Some quick formulas for the volumes of and the number of integer points in higher-dimensional polyhedra

Alexander Barvinok, based joint works with J.A. Hartigan and Mark Rudelson

August 2023

The problem

Let $P \subset \mathbb{R}^n$ be a polyhedron defined by the system of linear equations $Ax = b$ and inequalities $x \geq 0$. Here A is an $m \times n$ matrix with $\operatorname{rank} A = m < n$.

Suppose that P is bounded and has a non-empty relative interior, that is, contains a point $x = (x_1, \ldots, x_n)$ where $x_j > 0$ for $j = 1, \ldots, n$.

Our goal is to estimate quickly $\operatorname{vol} P$, the $(n - m)$-dimensional volume of P. When A and b are integer, we also want to estimate quickly $|P \cap \mathbb{Z}^n|$, the number of integer points in P.

The entropy maximization problem

We define $f : \mathbb{R}^n_+ \longrightarrow \mathbb{R}$ by

$$f(x) = n + \sum_{j=1}^{n} \ln x_j \quad \text{where} \quad x = (x_1, \ldots, x_n)$$

and find the necessarily unique $z \in P$, $z = (z_1, \ldots, z_n)$, such that

$$f(z) = \max_{x \in P} f(x).$$

The point z is called the *analytic center* of P. Since $\operatorname{relint} P \neq \emptyset$, we have $z_j > 0$ for $j = 1, \ldots, n$.

The formula

Given a bounded polyhedron P defined by the system $Ax = b$, $x \geq 0$, we compute its analytic center $z = (z_1, \ldots, z_n)$. Let B be the $m \times n$ matrix obtained by multiplying the j-th column of A by z_j for $j = 1, \ldots, n$. Then

$$\mathcal{E}(A, b) = e^{f(z)} \frac{\sqrt{\det AA^T}}{\sqrt{\det BB^T}} = e^n z_1 \cdots z_n \frac{\sqrt{\det AA^T}}{\sqrt{\det BB^T}}$$

approximates $\operatorname{vol} P$ within a multiplicative factor of γ^m, where $\gamma > 0$ is an absolute constant.

Note that it scales correctly:

$$\mathcal{E}(A, \tau b) = \tau^{n-m} \mathcal{E}(A, b) \quad \text{for} \quad \tau > 0.$$

Example: simplex

Example

Suppose that P is defined by

$$\sum_{j=1}^{n} a_j x_j = n \quad \text{and} \quad x_j \geq 0 \quad \text{for} \quad j = 1, \ldots, n.$$

We must have $a_j > 0$ for $j = 1, \ldots, n$. Then

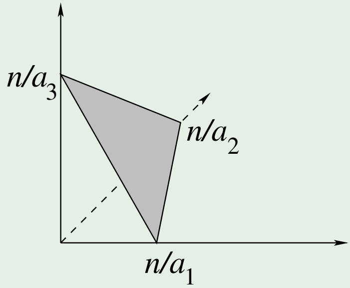
$$z = \left(\frac{1}{a_1}, \ldots, \frac{1}{a_n} \right) \quad \text{and} \quad \mathcal{E}(A, b) = \frac{e^n}{a_1 \cdots a_n} \frac{\sqrt{a_1^2 + \ldots + a_n^2}}{\sqrt{n}}.$$

On the other hand,

$$\mathrm{vol}\ P = \frac{n^n}{n! a_1 \cdots a_n} \sqrt{a_1^2 + \ldots + a_n^2}.$$

Example: simplex

Example



Since

$$n! = \sqrt{2\pi n}e^{-n}n^n\left(1 + o(1)\right) \quad \text{as} \quad n \longrightarrow +\infty,$$

we get

$$\mathrm{vol}\ P = \frac{1}{\sqrt{2\pi}}\mathcal{E}(A, b)\left(1 + o(1)\right) \quad \text{as} \quad n \longrightarrow +\infty.$$

Example: doubly stochastic matrices

Example

Consider the polytope P_r of $r \times r$ doubly stochastic matrices $X = (x_{ij})$:

$$\sum_{j=1}^{r} x_{ij} = 1 \quad \text{for} \quad i = 1, \ldots, r, \quad \sum_{i=1}^{r} x_{ij} = 1 \quad \text{for} \quad j = 1, \ldots, r$$

$$\text{and} \quad x_{ij} \geq 0 \quad \text{for} \quad i, j = 1, \ldots, r.$$

*	*	*	*
*	*	*	*
*	*	*	*
*	*	*	*

Example: doubly stochastic matrices

Example

We have $\dim P_r = (r-1)^2$. By symmetry, the analytic center is

$$z_{ij} = \frac{1}{r} \quad \text{for} \quad i, j = 1, \ldots, r \quad \text{and hence} \quad \mathcal{E}(A, b) = \frac{e^{r^2}}{r^{(r-1)^2}}.$$

Canfield and McKay (2009) proved that

$$\operatorname{vol} P_r = e^{1/3} \frac{e^{r^2}}{(\sqrt{2\pi})^{2r-1} r^{(r-1)^2}} (1 + o(1)) \quad \text{as} \quad r \longrightarrow +\infty.$$

In Barvinok and Hartigan (2010), we called

$$\operatorname{vol} P \approx \frac{\mathcal{E}(A, b)}{(2\pi)^{m/2}}$$

Gaussian approximation and showed that it holds under some conditions (more on this later).

Example: 3-way planar transportation polytopes

Example

Consider the polytope P_r of $r \times r \times r$ arrays (tensors) $X = (x_{ijk})$ such that

$$\sum_{i=1}^{r} x_{ijk} = 1 \quad \text{for} \quad j, k = 1, \ldots, r,$$

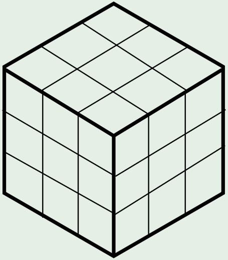
$$\sum_{j=1}^{r} x_{ijk} = 1 \quad \text{for} \quad i, k = 1, \ldots, r,$$

$$\sum_{k=1}^{r} x_{ijk} = 1 \quad \text{for} \quad i, j = 1, \ldots, r \quad \text{and}$$

$$x_{ijk} \geq 0 \quad \text{for} \quad i, j, k = 1, \ldots, r.$$

Example: 3-way planar transportation polytopes

Example



Then $\dim P_r = (r-1)^3$. By symmetry,

$$z_{ijk} = \frac{1}{r} \quad \text{for} \quad i, j, k = 1, \ldots, r \quad \text{and hence} \quad \mathcal{E}(A, b) = \frac{e^{r^3}}{r^{(r-1)^3}}$$

approximates $\operatorname{vol} P_r$ within a factor of $e^{O(r^2)}$ as $r \longrightarrow +\infty$.

The main theorem (with M. Rudelson)

Theorem

- *Let* $\alpha_0 \approx 1.398863726$ *be the necessarily unique number in the interval* $(1, +\infty)$ *satisfying*

$$\frac{1}{2\pi}\int_{-\infty}^{+\infty}(1+s^2)^{-\alpha_0/2}\,ds = 1.$$

  Then

$$\operatorname{vol} P \ \leq\ \alpha_0^{m/2}\mathcal{E}(A,b)\ \leq\ (1.183)^m\mathcal{E}(A,b).$$

- *We have*

$$\operatorname{vol} P \ \geq \frac{2\Gamma\left(\frac{m+2}{2}\right)}{\pi^{m/2}e^{(m+2)/2}(m+2)^{m/2}}\mathcal{E}(A,b)$$

$$\approx \left(\frac{1}{e\sqrt{2\pi}}\right)^m \approx (0.14)^m\mathcal{E}(a,b).$$

The main theorem

In fact, we can prove

$$\operatorname{vol} P \ \geq \ \gamma^m \mathcal{E}(A, b)$$

for any

$$\gamma < \frac{1}{\sqrt{2\pi e}} \approx 0.24$$

and sufficiently large m. The proof requires thin shell estimates (Klartag 2007, Chen 2021, Klartag and Lehec 2022), although pretty much any non-trivial estimate will do.

Ideas of the proof: the maximum entropy distribution

Recall that a random variable X is standard exponential, if its density is

$$p_X(t) = \begin{cases} e^{-t} & \text{if } t > 0 \\ 0 & \text{if } t \leq 0. \end{cases}$$

The following lemma was proved in Barvinok and Hartigan (2010):

Lemma

Let $X_1, \ldots, X_n$ be independent standard exponential random variables and let $z = (z_1, \ldots, z_n)$ be the analytic center of P. Then the density of the random vector $(z_1 X_1, \ldots, z_n X_n)$ is constant on P and equal to

$$e^{-f(z)} = \frac{e^{-n}}{z_1 \cdots z_n}.$$

Ideas of the proof: the maximum entropy distribution

The proof is an exercise with Lagrange multipliers. A "deeper" reason why it works is that the distribution of $(z_1 X_1, \ldots, z_n X_n)$ is the maximum entropy distribution among all distributions supported on $\mathbb{R}^n_+$ and with expectation in the affine subspace $Ax = b$.

Corollary

Let $a_1, \ldots, a_n$ be the columns of A, so $A = [a_1, \ldots, a_n]$ and let

$$Y = \sum_{j=1}^{n} z_j X_j a_j = \sum_{j=1}^{n} X_j b_j \quad \textit{where} \quad B = [b_1, \ldots, b_n].$$

Then

$$\operatorname{vol} P = e^{f(z)} \sqrt{\det AA^T} p_Y(b),$$

where p is the density of Y.

Note that

$$\mathbf{E}\, Y = b \quad \text{and} \quad \mathbf{Cov}\, Y = BB^T.$$

Example: Simplex

Example

Suppose that P is defined by

$$\sum_{j=1}^{n} a_j x_j = n \quad \text{and} \quad x_j \geq 0 \quad \text{for} \quad j = 1, \ldots, n.$$

$$\text{We have} \quad z_j = \frac{1}{a_j} \quad \text{for} \quad j = 1, \ldots, n \quad \text{and} \quad Y = \sum_{j=1}^{n} X_j.$$

Hence

$$p_Y(t) = \begin{cases} \frac{t^n}{n!} e^{-t} & \text{if } t > 0 \\ 0 & \text{if } t \leq 0. \end{cases}$$

Then

$$e^{f(z)} \sqrt{\det AA^T} p_Y(b) = \frac{n^n}{n! a_1 \cdots a_n} \sqrt{a_1^2 + \ldots + a_n^2} = \mathrm{vol}\ P.$$

Ideas of the proof: log-concave isotropic densities

The density p_Y of Y is log-concave, and we are interested in $p_Y(b)$ where $\mathbf{E}\, Y = b$. Furthermore, there is some freedom in choosing A:

$$A \longmapsto WA, \quad b \longmapsto Wb \quad \text{and} \quad B \longmapsto WB,$$

where W is an $m \times m$ invertible matrix. Then

$$AA^T \longmapsto W(AA^T)W^T, \quad B \longmapsto W(BB^T)W^T$$

and

$$\frac{\sqrt{\det AA^T}}{\sqrt{\det BB^T}}$$

does not change. Hence we can assume that $BB^T = I$ and

$$\mathbf{Cov}\, Y = I.$$

Ideas of the proof: log-concave isotropic densities

The proof for the lower bound of $p_Y(b)$: applies to all log-concave isotropic densities.
The proof for the upper upper bound of $p_Y(b)$ uses the formula for the characteristic function of Y:

$$\phi_Y(t) = \prod_{j=1}^{n} \frac{1}{1 - \sqrt{-1}\langle b_j, t\rangle}$$

and is inspired by the proof of Ball (1989) of the upper bound for the volume of a section of the cube (but easier).

The Gaussian formula

Recall the corollary: if $X_1, \ldots, X_n$ are independent standard exponential,

$$Y = \sum_{j=1}^{n} z_j X_j a_j = \sum_{j=1}^{n} X_j b_j,$$

then $\mathrm{vol}\ P = e^{f(z)} \sqrt{\det AA^T}\, p_Y(b)$. In addition,

$$\mathbf{E}\, Y = b \quad \text{and} \quad \mathbf{Cov}\, Y = BB^T.$$

It stands to reason that, being a sum of independent random variables, Y is close to Gaussian, and hence

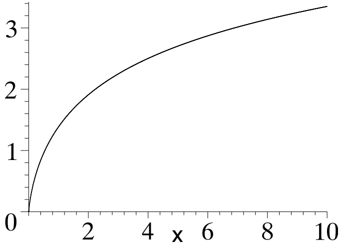
$$p_Y(b) \approx \frac{1}{(2\pi)^{m/2}\sqrt{\det BB^T}} \quad \text{and} \quad \mathrm{vol}\, P \approx \frac{e^{f(z)}\sqrt{\det AA^T}}{(2\pi)^{m/2}\sqrt{\det BB^T}}.$$

Barvinok and Hartigan (2010, 2012) showed that this indeed holds asymptotically for some families of polyhedra, sometimes with the "Edgeworth correction" factor (like $e^{1/3}$ for the polytope of doubly stochastic matrices).

Counting integer points: the Gaussian formula

Suppose we want to count integer points in $P = \{x \geq 0 : Ax = b\}$ (assume that A and b are integer). Consider the function

$$g(x) = (x+1)\ln(x+1) - x\ln x \quad \text{for} \quad x \geq 0.$$



Remark: $g(x)$ is the maximum entropy of a probability distribution (necessarily geometric) on $\mathbb{Z}_+$ with expectation x:

$$\mathbf{P}(X = k) = pq^k \quad \text{for} \quad k = 0, 1, \ldots ;$$

$$\mathbf{E}\, X = \frac{q}{p} := x, \quad \mathbf{var}\, X = \frac{q}{p^2} = x + x^2.$$

Counting integer points: the Gaussian formula

In Barvinok and Hartigan (2010), we prove:

Lemma

Let $z = (z_1, \ldots, z_n)$ be the necessarily unique point where the concave function

$$g(x) = \sum_{j=1}^{n} g(x_j) \quad \text{for} \quad x = (x_1, \ldots, x_n)$$

attains its maximum on P. Let $X = (X_1, \ldots, X_n)$ be the vector of independent geometric random variables with

$$\mathbf{E}(X_j) = z_j \quad \text{for} \quad j = 1, \ldots, n.$$

Then the probability mass function of X is constant on the points $P \cap \mathbb{Z}^n$ and equal to $e^{-g(z)}$.

Counting integer points: the Gaussian formula

The distribution of X is the maximum entropy distribution supported on $\mathbb{Z}_+^n$ and with expectation in the affine subspace $Ax = b$.

Let $a_1, \ldots, a_n$ be the columns of A. We let

$$Y = \sum_{j=1}^{n} X_j a_j$$

and conclude that

$$|P \cap \mathbb{Z}^n| = e^{g(z)} \mathbf{P}(Y = b).$$

Given an $m \times n$ matrix $A = (a_{ij})$ with $\operatorname{rank} A = m < n$, we compute the $m \times m$ matrix $B = (b_{ij})$ by

$$b_{ij} = \sum_{k=1}^{n} a_{ik} a_{jk} \left(z_k + z_k^2 \right),$$

so that $\mathbf{E}\, Y = b$ and $\mathbf{Cov}\, Y = B$.

Counting integer points: the Gaussian formula

Assuming that Y is close to Gaussian, we get the following estimate for $|P \cap \mathbb{Z}^n|$, where $P = \{x \geq 0 : \; Ax = b\}$:

$$\mathcal{E}_I = \frac{e^{g(z)} \det \Lambda}{(2\pi)^{m/2} \sqrt{\det B}},$$

where $\Lambda \subset \mathbb{Z}^m$ is the lattice generated by the columns of A. In a similar way, we can get an estimate for the number of 0-1 points in P. The function g is replaced by

$$h(x) = x \ln \frac{1}{x} + (1-x) \ln \frac{1}{1-x} \quad \text{for} \quad 0 \leq x \leq 1$$

and B is computed as follows:

$$b_{ij} = \sum_{k=1}^{n} a_{ik} a_{jk} \left(z_k - z_k^2\right).$$

The Gaussian formula for integer points: example

Example

The number of 4×4 non-negative integer matrices with row sums $[220, 215, 93, 64]$ and column sums $[108, 286, 71, 127]$ is $1,225,914,276,768,514 \approx 1.2 \times 10^{15}$ (Diaconis and Efron, 1985). The value of $\mathcal{E}_I(A, b)$ approximates it within relative error of 0.06 (De Loera, 2009).

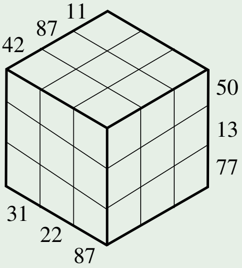
	108	286	71	127
220	*	*	*	*
215	*	*	*	*
93	*	*	*	*
64	*	*	*	*

Here Y is a sum of 16 independent 7-vectors.

The Gaussian formula for integer points: example

Example

The number of $3 \times 3 \times 3$ non-negative integer arrays with slice sums $[31, 22, 87], [50, 13, 77]$ and $[42, 97, 11]$ is $8,846,838,772,161,591 \approx 8.8 \times 10^{15}$. The value of $\mathcal{E}_I(A, b)$ approximates it within relative error 0.002 (De Loera 2009).



Here Y is the sum of 27 independent 7-vectors.