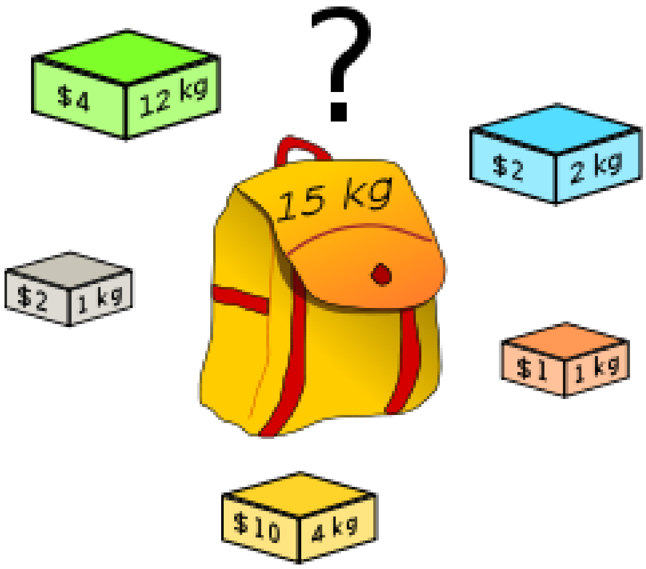
On the Frobenius problem and its generalization

Lenny Fukshansky
Claremont McKenna College

Universität des Saarlandes
Oberseminar Zahlentheorie
July 9, 2012

Integer knapsack problem



Given unlimited supply of $N \geq 2$ types of objects of respective integer weights $a_1, \ldots, a_N$ and corresponding integer prices $p_1, \ldots, p_N$, maximize the value of a knapsack that can hold at most the weight W. In other words, maximize the expression

$$p_1 x_1 + \cdots + p_N x_N$$

under the constraint

$$a_1 x_1 + \cdots + a_N x_N \leq W$$

for nonnegative integers $x_1, \ldots, x_N$. This problem often arises in resource allocation with financial constraints.

Feasibility of integer knapsacks

Integer knapsack problem is known to be NP-complete. Here is one way to think about it:

- For each integer weight $0 < w \leq W$, decide whether the equation

$$a_1 x_1 + \cdots + a_N x_N = w \tag{1}$$

  has nonnegative integer solutions, i.e. is this problem *feasible*.

- Find all such solutions $x_1, \ldots, x_N$ - there can only be finitely many of them.

- Maximize $p_1 x_1 + \cdots + p_N x_N$ on the finite set of solutions.

Hence it is important to understand for which weights w is equation (1) feasible. This leads us to the main subject of this talk, the *Frobenius problem*.

Frobenius number

Let $N \geq 2$ be an integer, and let

$$1 < a_1 < a_2 < \cdots < a_N$$

be relatively prime integers.

Define the **Frobenius number**

$$g_0 = g_0(\boldsymbol{a})$$

of the N-tuple $\boldsymbol{a} := (a_1, \ldots, a_N)$ to be the largest positive integer that has NO **representation** as

$$\sum_{i=1}^{N} a_i x_i$$

where $x_1, ..., x_N$ are *nonnegative* integers.

Fact: g_0 exists because

$$\text{gcd}(a_1, ..., a_N) = 1.$$

Example

What is $g_0(5,7)$?

$$5 = 1 \times 5 + 0 \times 7,\ \ 7 = 0 \times 5 + 1 \times 7,$$

$$10 = 2 \times 5 + 0 \times 7,\ \ 12 = 1 \times 5 + 1 \times 7,$$

$$14 = 0 \times 5 + 2 \times 7, 15 = 3 \times 5 + 0 \times 7,$$

$$17 = 2 \times 5 + 1 \times 7,\ \ 19 = 1 \times 5 + 2 \times 7,$$

$$20 = 4 \times 5 + 0 \times 7,\ \ 21 = 0 \times 5 + 3 \times 7,$$

$$22 = 3 \times 5 + 1 \times 7,\ \ 24 = 2 \times 5 + 2 \times 7,$$

25, 26, 27, ... - in fact, any integer greater than 23 can be represented by 5 and 7 with nonnegative coefficients. Hence:

$$g_0(5,7) = 23.$$

Frobenius problem

How do we find the Frobenius number?

Frobenius Problem (FP): Construct an algorithm that would take N and the relatively prime numbers $a_1, \ldots, a_N$ on the input, and return $g_0(a_1, \ldots, a_N)$ on the output.

Theorem 1 (Ramirez-Alfonsin, 1994)**.** *FP is NP-hard.*

What if we fix N? When $N = 2$, there is a simple formula:

$$g_0(a_1, a_2) = (a_1 - 1)(a_2 - 1) - 1.$$

This formula is usually attributed to *James Sylvester*, although there is no formal record of it in Sylvester's work; Sylvester proposed a related problem in *Educational Times in 1884*, a solution to which was presented in the same article by *Curran Sharp*.

For $N \geq 3$ there currently are no known *elementary* formulas for the Frobenius number, but...

Some work done

Theorem 2 (Kannan, 1992). *For each fixed N, the problem of finding the Frobenius number of a given N-tuple is P.*

The literature on FP is vast, including a book by Ramirez-Alfonsin; FP has numerous applications in graph theory, computer science, group theory, coding theory, tilings, etc. Some recent research on FP included:

Faster algorithms for fixed N (some fast algorithms are implemented in Mathematica).

Lower bounds: Davison (1994) for $N = 3$ (sharp - $\sqrt{3}$ cannot be improved):

$$g_0 \geq \sqrt{3a_1a_2a_3} - a_1 - a_2 - a_3$$

Aliev & Gruber (2007) for any N:

$$g_0 > \left((N-1)! \prod_{i=1}^{N} a_i \right)^{\frac{1}{N-1}} - \sum_{i=1}^{N} a_i.$$

Upper bounds for $N \geq 3$

Erdös, Graham (1972):

$$g_0 \leq 2a_N \left[\frac{a_1}{N}\right] - a_1. \tag{2}$$

Vitek (1975):

$$g_0 \leq \left[\frac{(a_2-1)(a_N-2)}{2}\right] - 1. \tag{3}$$

Selmer (1977):

$$g_0 \leq 2a_{N-1} \left[\frac{a_N}{N}\right] - a_N. \tag{4}$$

Beck, Diaz, Robins (2002):

$$g_0 \leq \frac{\sqrt{a_1 a_2 a_3 (a_1 + a_2 + a_3)} - a_1 - a_2 - a_3}{2}. \tag{5}$$

Kannan's approach

Frobenius number g_0 can be related to the covering radius of a certain convex body with respect to a certain lattice.

Lattice:

$$\mathcal{L} = \left\{ \boldsymbol{x} \in \mathbb{Z}^{N-1} : \sum_{i=1}^{N-1} a_i x_i \equiv 0 \pmod{a_N} \right\}.$$

Convex body:

$$\mathcal{S} = \left\{ \boldsymbol{x} \in \mathbb{R}_{\geq 0}^{N-1} : \sum_{i=1}^{N-1} a_i x_i \leq 1 \right\}.$$

Covering radius:

$$\mu(\mathcal{S}, \mathcal{L}) = \inf \left\{ t \in \mathbb{R}_{>0} : t\mathcal{S} + \mathcal{L} = \mathbb{R}^{N-1} \right\}.$$

A formula!

Theorem 3 (Kannan, 1992)**.**

$$g_0 = \mu(\mathcal{S}, \mathcal{L}) - \sum_{i=1}^{N} a_i.$$

The simplex $\mathcal{S}$ is not 0-symmetric, which makes bounds on $\mu(\mathcal{S}, \mathcal{L})$ difficult to produce.

However, this approach motivates applying techniques from geometry of numbers to produce upper bounds for g_0.

It is possible to bound the Frobenius number in terms of the covering radius of a Euclidean ball with respect to a different lattice, which is much easier to estimate.

A related geometric approach

Lattice:

$$\Lambda_{\boldsymbol{a}} = \left\{ \boldsymbol{x} \in \mathbb{Z}^N : \sum_{i=1}^{N} a_i x_i = 0 \right\}.$$

Covering radius:

$$R_{\boldsymbol{a}} = \inf \left\{ R \in \mathbb{R}_{>0} : B(R) + \Lambda_{\boldsymbol{a}} = V_{\boldsymbol{a}} \right\},$$

where $V_{\boldsymbol{a}} = \operatorname{span}_{\mathbb{R}} \Lambda_{\boldsymbol{a}}$, and $B(R)$ = ball of radius R centered at the origin in $V_{\boldsymbol{a}}$.

Simplex: For each $t \in \mathbb{Z}_{>0}$,

$$S_{\boldsymbol{a}}(t) = \left\{ \boldsymbol{x} \in \mathbb{R}^N_{\geq 0} : \sum_{i=1}^{N} a_i x_i = t \right\}.$$

Then

$$s(\boldsymbol{a}) = \frac{\sum_{i=1}^{N} a_i \sqrt{\|\boldsymbol{a}\|^2 - a_i^2}}{\|\boldsymbol{a}\|^{1-\frac{1}{N-1}}}$$

is the inverse of the normalized inradius of the simplex $S_{\boldsymbol{a}}(1)$.

κ_{N-1} = the volume of a unit ball in $\mathbb{R}^{N-1}$.

Two geometric bounds

Theorem 4 (F. - Robins, 2007)**.**

$$g_0 \le \frac{(N-1)R_{\boldsymbol{a}}}{\|\boldsymbol{a}\|} \sum_{i=1}^{N} a_i \sqrt{\|\boldsymbol{a}\|^2 - a_i^2}.$$

For each $1 \le i \le N-1$, the i-th **successive minimum** of $\Lambda_{\boldsymbol{a}}$ is

$\lambda_i = \inf\left\{\lambda \in \mathbb{R}_{>0} : \dim \operatorname{span}_{\mathbb{R}} \left(B(\lambda) \cap \Lambda_{\boldsymbol{a}}\right) \ge i\right\}.$

Corollary 5 (F. - Robins, 2007)**.**

$$g_0 \le \frac{(N-1)^2}{(\kappa_{N-1})^{\frac{1}{N-1}}} \times \frac{\lambda_{N-1}}{\lambda_1} \times s(\boldsymbol{a}).$$

These bounds are symmetric in all $a_1, \ldots, a_N$, unlike the previously known ones.

How good are these bounds?

It is easy to observe that

$$\lambda_1 \leq \lambda_2 \leq \ldots \lambda_{N-1}.$$

The bound of Corollary 5 is especially good compared to the previously known ones when the ratio λ_{N-1}/λ_1 is small.

Moreover, the dependence of our bound on the geometric constant $s(\boldsymbol{a})$ turns out to be "correct", in a certain sense, as we will discuss next.

What should we typically expect?

The investigation of asymptotic behavior of the Frobenius number for a "typical" N-tuple $(a_1, \ldots, a_N)$ was initiated by V. I. Arnold in a series of papers (1999 - 2007).

In particular, let Ω_N^1 be an ensemble of relatively prime positive integer N-tuples $\boldsymbol{a} = (a_1, \ldots, a_N)$ with

$$\Sigma(\boldsymbol{a}) := a_1 + \cdots + a_N \to \infty.$$

Arnold conjectured that for a "typical" N-tuple $\boldsymbol{a}$ from Ω_N^1,

$$g_0 \text{ grows like } \Sigma(\boldsymbol{a})^{1+\frac{1}{N-1}} \text{ as } \Sigma(\boldsymbol{a}) \to \infty.$$

Probabilistically speaking...

In a recent paper (2007), J. Bourgain and Y. Sinai considered a variation of Arnold's conjecture. Namely, they looked at the set

$$\Omega_N^\infty(\alpha) = \{\boldsymbol{a} \in \mathbb{Z}_{>0}^N \ : \ \mathrm{gcd}(\boldsymbol{a}) = 1, \\ a_i > \alpha|\boldsymbol{a}| \ \forall\ 1 \le i \le N\},$$

where $0 < \alpha < 1$ is a fixed real number and

$$|\boldsymbol{a}| = \max_{1 \le i \le N} |a_i|,$$

and proved that for a "typical" N-tuple $\boldsymbol{a}$ from $\Omega_N^\infty(\alpha)$,

$$g_0 \text{ grows like } |\boldsymbol{a}|^{1+\frac{1}{N-1}} \text{ as } |\boldsymbol{a}| \to \infty.$$

Specifically, they showed that

$$\mathrm{Prob}_{\infty,\alpha}\left(\frac{g_0(\boldsymbol{a})}{|\boldsymbol{a}|^{1+\frac{1}{N-1}}} \ge T\right) \to 0 \text{ as } T \to \infty,$$

with respect to a uniform distribution on $\Omega_N^\infty(\alpha)$.

What about $s(\boldsymbol{a})$?

In 2009, I. Aliev and M. Henk proved the following result. Let

$$\Omega_N^2(T) = \{\boldsymbol{a} \in \mathbb{Z}_{>0}^N : \mathrm{gcd}(\boldsymbol{a}) = 1,\ \|\boldsymbol{a}\| \le T\}.$$

Then for all $N \ge 3$,

$$\mathrm{Prob}_{N,T}\left(\frac{g_0(\boldsymbol{a}) + \Sigma(\boldsymbol{a})}{s(\boldsymbol{a})} > D\right) \ll_N \frac{1}{D^2},$$

where $\mathrm{Prob}_{N,T}$ stands for the uniform probability distribution on $\Omega_N^2(T)$, and $\ll_N$ is Vinogradov's big-O notation with the constant depending on N only.

Thus, for a "typical" N-tuple $\boldsymbol{a}$ one can expect $g_0(\boldsymbol{a})+\Sigma(\boldsymbol{a})$ to be of the order of magnitude of the geometric constant $s(\boldsymbol{a})$.

The modified Frobenius number $g_0(\boldsymbol{a})+\Sigma(\boldsymbol{a})$ is also meaningful: it is the largest positive integer that has no representations in terms of $a_1, \dots, a_N$ with *positive* coefficients.

A generalization

In 2003, Beck & Robins defined the generalized s-**Frobenius number** $g_s = g_s(\boldsymbol{a})$ for each nonnegative integer s to be the largest positive integer that has *precisely* s distinct representations in terms of $\boldsymbol{a}$ with *nonnegative* coefficients. Properties of s-Frobenius numbers have recently been studied by Beck & Kifer (2010), Shallit & Stankewicz (2010).

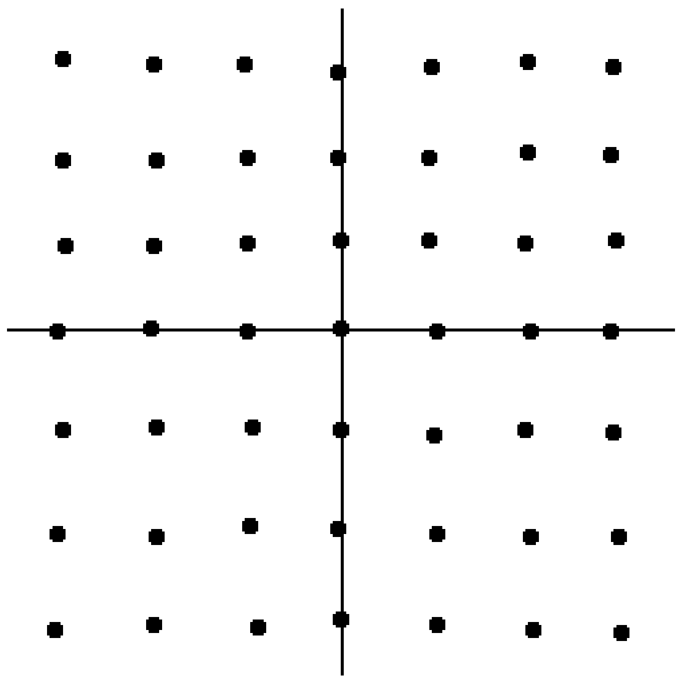
The first upper and lower bounds on g_s have been obtained by F. & Schürmann (2010) by an extension of F. & Robins method for g_0:

$$\left(s\prod_{i=1}^{N-1} a_i\right)^{\frac{1}{N-1}} \ll_N g_s(\boldsymbol{a})$$

$$\ll_N \quad \max\left\{\frac{R_{\boldsymbol{a}}\sum_{i=1}^{N} a_i\|\boldsymbol{\alpha}_i\|}{\|\boldsymbol{a}\|}, \left(s\prod_{i=1}^{N-1} a_i\right)^{\frac{1}{N-2}}\right\},$$

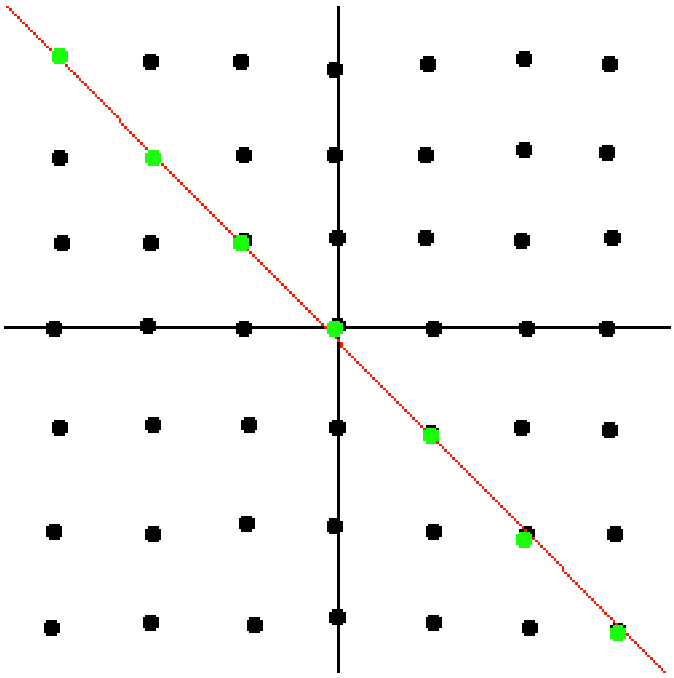
where the lower bound holds for sufficiently large s, and $\boldsymbol{\alpha}_i$ is $\boldsymbol{a}$ with i-th coordinate removed.

Idea of the proof



Integer lattice $\mathbb{Z}^N$ in $\mathbb{R}^N$

Idea of the proof

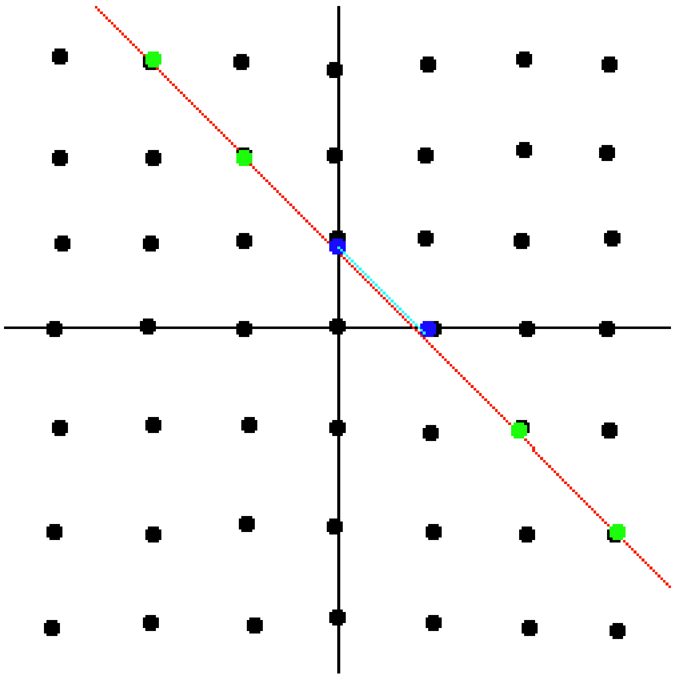


Subspace

$$V_{\boldsymbol{a}} = \left\{ \boldsymbol{x} \in \mathbb{R}^N : \sum_{i=1}^{N} a_i x_i = 0 \right\}$$

with the lattice $\Lambda_{\boldsymbol{a}} = V_{\boldsymbol{a}} \cap \mathbb{Z}^N$ in it

Idea of the proof

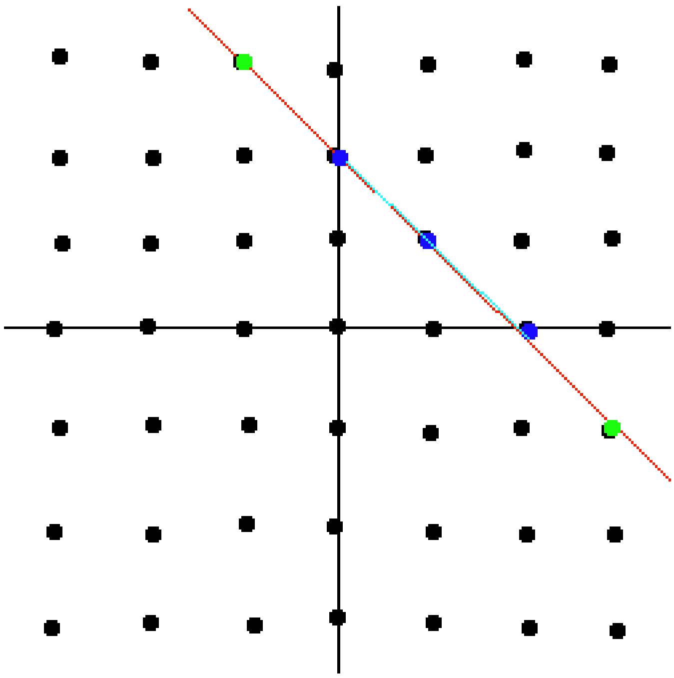


Hyperplane

$$V_{\boldsymbol{a}}(1) = \left\{ \boldsymbol{x} \in \mathbb{R}^N : \sum_{i=1}^{N} a_i x_i = 1 \right\}$$

with the hyperplane lattice
$\Lambda_{\boldsymbol{a}}(1) = V_{\boldsymbol{a}}(1) \cap \mathbb{Z}^N$ and simplex
$S_{\boldsymbol{a}}(1) = V_{\boldsymbol{a}}(1) \cap \mathbb{R}^N_{\geq 0}$ in it

Idea of the proof

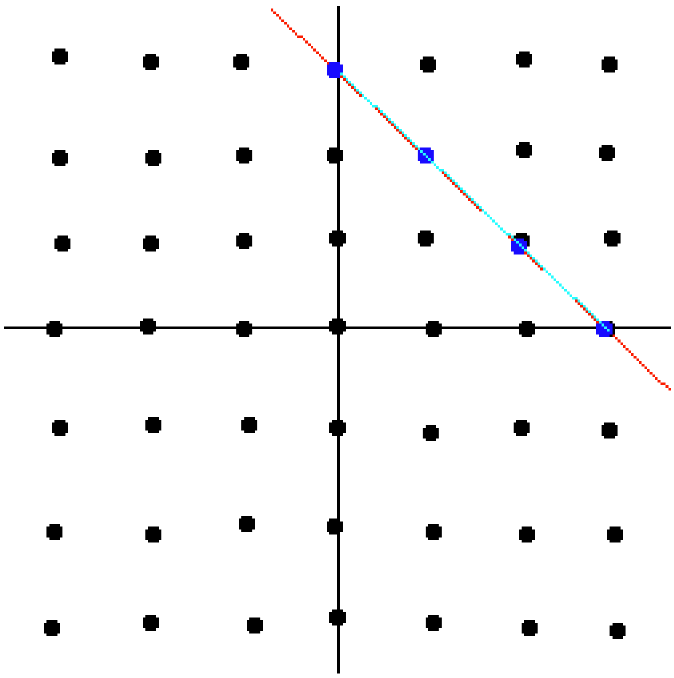


Hyperplane

$$V_{\boldsymbol{a}}(2) = \left\{ \boldsymbol{x} \in \mathbb{R}^N : \sum_{i=1}^{N} a_i x_i = 2 \right\}$$

with the hyperplane lattice $\Lambda_{\boldsymbol{a}}(2) = V_{\boldsymbol{a}}(2) \cap \mathbb{Z}^N$ and simplex $S_{\boldsymbol{a}}(2) = V_{\boldsymbol{a}}(2) \cap \mathbb{R}^N_{\geq 0}$ in it

Idea of the proof



Hyperplane

$$V_{\boldsymbol{a}}(3) = \left\{ \boldsymbol{x} \in \mathbb{R}^N : \sum_{i=1}^{N} a_i x_i = 3 \right\}$$

with the hyperplane lattice

$\Lambda_{\boldsymbol{a}}(3) = V_{\boldsymbol{a}}(3) \cap \mathbb{Z}^N$ and simplex

$S_{\boldsymbol{a}}(3) = V_{\boldsymbol{a}}(3) \cap \mathbb{R}^N_{\geq 0}$ in it

Idea of the proof

An integer lattice point in $S_{\boldsymbol{a}}(t)$ corresponds to a representation of t in terms of $\boldsymbol{a}$ with nonnegative coefficients. Hence for every $t > g_0$ such a point must always exist.

Moreover, for every $s \geq 0$, g_s is precisely the smallest positive integer such that for each integer $t > g_s$ the simplex $S_{\boldsymbol{a}}(t)$ contains more than s points of $\mathbb{Z}^N$.

Hence bounds on g_s follow from lattice point counting estimates in simplices.

Additional bounds on g_s

Here are further bounds on g_s that work for all s, obtained by a different method.

Theorem 6 (Aliev, F., Henk (2011))**.** *Let* $N \geq 3$, $s \geq 0$. *Then*

$$g_s(\boldsymbol{a}) \geq \left((s+1)(N-1)! \prod_{i=1}^{N-1} a_i \right)^{\frac{1}{N-1}} - \sum_{i=1}^{N-1} a_i$$

and

$$g_s(\boldsymbol{a}) \leq g_0(\boldsymbol{a}) + \left(s \ (N-1)! \prod_{i=1}^{N-1} a_i \right)^{\frac{1}{N-1}} .$$

Average value estimate for g_s

These bounds lead to an average value estimate on $g_s(\boldsymbol{a})$.

Theorem 7 (Aliev, F., Henk (2011))**.** *Let* $N \geq 3$*,* $s \geq 0$*. Then:*

$$\mathrm{Prob}\left(\frac{g_s(\boldsymbol{a})}{\left((s+1)\prod_{i=1}^{N-1} a_i\right)^{\frac{1}{N-1}}} \geq D\right) \ll_N \frac{1}{D^{N-1}},$$

where Prob$(\cdot)$ *is meant with respect to the uniform probability distribution on*

$$\mathrm{G}(T) = \left\{\boldsymbol{a} \in \mathbb{Z}^N_{>0} : \mathrm{gcd}(\boldsymbol{a}) = 1, |\boldsymbol{a}|_\infty \leq T\right\}.$$

In case of the classical Frobenius number, i.e. when $s = 0$, this probability estimate has been obtained by H. Li (2011). Our method uses his result.

Idea of the proof

The argument here is an extension of Kannan's method: g_s can be related to the s-**covering radius** of the same simplex with respect to the same lattice as in Kannan's work.

Lattice:

$$\mathcal{L} = \left\{ \boldsymbol{x} \in \mathbb{Z}^{N-1} : \sum_{i=1}^{N-1} a_i x_i \equiv 0 \pmod{a_N} \right\}.$$

Convex body:

$$\mathcal{S} = \left\{ \boldsymbol{x} \in \mathbb{R}_{\geq 0}^{N-1} : \sum_{i=1}^{N-1} a_i x_i \leq 1 \right\}.$$

s-**Covering radius:**

$$\mu_s(\mathcal{S}, \mathcal{L}) = \inf \Big\{ t \in \mathbb{R}_{>0} \ : \ \forall\ \boldsymbol{y} \in \mathbb{R}^N \ \exists\ \boldsymbol{x}_1, \ldots, \boldsymbol{x}_s \in \mathcal{L} \ \text{s.t.}\ \boldsymbol{y} \in t\mathcal{S} + \boldsymbol{x}_i \Big\},$$

hence $\mu(\mathcal{S}, \mathcal{L}) = \mu_1(\mathcal{S}, \mathcal{L})$.

Idea of the proof

We extend Kannan's formula, connecting $(s-1)$-Frobenius number to the s-covering radius:

$$g_{s-1} = \mu_s(\mathcal{S}, \mathcal{L}) - \sum_{i=1}^{N} a_i.$$

On the other hand, we obtain bounds on s-covering radius:

$$\begin{aligned} s^{\frac{1}{N}} \left(\frac{\det \mathcal{L}}{\operatorname{Vol} \mathcal{S}}\right)^{\frac{1}{N}} &\leq \mu_s(\mathcal{S}, \mathcal{L}) \\ \leq \quad & \mu_1(\mathcal{S}, \mathcal{L}) + (s-1)^{\frac{1}{N}} \left(\frac{\det \mathcal{L}}{\operatorname{Vol} \mathcal{S}}\right)^{\frac{1}{N}} \\ = \quad & g_0 + \sum_{i=1}^{N} a_i + (s-1)^{\frac{1}{N}} \left(\frac{\det \mathcal{L}}{\operatorname{Vol} \mathcal{S}}\right)^{\frac{1}{N}}, \end{aligned}$$

where the last identity follows by Kannan's formula.

Our bounds on g_s are produced by combining these two equations.

Idea of the proof

The probability estimate is then derived from these bounds with the use of Li's result for g_0 and the estimate

$$\frac{1}{\#\mathsf{G}(T)} \sum_{\boldsymbol{a} \in \mathsf{G}(T)} \frac{\sum_{i=1}^{N} a_i}{\left(\prod_{i=1}^{N} a_i\right)^{\frac{1}{N-1}}} \ll_N T^{-\frac{1}{N-1}},$$

which was previously obtained by Aliev, Henk, and Hinrichs (2009), using the fact that "reverse" arithmetic-geometric mean inequality holds with high probability.

Recall here that

$$\mathsf{G}(T) = \left\{ \boldsymbol{a} \in \mathbb{Z}_{>0}^{N} : \mathrm{gcd}(\boldsymbol{a}) = 1, |\boldsymbol{a}|_\infty \leq T \right\}.$$

Limiting probability distribution for g_0

Finally, we discuss the existence of a limiting probability distribution for the Frobenius number, which was recently obtained by J. Marklof.

Let $N \geq 3$ and let $\mathcal{D} \subset \mathbb{R}^N_{\geq 0}$ be any bounded set with boundary of Lebesgue measure zero. Let

$$\widehat{\mathbb{Z}}^N_{\geq 2} := \{\boldsymbol{a} \in \mathbb{Z}^N : \gcd(a_1, \ldots, a_N) = 1, \\ a_i \geq 2 \ \forall \ 1 \leq i \leq N\}.$$

Theorem 8 (Marklof (2010))**.** $\forall \ R \geq 0$,

$$\lim_{T \to \infty} \frac{1}{T^N} \# \left\{ \boldsymbol{a} \in \widehat{\mathbb{Z}}^N_{\geq 2} \cap T\mathcal{D} : \frac{g_0(\boldsymbol{a})}{\left(\prod_{i=1}^N a_i\right)^{\frac{1}{N-1}}} > R \right\} \\ = \frac{\mathrm{Vol}(\mathcal{D})}{\zeta(N)} \Psi_N(R),$$

where $\Psi_N : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is a non-increasing function with $\Psi_N(0) = 1$.

Limiting probability distribution for g_0

In fact, Marklof shows that $\Psi_N(R)$ is equal to the value of the unique $\mathrm{SL}(N-1,\mathbb{R})$-right invariant probability measure of the set

$$\{A \in \mathrm{SL}(N-1,\mathbb{Z}) \setminus \mathrm{SL}(N-1,\mathbb{R}) : \rho(A) > R\}\,,$$

where $\rho(A)$ is the covering radius of the simplex

$$\Delta = \left\{ \boldsymbol{x} \in \mathbb{R}^{N-1}_{\geq 0} : \sum_{i=1}^{N-1} x_i \leq 1 \right\}$$

with respect to the lattice $\mathbb{Z}^{N-1}A$, i.e.,

$$\rho(A) = \inf \left\{ \rho \in \mathbb{R}_{>0} : \mathbb{Z}^{N-1}A + \rho\Delta = \mathbb{R}^{N-1} \right\}.$$

Moreover, the expression for $\Psi_N(R)$ connects naturally with the optimal lower bound on g_0, obtained by I. Aliev and P. Gruber (2007):

$$g_0(\boldsymbol{a}) \geq \left(\prod_{i=1}^{N} a_i \right)^{\frac{1}{N-1}} \inf \rho(A),$$

where infimum is taken over all $A \in \mathrm{SL}(N-1,\mathbb{Z}) \setminus \mathrm{SL}(N-1,\mathbb{R})$.