

Counting integer points in polyhedra

Siddharth Bhat

June 22nd, 2018

Definitions

- ▶ Polyhedra: $\{\vec{x} \in \mathbb{Q}^d \mid A\vec{x} \leq \vec{b}\}$
- ▶ Polytope: bounded polyhedra.
- ▶ Cone: $\text{cone}(\vec{u}_i) = \left\{ \sum_i \lambda_i \vec{u}_i \mid \lambda_i \geq 0 \right\}$, $\vec{u}_i \in \mathbb{Q}^d$
- ▶ Simple cone: $SK = \text{cone}(\vec{u}_i)$, $\vec{u}_i \in \mathbb{Z}^d$, \vec{u}_i are linearly independent.
- ▶ Unimodular cone: $UK = \text{cone}(\vec{u}_i)$, $\text{Volume}(\vec{u}_i) = 1$
- ▶ Line: subspace.

Pictures of defintions!

- ▶ polytope



- ▶ cone



- ▶ polyhedra



Example 1: valuation of line

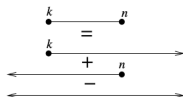
- ▶ P is a polyhedra, then $\mathcal{F}([P]) = \sum_{\vec{m} \in P \cap \mathbb{Z}^d} (x^{\vec{m}})$
- ▶ $\mathcal{F}([P])(\vec{1}) = \text{number of points.}$

$$\mathcal{F}((-\infty, \infty)) = \sum_{i \in \mathbb{Z}} x^i$$

$$\begin{aligned}\text{count}(x) &= \mathcal{F}((-\infty, \infty)) \\ &= \mathcal{F}((-\infty, 0]) + \mathcal{F}([0, \infty)) - \mathcal{F}(0) \\ &= (\dots + x^{-2} + x^{-1} + x^0) + (x^0 + x^1 + x^2 + \dots) - x^0 \\ &= \frac{1}{1 - \frac{1}{x}} + \frac{1}{1 - x} - 1 \\ &= \frac{-x}{1 - x} + \frac{1}{1 - x} = \frac{1 - x}{1 - x} - 1 = 0\end{aligned}$$

- ▶ number of points in a line is 0!

Example 2: valuation of interval



$$\begin{aligned}\text{count}(x) &= \mathcal{F}([0, n]) = \mathcal{F}([k, \infty)) + \mathcal{F}((-\infty, n]) - \mathcal{F}((\infty, \text{infy})) \\ &= (x^k + x^{k+1} + \dots) + \\ &\quad (\dots + x^{n-2} + x^{n-1} + x^n) + \\ &\quad (\dots + x^{-2} + x^{-1} + x^0 + x^1 + \dots) \\ &= \frac{x^k}{1-x} + \frac{x^n}{1-x^{-1}} + 0 \\ &= \frac{x^k - x^{n+1}}{1-x}\end{aligned}$$

$$\text{count}(1) = \text{L'hospital} = (n+1) - k = n - k + 1$$

Proof outline

- ▶ Algebra of polyhedra, $P(\mathbb{Q}^d)$
- ▶ $[] : \mathbb{Q}^d \rightarrow P(\mathbb{Q}^d)$
- ▶ Existence of $\mathcal{F} : P(\mathbb{Q}^d) \rightarrow \mathbb{C}(x)$, such that:
 - ▶ \mathcal{F} is linear
 - ▶ P is a polyhedra, then $\mathcal{F}([P]) = \sum_{\vec{m} \in P \cap \mathbb{Z}^d} (x^{\vec{m}})$
 - ▶ $\mathcal{F}([\text{line}]) = 0$ (important, allows modulo line decompositions)
- ▶ $\mathcal{F}(P)(1) = \text{number of points in } P$
- ▶ reduction: \mathcal{F} for cones gives full \mathcal{F}
- ▶ reduction: \mathcal{F} for simple cones gives \mathcal{F} for cones
- ▶ performance: \mathcal{F} for unimodular cones gives \mathcal{F} for simple cones

Caveats

- ▶ Self taught :)
- ▶ Do not understand subtleties of convergence arguments (how is evaluating at $\vec{1}$ correct?).
- ▶ No intuition for LLL, Lattice reduction.

Assuming \mathcal{F} for cones, derive full \mathcal{F} : Part 1 (Polytopes)

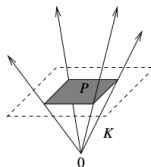


FIGURE 66. A polytope $P \subset \mathbb{R}^d$ and a cone $K \subset \mathbb{R}^{d+1}$ based on P .

- Write polytope as intersection of hyperplane + cone.
- $\mathcal{F}(\text{polytope}) = (\frac{d}{dx_{d+1}} \mathcal{F}(\text{cone}))(\langle \vec{1}^d, 0 \rangle)$
- $\mathcal{F}(\text{cone}) = x_{d+1}^0(\dots) + x_{d+1}(\text{POLYTOPE}) + x_{d+1}^2(\dots) + \dots$
- $\frac{d}{dx_d} \mathcal{F}(\text{cone}) = 0 + 0 \cdot (\dots) + 1 \cdot \text{POLYTOPE} + 2x_{d+1}(\dots) + \dots$
- $\frac{d}{dx_d} \mathcal{F}(\text{cone})(\langle \vec{1}^d, 0 \rangle) = \text{POLYTOPE}(\vec{1}) + 2 \cdot 0 \cdot (\dots) + \dots$
- $\frac{d}{dx_d} \mathcal{F}(\text{cone})(\langle \vec{1}^d, 0 \rangle) = \text{POLYTOPE}(\vec{1})$

Assuming \mathcal{F} for cones, derive full \mathcal{F} : Part 2 (Lines)

- ▶ Line = $\sum_{\text{dimension}} \text{cone} + \text{cone} - \text{point}$.
- ▶ Since line can be translated:

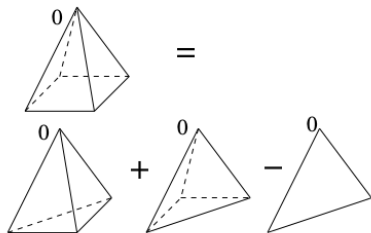
$$\begin{aligned}\forall \vec{x} \in L, L &= \vec{x} + L \\ \forall x \in L, \mathcal{F}(L) &= \mathcal{F}(L) + \mathcal{F}(\vec{x}) \\ \mathcal{F}(L) &= 0\end{aligned}$$

$$\begin{aligned}\text{count}(x) &= \mathcal{F}((-\infty, \infty)) \\ &= (\dots + x^{-2} + x^{-1} + x^0) + (x^0 + x^1 + x^2 + \dots) - x^0 \\ &= \frac{1}{1 - \frac{1}{x}} + \frac{1}{1 - x} - 1\end{aligned}$$

- ▶ In 1-d example, radius of convergence of left and right cone was 0
- ▶ Is this really well-defined? (what is this ring which admits $f(x) = \dots + x^{-1} + x^0 + x^1 + \dots$)

Assuming \mathcal{F} for simple cone, derive for cone

- ▶ Simple cone: $SK = co(u_i) = \{\sum_i \lambda_i u_i | \lambda_i \geq 0\}$, $u_i \in \mathbb{Z}^d$, u_i are linearly independent.
- ▶ Cone: $C = co(u_i)$, $u_i \in \mathbb{Q}^d$
- ▶ inclusion exclusion: decompose cone into simple cones.



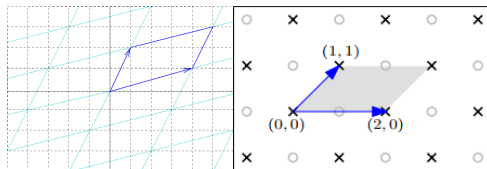
\mathcal{F} for simple cones: Part 1

- ▶ Consider the positive orthant in 3D: $P \subset \mathbb{Q}^3 = \{(x, y, z) \mid x, y, z \geq 0\}$
- ▶ $P = \text{cone}((1, 0, 0), (0, 1, 0), (0, 0, 1))$
- ▶ this is a simple cone, and here's how we count it:

$$\begin{aligned}\mathcal{F}([P]) &= \sum_{i,j,k \in [0, \infty)} x^i y^j z^k \\ &= \sum_{i=0}^{\infty} x^i \left(\sum_{j=0}^{\infty} y^j \left(\sum_{k=0}^{\infty} z^k \right) \right) \\ &= \frac{1}{1-x} \cdot \frac{1}{1-y} \cdot \frac{1}{1-z}\end{aligned}$$

\mathcal{F} for simple cones: Part 2

- ▶ General story is similar
- ▶ $SK = co(u_i)$, u_i linearly independent.
- ▶ Since u_i is linearly independent, some points $\vec{x} \in cone(u_i)$ have unique representation $\vec{x} = \sum_i \lambda_i u_i$, $\lambda_i \in \mathbb{Z}$
- ▶ fundamental parallelepiped (Π) will tile the plane.
- ▶ We can count the \vec{x} , and make \vec{x} responsible for the "tile" of skipped points.



$$\mathcal{F}(SK) = \underbrace{\left(\sum_{\vec{p} \in \Pi \cap \mathbb{Z}^d} x^{\vec{p}} \right)}_{\text{per-tile points}} \underbrace{\prod_i \frac{1}{1 - x^{u_i}}}_{\text{tile starting point } \vec{x}}$$

Performance - How?

- Write simple cone as sum of unimodular cones:

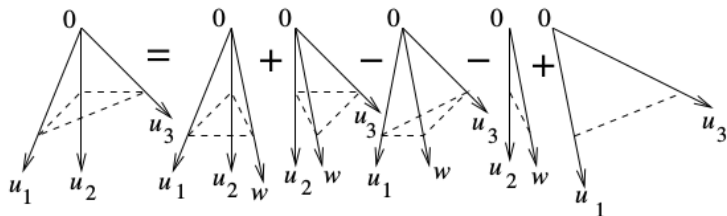
$$[K] = \sum_i \alpha_i [K_i] + \text{lower dimensional cones}$$

- We concentrate on $\sum_i \alpha_i [K_i]$

$\alpha_i \in \{-1, 1\}$ and K_i are unimodular.

- Lower dimensional cones are taken care of by a trick.

Unimodular decomposition of a simple cone K : Part 1



Unimodular decomposition of simple cone K : Part 2

- ▶ $\text{Index}(K) = \text{Volume}(\Pi(K))$

$\text{Index}(K) = 1 \leftrightarrow K$ is unimodular. $\text{Index}(K)$ is a measure of non-unimodularity.

- ▶ Introduce procedure which takes **polynomial steps** to **reduce $\text{Index}(K)$**
- ▶ Let $K = \text{cone}(u_1, u_2, \dots, u_d)$, $u_i \in \mathbb{Z}^d$, u_i are linearly independent.
- ▶ High level idea:
 - ▶ Pick a non-zero integer point p .
 - ▶ create d new "potential basis sets",
 $\text{PotentialBasis}_j = \{u_1, u_2, \dots, u_d\} \setminus \{u_j\} \cup \{p\}$
 - ▶ make $\text{Basis}_j = \text{LLL}(\text{PotentialBasis}_j)$ (+ ellided details)
 - ▶ make new cones, $K_i = \text{cone}(\text{Basis}_j)$ and show that $\text{Index}(K_i) < \text{Index}(K)$
 - ▶ $K = \sum \alpha_i K_i$ + faces of K_i
 - ▶ show that $\text{Index}(K_i)$ reduces by a large enough factor that poly rounds are enough to reduce to 1

Decomposition example

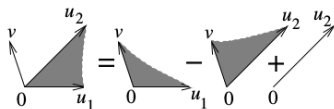
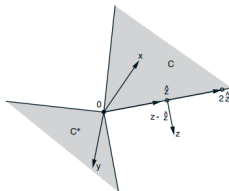


Figure 20. Writing the cone as a linear combination of cones with smaller indices

Polar trick

- Polar:

$$P^\circ = \left\{ \vec{y} \in \mathbb{Q}^d : \forall \vec{p} \in P, \vec{p} \cdot \vec{y} \geq 0 \right\}$$



- Lower dimensional cones do not matter. First take $[K^\circ]$, then compute unimodular decomposition of this:

$$[K^\circ] = \sum_i \alpha_i [K_i] + \text{lower dimensional cones}$$

$$[(K^\circ)^\circ] = [K] = \sum_i \alpha_i K_i + \text{cones with lines}$$

$$\mathcal{F}([K]) = \sum_i \alpha_i \mathcal{F}(K_i) + \mathcal{F}(\text{cones with lines}) = \sum_i \alpha_i \mathcal{F}(K_i) + 0$$

References

- ▶ Lattice Points, Polyhedra, and Complexity: Alexander Barvinok
- ▶ Integer points in polyhedra: Alexander Barvinok

Thanks!

Questions?

Minkowski convex body theorem

- ▶ Statement: Convex set $P \subset \mathbb{R}^d$, which is symmetric with respect to the origin ($\forall x \in P, -x \in P$), has volume greater than or equal to 2^d contains a non-zero integer point.
- ▶ Recap: Let $K = \text{cone}(u_1, u_2, \dots, u_d)$, $u_i \in \mathbb{Z}^d$, u_i are linearly independent.
 - ▶ Pick a non-zero integer point p in K (why does this integer point exist?).
- ▶ Construct

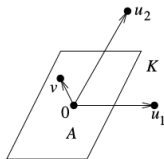
$$\Pi_0 = \left\{ \sum_i \alpha_i u_i : |\alpha_i| \leq \frac{1}{\sqrt[d]{\text{Index}(K)}} \right\}$$

- ▶ Symmetric
 - ▶ Length per axis: $\frac{2|u_i|}{\sqrt[d]{\text{Index}(K)}}$
- ▶ Total volume:

$$\begin{aligned} \text{Volume}(\Pi_0) &= \prod_{i=1}^d \frac{2|u_i|}{\sqrt[d]{\text{Index}(K)}} \\ &= 2^d \frac{\prod_{i=1}^d |u_i|}{\text{Index}(K)} = 2^d \end{aligned}$$

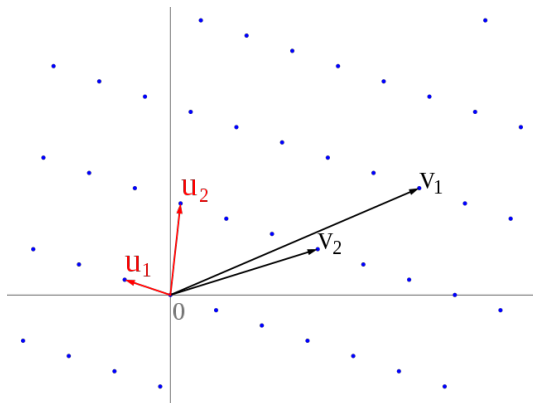
- ▶ Hence, by Minkowski convex body, we find a point $p \in \mathbb{Z}^d$ in Π_0 . If this point is in the wrong direction (facing outward), pick $-p$.

Minkowski convex body theorem example



LLL (Lenstra–Lenstra–Lovász lattice basis reduction)

- ▶ Given an arbitrary basis $u_i \in \mathbb{Z}^d$ of a lattice, produces a new basis which is "nicer".
- ▶ New basis consists of shorter vectors that are "more orthogonal"
- ▶ Runs in polynomial time.
- ▶ Determining *shortest basis* is hard - used in cryptosystems IIUC.



- ▶ Black is input, red is output.

Using LLL

- ▶ High level idea:
 - ▶ Pick a non-zero integer point p .
 - ▶ create d new "potential basis sets",
 $\text{PotentialBasis}_j = \{u_1, u_2, \dots, u_d\} \setminus \{u_j\} \cup \{p\}$
 - ▶ make $\text{Basis}_j = \text{LLL}(\text{PotentialBasis}_j)$ (+ ellided details)

Assuming \mathcal{F} for cones, derive full \mathcal{F} : Part 1.2 (Polytopes)

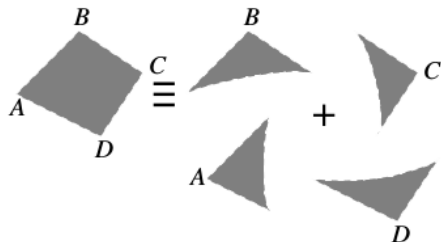


FIGURE 36. Representing the interior of a polytope as the sum of the interiors of its tangent cones at the vertices modulo polyhedra with lines.