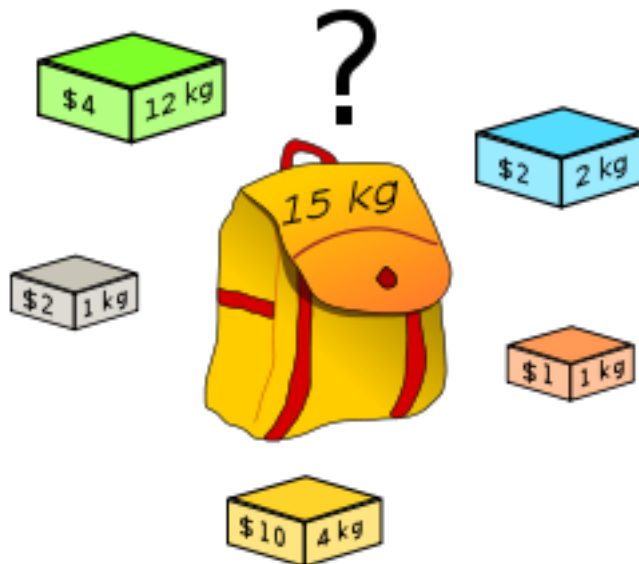


Integer knapsacks and the Frobenius problem

Lenny Fukshansky
Claremont McKenna College

Claremont Statistics, Operations Research,
and Math Finance Seminar
April 21, 2011

Integer knapsack problem



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

$$p_1x_1 + \dots + p_Nx_N$$

under the constraint

$$a_1x_1 + \dots + a_Nx_N \leq W$$

for nonnegative integers x_1, \dots, 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

$$a_1x_1 + \cdots + a_Nx_N = w \quad (1)$$

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

- Find all such solutions x_1, \dots, x_N - there can only be finitely many of them.
- Maximize $p_1x_1 + \cdots + p_Nx_N$ 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**

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

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

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

where x_1, \dots, x_N are *nonnegative* integers.

Fact: g_0 exists because

$$\gcd(a_1, \dots, a_N) = 1.$$

Example

What is $g_0(5, 7)$?

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

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

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

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

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

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

25, 26, 27, ... - it appears that 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, \dots, a_N on the input, and return $g_0(a_1, \dots, a_N)$ 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 $N \geq 3$

Erdős, Graham (1972):

$$g_0 \leq 2a_N \left\lceil \frac{a_1}{N} \right\rceil - a_1. \quad (2)$$

Vitek (1975):

$$g_0 \leq \left\lceil \frac{(a_2 - 1)(a_N - 2)}{2} \right\rceil - 1. \quad (3)$$

Selmer (1977):

$$g_0 \leq 2a_{N-1} \left\lceil \frac{a_N}{N} \right\rceil - a_N. \quad (4)$$

Beck, Diaz, Robins (2002):

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

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:

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

Convex body:

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

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:

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

Covering radius:

$$R_a = \inf \{ R \in \mathbb{R}_{>0} : B(R) + \Lambda_a = V_a \},$$

where $V_a = \text{span}_{\mathbb{R}} \Lambda_a$, and $B(R) =$ ball of radius R centered at the origin in V_a .

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

$$S_a(t) = \left\{ \mathbf{x} \in \mathbb{R}_{\geq 0}^N : \sum_{i=1}^N a_i x_i = t \right\}.$$

Then

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

is the inverse of the normalized inradius of the simplex $S_a(1)$.

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

Two geometric bounds

Theorem 4 (F. - Robins, 2007).

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

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

$$\lambda_i = \inf \{ \lambda \in \mathbb{R}_{>0} : \dim \text{span}_{\mathbb{R}} (B(\lambda) \cap \Lambda_{\mathbf{a}}) \geq i \}.$$

Corollary 5 (F. - Robins, 2007).

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

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

How good are these bounds?

It is easy to observe that

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

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 $s(\mathbf{a})$ 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, \dots, 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 $\mathbf{a} = (a_1, \dots, a_N)$ with

$$\Sigma(\mathbf{a}) := a_1 + \dots + a_N \rightarrow \infty.$$

Arnold conjectured that for a “typical” N -tuple \mathbf{a} from Ω_N^1 ,

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

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

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

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

$$|\mathbf{a}| = \max_{1 \leq i \leq N} |a_i|,$$

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

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

Specifically, they showed that

$$\text{Prob}_{\infty, \alpha} \left(\frac{g_0(\mathbf{a})}{|\mathbf{a}|^{1+\frac{1}{N-1}}} \geq T \right) \rightarrow 0 \text{ as } T \rightarrow \infty,$$

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

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

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

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

Then for all $N \geq 3$,

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

where $\text{Prob}_{N,T}$ 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 \mathbf{a} one can expect $g_0(\mathbf{a}) + \Sigma(\mathbf{a})$ to be of the order of magnitude of the geometric constant $s(\mathbf{a})$.

The modified Frobenius number $g_0(\mathbf{a}) + \Sigma(\mathbf{a})$ 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** $g_s = g_s(\mathbf{a})$ for each nonnegative integer s to be the largest positive integer that has *precisely* s distinct representations in terms of \mathbf{a} with *nonnegative* coefficients. Properties of s -Frobenius numbers have recently been studied by Beck & Kifer (2010), Shallit & Stankewicz (2010).

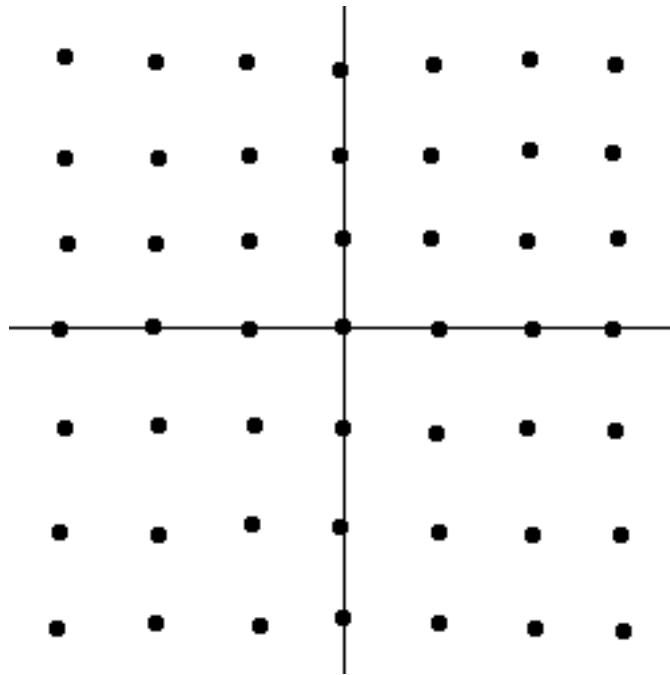
The first upper and lower bounds on g_s have been obtained by F. & Schürmann (2010) by an extension of F. & Robins method for g_0 :

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

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

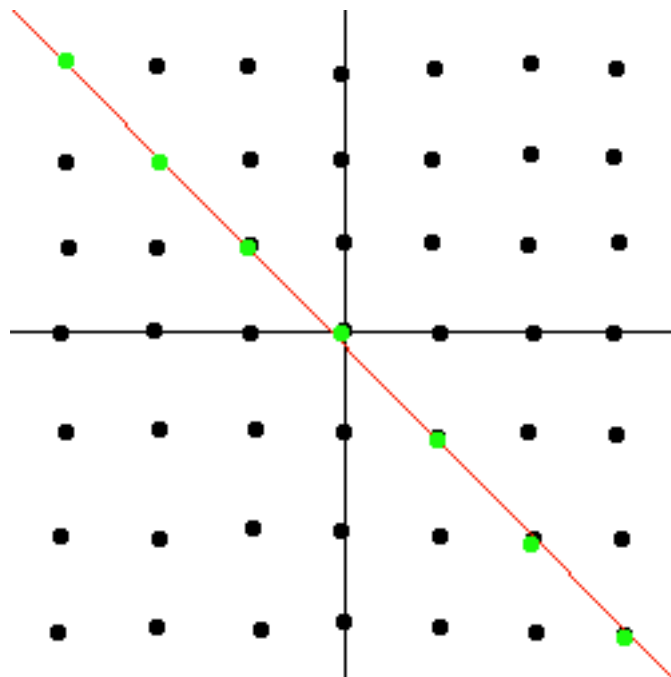
where the lower bound holds for sufficiently large s , and $\boldsymbol{\alpha}_i$ is \mathbf{a} with i -th coordinate removed.

Idea of the method



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

Idea of the method

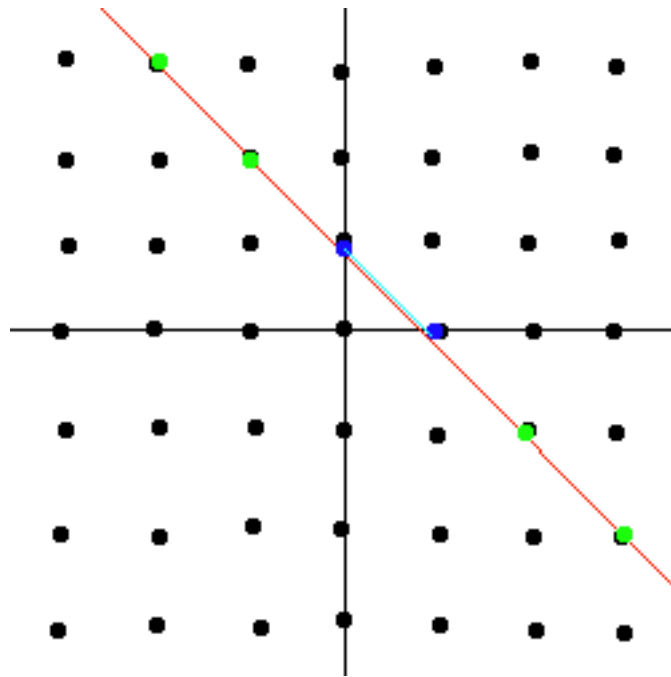


Subspace

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

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

Idea of the method



Hyperplane

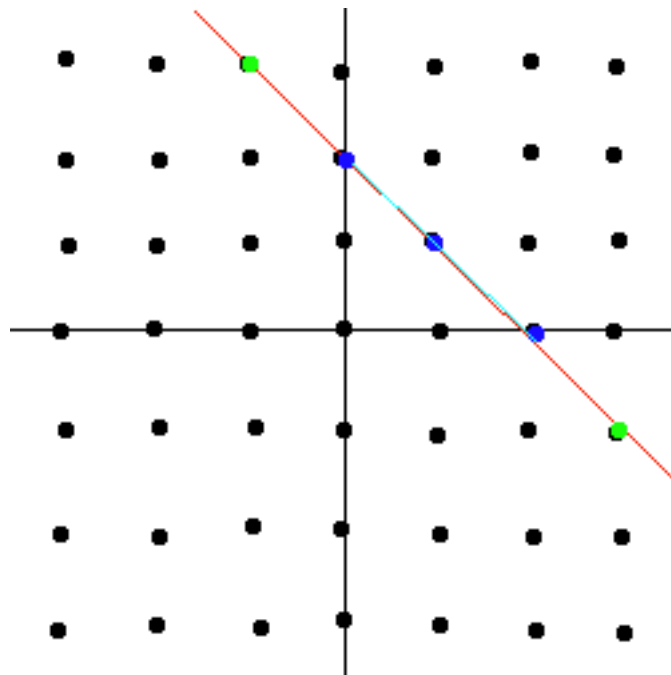
$$V_{\mathbf{a}}(1) = \left\{ \mathbf{x} \in \mathbb{R}^N : \sum_{i=1}^N a_i x_i = 1 \right\}$$

with the hyperplane lattice

$$\Lambda_{\mathbf{a}}(1) = V_{\mathbf{a}}(1) \cap \mathbb{Z}^N \text{ and simplex}$$

$$S_{\mathbf{a}}(1) = V_{\mathbf{a}}(1) \cap \mathbb{R}_{\geq 0}^N \text{ in it}$$

Idea of the method



Hyperplane

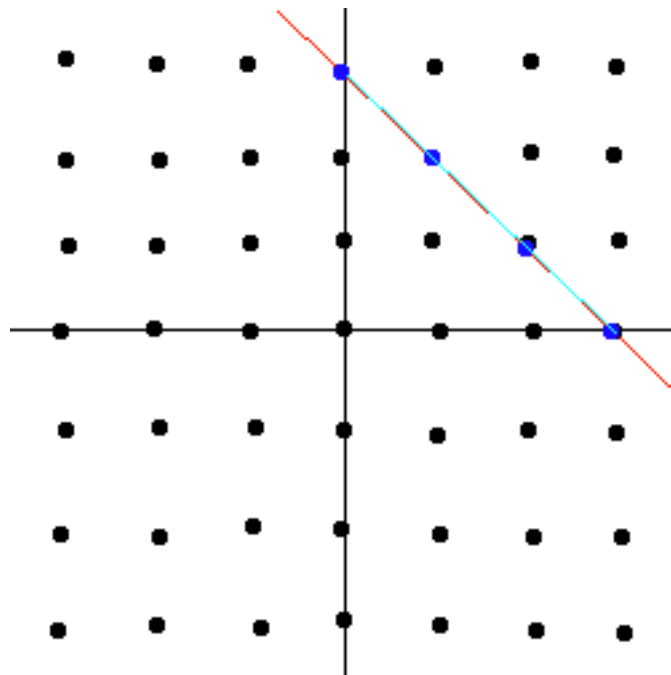
$$V_{\mathbf{a}}(2) = \left\{ \mathbf{x} \in \mathbb{R}^N : \sum_{i=1}^N a_i x_i = 2 \right\}$$

with the hyperplane lattice

$$\Lambda_{\mathbf{a}}(2) = V_{\mathbf{a}}(2) \cap \mathbb{Z}^N \text{ and simplex}$$

$$S_{\mathbf{a}}(2) = V_{\mathbf{a}}(2) \cap \mathbb{R}_{\geq 0}^N \text{ in it}$$

Idea of the method



Hyperplane

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

with the hyperplane lattice

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

$$S_{\mathbf{a}}(3) = V_{\mathbf{a}}(3) \cap \mathbb{R}_{\geq 0}^N \text{ in it}$$

Idea of the method

An integer lattice point in $S_{\mathbf{a}}(t)$ corresponds to a representation of t in terms of \mathbf{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 $S_{\mathbf{a}}(t)$ 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*

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

and

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

Average value estimate for g_s

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

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

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

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

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

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.