On the Frobenius problem and its generalization

Lenny Fukshansky
Claremont McKenna College & IHES

Universität Rostock
Mathematisches Kolloquium
November 3, 2010
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**
\[
g_0 = g_0(a)
\]
of the \( N \)-tuple \( a := (a_1, \ldots, a_N) \) to be the largest positive integer that has NO representation as
\[
\sum_{i=1}^{N} a_i x_i
\]
where \( x_1, \ldots, x_N \) are nonnegative integers.

**Fact:** \( g_0 \) exists because
\[
\gcd(a_1, \ldots, a_N) = 1.
\]
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, ... - 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 $a_1, \ldots, a_N$ 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 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):

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

Killingbergtro, 2000 for any $N$:

$$g_0 \geq ((N - 1)!a_1 \ldots a_N)^{1/(N-1)} - \sum_{i=1}^{N} a_i$$

Aliev & Gruber, 2007 - an optimal lower bound in terms of the absolute inhomogeneous minimum of the standard simplex in $\mathbb{R}^{N-1}$.  

5
Upper bounds for $N \geq 3$

Erdős, Graham (1972):

$$g_0 \leq 2a_N \left\lfloor \frac{a_1}{N} \right\rfloor - a_1.$$ (1)

Vitek (1975):

$$g_0 \leq \left\lfloor \frac{(a_2 - 1)(a_N - 2)}{2} \right\rfloor - 1.$$ (2)

Selmer (1977):

$$g_0 \leq 2a_{N-1} \left\lfloor \frac{a_N}{N} \right\rfloor - a_N.$$ (3)

Beck, Diaz, Robins (2002):

$$g_0 \leq \frac{\sqrt{a_1 a_2 a_3(a_1 + a_2 + a_3)} - a_1 - a_2 - a_3}{2}.$$ (4)
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).

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

Standard techniques for bounding a covering radius only work in the case when the convex body is symmetric with respect to the origin, which is clearly not the case here.

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:

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

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 \( B(R) = \text{ball of radius } R \) centered at the origin in \( V_a \).

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

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

Then

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

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

\[ \kappa_{N-1} = \text{the volume of a unit ball in } \mathbb{R}^{N-1}. \]
Two geometric bounds

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

\[ g_0 \leq \frac{(N - 1)R_a}{\|a\|} \sum_{i=1}^{N} a_i \sqrt{\|a\|^2 - a_i^2}. \]

For each \( 1 \leq i \leq N - 1 \), the \( i \)-th **successive minimum** of \( \Lambda_a \) is

\[ \lambda_i = \inf \{ \lambda \in \mathbb{R}_{>0} : \dim \text{span}_{\mathbb{R}} (B(\lambda) \cap \Lambda_a) \geq i \}. \]

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

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

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 \( \lambda_{N-1}/\lambda_1 \) is small.

Moreover, the dependence of our bound on the geometric constant \( s(a) \) 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 $\Omega^1_N$ be an ensemble of relatively prime positive integer $N$-tuples $a = (a_1, \ldots, a_N)$ with

$$\sum(a) := a_1 + \cdots + a_N \to \infty.$$  

Arnold conjectured that for a “typical” $N$-tuple $a$ from $\Omega^1_N$,

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

\[
\Omega_N^\infty(\alpha) = \{ a \in \mathbb{Z}_0^N : \gcd(a) = 1, \ a_i > \alpha |a| \ \forall \ 1 \leq i \leq N \},
\]

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

\[
|a| = \max_{1 \leq i \leq N} |a_i|,
\]

and proved that for a “typical” \(N\)-tuple \(a\) from \(\Omega_N^\infty(\alpha)\),

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

Specifically, they showed that

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

with respect to a uniform distribution on \(\Omega_N^\infty(\alpha)\).
What about \(s(a)\)?

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

\[
\Omega^2_N(T) = \{a \in \mathbb{Z}_{>0}^N : \gcd(a) = 1, \|a\| \leq T\}.
\]

Then for all \(N \geq 3\),

\[
\text{Prob}_{N,T}\left(\frac{g_0(a) + \sum(a)}{s(a)} > t\right) \ll_N t^{-2},
\]

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

Thus, for a “typical” \(N\)-tuple \(a\) one can expect \(g_0(a) + \sum(a)\) to be of the order of magnitude of the geometric constant \(s(a)\).

The modified Frobenius number \(g_0(a) + \sum(a)\) is also meaningful: it is the largest positive integer that has no representations in terms of \(a_1, \ldots, a_N\) with positive coefficients.
A generalization

Recently a number of authors studied the generalized $s$-Frobenius numbers $g_s = g_s(a)$ for each nonnegative integer $s$, which is the largest positive integer that has precisely $s$ distinct representations in terms of $a$ with nonnegative coefficients.

In particular Shallit & Stankewicz (2010) and Beck & Kifer (2010) investigated families of $N$-tuples $a$ for which the difference

$$g_s - g_0$$

grows unboundedly.

This motivates a natural question: how big and how small can $g_s$ be in general?
Upper bounds on $g_s$

Let $\tau_{N-1}$ be the **kissing number** in dimension $N - 1$, i.e. the maximal number of unit balls in $\mathbb{R}^{N-1}$ that can touch another unit ball.

**Theorem 6** (F. Schürmann, 2010).

$$g_s(a) \leq \max \left\{ \frac{Ra(N - 1) \sum_{i=1}^{N} a_i \sqrt{\|a\|^2 - a_i^2}}{\|a\|}, \left( s(N - 1)! \prod_{i=1}^{N} a_i \right)^{\frac{1}{N-2}} \right\}.$$  

If in addition $s \leq \tau_{N-1} + 1$, then

$$g_s(a) \leq \frac{3Ra(N - 1) \sum_{i=1}^{N} a_i \sqrt{\|a\|^2 - a_i^2}}{\|a\|}.$$
Lower bounds on $g_s$

Define the dimensional constant

$$C_N = \frac{2^{N^2-\frac{7N}{2}}+2(N-1)^\frac{N}{2}((N-1)!)^{N-1}}{\pi^{\frac{N-2}{2}}\kappa_{N-2}^{N-1}}.$$ 

**Theorem 7** (F. - Schürmann, 2010).

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

and

$$g_s(a) \geq \left(\frac{s(N-1)!\kappa_{N-1}R_a^{N-1}}{2\|a\|}\prod_{i=1}^{N} a_i\right)^{\frac{1}{N-1}}.$$ 

Also if $\rho > 1$ and

$$s \geq \frac{\left(\prod_{i=1}^{N} a_i\right)^{N-2}}{(N-1)!}\left(\frac{C_N\lambda_{N-1}^{N-1}}{\rho-1}\right)^{N-1},$$

then

$$g_s(a) \geq \left(\frac{s(N-1)!}{\rho}\prod_{i=1}^{N} a_i\right)^{\frac{1}{N-1}}.$$
Idea of the proof

Integer lattice $\mathbb{Z}^N$ in $\mathbb{R}^N$
Idea of the proof

Subspace

\[ V_a = \left\{ \mathbf{x} \in \mathbb{R}^N : \sum_{i=1}^{N} a_i x_i = 0 \right\} \]

with the lattice \( \Lambda_a = V_a \cap \mathbb{Z}^N \) in it
Idea of the proof

Hyperplane

\[ V_a(1) = \left\{ x \in \mathbb{R}^N : \sum_{i=1}^{N} a_i x_i = 1 \right\} \]

with the hyperplane lattice

\[ \Lambda_a(1) = V_a(1) \cap \mathbb{Z}^N \]

and simplex

\[ S_a(1) = V_a(1) \cap \mathbb{R}^N_{\geq 0} \]

in it
Idea of the proof

Hyperplane

\[ V_a(2) = \left\{ x \in \mathbb{R}^N : \sum_{i=1}^{N} a_i x_i = 2 \right\} \]

with the hyperplane lattice

\[ \Lambda_a(2) = V_a(2) \cap \mathbb{Z}^N \]

and simplex

\[ S_a(2) = V_a(2) \cap \mathbb{R}_{\geq 0}^N \]
Idea of the proof

Hyperplane

\[ V_a(3) = \left\{ x \in \mathbb{R}^N : \sum_{i=1}^{N} a_i x_i = 3 \right\} \]

with the hyperplane lattice
\[ \Lambda_a(3) = V_a(3) \cap \mathbb{Z}^N \]
and simplex
\[ S_a(3) = V_a(3) \cap \mathbb{R}^N_{\geq 0} \]
Idea of the proof

An integer lattice point in $S_a(t)$ corresponds to a representation of $t$ in terms of $a$ 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 $S_a(t)$ contains more than $s$ points of $\mathbb{Z}^N$.

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

**Problem:** Analyze the bounds of Theorems 6 and 7 to understand the asymptotic behavior of $g_s(a)$ for a “typical” $N$-tuple $a$. 

23