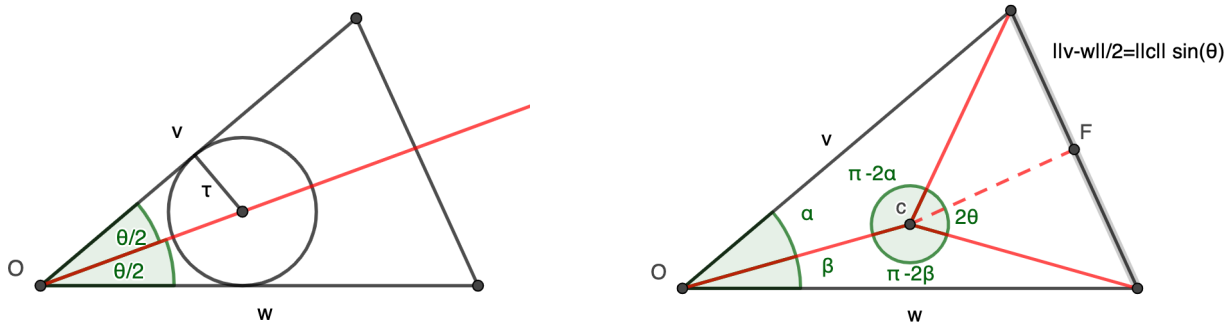
3.1 Wideness of the normal cones of the Voronoi cell

If we can lower-bound the wideness of the normal cones of the Voronoi cell, then using the shadow simplex algorithm (see Section 5) we can get an upper bound on the number of cells crossed that is polynomial in the dimension and the wideness of the cones. This is the purpose of the two following theorems.

Theorem 2. *Let $\mathcal{L}$ be a 2-dimensional lattice. Then the normal cones of the Voronoi cell are $\dfrac{\lambda_1(\mathcal{L})}{2 \cdot 2\mu(\mathcal{L})}$-wide.*

Proof. In 2 dimensions, the normal cones of the Voronoi cell are generated by pairs of adjacent vectors in VR. Let $\mathbf{v}, \mathbf{w} \in VR$ be adjacent vectors. First we prove that the triangle with vertices $\mathbf{0}$,$\mathbf{v}$ and $\mathbf{w}$ has sharp angles. This is the case if and only if the inner products $\langle \mathbf{v}, \mathbf{w} \rangle$, $\langle -\mathbf{w}, \mathbf{v} - \mathbf{w} \rangle$ and $\langle -\mathbf{v}, \mathbf{w} - \mathbf{v} \rangle$ are all nonnegative.

- $\mathbf{v}, \mathbf{w}$ are adjacent so $\mathbf{v} - \mathbf{w} \in VR$ and $\|(\mathbf{v} - \mathbf{w}) + 2\mathbf{w}\|^2 \geqslant \|\mathbf{v} - \mathbf{w}\|^2$. Therefore $\langle \mathbf{v}, \mathbf{w} \rangle \geqslant 0$.
- $\|\mathbf{w} - 2\mathbf{v}\|^2 \geqslant \|\mathbf{w}\|^2$ so $\langle \mathbf{v}, \mathbf{w} \rangle \leqslant \|\mathbf{v}\|^2$ and $\langle -\mathbf{v}, \mathbf{w} - \mathbf{v} \rangle \geqslant 0$. Similarly $\langle -\mathbf{w}, \mathbf{v} - \mathbf{w} \rangle \geqslant 0$.



Let now $0 < \theta \leqslant \dfrac{\pi}{2}$ be the non-oriented angle between $\mathbf{v}$ and $\mathbf{w}$. Consider a unit vector on the bisector of θ. Then this vector is at distance $\tau = \sin\left(\dfrac{\theta}{2}\right)$ of the borders of the cones, and therefore the cone is τ-wide.
Now consider the circumcenter $\mathbf{c}$ of the triangle, we have $\|\mathbf{c}\| \leqslant \mu(\mathcal{L})$. As the triangle has sharp angles, $\mathbf{c}$ lies inside it. Let α, β be the non-oriented angles between $\mathbf{v}$ and $\mathbf{c}$, $\mathbf{w}$ and $\mathbf{c}$ respectively. We have $\alpha + \beta = \theta$. Using the above picture and trigonometry, we find that

$$\frac{\lambda_1(\mathcal{L})}{2\mu(\mathcal{L})} \leqslant \frac{\|\mathbf{v} - \mathbf{w}\|}{2\|\mathbf{c}\|} = \sin(\theta) \leqslant 2\tau.$$

□

Remark. Consider the lattice in $\mathbb{R}^2$ generated by $\mathbf{v} = (0, 1)$ and $\mathbf{w} = \left(K, \dfrac{1}{2}\right)$ and the cone generated by $\mathbf{w}$ and $\mathbf{w} - \mathbf{v}$. For K big enough, all precedent inequalities are equalities except for the last one. But this last inequality becomes tighter as $K \to +\infty$, and is asymptotically an equality. Therefore the above bound on the wideness of the normal cones in two dimensions is tight.

Theorem 3. *Let $\mathcal{L}$ be an n-dimensional lattice and $\mathcal{B} \subset VR$ be a basis of $\mathcal{L}$.*
Then $\mathcal{B}$ satisfies the $\left(\dfrac{\lambda_1(\mathcal{L})}{2\sqrt{n}\mu(\mathcal{L})}\right)^n$-distance property.

Proof. Let $\mathcal{B} = (\mathbf{b}_1, \cdots, \mathbf{b}_n)$. Let $\tilde{\mathcal{B}} = (\tilde{\mathbf{b}_1}, \cdots, \tilde{\mathbf{b}_n})$ be the Gram-Schmidt orthogonalization of $\mathcal{B}$. By Minkowski's first theorem (Theorem 1), we have

$$\lambda_1(\mathcal{L}) \leqslant \sqrt{n}(\det(\mathcal{B}))^{1/n} = \sqrt{n}(\det(\tilde{\mathcal{B}}))^{1/n} = \sqrt{n}\left(\prod_{i=1}^{n} \|\tilde{\mathbf{b}_i}\|\right)^{1/n}.$$

As $\|\tilde{\mathbf{b}_i}\| \leqslant \|\mathbf{b}_i\| \leqslant 2\mu(\mathcal{L})$, we have

$$\left(\frac{\lambda_1(\mathcal{L})}{\sqrt{n}}\right)^n \leqslant \frac{\|\tilde{\mathbf{b}_i}\|}{\|\mathbf{b}_i\|}(2\mu(\mathcal{L}))^n.$$

But $\|\tilde{\mathbf{b}_n}\|$ is the distance between $\mathbf{b}_n$ and $\mathrm{Span}(\tilde{\mathbf{b}_1}, \cdots, \tilde{\mathbf{b}_{n-1}}) = \mathrm{Span}(\mathbf{b}_1, \cdots, \mathbf{b}_{n-1})$ so $\mathbf{b}_n$ is at distance at least $\left(\dfrac{\lambda_1(\mathcal{L})}{2\sqrt{n}\mu(\mathcal{L})}\right)^n \|\mathbf{b}_n\|$ of $\mathrm{Span}(\mathbf{b}_1, \cdots, \mathbf{b}_{n-1})$. As we can reorder $\mathcal{B}$ as we want, this prove the theorem. □

Remark.
- We also have the $\frac{\det \mathcal{L}}{(2\sqrt{n}\mu(\mathcal{L}))^n}$-distance property.
- This bound is exponential in the dimension, so we can not use it to get a polynomial bound on the number of cells crossed. However, the bound is not tight in two dimensions, and the inequalities in the proof are coarse, so a better bound certainly exists in general.

3.2 Orthogonal projection of a lattice on a subspace

An other way of seeing the problem is simply to find a better analysis for the random straight line algorithm. To do that, an induction on the dimension seems like a good idea. However, lattices do not necessarily react well to projecting. This section tries to understand how "nice" would a lattice projection be.

Lemma 4. Let $\mathcal{L}$ be a 2-dimensional lattice. Then any vector $\mathbf{w} \in VR$ can be extended to a basis of the lattice $(\mathbf{u}, \mathbf{w}) \in VR^2$.

Proof. We know that VR is a symmetric set that generates the lattice with at most 6 elements. Therefore $|VR| \in \{4, 6\}$. If $|VR| = 4$, then $VR = \{\pm\mathbf{u}, \pm\mathbf{v}\}$ and the lattice is a scaling of $\mathbb{Z}^2$ and the result is trivial. Else, $VR = \{\pm u, \pm v, \pm(u-v)\}$ for some $u, v \in \mathcal{L}$. Then the result is also clearly true, as any two linearly independent vectors in VR generate VR, and therefore $\mathcal{L}$. □

Proposition 6. Let $\mathcal{L}$ be a lattice and $\mathbf{w} \in VR$. Let π be the orthogonal projector onto $\mathbf{w}^\perp$. Then for any $\mathbf{x} \in \mathbb{R}^n$, $\|\pi(\mathbf{x})\|_{\mathcal{V}(\pi(\mathcal{L}))} \leqslant 2\|\mathbf{x}\|_{\mathcal{V}(\mathcal{L})}$. This means that the projection of the Voronoi cell is included in twice the Voronoi cell of the projected lattice.

Proof.

$$\begin{aligned}
\forall \mathbf{x} \in \mathbb{R}^n,\ \|\pi(\mathbf{x})\|_{\mathcal{V}(\pi(\mathcal{L}))} \leqslant 2\|\mathbf{x}\|_{\mathcal{V}(\mathcal{L})} &\Leftrightarrow \forall \mathbf{x} \in \mathbb{R}^n, \forall s > 0,\ \|2\mathbf{x}\|_{\mathcal{V}(\mathcal{L})} \leqslant s \rightarrow \|\pi(\mathbf{x})\|_{\mathcal{V}(\pi(\mathcal{L}))} \leqslant s \\
&\Leftrightarrow \forall \mathbf{x} \in \mathbb{R}^n,\ \|\mathbf{x}\|_{\mathcal{V}(\mathcal{L})} \leqslant 1 \rightarrow \left\|\pi\left(\frac{\mathbf{x}}{2}\right)\right\|_{\mathcal{V}(\pi(\mathcal{L}))} \leqslant 1 \\
&\Leftrightarrow \forall \mathbf{x} \in \mathcal{V}(\mathcal{L}),\ \pi\left(\frac{\mathbf{x}}{2}\right) \in \mathcal{V}(\pi(\mathcal{L})) \\
&\Leftrightarrow \forall \mathbf{x} \in \mathcal{V}(\mathcal{L}), \forall \mathbf{v} \in \mathcal{L},\ \left\langle \frac{\pi(\mathbf{x})}{2}, \pi(\mathbf{v}) \right\rangle \leqslant \frac{\|\pi(\mathbf{v})\|^2}{2} \\
&\Leftrightarrow \forall \mathbf{x} \in \mathcal{V}(\mathcal{L}), \forall \mathbf{v} \in \mathcal{L},\ \left\langle \mathbf{x} - \frac{\langle \mathbf{x}, \mathbf{w}\rangle}{\|\mathbf{w}\|^2}\mathbf{w}, \mathbf{v} - \frac{\langle \mathbf{v}, \mathbf{w}\rangle}{\|\mathbf{w}\|^2}\mathbf{w} \right\rangle \leqslant \left\|\mathbf{v} - \frac{\langle \mathbf{v}, \mathbf{w}\rangle}{\|\mathbf{w}\|^2}\mathbf{w}\right\|^2 \\
&\Leftrightarrow \forall \mathbf{x} \in \mathcal{V}(\mathcal{L}), \forall \mathbf{v} \in \mathcal{L},\ \|\mathbf{w}\|^2\langle \mathbf{x}, \mathbf{v}\rangle - \langle \mathbf{x}, \mathbf{w}\rangle\langle \mathbf{v}, \mathbf{w}\rangle \leqslant \|\mathbf{v}\|^2\|\mathbf{w}\|^2 - \langle \mathbf{v}, \mathbf{w}\rangle^2
\end{aligned}$$

Let us name (I) this last inequality. Let $\mathbf{x} \in \mathcal{V}(\mathcal{L}), \mathbf{v} \in \mathcal{L}$. Without loss of generality, we can assume $\mathbf{x} \in \mathrm{Span}(\mathbf{v}, \mathbf{w})$ (by projecting onto this subspace). We can also only consider the lattice generated by $\mathbf{v}, \mathbf{w}$, as its Voronoi cell contains the projection of $\mathcal{V}(\mathcal{L})$. This reduces the problem to a 2-dimensional one.
If $\mathbf{v}, \mathbf{w}$ are colinear, (I) is clear. Else, we have $\mathbf{x} = \alpha\mathbf{v} + \beta\mathbf{w}$ for some $\alpha, \beta \in \mathbb{R}$. We have :

$$\begin{aligned}
(I) &\Leftrightarrow \alpha\|\mathbf{w}\|^2\|\mathbf{v}\|^2 + \beta\|\mathbf{w}\|^2\langle \mathbf{v}, \mathbf{w}\rangle - \alpha\langle \mathbf{v}, \mathbf{w}\rangle^2 - \beta\|\mathbf{w}\|^2\langle \mathbf{v}, \mathbf{w}\rangle \leqslant \|\mathbf{v}\|^2\|\mathbf{w}\|^2 - \langle \mathbf{v}, \mathbf{w}\rangle^2 \\
&\Leftrightarrow (\|\mathbf{v}\|^2\|\mathbf{w}\|^2 - \langle \mathbf{v}, \mathbf{w}\rangle^2)(1-\alpha) \geqslant 0 \\
&\Leftrightarrow \alpha \leqslant 1 \text{ by Cauchy-Schwarz inequality.}
\end{aligned}$$

It remains to show that $\mathcal{V}(\mathcal{L}) \subset]-\infty, 1]\mathbf{v} + \mathbb{R}\mathbf{w}$. Assume first that $\mathbf{v} \in VR$. We will show that $\mathcal{V}(\mathcal{L}) \subset [-1, 1]\mathbf{v} + [-1, 1]\mathbf{w}$. We know that $\mathcal{V}(\mathcal{L})$ is the convex hull of its vertices. But in 2 dimensions, any vertex of $\mathcal{V}(\mathcal{L})$ is the circumcenter of a triangle with sharp angles generated by two adjacent vectors of VR, therefore any vertex of $\mathcal{V}(\mathcal{L})$ belongs to $\mathrm{conv}(VR)$. Finally $VR \subset [-1, 1]\mathbf{v} + [-1, 1]\mathbf{w}$ which is convex. Therefore

$$\mathcal{V}(\mathcal{L}) \subset \mathrm{conv}(VR) \subset [-1, 1]\mathbf{v} + [-1, 1]\mathbf{w}.$$

Now assume $\mathbf{v} \notin VR$. Then, extend $\mathbf{w}$ to a basis ($\mathbf{w}$,$\mathbf{u}$) of the lattice with $\mathbf{u} \in VR$ (this is possible by lemma 4). Then we have $\mathbf{v} = p\mathbf{u} + q\mathbf{w}$ for some $p, q \in \mathbb{Z}, p \neq 0$ and $\mathbf{x} = \alpha'\mathbf{u} + \beta'\mathbf{w}$ for some $\alpha', \beta' \in [-1, 1]$. Then

$$\mathbf{x} = \frac{\alpha'}{p}\mathbf{v} + \beta'\frac{q}{p}\mathbf{w} \in]-\infty, 1]\mathbf{v} + \mathbb{R}\mathbf{w}.$$

□

Proposition 7. Let $\mathbf{v}_1, \cdots, \mathbf{v}_m \in \mathbb{R}^n$ be a family of linearly independent vectors. Let $\mathcal{L}$ be the lattice they generate. Let $k < m$ and let $\mathcal{L}'$ be the lattice generated by $\mathbf{v}_1, \cdots, \mathbf{v}_k$. Let π be the orthogonal projector onto $\text{Span}(\mathbf{v}_1, \cdots, \mathbf{v}_k)$. Then

$$\mathcal{V}(\mathcal{L}) \cap \text{Span}(\mathbf{v}_1, \cdots, \mathbf{v}_k) \subset \pi(\mathcal{V}(\mathcal{L})) \subset \mathcal{V}(\mathcal{L}').$$

and all these inclusions are strict in general.

Proof. Let $\mathbf{x} \in \mathcal{V}(\mathcal{L}) \cap \text{Span}(\mathbf{v}_1, \cdots, \mathbf{v}_k)$. Then $\pi(\mathbf{x}) = \mathbf{x}$ and $\mathbf{x} \in \pi(\mathcal{V}(\mathcal{L}))$.
Let $\mathbf{x} = \pi(\mathbf{y})$, $\mathbf{y} \in \mathcal{V}(\mathcal{L})$. Then $\mathbf{x} \in \text{Span}(\mathcal{L}')$ and for all $\mathbf{v} \in \mathcal{L}'$,

$$\langle \mathbf{x}, \mathbf{v} \rangle = \langle \mathbf{y}, \mathbf{v} \rangle \leqslant \frac{\|\mathbf{v}\|^2}{2}$$

so $\mathbf{x} \in \mathcal{V}(\mathcal{L}')$.
For the strictness, see `Voronoi_3D_5.ggb` with $\mathbf{v}_1 = \vec{SH}$, $\mathbf{v}_2 = \vec{SX}$ for the first inclusion and $\mathbf{v}_1 = \vec{SI}$, $\mathbf{v}_2 = \vec{SM}$ for the second inclusion. □

4 Delauney polytopes and sharp polytopes

When following the straight line, the problems arise when the target is almost equally close to a lot of points. Here, we prove that if a point in space has exactly 2^n neighbors, then the lattice is orthogonal.

Definition 10 (Delauney polytope)**.** Let K be a polytope in $\mathbb{R}^n$ with vertices $\mathbf{v}_1, \cdots, \mathbf{v}_p \in \mathbb{R}^n$. We say that K is a *Delauney polytope* if there exists $\mathbf{c} \in \mathbb{R}^n$ so that :

- $\forall i, j \in [\![1, p]\!]$, $\|\mathbf{v}_i - \mathbf{c}\| = \|\mathbf{v}_j - \mathbf{c}\|$ ($\mathbf{c}$ is the center of a sphere containing all the vertices).
- $\forall i, j, k \in [\![1, p]\!]$, $\langle \mathbf{v}_i - \mathbf{v}_j, \mathbf{v}_i - \mathbf{v}_k \rangle \geqslant 0$ (the angle $(\mathbf{v}_j, \mathbf{v}_i, \mathbf{v}_k)$ is sharp).

The goal is to show the following theorem :

Theorem 4. *Let K be a Delauney polytope in $\mathbb{R}^n$ with p vertices. Then $p \leqslant 2^n$ with equality if and only if K is a dilated n-dimensional hypercube.*

Lemma 5. Let S be a convex n-dimensional set in $\mathbb{R}^n$. Then $\text{Vol}_n(S) > 0$.

Proof. By translating, we can assume $\mathbf{0} \in S$. Let $\mathbf{v}_1, \cdots, \mathbf{v}_n \in S$ so that $\det(\mathbf{v}_1, \cdots, \mathbf{v}_n) > 0$. Let $\lambda = \frac{1}{n}$, then

$$\lambda([0, 1]\mathbf{v}_1 + \cdots + [0, 1]\mathbf{v}_n) \subset S \text{ as } S \text{ is convex and } \mathbf{0} \in S.$$

Therefore

$$0 < \lambda^n \det(\mathbf{v}_1, \cdots, \mathbf{v}_n) \leqslant \text{Vol}_n(S).$$

□

Lemma 6. Let A, B be convex, closed polytope in $\mathbb{R}^n$ so that $A \subset B$ and $\text{Vol}_n(A + B) = \text{Vol}_n(2B) > 0$. Then $A = B$.

Proof. First, let us show that for any $\mathbf{x} \in 2B$, for any $\varepsilon > 0$,

$$\mathrm{Vol}_n((2B) \cap (\mathbf{x} + \varepsilon \mathcal{B}_2^n(\mathbf{0}, 1))) > 0.$$

We can assume with a translation that $\mathbf{x} = \mathbf{0}$, let $S = B \cap (\varepsilon \mathcal{B}_2^n(\mathbf{0}, 1))$. S is the intersection of two convex set so it is convex. By contradiction, assume that S is not n-dimensional. Then $S \subset H$ for some hyperplane H of $\mathbb{R}^n$. As $\mathrm{Vol}_n(2B) > 0$, $2B \not\subset H$ so let $\mathbf{y} \in 2B \backslash H$. We have

$$\min\left(1, \frac{\varepsilon}{\|\mathbf{y}\|}\right) \mathbf{y} \in (2B \backslash H) \cap (\varepsilon \mathcal{B}_2^n(\mathbf{0}, 1)) = S \backslash H$$

which contradicts $S \subset H$. By lemma 5, $\mathrm{Vol}_n(S) > 0$.
Now let us show that $A + B = 2B$. By contradiction, consider $\mathbf{x} \in 2B \backslash (A + B)$. A, B are closed and bounded in $\mathbb{R}^n$ so they are compact, so $A + B$ is compact and therefore closed. This means that there exists some $\varepsilon > 0$ so that $\mathbf{x} + \varepsilon \mathcal{B}_2^n(\mathbf{0}, 1) \subset \mathbb{R}^n \backslash (A + B)$. Let $S = (2B) \cap (\mathbf{x} + \varepsilon \mathcal{B}_2^n(\mathbf{0}, 1))$. Then $(A + B) \subset (2B) \backslash S$ so

$$\mathrm{Vol}_n(A + B) \leqslant \mathrm{Vol}_n(2B) - \mathrm{Vol}_n(S) < \mathrm{Vol}_n(2B)$$

which contradicts $\mathrm{Vol}_n(A + B) = \mathrm{Vol}_n(2B)$.
Finally, let us show that $B \subset A$ which will conclude. By contradiction, consider a vertex $\mathbf{v}$ of B so that $\mathbf{v} \notin A$. Let $\mathbf{d} \in \mathbb{R}^n$ so that

$$\{\mathbf{v}\} = \underset{\mathbf{x} \in B}{\mathrm{argmin}} \langle \mathbf{d}, \mathbf{x} \rangle \qquad (\mathbf{d} \text{ is a direction that } \mathbf{v} \text{ optimizes in } B).$$

Then, $\forall \mathbf{y} \in A$, $\langle \mathbf{d}, \mathbf{y} \rangle < \langle \mathbf{d}, \mathbf{v} \rangle$. Now let $\mathbf{a} \in A$, $\mathbf{b} \in B$ so that $2\mathbf{v} = \mathbf{a} + \mathbf{b}$. Then

$$2\langle \mathbf{d}, \mathbf{v} \rangle = \langle \mathbf{d}, \mathbf{a} \rangle + \langle \mathbf{d}, \mathbf{b} \rangle < 2\langle \mathbf{d}, \mathbf{v} \rangle$$

which is a contradiction. □

Lemma 7. Let K be a Delauney polytope in $\mathbb{R}^n$ with p vertices $\mathbf{v}_1, \cdots, \mathbf{v}_p$. Then $p \leqslant 2^n$.

Proof. First, let us show that for $i \neq j \in [\![1, p]\!]$, $(\mathbf{v}_i + \mathring{K}) \cap (\mathbf{v}_j + \mathring{K}) = \varnothing$. By translating, we can assume $\mathbf{v}_j = \mathbf{0}$. In particular, for all $i, k \in [\![1, p]\!]$,

$$\langle \mathbf{v}_i - \mathbf{v}_k, \mathbf{v}_i - \mathbf{v}_j \rangle \geqslant 0 \text{ so } \langle \mathbf{v}_i, \mathbf{v}_k \rangle \leqslant \|\mathbf{v}_i\|^2$$

$$\langle \mathbf{v}_j - \mathbf{v}_i, \mathbf{v}_j - \mathbf{v}_k \rangle \geqslant 0 \text{ so } \langle \mathbf{v}_i, \mathbf{v}_k \rangle \geqslant 0.$$

These inequalities are true whenever $\mathbf{0}$ is a vertex of K and will be used again is this context in other proofs.
Let $\mathbf{x} = \sum_{k=1}^{p} \lambda_k \mathbf{v}_k \in K$ for some $\lambda_1, \cdots, \lambda_p \in [0, 1]$ so that $\sum_{k=1}^{p} \lambda_k = 1$. Then

$$\langle \mathbf{x}, \mathbf{v}_i \rangle = \sum_{k=1}^{p} \lambda_k \langle \mathbf{v}_k, \mathbf{v}_i \rangle \leqslant \sum_{k=1}^{p} \lambda_k \|\mathbf{v}_i\|^2 = \|\mathbf{v}_i\|^2.$$

Let $\mathbf{x} = \mathbf{v}_i + \sum_{k=1}^{p} \lambda_k \mathbf{v}_k \in K$ for some $\lambda_1, \cdots, \lambda_p \in [0, 1]$ so that $\sum_{k=1}^{p} \lambda_k = 1$. Then

$$\langle \mathbf{x}, \mathbf{v}_i \rangle = \|\mathbf{v}_i\| + \sum_{k=1}^{p} \lambda_k \langle \mathbf{v}_k, \mathbf{v}_i \rangle \geqslant \|\mathbf{v}_i\|^2.$$

Therefore K and $\mathbf{v}_i + K$ are separated by the affine hyperplane $\{\mathbf{x} \in \mathbb{R}^n : \langle \mathbf{x}, \mathbf{v}_i \rangle = \|\mathbf{v}_i\|^2\}$ and $\mathring{K} \cap (\mathbf{v}_i + \mathring{K}) = \varnothing$.
We have

$$\bigcup_{i=1}^{p} (\mathbf{v}_i + K) = \{\mathbf{v}_1, \cdots, \mathbf{v}_p\} + K \subset K + K = 2K \text{ as } K \text{ is convex.}$$

Assume that K is d-dimensional for some $d \leqslant n$, by lemma 5 we get $\mathrm{Vol}_d(K) > 0$ so

$$p\mathrm{Vol}_d(K) = \mathrm{Vol}_d\left(\bigcup_{i=1}^{p}(\mathbf{v}_i + K)\right) \leqslant \mathrm{Vol}_d(2K) \text{ so } p\mathrm{Vol}_d(K) \leqslant 2^d\mathrm{Vol}_d(K) \leqslant 2^n\mathrm{Vol}_d(K).$$

Therefore $p \leqslant 2^n$. □

Remark. We did not use the existence of a center in this lemma, only the sharpness of all angles.

Lemma 8. Let K be an n-dimensional Delauney polytope in $\mathbb{R}^n$ with p vertices $\mathbf{v}_1, \cdots, \mathbf{v}_p$. Let

$$L = \bigcap_{1\leqslant i,j\leqslant p} \left\{\mathbf{x} \in \mathbb{R}^n : \langle \mathbf{v}_i, \mathbf{v}_j\rangle - \|\mathbf{v}_j\|^2 \leqslant \langle \mathbf{v}_i - \mathbf{v}_j, \mathbf{x}\rangle \leqslant \|\mathbf{v}_i\|^2 - \langle \mathbf{v}_i, \mathbf{v}_j\rangle\right\}.$$

Then $K \subset L$ with equality if $p = 2^n$.

Proof. Let $i, j, k \in [\![1, p]\!]$.

$$\begin{cases} \langle \mathbf{v}_i - \mathbf{v}_j, \mathbf{v}_i - \mathbf{v}_k\rangle \geqslant 0 \\ \langle \mathbf{v}_j - \mathbf{v}_i, \mathbf{v}_j - \mathbf{v}_k\rangle \geqslant 0 \end{cases} \quad \text{so } \langle \mathbf{v}_i - \mathbf{v}_j, \mathbf{v}_j\rangle \leqslant \langle \mathbf{v}_i - \mathbf{v}_j, \mathbf{v}_k\rangle \leqslant \langle \mathbf{v}_i - \mathbf{v}_j, \mathbf{v}_i\rangle.$$

Let $\mathbf{x} = \sum_{k=1}^{p} \lambda_k \mathbf{v}_k \in K$ for some $\lambda_1, \cdots, \lambda_p \in [0, 1]$ so that $\sum_{k=1}^{p} \lambda_k = 1$. Let $i, j \in [\![1, p]\!]$. We have

$$\sum_{k=1}^{p} \lambda_k \langle \mathbf{v}_i - \mathbf{v}_j, \mathbf{v}_j\rangle \leqslant \sum_{k=1}^{p} \lambda_k \langle \mathbf{v}_i - \mathbf{v}_j, \mathbf{v}_k\rangle \leqslant \sum_{k=1}^{p} \lambda_k \langle \mathbf{v}_i - \mathbf{v}_j, \mathbf{v}_i\rangle$$
$$\text{so } \langle \mathbf{v}_i, \mathbf{v}_j\rangle - \|\mathbf{v}_j\|^2 \leqslant \langle \mathbf{v}_i - \mathbf{v}_j, \mathbf{x}\rangle \leqslant \|\mathbf{v}_i\|^2 - \langle \mathbf{v}_i, \mathbf{v}_j\rangle$$

so $\mathbf{x} \in L$ and $K \subset L$.
Assume now that $p = 2^n$. L is clearly a closed convex polyhedron in $\mathbb{R}^n$. The $(\mathbf{v}_i)$ are n-dimensional and L has constraints in all the directions $(\pm\mathbf{v}_i)$ so L is a polytope. Let $i \neq j \in [\![1, p]\!]$.
Let $\mathbf{x} \in \mathbf{v}_i + L$, then

$$\langle \mathbf{v}_i - \mathbf{v}_j, \mathbf{x}\rangle \geqslant \|\mathbf{v}_i\|^2 - \langle \mathbf{v}_i, \mathbf{v}_j\rangle + \langle \mathbf{v}_i, \mathbf{v}_j\rangle - \|\mathbf{v}_j\|^2 = \|\mathbf{v}_i\|^2 - \|\mathbf{v}_j\|^2.$$

Let $\mathbf{x} \in \mathbf{v}_j + L$, then

$$\langle \mathbf{v}_i - \mathbf{v}_j, \mathbf{x}\rangle \leqslant \langle \mathbf{v}_i, \mathbf{v}_j\rangle - \|\mathbf{v}_j\|^2 + \|\mathbf{v}_i\|^2 - \langle \mathbf{v}_i, \mathbf{v}_j\rangle = \|\mathbf{v}_i\|^2 - \|\mathbf{v}_j\|^2.$$

Therefore $\mathbf{v}_i + L$ and $\mathbf{v}_j + L$ are separated by the affine hyperplane $\{\mathbf{x} \in \mathbb{R}^n : \langle \mathbf{x}, \mathbf{v}_i - \mathbf{v}_j\rangle = \|\mathbf{v}_i\|^2 - \|\mathbf{v}_j\|^2\}$ and $(\mathbf{v}_i + \mathring{L}) \cap (\mathbf{v}_j + \mathring{L}) = \varnothing$. We now have

$$\bigcup_{i=1}^{p}(\mathbf{v}_i + L) \subset K + L \subset L + L = 2L \text{ as } L \text{ is convex}$$
$$\text{so } p\mathrm{Vol}_n(L) \leqslant \mathrm{Vol}_n(K + L) \leqslant \mathrm{Vol}_n(2L) = 2^n\mathrm{Vol}_n(L) = p\mathrm{Vol}_n(L)$$
$$\text{so } \mathrm{Vol}_n(K + L) = \mathrm{Vol}_n(2L) > 0 \text{ by lemma 5.}$$

By lemma 6, we have $K = L$. □

Lemma 9. Let K be an n-dimensional Delauney polytope in $\mathbb{R}^n$ with p vertices $\mathbf{v}_1, \cdots, \mathbf{v}_p$. Let $\mathbf{c}$ be the center of a sphere containing all the vertices of K. If $p = 2^n$, then

$$\forall i \in [\![1, p]\!],\ \exists j \in [\![1, p]\!],\ 2\mathbf{c} - \mathbf{v}_i = \mathbf{v}_j$$

(the symmetric by $\mathbf{c}$ of any vertex is still a vertex).

Proof. Let $i \in [\![1,p]\!]$. By translating, we can assume that $\mathbf{v}_i = \mathbf{0}$. We only need to show that $2\mathbf{c}$ is a vertex of $K = L$ by lemma 8. Let $j,k \in [\![1,p]\!]$, we have

$$\begin{cases} \|\mathbf{c}-\mathbf{v}_j\| = \|\mathbf{c}\| \\ \|\mathbf{c}-\mathbf{v}_k\| = \|\mathbf{c}\| \end{cases} \text{ so } \begin{cases} \langle 2\mathbf{c}, \mathbf{v}_j\rangle = \|\mathbf{v}_j\|^2 \\ \langle 2\mathbf{c}, \mathbf{v}_k\rangle = \|\mathbf{v}_k\|^2 \end{cases}$$

Therefore

$$\langle 2\mathbf{c}, \mathbf{v}_j - \mathbf{v}_k\rangle = \|\mathbf{v}_j\|^2 - \|\mathbf{v}_k\|^2 \in [\langle \mathbf{v}_j, \mathbf{v}_k\rangle - \|\mathbf{v}_k\|^2, \|\mathbf{v}_j\|^2 - \langle \mathbf{v}_j, \mathbf{v}_k\rangle] \text{ so } 2\mathbf{c} \in L.$$

Furthermore, as K is n-dimensional, the constraints tight at $2\mathbf{c}$ are also n-dimensional, so $2\mathbf{c}$ is a vertex of L. □

Proof of **Theorem 4**. The first part of the theorem is given by lemma 7. We prove the second part by induction on $n \in \mathbb{N}^*$. If $n = 1$, the result is trivial as any two points in $\mathbb{R}$ form a segment, which is a 1-dimensional hypercube. We now assume $n \geqslant 2$. If K is not n-dimensional, then $p \leqslant 2^{n-1}$ by lemma 7, which contradicts $p = 2^n$. Now assume K is n-dimensional. Consider a facet F of K. By translation and rotation we can assume $F \subset \mathbb{R}^{n-1} \times \{0\} =: H$ and $K \subset \mathbb{R}^{n-1} \times \mathbb{R}_+$. We can also assume by re-ordering the vertices that $F = \text{conv}(\mathbf{v}_1, \cdots, \mathbf{v}_q)$ for some $q < p$.
For $i \leqslant q$, we have $H \cap (K + \mathbf{v}_i) = F + \mathbf{v}_i$.
For $i > q$, we have $\mathbf{v}_i \in \mathbb{R}^{n-1} \times \mathbb{R}_+^*$ so $H \cap (K + \mathbf{v}_i) = \varnothing$. Then

$$2K = \bigcup_{i=1}^{p} (\mathbf{v}_i + K) \text{ so } 2F = (2K) \cap H = \bigcup_{i=1}^{p} (\mathbf{v}_i + F) \cap H = \bigcup_{i=1}^{q} (\mathbf{v}_i + F).$$

Furthermore, for $i \in [\![1,q]\!]$, K and $\mathbf{v}_i + K$ are separated by $\{\mathbf{x} \in \mathbb{R}^n : \langle \mathbf{v}_i, \mathbf{x}\rangle = \|\mathbf{v}_i\|^2\}$ therefore so are F and $\mathbf{v}_i + F$. By translation, the $(\mathbf{v}_i + F)$ are all disjoints, so

$$2^{n-1}(F) = q(F).$$

F is a facet so it is convex and $(n-1)$-dimensional, so by lemma 5, we have $(F) > 0$ and $q = 2^{n-1}$. As the projection on H of the center of a sphere containing all vertices of K is the center of a sphere containing all vertices of F, F is clearly a Delaunay polytope in H, and as it has 2^{n-1} vertices, we know by induction that F is a dilated $(n-1)$-dimensional hypercube. By rotation and translation, we can assume that $F = [0,\lambda_1] \times \cdots \times [0,\lambda_{n-1}] \times \{0\}$ for some $\lambda_1, \cdots, \lambda_{n-1} > 0$ and that $K \subset \mathbb{R}^{n-1} \times \mathbb{R}_+$. Let $\mathbf{c} = (c_1, \cdots, c_n)$ be the center of a sphere containing all vertices of K. $\lambda_i \mathbf{e}_i$ is a vertex of F so it is a vertex of K and we have $\|\mathbf{c} - \lambda_i \mathbf{e}_i\| = \|\mathbf{c}\|$ so $c_i = \dfrac{\lambda_i}{2}$. If $c_n \leqslant 0$, consider a vertex of K with positive last coordinate (exists as K is not included in H), then its symmetric by $\mathbf{c}$ is a vertex of K (by lemma 9) with negative last coordinate, which contradicts $K \subset \mathbb{R}^{n-1} \times \mathbb{R}_+$. Therefore $c_n > 0$. Let $\lambda_n = 2c_n$. By lemma 9

$$\{\mathbf{v}_1, \cdots, \mathbf{v}_q\} \cup (2\mathbf{c} - \{\mathbf{v}_1, \cdots, \mathbf{v}_q\}) \subset \{\mathbf{v}_1, \cdots, \mathbf{v}_p\}$$

and those two sets have the same cardinality, as $c_n > 0$ so $F \cap (2c - F) = \varnothing$. The vertices of K are therefore exactly the set $\{0,\lambda_1\} \times \cdots \times \{0,\lambda_n\}$ and $K = [0,\lambda_1] \times \cdots \times [0,\lambda_n]$ is a dilated n-dimensional hypercube. □

Definition 11 (Sharp polytope)**.** Let K be a polytope in $\mathbb{R}^n$ with vertices $\mathbf{v}_1, \cdots, \mathbf{v}_p \in \mathbb{R}^n$. We say that K is a *sharp polytope* if $\forall i,j,k \in [\![1,p]\!]$, $\langle \mathbf{v}_i - \mathbf{v}_j, \mathbf{v}_i - \mathbf{v}_k\rangle \geqslant 0$ (the angle $(\mathbf{v}_j, \mathbf{v}_i, \mathbf{v}_k)$ is sharp).

Remark. Delaunay polytopes are special cases of sharp polytopes.

Theorem 5. *Let K be a sharp polytope in $\mathbb{R}^n$ with p vertices. Then $p \leqslant 2^n$ with equality if and only if K is a dilated n-dimensional hypercube.*

Remark. We can therefore get rid of the condition of existence of a center in Theorem 4.

Lemma 10. Let K be a sharp polytope in $\mathbb{R}^n$ with p vertices $\mathbf{v}_1, \cdots, \mathbf{v}_p$. Then $p \leqslant 2^n$.

Proof. The proof is exactly the same as for lemma 7, as we did not use the existence of a center. □

Proof of **Theorem 5**. The first part of the theorem is given by lemma 10. We prove the second part by induction on $n \in \mathbb{N}^*$. If $n = 1$, the result is trivial as any two points in $\mathbb{R}$ form a segment, which is a 1-dimensional hypercube. We now assume $n \geqslant 2$. If K is not n-dimensional, then $p \leqslant 2^{n-1}$ by lemma 10, which contradicts $p = 2^n$. Now assume K is n-dimensional.
Let $d < n$. Consider a d-dimensional face F of K. By translation and rotation we can assume $F \subset \mathbb{R}^d \times \{0\}^{n-d} =: H$. We can also assume by re-ordering the vertices that $F = \text{conv}(\mathbf{v}_1, \cdots, \mathbf{v}_q)$ for some $q < p$.
For $i \leqslant q$, we have $H \cap (K + \mathbf{v}_i) = F + \mathbf{v}_i$.
For $i > q$, we have $H \cap (K + \mathbf{v}_i) = \varnothing$. Then

$$2K = \bigcup_{i=1}^{p} (\mathbf{v}_i + K) \text{ so } 2F = (2K) \cap H = \bigcup_{i=1}^{p} (\mathbf{v}_i + F) \cap H = \bigcup_{i=1}^{q} (\mathbf{v}_i + F).$$

Furthermore, for $i \in [\![1, q]\!]$, K and $\mathbf{v}_i + K$ are separated by $\{\mathbf{x} \in \mathbb{R}^n : \langle \mathbf{v}_i, \mathbf{x} \rangle = \|\mathbf{v}_i\|^2\}$ therefore so are F and $\mathbf{v}_i + F$. By translation, the $(\mathbf{v}_i + F)$ are all interior-disjoints, so

$$2^d \text{Vol}_d(F) = q \text{Vol}_d(F).$$

F is a d-dimensional face so it is convex, so by lemma 5, we have $\text{Vol}_d(F) > 0$ and $q = 2^d$. F is clearly a sharp polytope in H, and as it has 2^d vertices, we know by induction that F is a dilated d-dimensional hypercube. Therefore, any proper face of K is a dilated hypercube.
Now fix a facet F of K. We can assume that $F = [0, \lambda_1] \times \cdots \times [0, \lambda_{n-1}] \times \{0\}$ and that $K \subset \mathbb{R}^{n-1} \times \mathbb{R}_+$. Consider the ridge $R_1 = [0, \lambda_1] \times \cdots \times [0, \lambda_{n-2}] \times \{0\}^2$. There exists a facet F_1 of K sharing the ridge R_1 with F. As F_1 is a dilated hypercube, there exist a vector $\mathbf{v}_1 \in R_1^\perp$ so that $F_1 = R_1 + [0, 1]\mathbf{v}_1$. $\mathbf{v}_1 \in R_1^\perp$ so there exists some $x_1, y_1 \in \mathbb{R}$ so that $\mathbf{v}_1 = (0, \cdots, 0, x_1, y_1)$. $\mathbf{v}_1 \in K$ so $y_1 \geqslant 0$, and as F and F_1 can not be in the same hyperplane, we have $y_1 \neq 0$ so $y_1 > 0$. We know that any vertex $\mathbf{w}$ of K satisfies $\langle \mathbf{w}, \lambda_i \mathbf{e}_i \rangle \geqslant 0$ for any $i \in [\![1, n-1]\!]$ so $K \subset (\mathbb{R}_+)^n$. Therefore $\mathcal{F} = K \cap \{0\}^{n-2} \times \mathbb{R}^2$ is a face of K. $\mathcal{F}$ is at most 2-dimensional, and as it contains $\lambda_{n-1}\mathbf{e}_{n-1}$ and $\mathbf{v}_1$, $\mathcal{F}$ is exactly 2-dimensional. It is therefore a rectangle, and three of its vertices are $\mathbf{0}$, $\lambda_{n-1}\mathbf{e}_{n-1}$ and $\mathbf{v}_1$. Let $\mathbf{w} \in K$ be the fourth vertex. $\mathbf{w} \in K \cap (\{0\}^{n-2} \times \mathbb{R}^2)$ so $\mathbf{w} = \alpha \mathbf{e}_{n-1} + \beta \mathbf{e}_n$ for some $\alpha, \beta \geqslant 0$. As $\mathcal{F} \subset \{0\}^{n-2} \times (\mathbb{R}_+)^2$, $[\mathbf{0}, \lambda_{n-1}\mathbf{e}_{n-1}]$ is a side of $\mathcal{F}$. The other side has to be $[y_1\mathbf{e}_n, y_1\mathbf{e}_n + \lambda_{n-1}\mathbf{e}_{n-1}]$, so either $x_1 = 0$, $\alpha = \lambda_{n-1}$, $\beta = y_1$ or $x_1 = \lambda_{n-1}$, $\alpha = 0$, $\beta = y_1$.
By contradiction, assume $x_1 = \lambda_{n-1}$, $\alpha = 0$, $\beta = y_1$. Then $\lambda_{n-1}\mathbf{e}_{n-1} \in F_1 + \lambda_{n-1}\mathbf{e}_{n-1}$ and $\mathbf{w} = y_1\mathbf{e}_n = (\lambda_{n-1}\mathbf{e}_{n-1} + y_1\mathbf{e}_n) - \lambda_{n-1}\mathbf{e}_{n-1} \in F_1 - \lambda_{n-1}\mathbf{e}_{n-1}$. There are elements of K on both sides of F_1, which contradicts the fact that F_1 is a facet of K. Therefore $x_1 = 0$ and $\mathbf{v}_1 = y_1\mathbf{e}_n$.
Finally, consider the ridge $R_2 = R_1 + \lambda_{n-1}\mathbf{e}_{n-1}$ of F, and the associated facet F_2 of K. Similarly, we know that $F_2 = R_2 + [0, 1]\mathbf{v}_2$ for some $\mathbf{v}_2 = y_2\mathbf{e}_n$, $y_2 > 0$. $\mathbf{0}, \lambda_{n-1}\mathbf{e}_{n-1}, \mathbf{v}_1, \lambda_{n-1}\mathbf{e}_{n-1} + \mathbf{v}_2$ are vertices of K so

$$\langle \mathbf{v}_1 - \mathbf{0}, \mathbf{v}_1 - (\mathbf{v}_2 + \lambda_{n-1}\mathbf{e}_{n-1}) \rangle \geqslant 0 \text{ so } y_1(y_1 - y_2) \geqslant 0 \text{ so } y_1 \geqslant y_2$$

$$\langle (\mathbf{v}_2 + \lambda_{n-1}\mathbf{e}_{n-1}) - \lambda_{n-1}\mathbf{e}_{n-1}, (\mathbf{v}_2 + \lambda_{n-1}\mathbf{e}_{n-1}) - \mathbf{0} \rangle \geqslant 0 \text{ so } y_2(y_2 - y_1) \geqslant 0 \text{ so } y_2 \geqslant y_1.$$

Therefore $y_1 = y_2$ and $\mathbf{v}_1 = \mathbf{v}_2 = y_1\mathbf{e}_n$. F_1, F_2 both have 2^{n-1} vertices, and all those vertices are disjoints so they are all the vertices of K. Therefore,

$$K = \text{conv}(F_1, F_2) = \text{conv}(R_1, R_2) + [0, 1]\mathbf{v}_1 = F + [0, y_1]\mathbf{e}_n = [0, \lambda_1] \times \cdots \times [0, \lambda_{n-1}] \times [0, y_1]$$

so K is a dilated hypercube. □

Theorem 6. *Let $\mathcal{L}$ be an n-dimensional lattice in $\mathbb{R}^n$. Let $\mathbf{t} \in \mathbb{R}^n$ and let $\Lambda(\mathbf{t})$ be the set of closest vectors to $\mathbf{t}$. Then $|\Lambda(\mathbf{t})| \leqslant 2^n$. Furthermore, if $|\Lambda(\mathbf{t})| = 2^n$, then the lattice is orthogonal.*

Proof. Let $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \Lambda(\mathbf{t})$. We want to show that $\langle \mathbf{w}-\mathbf{u}, \mathbf{w}-\mathbf{v} \rangle \geqslant 0$. We can assume by translating that $\mathbf{v} = \mathbf{0}$. Then

$$\|\mathbf{u}-\mathbf{t}\|^2 = \|\mathbf{w}-\mathbf{t}\|^2 \Rightarrow \|\mathbf{u}\|^2 - \|\mathbf{w}\|^2 = \langle \mathbf{t}, \mathbf{u}-\mathbf{w} \rangle$$

and

$$0 \leqslant \|\mathbf{t}-(\mathbf{u}-\mathbf{w})\|^2 - \|\mathbf{x}\|^2 = \|\mathbf{u}-\mathbf{w}\|^2 - 2\langle \mathbf{t}, \mathbf{u}-\mathbf{w} \rangle = 2\langle \mathbf{w}-\mathbf{u}, \mathbf{w} \rangle.$$

Let $K = \text{conv}(\Lambda(\mathbf{t}))$. Any strictly convex combination of elements of $\Lambda(\mathbf{t})$ is in $\|\mathbf{t}\|\mathcal{B}(\mathbf{t}, 1)$ so no element of $\Lambda(\mathbf{t})$ is a convex combination of the others. Therefore K is a sharp polytope with $|\Lambda(\mathbf{t})|$ vertices. By theorem 5, $|\Lambda(\mathbf{t})| \leqslant 2^n$.
Assume there is equality, then K is a dilated hypercube and $\Lambda(\mathbf{t}) = \{0, \lambda_1\} \times \cdots \times \{0, \lambda_n\}$ after rotation and translation for some $\lambda_1, \cdots, \lambda_n > 0$. As two distinct points of $\Lambda(\mathbf{t})$ can not be in the same coset of $\mathcal{L}$ – else their average would be strictly closer to $\mathbf{t}$ – we know that $\Lambda(\mathbf{t})$ contains representatives of 2^n cosets of $\mathcal{L}$, therefore of all the cosets of $\mathcal{L}$. $\Lambda(\mathbf{t})$ therefore generates $\mathcal{L}$, and $\mathcal{L}$ is orthogonal. □

5 Shadow Simplex method for linear programing

We recall that a way to measure the efficiency of a simplex algorithm is to bound the number of simplex pivots – *ie* the number of vertices crossed during the algorithm. In [13], Dadush & Bonifas found a polynomial bound in the dimension, the number of constraints and the parameter δ of the δ-distance property. However, they needed in the algorithm the knowledge of δ. In this section, we simpler algorithms that do not need the knowledge of δ, with no additional cost in the bounded case and at a cost of $O\left(\frac{m\ln(m/\delta)}{n\ln(n/\delta)}\right)$ on the number of shadow simplex pivots for the general case.
In the shadow simplex method, instead of moving from a vertex to another until the optimal solution is attained, we look at a dual version of the problem : to each vertex is associated a normal cone, defined by the tight constraints at this vertex. We move among normal cones, each step crossing a common facet of two adjacent normal cones. Therefore, the distance between two vertices is bounded by the number of crossings, as given a path among normal cones we can obtain a path among vertices of same length. Let $A = (\mathbf{a}_1, \cdots, \mathbf{a}_m)$ be a set of unit constraints defining a LP, satisfying the δ-distance property.

5.1 Special case : bounded polytopes

Lemma 11. Let $C \subset \mathbb{R}^n$ be a cone, $\mathbf{a}, \mathbf{b} \in \mathbb{R}^n$, $\gamma > 0$. Then

$$C \cap [\mathbf{a}, \mathbf{b}] \neq \varnothing \Leftrightarrow C \cap [\gamma\mathbf{a}, \mathbf{b}] \neq \varnothing.$$

Proof. $C \cap [\mathbf{a}, \mathbf{b}] \neq \varnothing \Leftrightarrow C \cap \text{cone}(\mathbf{a}, \mathbf{b}) \neq \varnothing \Leftrightarrow C \cap \text{cone}(\gamma\mathbf{a}, \mathbf{b}) \neq \varnothing \Leftrightarrow C \cap [\gamma\mathbf{a}, \mathbf{b}] \neq \varnothing$. □

Lemma 12 (Path crossings Bounds)**.** Consider $X \sim \text{Exp}_{\mathbb{R}^n}(1)$ and $\mathbf{c}, \mathbf{d} \in \mathbb{R}^n$. Let $\mathcal{T} = (C_i)_{i\in I}$ be a partition of $\mathbb{R}^n$ into n-dimensional interior disjoint polyhedral τ-wide cones. Define $\partial\mathcal{T} = \bigcup_{i\in I} \partial C_i$. Then :

1. $\mathbb{E}\left[|[\mathbf{c}+X, \mathbf{d}+X] \cap \partial\mathcal{T}|\right] \leqslant \dfrac{\|\mathbf{d}-\mathbf{c}\|}{\tau}$.
2. Let $\alpha \in (0, 1]$, $\mathbb{E}[|[\mathbf{c}+X, \mathbf{c}+\alpha X] \cap \partial\mathcal{T}|] \leqslant \dfrac{2n}{\tau}\ln\left(\dfrac{1}{\alpha}\right)$.
3. Let $0 < \varepsilon < 1$, $\mathbb{E}\left[\left|\left[X, \dfrac{\varepsilon}{1+\varepsilon}X + \dfrac{1}{1+\varepsilon}\mathbf{d}\right] \cap \partial\mathcal{T}\right|\right] \leqslant \min\left(\dfrac{\|\mathbf{d}\|}{\varepsilon\tau}, \dfrac{\|\mathbf{d}\|}{\tau} + \dfrac{2n}{\tau}\ln\left(\dfrac{1}{\varepsilon}\right)\right)$.

Proof. 1 and 2 are proven in [13], Theorem 10. Let us prove 3. We have :

$$\begin{aligned}\mathbb{E}\left[\left|\left[X, \frac{\varepsilon}{1+\varepsilon}X + \frac{1}{1+\varepsilon}\mathbf{d}\right] \cap \partial\mathcal{T}\right|\right] &= \mathbb{E}\left[\left|\left[X, X + \frac{1}{\varepsilon}\mathbf{d}\right] \cap \partial\mathcal{T}\right|\right] \text{ by lemma 11} \\ &\leqslant \frac{\|\mathbf{d}\|}{\varepsilon\tau} \text{ by 1.}\end{aligned}$$

Furthermore :

$$\begin{aligned}\mathbb{E}\left[\left|\left[X, \frac{\varepsilon}{1+\varepsilon}X + \frac{1}{1+\varepsilon}\mathbf{d}\right] \cap \partial\mathcal{T}\right|\right] &= \mathbb{E}\left[|[X, X+\mathbf{d}] \cap \partial\mathcal{T}|\right] + \mathbb{E}\left[\left|\left[X+\mathbf{d}, X + \frac{1}{\varepsilon}\mathbf{d}\right] \cap \partial\mathcal{T}\right|\right] \\ &= \mathbb{E}\left[|[X, X+\mathbf{d}] \cap \partial\mathcal{T}|\right] + \mathbb{E}\left[|[X+\mathbf{d}, \varepsilon X+\mathbf{d}] \cap \partial\mathcal{T}|\right] \\ &\leqslant \frac{\|\mathbf{d}\|}{\tau} + \frac{2n}{\tau}\ln\left(\frac{1}{\varepsilon}\right) \text{ by 1 and 2.}\end{aligned}$$

□

Algorithm 1: Straight line Shadow Simplex algorithm

Input: Polytope $P = \{\mathbf{x} \in \mathbb{R}^n : A\mathbf{x} \leqslant \mathbf{b}\}$ with m constraints, objective $\mathbf{d} \in \mathbb{R}^n$, feasible basis $\mathcal{B} \subset [\![1, m]\!]$
Result: Optimal basis $\mathcal{B} \subset [\![1, m]\!]$
$\mathbf{c} \leftarrow \sum_{i\in\mathcal{B}} \frac{\mathbf{a}_i}{\|\mathbf{a}_i\|}$;
Sample $X \sim \mathcal{U}(\mathbb{S}^{n-1})$;
Follow segments $[c, X], [X, d]$ using Shadow Simplex;
return current basis

Remark. **Algorithm 1** correctly computes an optimal basis for the objective $\mathbf{d}$.

Theorem 7. *If P satisfies the local δ-distance property, the expected number of shadow simplex pivots in* **Algorithm 1** *is* $O\left(\frac{n^3}{\delta}\ln\left(\frac{n}{\delta}\right)\right)$.

Proof. We will bound separately the number of crossings with segment $[\mathbf{c}, X]$ ($\mathbf{c} \to X$) and with segment $[\mathbf{d}, X]$ ($\mathbf{d} \to X$). Let $r \sim \mathrm{Exp}_{\mathbb{R}_+}(1)$ independent of X, then $rX \sim \mathrm{Exp}_{\mathbb{R}^n}(1)$. By lemma 11, scaling X does not affect the number of shadow simplex pivots, so we can assume that X is exponentially distributed conditioned on $\|X\| \leqslant 2n$ in the proof. By lemma 1, the normal cones of P are $\frac{\delta}{n}$-wide.

For $\mathbf{c} = \sum_{i\in\mathcal{B}} \frac{\mathbf{a}_i}{\|\mathbf{a}_i\|} \to X$, consider $\varepsilon = \frac{\delta}{4n^2}$ and $\mathbf{v} = \frac{\varepsilon}{1+\varepsilon}X + \frac{1}{1+\varepsilon}\mathbf{c}$. Then

$$\|\mathbf{c} - \mathbf{v}\| = \frac{\varepsilon}{1+\varepsilon}\|X - \mathbf{c}\| \leqslant \varepsilon(2n+n) < \frac{\delta}{n}.$$

By lemma 1, we know that $\mathbf{c}$ and $\mathbf{v}$ are in the same cone, therefore there are no shadow simplex pivots between them. If X were not conditioned on $\|X\| \leqslant 2n$, we would get by lemma 12 that $\mathbb{E}[N] = O\left(\frac{n^3}{\delta}\ln\left(\frac{n}{\delta}\right)\right)$, where N is the expected number of shadow simplex pivots between $\mathbf{v}$ and X. As $\mathbb{E}[X] = n$, $\|X\| \leqslant 2n$ with probability greater than $1/2$ by Markov inequality and

$$\mathbb{E}[N | \|X\| \leqslant 2n] \leqslant 2\mathbb{E}[N] = O\left(\frac{n^3}{\delta}\ln\left(\frac{n}{\delta}\right)\right).$$

The same line of reasoning enables us to bound the expected number of crossing for a conditioned random variable the same way we would for an unconditioned one.

For $X \to \mathbf{d}$, consider $\varepsilon = \dfrac{2\delta}{3n(n+1)}$ and $\mathbf{v} = \dfrac{\varepsilon}{1+\varepsilon}X + \dfrac{1}{1+\varepsilon}\mathbf{d}$. By rescaling we can assume $\|\mathbf{d}\| = 2$. For $\lambda \in \left[0, \dfrac{\varepsilon}{1+\varepsilon}\right]$, let $\mathbf{v}_\lambda = \lambda X + (1-\lambda)\mathbf{d}$. Notice that $\mathbf{v} = \mathbf{v}_{\varepsilon/(1+\varepsilon)}$ Let us write $\mathbf{v}_\lambda = \sum_{i=1}^{m} \alpha_i^\lambda \dfrac{\mathbf{a}_i}{\|\mathbf{a}_i\|}$ where α_i^λ is the coordinate associated to $\dfrac{\mathbf{a}_i}{\|\mathbf{a}_i\|}$ in $\mathbf{v}_\lambda$ ($\alpha_i^\lambda = 0$ if $\mathbf{v}_\lambda$ is not in a normal cone generated by $\mathbf{a}_i$). At most n of the α_i^λ are non-zero for any λ. Then for any normal cone $C = \mathrm{cone}((\mathbf{a}_j)_{j\in J})$ entered at $\lambda_{\mathrm{in}}(C)$ and left at $\lambda_{\mathrm{out}}(C)$, we have

$$\begin{aligned}
(\lambda_{\mathrm{in}}(C) - \lambda_{\mathrm{out}}(C))(2\|X\| + 2) &\geqslant (\lambda_{\mathrm{in}}(C) - \lambda_{\mathrm{out}}(C))(\|X\| + \|\mathbf{d}\|) \geqslant \|(\lambda_{\mathrm{in}}(C) - \lambda_{\mathrm{out}}(C))(X - \mathbf{d})\| \\
&= \|\mathbf{v}_{\lambda_{\mathrm{in}}(C)} - \mathbf{v}_{\lambda_{\mathrm{out}}(C)}\| \\
&= \left\| \sum_{j\in J} (\alpha_j^{\lambda_{\mathrm{in}}(C)} - \alpha_j^{\lambda_{\mathrm{out}}(C)}) \frac{\mathbf{a}_j}{\|\mathbf{a}_j\|} \right\| \\
&\geqslant \delta \max_{j\in J} |\alpha_j^{\lambda_{\mathrm{in}}(C)} - \alpha_j^{\lambda_{\mathrm{out}}(C)}| \text{ by lemma 2} \\
&= \delta \max_{1\leqslant i\leqslant m} |\alpha_i^{\lambda_{\mathrm{in}}(C)} - \alpha_i^{\lambda_{\mathrm{out}}(C)}| \text{ as the other coefficients are zero.}
\end{aligned}$$

Therefore, for any $i \in [\![1, m]\!]$, the total variation of coefficient α_i^λ for λ varying between $\dfrac{\varepsilon}{1+\varepsilon}$ and 0 is at most

$$\sum_{C \text{ crossed by } [X,\mathbf{d}]} |\alpha_i^{\lambda_{\mathrm{in}}(C)} - \alpha_i^{\lambda_{\mathrm{out}}(C)}| \leqslant \frac{\|X\| + 2}{\delta} \sum_{C \text{ visited}} (\lambda_{\mathrm{in}}(C) - \lambda_{\mathrm{out}}(C)) \leqslant \frac{(\|X\| + 2)\varepsilon}{\delta(1+\varepsilon)} \leqslant \frac{(\|X\| + 2)\varepsilon}{\delta} < \frac{2}{n}.$$

Write $\mathbf{d} = \sum_{j\in J} \alpha_j^0 \mathbf{a}_j$, $|J| = n$, then $2 = \|d\| \leqslant \sum_{j\in J} \alpha_j^0$ so at least one of the α_j is greater or equal to $\dfrac{2}{n}$. As this coefficient varies by strictly less than $\dfrac{2}{n}$ between $\mathbf{v}$ and $\mathbf{d}$, it was already positive in $\mathbf{v}$ and stays positive all the way to $\mathbf{d}$.

Consider π the orthogonal projector onto $\mathbf{a}_j^\perp$, and consider, for any cone with $\mathbf{a}_j$ in its set of generator, its image by π. Then, as a change of cone corresponds to a coefficient going to zero, and as the coefficient associated with $\mathbf{a}_j$ can not go to zero, any change of cone corresponds to a change of cone in the projection. Therefore, denoting by $(C_i)_{i\in I}$ the cones, we have

$$\begin{aligned}
\mathbb{E}\left[\left|[\mathbf{v}, \mathbf{d}] \cap \bigcup_{i\in I} \partial C_i\right|\right] &= \mathbb{E}\left[\left|[\pi(\mathbf{v}), \pi(\mathbf{d})] \cap \bigcup_{\mathbf{a}_j \text{ generating } C_i} \partial(\pi(C_i))\right|\right] \\
&\leqslant \mathbb{E}\left[\left|[\pi(X), \pi(\mathbf{d})] \cap \bigcup_{\mathbf{a}_j \text{ generating } C_i} \partial(\pi(C_i))\right|\right].
\end{aligned}$$

$\mathbf{a}_j$ does not depend on the choice of X, but only on $\mathbf{d}$. Therefore, π is a deterministic function and $\pi(X)$ is a rotationally symmetric variable, as a deterministic projection of a centrally symmetric variable. This means we can normalize it to make it uniform over $\mathbb{S}^{n-2}$. We can also normalize $\pi(\mathbf{d})$ so that its norm becomes 2 (if this projection is zero then $\mathbf{d}$ is generated only by $\mathbf{a}_j$ and we are done). The projected cones still satisfy the δ-distance property, so we can iterate and get :

$$\mathbb{E}\left[\left|[X, \mathbf{d}] \cap \bigcup_{i\in I} \partial C_i\right|\right] \leqslant \sum_{k=1}^{n} \mathbb{E}\left[\left|[\pi_k(X), \pi_k(\mathbf{v}_k)] \cap \bigcup_{\mathbf{a}_{j_1}, \cdots, \mathbf{a}_{j_k} \text{ generating } C_i} \partial(\pi_k(C_i))\right|\right] + O(1)$$

where π_k is the orthogonal projector onto $(\mathbf{a}_{j_1}, \cdots, \mathbf{a}_{j_k})^\perp$. Therefore

$$\mathbb{E}\left[\left|[X, \mathbf{d}] \cap \bigcup_{i\in I} \partial C_i\right|\right] \leqslant \sum_{k=1}^{n} \left(\frac{n\|\mathbf{d}\|}{\delta} + \frac{2n^2}{\delta} \ln\left(\frac{1}{\varepsilon}\right)\right) = O\left(\frac{n^3}{\delta} \ln\left(\frac{1}{\varepsilon}\right)\right).$$

□

Remark. As opposed to **Algorithm 1** of [13], the knowledge of δ is not necessary. Furthermore, the algorithm is simpler, as it only follows a straight line.

5.2 Generalizing to the unbounded case

We are now able to solve a bounded LP without any knowledge of δ, assuming we have a feasible point. These two hypothesis are however really strong. Therefore, we want to extend our result to general LPs. To do so, it is enough to be able to solve unbounded LPs, because then we can find a feasible point by solving m successive unbounded LPs (see [13], Theorem 9 for more details). The problem here is that if we take X to be a centrally symmetric random variable, X could be outside the union Σ of the normal cones of the polyhedra, and therefore it is not possible to use Shadow Simplex from $\mathbf{c}$ to X to $\mathbf{d}$, as we could meet an unbounded ray. This problem does not happen if $X \in \Sigma$. We will therefore sample X at random in Σ. To do so, we could sample X as before, conditioned on $X \in \Sigma$, but we have no way of checking if a point is in Σ more efficiently than solving an LP, which would defeat the purpose.

Definition 12 (Cone-exponential distribution)**.** Let $C = \text{cone}(\mathbf{a}_1, \cdots, \mathbf{a}_m)$ be a cone. We say that a random variable X follows a *cone-exponential distribution* with generators $\mathbf{a}_1, \cdots, \mathbf{a}_m$ if there exist independent random variables $\lambda_1, \cdots, \lambda_m$ following exponential distributions of parameter 1 on $\mathbb{R}$ so that $X = \sum_{i=1}^{m} \lambda_i \mathbf{a}_i$.

Proposition 8. Let X be a cone-exponentially distributed random variable with generators $\mathbf{a}_1, \cdots, \mathbf{a}_m$. Then X has borelian probability measure $\mu = \mu_1 * \cdots * \mu_m$ on $\mathbb{R}^n$ where :

- For all $i \in [\![1, m]\!]$, μ_i is the borelian measure on $\mathbb{R}^n$ defined by
$$\forall A \subset \mathbb{R}^n \text{ borelian, } \mu(A) = \int_0^{+\infty} \mathbb{1}_A(t\mathbf{a}_i) e^{-t} \mathrm{d}t.$$
- $*$ is the convolution between measures, namely if ν, η are borelian measures on $\mathbb{R}^n$, for all borelian $A \subset \mathbb{R}^n$, we have
$$(\nu * \eta)(A) = \int_{\mathbb{R}^n \times \mathbb{R}^n} \mathbb{1}_A(\mathbf{x} + \mathbf{y}) \mathrm{d}(\nu \times \eta)(\mathbf{x}, \mathbf{y}).$$
where $\nu \times \eta$ is the product measure of ν and η.

Remark.
- $*$ is an associative and commutative operator by Fubini's theorem.
- For all $A \subset \mathbb{R}^n$ borelian, for μ, ν borelian measures on $\mathbb{R}^n$,
$$\mu(A) = \int_{\mathbb{R}^n} \mathbb{1}_A(\mathbf{x}) \mathrm{d}\mu(\mathbf{x}) = \int_A \mathrm{d}\mu(\mathbf{x})$$
and
$$(\mu_1 * \mu_2)(A) = \int_{\mathbb{R}^n} \int_{\mathbb{R}^n} \mathbb{1}_A(\mathbf{x} + \mathbf{y}) \mathrm{d}\mu(\mathbf{x}) \mathrm{d}\nu(\mathbf{y}) = \int_{\mathbb{R}^n} \int_{\mathbb{R}^n} \mathbb{1}_{A-\mathbf{y}}(\mathbf{x}) \mathrm{d}\mu(\mathbf{x}) \mathrm{d}\nu(\mathbf{y}) = \int_{\mathbb{R}^n} \mu_1(A - \mathbf{y}) \mathrm{d}\mu_2(\mathbf{y})$$

Lemma 13. Let X be a random variable following a cone-exponential distribution with generators $\mathbf{a}_1, \cdots, \mathbf{a}_m$. If the generators induce a fully-dimensional space on $\mathbb{R}^n$, then X has a density with respect to the Lebesgue measure.

Proof. If $m = n$, let
$$f : \mathbb{R}^n \to \mathbb{R}^n, \qquad (t_1, \cdots, t_n) \mapsto \sum_{i=1}^{n} t_i \mathbf{a}_i$$
f is continuous. Let A be a borelian set with Lebesgue measure 0, then so is $f^{-1}(A)$. Let $\Lambda = (\lambda_1, \cdots, \lambda_n)$ be independent random variables following exponential distribution of parameter 1 on $\mathbb{R}$ so that $X = \sum_{i=1}^{n} \lambda_i \mathbf{a}_i$. Λ trivially has a density on $\mathbb{R}^n$. Then
$$\mu_1 * \cdots * \mu_n(A) = \mathbb{P}(X \in A) = \mathbb{P}(\Lambda \in f^{-1}(A)) = 0$$

and X has a density with respect to the Lebesgue measure by Radon-Nikodym theorem. If $m > n$, after re-ordering we can assume that $\mathbf{a}_1, \cdots, \mathbf{a}_n$ are linearly independent. Let $\nu = \mu_1 * \cdots * \mu_n$ and $\eta = \mu_{n+1} * \cdots * \mu_m$. Let $\mu = \nu * \eta$ be the probability distribution of X. Then for any borelian set A with Lebesgue measure 0, we have

$$\mu(A) = \nu * \eta(A) = \int_{\mathbb{R}^n} \nu(A - \mathbf{y}) \mathrm{d}\eta(\mathbf{y}) = 0$$

as ν is absolutely continuous with respect to the Lebesgue measure. Therefore, by Radon-Nikodym theorem, X has a density with respect to the Lebesgue measure. □

Lemma 14. Let X be a random variable following a cone-exponential distribution with generators $\mathbf{a}_1, \cdots, \mathbf{a}_m$ and let μ be the associated probability measure. Then

1. For any $i \in [\![1, m]\!]$, for any $s \geqslant 0$, for any borelian set A, $\mu(A + s\mathbf{a}_i) \geqslant e^{-s}\mu(A)$.
2. If μ has a density f, then the set $E = \{\mathbf{x} \in \mathbb{R}^n : f(\mathbf{x} + s\mathbf{a}_i) \geqslant e^{-s} f(\mathbf{x})\}$ has measure 1.

Proof. 1. For $A \subset \mathbb{R}^n$ borelian, for $s \geqslant 0$ and $i \in [\![1, m]\!]$,

$$\mu_i(A + s\mathbf{a}_i) = \int_0^{+\infty} e^{-t} \mathbb{1}_{A + s\mathbf{a}_i}(t\mathbf{a}_i) \mathrm{d}t = \int_0^{+\infty} e^{-t} \mathbb{1}_A((t-s)\mathbf{a}_i) \mathrm{d}t = \int_{-s}^{+\infty} e^{-s} e^{-t} \mathbb{1}_A(t\mathbf{a}_i) \mathrm{d}t \geqslant e^{-s} \mu_i(A)$$

Therefore, denoting $\mu_{-i} = \mu_1 * \cdots * \mu_{i-1} * \mu_{i+1} * \cdots * \mu_m$, we have

$$\mu(A + s\mathbf{a}_i) = \int_{\mathbb{R}^n} \mu_i(A - \mathbf{y} + s\mathbf{a}_i) \mathrm{d}\mu_{-i}(\mathbf{y}) \geqslant e^{-s} \int_{\mathbb{R}^n} \mu_i(A - \mathbf{y}) \mathrm{d}\mu_{-i}(\mathbf{y}) = e^{-s}\mu(A)$$

2. If E does not have measure 1, consider an $\varepsilon > 0$ and a borelian set B with no-zero measure so that $\forall \mathbf{x} \in B$, $f(\mathbf{x} + s\mathbf{a}_i) < e^{-s} f(\mathbf{x}) - \varepsilon$ – if ε, B do not exist, we can prove by taking the union over all $\varepsilon = \frac{1}{n}$ that E that measure 1. Then

$$0 \leqslant \mu(B + s\mathbf{a}_i) - e^{-s}\mu(B) = \int_{B + s\mathbf{a}_i} f(\mathbf{x}) \mathrm{d}\mathbf{x} - \int_B e^{-s} f(\mathbf{x}) \mathrm{d}\mathbf{x} = \int_B (f(\mathbf{x} + s\mathbf{a}_i) - e^{-s} f(\mathbf{x})) \mathrm{d}\mathbf{x} \leqslant -\varepsilon\mu(B) < 0.$$

This is a contradiction. □

Algorithm 2: Straight line Shadow Simplex algorithm with cone-exponential distribution

Input: Polyhedron $P = \{\mathbf{x} \in \mathbb{R}^n : A\mathbf{x} \leqslant \mathbf{b}\}$ with m constraints, objective $\mathbf{d} \in \mathbb{R}^n$, feasible basis $\mathcal{B} \subset [\![1, m]\!]$

Result: Optimal basis $\mathcal{B} \subset [\![1, m]\!]$

$\mathbf{c} \leftarrow \sum_{i \in \mathcal{B}} \frac{\mathbf{a}_i}{\|\mathbf{a}_i\|}$;

Sample $\lambda_1, \cdots, \lambda_m$ independent random variables following $\mathrm{Exp}_{\mathbb{R}_+}(1)$ conditioned on $\lambda_i \leqslant 1$;

Set $X = \sum_{i=1}^m \lambda_i \mathbf{a}_i$;

Follow segments $[c, X], [X, d]$ using Shadow Simplex;

return current basis

Theorem 8 (Path crossings Bounds for cone-exponentially distributed middle point)**.** *Let $0 \leqslant p \leqslant n$ and let π be the orthogonal projector onto $(\mathbf{a}_1, \cdots, \mathbf{a}_p)^\perp$. Let $\mathcal{T} = (C_i)_{i \in I}$ the set of normal cones of A having $\mathbf{a}_1, \cdots, \mathbf{a}_p$ among their generators, they partition a convex cone and meet at faces. Let $\pi(\mathcal{T}) = (\pi(C_i))_{i \in I}$. Assume these cones are n-dimensional, interior disjoint and polyhedral. Consider X following a cone-exponential distribution with generators $\mathbf{a}_1, \cdots, \mathbf{a}_m$ and $\mathbf{c}, \mathbf{d} \in \mathbb{R}^n$ conditioned on $X \leqslant m$ (can be done easily by conditioning all the components to be smaller than 1). Then :*

1. $\mathbb{E}\left[|[\pi(\mathbf{c}) + \pi(X), \pi(\mathbf{d}) + \pi(X)] \cap \partial\pi(\mathcal{T})|\right] \leqslant \frac{n}{\delta} \|\mathbf{d} - \mathbf{c}\|$.

2. *Let* $\alpha \in (0,1]$, $\mathbb{E}[|[\pi(\mathbf{c})+\pi(X), \pi(\mathbf{c})+\alpha\pi(X)] \cap \partial\pi(\mathcal{T})|] \leqslant \dfrac{2nm}{\delta}\ln\left(\dfrac{1}{\alpha}\right)$.

3. *Let* $0<\varepsilon<1$, $\mathbb{E}\left[\left|\left[\pi(X), \dfrac{\varepsilon}{1+\varepsilon}\pi(X)+\dfrac{1}{1+\varepsilon}\pi(\mathbf{d})\right] \cap \partial\pi(\mathcal{T})\right|\right] \leqslant \min\left(\dfrac{n}{\varepsilon\delta}\|\mathbf{d}\|, \dfrac{n}{\delta}\|\mathbf{d}\| + \dfrac{2nm}{\delta}\ln\left(\dfrac{1}{\varepsilon}\right)\right)$.

Proof. Note that if we prove 1 and 2, 3 follows immediately with the same proof as in lemma 12.
We will follow the proofs of lemmas 21-25 of [13].

Let μ be the probability measure of $\pi(X)$. $\pi(X)$ follows a cone-exponential distribution with generators $\pi(\mathbf{a}_1), \cdots, \pi(\mathbf{a}_m)$. Let $\mu_1, \cdots, \mu_m$ be the probability measures associated with $\pi(\mathbf{a}_1), \cdots, \pi(\mathbf{a}_m)$, so that $\mu = \mu_1 * \cdots * \mu_m$. By lemma 13, μ admits a density f with respect to the Lebesgue measure on $\pi(\mathbb{R}^n)$.
Let $i \in I$, by re-ordering the constraints we can assume that C_i is generated by $\mathbf{a}_1, \cdots, \mathbf{a}_n$. Let $\tau = \dfrac{\delta}{n}$, we know that C_i is τ-wide by lemma 1. Let $\mathbf{u} = \sum_{i=1}^{n} \dfrac{1}{n}\mathbf{a}_i \in C_i$. We know by the proof of [13], lemma 5 that $\mathbf{u} + \tau\mathcal{B}_2^n \subset C_i$ and $\|\mathbf{u}\| \leqslant 1$.

1. Let F be a facet of $\pi(C_i)$. $\pi(X)$ has a density with respect to the Lebesgue measure, therefore the line segment $[\pi(\mathbf{c})+\pi(X), \pi(\mathbf{d})+\pi(X)]$ passes through F at most once. By linearity we see that

$$\mathbb{E}[|[\pi(\mathbf{c})+\pi(X), \pi(\mathbf{d})+\pi(X)] \cap \partial\pi(C_i)|] = \sum_{F \text{ facet of } \pi(C_i)} \mathbb{P}[F \cap [\pi(\mathbf{c})+\pi(X), \pi(\mathbf{d})+\pi(X)] \neq \varnothing].$$

We now bound the crossing probability for any facet F. We first calculate the hitting probability as

$$\begin{aligned}
\mathbb{P}[F \cap [\pi(\mathbf{c})+\pi(X), \pi(\mathbf{d})+\pi(X)] \neq \varnothing] = \mathbb{P}[\pi(X) \in F - [\pi(\mathbf{c}), \pi(\mathbf{d})]] &= \int_{F-[\pi(\mathbf{c}),\pi(\mathbf{d})]} f(\mathbf{x})\mathrm{d}\mathbf{x} \\
&= |\langle \mathbf{n}, \pi(\mathbf{d}) - \pi(\mathbf{c})\rangle| \int_0^1 \int_{F-((1-\lambda)\pi(\mathbf{c})+\lambda\pi(\mathbf{d}))} f(\mathbf{x})\mathrm{d}\mathbf{x}\mathrm{d}\lambda \\
&\leqslant \|\mathbf{d}-\mathbf{c}\| \int_0^1 \int_{F-((1-\lambda)\pi(\mathbf{c})+\lambda\pi(\mathbf{d}))} f(\mathbf{x})\mathrm{d}\mathbf{x}\mathrm{d}\lambda
\end{aligned}$$

where $\mathbf{n}$ is a unit normal vector to F in $\mathrm{Span}(C_i)$. Bounding the hitting probability therefore boils down to bounding the measure of a shift of the facet F. We know that $\pi(\mathbf{u}) + \tau\pi(\mathcal{B}_2^n) \subset \pi(C_i)$, which means that, letting $h = |\langle \mathbf{n}, \pi(\mathbf{u})\rangle|$, we have $h \geqslant \tau$. For any shift $\mathbf{t} \in \pi(\mathbb{R}^n)$, we have that

$$\begin{aligned}
\int_{F+\mathbf{t}+\mathrm{cone}(\pi(\mathbf{u}))} f(\mathbf{x})\mathrm{d}\mathbf{x} &= \int_0^{+\infty} \int_{F+\mathbf{t}+\frac{r}{h}\sum_{i=1}^{n}\frac{1}{n}\pi(\mathbf{a}_i)} f(\mathbf{x})\mathrm{d}\mathbf{x}\mathrm{d}r \\
&\geqslant \int_0^{+\infty} e^{-\frac{r}{hn}} \int_{F+\mathbf{t}+\frac{r}{h}\sum_{i=2}^{n}\frac{1}{n}\pi(\mathbf{a}_i)} f(\mathbf{x})\mathrm{d}\mathbf{x}\mathrm{d}r \\
&\geqslant \cdots \geqslant \int_{F+\mathbf{t}} f(\mathbf{x})\mathrm{d}\mathbf{x} \int_0^{+\infty} e^{-\frac{r}{h}}\mathrm{d}r \text{ by lemma 14} \\
&= h\int_{F+\mathbf{t}} f(\mathbf{x})\mathrm{d}\mathbf{x} \geqslant \tau \int_{F+\mathbf{t}} f(\mathbf{x})\mathrm{d}\mathbf{x}
\end{aligned}$$

From that we get

$$\begin{aligned}\mathbb{E}[|[\pi(\mathbf{c})+\pi(X),\pi(\mathbf{d})+\pi(X)]\cap\partial\pi(C_i)|] &\leqslant \sum_{F \text{ facet of } \pi(C_i)} \|\mathbf{d}-\mathbf{c}\| \int_0^1 \int_{F-((1-\lambda)\pi(\mathbf{c})+\lambda\pi(\mathbf{d}))} f(\mathbf{x})\mathrm{d}\mathbf{x}\mathrm{d}\lambda \\ &\leqslant \frac{\|\mathbf{d}-\mathbf{c}\|}{\tau}\int_0^1 \sum_{F \text{ facet of } \pi(C_i)} \int_{F-((1-\lambda)\pi(\mathbf{c})+\lambda\pi(\mathbf{d}))+\mathrm{cone}(\mathbf{u})} f(\mathbf{x})\mathrm{d}\mathbf{x} \\ &\leqslant \frac{\|\mathbf{d}-\mathbf{c}\|}{\tau}\int_0^1 \int_{\pi(C_i-((1-\lambda)\mathbf{c}+\lambda\mathbf{d}))} f(\mathbf{x})\mathrm{d}\mathbf{x}\mathrm{d}\lambda\end{aligned}$$

as the $F+\mathrm{cone}(\pi(\mathbf{u}))$ partition the cone $\pi(C_i)$. Therefore

$$\begin{aligned}\mathbb{E}\left[|[\pi(\mathbf{c})+\pi(X),\pi(\mathbf{d})+\pi(X)]\cap\partial\pi(\mathcal{T})|\right] &\leqslant \sum_{i\in I}\mathbb{E}[|[\pi(\mathbf{c})+\pi(X),\pi(\mathbf{d})+\pi(X)]\cap\partial\pi(C_i)|] \\ &\leqslant \frac{\|\mathbf{d}-\mathbf{c}\|}{\tau}\int_0^1 \sum_{i\in I}\int_{\pi(C_i-((1-\lambda)\mathbf{c}+\lambda\mathbf{d}))} f(\mathbf{x})\mathrm{d}\mathbf{x}\mathrm{d}\lambda\end{aligned}$$

We proved in the proof of theorem 7 that the $\pi(C_i)$ are disjoint, therefore so are the $\pi(C_i)-((1-\lambda)\mathbf{c}+\lambda\mathbf{d})$ for any $\lambda\in[0,1]$. Therefore

$$\begin{aligned}\mathbb{E}\left[|[\pi(\mathbf{c})+\pi(X),\pi(\mathbf{d})+\pi(X)]\cap\partial\pi(\mathcal{T})|\right] &\leqslant \frac{\|\mathbf{d}-\mathbf{c}\|}{\tau}\int_0^1 \int_{\bigcup_{i\in I}\pi(C_i-((1-\lambda)\mathbf{c}+\lambda\mathbf{d}))} f(\mathbf{x})\mathrm{d}\mathbf{x}\mathrm{d}\lambda \\ &= \frac{\|\mathbf{d}-\mathbf{c}\|}{\tau}\int_0^1 \mathrm{d}\lambda \leqslant \frac{n}{\delta}\|\mathbf{d}-\mathbf{c}\|\end{aligned}$$

2. Let F be a facet of $\pi(C_i)$, let $\mathbf{n}$ be a unit normal vector to F so that $\langle\pi(\mathbf{u}),\mathbf{n}\rangle>0$. By linearity we have that

$$\mathbb{E}[|[\pi(\mathbf{c})+\pi(X),\pi(\mathbf{c})+\alpha\pi(X)]\cap\partial\pi(C_i)|] = \sum_{F \text{ facet of } C_i}\mathbb{P}[F\cap[\pi(\mathbf{c})+\pi(X),\pi(\mathbf{c})+\alpha\pi(X)]\neq\varnothing].$$

Furthermore,

$$\begin{aligned}\mathbb{P}[F\cap[\pi(\mathbf{c})+\pi(X),\pi(\mathbf{c})+\alpha\pi(X)]\neq\varnothing] &= \mathbb{P}\left[\pi(X)\in\left[1,\frac{1}{\alpha}\right]\cap(F-\pi(\mathbf{c}))\right] \\ &= \int_1^{1/\alpha}\int_{F-r\pi(\mathbf{c})}|\langle\mathbf{n},\pi(\mathbf{c})\rangle| f(\mathbf{x})\mathrm{d}\mathbf{x}\mathrm{d}r\end{aligned}$$

Again, letting $h=|\langle\mathbf{n},\pi(\mathbf{u})\rangle|=\langle\mathbf{n},\pi(\mathbf{u})\rangle\geqslant\tau$ and $\mathbf{t}\in\pi(\mathbb{R}^n)$, we have

$$\begin{aligned}\int_{F+\mathbf{t}+\mathrm{cone}(\pi(\mathbf{u}))}\|\mathbf{x}\|f(\mathbf{x})\mathrm{d}\mathbf{x} &= \int_0^{+\infty}\int_{F+\mathbf{t}+\frac{r}{h}\pi(\mathbf{u})}\|\mathbf{x}\|f(\mathbf{x})\mathrm{d}\mathbf{x}\mathrm{d}r \\ &= \int_0^{+\infty}\int_{F+\mathbf{t}}\left\|\mathbf{x}+\frac{r}{h}\pi(\mathbf{u})\right\| f\left(\mathbf{x}+\frac{r}{h}\pi(\mathbf{u})\right)\mathrm{d}\mathbf{x}\mathrm{d}r \\ &\geqslant \int_0^{+\infty}\int_{F+\mathbf{t}}\left|\left\langle\mathbf{n},\mathbf{x}+\frac{r}{h}\pi(\mathbf{u})\right\rangle\right| e^{-r/h}f(\mathbf{x})\mathrm{d}\mathbf{x}\mathrm{d}r \\ &= \int_0^{+\infty}\int_{F+\mathbf{t}}|\langle\mathbf{n},\mathbf{t}\rangle+r|\, e^{-r/h}f(\mathbf{x})\mathrm{d}\mathbf{x}\mathrm{d}r \\ &= h^2\int_0^{+\infty}\left|\frac{1}{h}\langle\mathbf{n},\mathbf{t}\rangle+r\right| e^{-r}\mathrm{d}r\int_{F+\mathbf{t}}f(\mathbf{x})\mathrm{d}\mathbf{x} \\ &\geqslant \frac{h}{2}|\langle\mathbf{n},\mathbf{t}\rangle|\int_{F+\mathbf{t}}f(\mathbf{x})\mathrm{d}\mathbf{x}\end{aligned}$$

Therefore we have

$$\begin{aligned}\mathbb{E}[|[\pi(\mathbf{c})+\pi(X),\pi(\mathbf{c})+\alpha\pi(X)]\cap\partial\pi(C_i)|] &\leqslant \sum_{F \text{ facet of } \pi(C_i)} \int_1^{1/\alpha} \frac{1}{r}\int_{F-r\pi(\mathbf{c})} |\langle \mathbf{n}, r\pi(\mathbf{c})\rangle| f(\mathbf{x})\mathrm{d}\mathbf{x}\mathrm{d}r \\ &\leqslant \frac{2}{h}\sum_{F \text{ facet of } \pi(C_i)} \int_1^{1/\alpha} \frac{1}{r}\int_{F-r\pi(\mathbf{c})+\mathrm{cone}(\pi(\mathbf{u}))} \|\mathbf{x}\| f(\mathbf{x})\mathrm{d}\mathbf{x}\mathrm{d}r \\ &\leqslant \frac{2}{\tau}\int_1^{1/\alpha}\frac{1}{r}\int_{\pi(C_i)-r\pi(\mathbf{c})} \|\mathbf{x}\| f(\mathbf{x})\mathrm{d}\mathbf{x}\mathrm{d}r\end{aligned}$$

Therefore

$$\begin{aligned}\mathbb{E}[|[\pi(\mathbf{c})+\pi(X),\pi(\mathbf{c})+\alpha\pi(X)]\cap\partial\pi(\mathcal{T})|] &\leqslant \sum_{i\in I}\mathbb{E}[|[\pi(\mathbf{c})+\pi(X),\pi(\mathbf{c})+\alpha\pi(X)]\cap\partial\pi(C_i)|] \\ &\leqslant \frac{2}{\tau}\sum_{i\in I}\int_1^{1/\alpha}\frac{1}{r}\int_{\pi(C_i)-r\pi(\mathbf{c})}\|\mathbf{x}\| f(\mathbf{x})\mathrm{d}\mathbf{x}\mathrm{d}r \\ &\leqslant \frac{2n}{\delta}\int_1^{1/\alpha}\frac{1}{r}\int_{\bigcup_{i\in I}\pi(C_i)-r\pi(\mathbf{c})}\|\mathbf{x}\| f(\mathbf{x})\mathrm{d}\mathbf{x}\mathrm{d}r \text{ as } \pi(C_i) \text{ are disjoint} \\ &\leqslant \frac{2n}{\delta}\int_1^{1/\alpha}\frac{1}{r}\mathbb{E}[\|X\|]\mathrm{d}r \leqslant \frac{2nm}{\delta}\ln\left(\frac{1}{\alpha}\right) \text{ as } \mathbb{E}[\|X\|]\leqslant\sum_{i=1}^m\mathbb{E}[\lambda_i]\leqslant m.\end{aligned}$$

□

Remark.
- By choosing the cone-exponential distribution, we lose a factor m on the second bound.
- The projector π is useful when inducting on the dimension.

Theorem 9. *If P satisfies the local δ-distance property, the expected number of shadow simplex pivots in* **Algorithm 2** *is $O\left(\frac{n^2 m}{\delta}\ln\left(\frac{m}{\delta}\right)\right)$.*

Proof. The proof is the same as for theorem 7, the theorem 8 giving all the necessary bounds on the number of crossings. However, as $\|X\|$ is now bounded by m, we have to take $\varepsilon = O\left(\frac{\delta}{m}\right)$. □

Remark. The big difference with **Algorithm 1** is that **Algorithm 2** takes as an input a polyhedron P potentially unbounded. As X is sampled inside the cones, we can follow the Shadow Simplex. This is done at a cost of $O\left(\frac{m\ln(m/\delta)}{n\ln(n/\delta)}\right)$ on the number of shadow simplex pivots.

Acknowledgements

I want to thank Daniel Dadush for following me during all the internship. I also want to thank (and congrats again) Dr. Sophie Huiberts, discussing with her enabled me to see clearly where I did not.

References

[1] Daniel Dadush, Oded Regev, and Noah Stephens-Davidowitz. On the closest vector problem with a distance guarantee. In *2014 IEEE 29th Conference on Computational Complexity (CCC)*, pages 98–109. IEEE, 2014.

[2] Divesh Aggarwal, Daniel Dadush, Oded Regev, and Noah Stephens-Davidowitz. Solving the shortest vector problem in 2n time using discrete gaussian sampling. In *Proceedings of the forty-seventh annual ACM symposium on Theory of computing*, pages 733–742, 2015.

[3] Divesh Aggarwal and Noah Stephens-Davidowitz. Just Take the Average! An Embarrassingly Simple 2^n-Time Algorithm for SVP (and CVP). *arXiv preprint arXiv:1709.01535*, 2017.

[4] Naftali Sommer, Meir Feder, and Ofir Shalvi. Finding the closest lattice point by iterative slicing. *SIAM Journal on Discrete Mathematics*, 23(2):715–731, 2009.

[5] Daniele Micciancio and Panagiotis Voulgaris. Faster exponential time algorithms for the shortest vector problem. In *Proceedings of the twenty-first annual ACM-SIAM symposium on Discrete Algorithms*, pages 1468–1480. SIAM, 2010.

[6] Daniel Dadush and Nicolas Bonifas. Short paths on the Voronoi graph and closest vector problem with preprocessing. In *Proceedings of the Twenty-Sixth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 295–314. SIAM, 2014.

[7] Francisco Santos. A counterexample to the hirsch conjecture. *Annals of mathematics*, pages 383–412, 2012.

[8] Denis Naddef. The hirsch conjecture is true for (0, 1)-polytopes. *Mathematical Programming: Series A and B*, 45(1):109–110, 1989.

[9] Michel L Balinski. The hirsch conjecture for dual transportation polyhedra. *Mathematics of Operations Research*, 9(4):629–633, 1984.

[10] Norman Zadeh. What is the worst case behavior of the simplex algorithm. *Polyhedral computation*, 48:131–143, 2009.

[11] Tobias Brunsch and Heiko Röglin. Finding short paths on polytopes by the shadow vertex algorithm. In *International Colloquium on Automata, Languages, and Programming*, pages 279–290. Springer, 2013.

[12] Daniele Micciancio and Shafi Goldwasser. *Complexity of lattice problems: a cryptographic perspective*, volume 671. Springer Science & Business Media, 2002.

[13] Daniel Dadush and Nicolai Hähnle. On the shadow simplex method for curved polyhedra. *Discrete & Computational Geometry*, 56(4):882–909, 2016.

Travel experiences

Before going to Amsterdam, I worked from Paris for around three weeks, as the Covid restrictions would not have allowed me to go to the lab more than twice a week. I went to Amsterdam at the beginning of March. There, I was living in a room whose landlord CWI put me in relation with. As it is often hard and expensive to find a place in Amsterdam, I was glad to find something so easily. I was at five minutes walking from the lab, so it was really easy to go there, even if I could also work from home due to Covid restrictions.
I was surprised to see that most of the people there were either PHD students or postdocs : for a team of approximately 20 people, only 3 were senior researchers. It made the integration easy, as they had almost the same background as I did.
During my internship, I also followed a course about Algorithmic Game Theory, given by Prof. Dr. Guido Schäfer, who was also a member of the team. This course had no relation with the topic I was studying, but it was interesting to discover.