

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

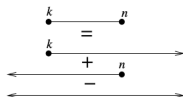
- ▶ P is a polyhedra, then $\mathcal{F}([P]) = \sum_{\vec{m} \in P \cap \mathbb{Z}^d} (x^{\vec{m}})$
- ▶ $\mathcal{F}([P])(\vec{1}) = \text{number of points.}$

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

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

- ▶ 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

Caveats

- ▶ 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)

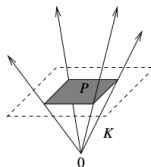


FIGURE 66. A polytope $P \subset \mathbb{R}^d$ and a cone $K \subset \mathbb{R}^{d+1}$ based on P .

- 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)

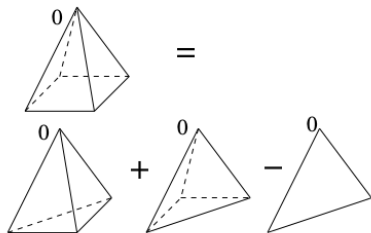
- ▶ Line = cone + cone - point.
- ▶ Since line can be translated, $\forall \vec{x} \in L, L = \vec{x} + L$
 - ▶ $\forall x \in L, \mathcal{F}(L) = \mathcal{F}(L) + \mathcal{F}(\vec{x})$
 - ▶ $\mathcal{F}(L) = 0$

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

- ▶ 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

\mathcal{F} for simple cones: Part 2

References

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

Thanks!

Questions?

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

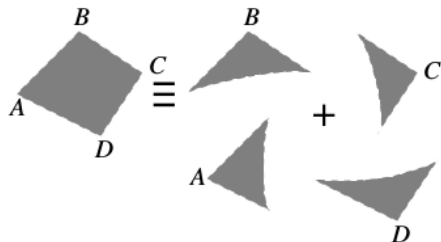


FIGURE 36. Representing the interior of a polytope as the sum of the interiors of its tangent cones at the vertices modulo polyhedra with lines.