

Frobenius number, covering radius, and well-rounded lattices

Lenny Fukshansky*
Claremont McKenna College

Sinai Robins
Temple University

*(Discrete and Computational Geometry, vol.
37 no. 3 (2007), pg. 471-483)*

Joint Mathematics Meeting, San Diego,
January 9, 2008

Introduction

- $N \geq 2$ an integer
- $a_1 < a_2 < \dots < a_N$ positive relatively prime integers

Define the *Frobenius number*

$$\mathcal{F} = \mathcal{F}(a_1, \dots, a_N)$$

to be the largest positive integer that *cannot* be expressed as

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

where x_1, \dots, x_N are *non-negative* integers. \mathcal{F} exists because

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

Frobenius Problem (FP): Given N and the numbers a_1, \dots, a_N find \mathcal{F} .

For $N = 2$:

$$\mathcal{F}(a_1, a_2) = (a_1 - 1)(a_2 - 1) - 1.$$

This formula is usually attributed to 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.

There is no known formula for an arbitrary N ; moreover:

Fact: FP is NP-hard.

Kannan (1992): For each fixed N , there exists a polynomial time algorithm for finding the Frobenius number of a given N -tuple.

Upper bounds for $N \geq 3$

Erdős, Graham (1972):

$$\mathcal{F} \leq 2a_N \left\lceil \frac{a_1}{N} \right\rceil - a_1. \quad (1)$$

Vitek (1975):

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

Selmer (1977):

$$\mathcal{F} \leq 2a_{N-1} \left\lceil \frac{a_N}{N} \right\rceil - a_N. \quad (3)$$

Beck, Diaz, Robins (2002):

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

Kannan's approach

Frobenius number \mathcal{F} 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:

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

Kannan (1992):

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

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 \mathcal{F} .

Geometry of numbers

We relate the Frobenius number to a covering radius of a Euclidean ball with respect to a different lattice, which is much easier to estimate.

Lattice:

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

Covering radius:

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

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

Theorem 1 (F., Robins (2005)).

$$\begin{aligned} \mathcal{F} &\leq \left[\frac{(N-1)Ra}{\|\mathbf{a}\|} \sum_{i=1}^N a_i \sqrt{\|\mathbf{a}\|^2 - a_i^2} + 1 \right] \\ &\leq \left[\frac{(N-1)^2}{\omega_{N-1}} \sum_{i=1}^N a_i \sqrt{\|\mathbf{a}\|^2 - a_i^2} + 1 \right], \end{aligned}$$

where

$$\omega_{N-1} = \text{Vol}_{N-1}(B(1)) = \frac{\pi^{\frac{N-1}{2}}}{\Gamma\left(\frac{N+1}{2}\right)}.$$

The last inequality follows by classical results of Jarnik and Minkowski.

For each $1 \leq i \leq N-1$, the i -th *successive minimum* λ_i of $\Lambda_{\mathbf{a}}$ is defined to be the infimum of all $\lambda > 0$ such that $B(\lambda) \cap \Lambda_{\mathbf{a}}$ contains i non-zero linearly independent vectors in $V_{\mathbf{a}}$.

Not hard to prove:

$$2 \leq \lambda_1 \leq \dots \leq \lambda_{N-1}. \quad (5)$$

Theorem 1 implies a bound in terms of the ratio of largest and smallest successive minima:

Corollary 2 (F., Robins (2005)). *Let the notation be as above. Then*

$$\mathcal{F} \leq \left[\frac{\lambda_{N-1}(N-1)^2 \sum_{i=1}^N a_i \sqrt{\|\mathbf{a}\|^2 - a_i^2}}{\lambda_1(\|\mathbf{a}\|^{N-2} \omega_{N-1})^{\frac{1}{N-1}}} + 1 \right].$$

In the special case when

$$\lambda_1 = \dots = \lambda_{N-1},$$

i.e. $\Lambda_{\mathbf{a}}$ is a lattice with *equal successive minima*, the bound of Corollary 2 is particularly good. Such lattices are called *well-rounded* (WR).

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

Question: How often is the lattice of the form $\Lambda_{\mathbf{a}}$ WR, if at all?

We start with some examples.

WR lattices

Theorem 3 (F., Robins (2005)). *Let $t \in \mathbb{Z}_{>0}$, and define*

$$a_1(t) = 6t^2 - 13t - 216, \quad a_2(t) = 6t^2 - 125, \\ a_3(t) = 7t^2 - 174, \quad a_4(t) = t^3 - 36t - 78.$$

Then for each $t \in \mathbb{Z}_{>0}$,

$$\mathbf{a}(t) = (a_1(t), a_2(t), a_3(t), a_4(t)) \in \mathbb{Z}^4,$$

and there exist infinitely many positive integer values of t such that

$$0 < a_1(t) < a_2(t) < a_3(t) < a_4(t),$$

$$\gcd(a_1(t), a_2(t), a_3(t), a_4(t)) = 1,$$

and the lattice

$$\Lambda_{\mathbf{a}(t)} = \left\{ \mathbf{x} \in \mathbb{Z}^4 : \sum_{i=1}^4 a_i(t)x_i = 0 \right\}$$

is WR. Moreover, for each such $\mathbf{a}(t)$ the minimum of bounds (1) - (4) on the Frobenius number $\mathcal{F}(\mathbf{a}(t))$ is $O(t^4)$ while our bound of Corollary 2 is $O(t^3)$. For instance, $\mathbf{a}(t)$ has these properties for all $t = 13s + 2$, where $s \geq 2$ is an integer.

Theorem 3 is a special case of a more general conjecture, which we believe to be true in all dimensions. To state it, we need some more notation.

An ordered collection of linearly independent vectors $\{\mathbf{x}_1, \dots, \mathbf{x}_k\} \subset \mathbb{Z}^N$, $2 \leq k \leq N$, is called *nearly orthogonal* if for each $1 < i \leq k$ the angle between \mathbf{x}_i and the subspace of \mathbb{R}^N spanned by $\mathbf{x}_1, \dots, \mathbf{x}_{i-1}$ is in the interval $[\frac{\pi}{3}, \frac{\pi}{2}]$. In other words, this condition means that for each $1 < i \leq k$

$$\frac{|\langle \mathbf{x}_i, \mathbf{y} \rangle|}{\|\mathbf{x}_i\| \|\mathbf{y}\|} \leq \frac{1}{2}, \quad (6)$$

for any nonzero vector $\mathbf{y} \in \text{span}_{\mathbb{R}}\{\mathbf{x}_1, \dots, \mathbf{x}_{i-1}\}$, where $\langle \cdot, \cdot \rangle$ stands for the usual inner product on \mathbb{R}^N .

Theorem 4 (Baraniuk, Dash, Neelamani). *Suppose that an ordered basis $\{\mathbf{x}_1, \dots, \mathbf{x}_k\}$ for sublattice Λ of \mathbb{Z}^N of rank $1 < k \leq N$ is nearly orthogonal. Then it contains the shortest non-zero vector of Λ .*

Conjecture 5 (F., Robins (2005)). *Let*

$$\mathbf{x}_1 = (t_1, \dots, t_N)$$

be a variable vector, and write S_N for the symmetric group on N letters where id stands for the identity permutation. There exist permutations

$$\sigma_1, \sigma_2, \dots, \sigma_{N-1} \in S_N$$

with $\sigma_1 = id$, and $N(N-1)$ integers

$$m_{11}, \dots, m_{(N-1)N} \in \{0, 1\}$$

such that for every $1 \leq i \leq N-1$

$$\mathbf{x}_i = \left((-1)^{m_{i1}} t_{\sigma_i(1)}, \dots, (-1)^{m_{iN}} t_{\sigma_i(N)} \right)$$

satisfy the following conditions for infinitely many positive integer values of the variables t_1, \dots, t_N :

1. $\mathbf{x}_1, \dots, \mathbf{x}_{N-1}$ are linearly independent,
2. For each $1 \leq i \leq N$ the corresponding Grassmann coordinate $\det(X_{I_i})$ of the matrix $X = (\mathbf{x}_1 \dots \mathbf{x}_{N-1})^t$ satisfies the condition

$$(-1)^{N+1-i} \det(X_{I_i}) > 0,$$

where $I_i = \{1, \dots, N\} \setminus \{i\}$,

3. Absolute values of Grassmann coordinates of X are relatively prime,
4. $\{\mathbf{x}_1, \dots, \mathbf{x}_{N-1}\}$ is a nearly orthogonal collection of vectors.

Corollary 6 (F., Robins (2005)). *For each such N -tuple t_1, \dots, t_N the lattice*

$$\text{span}_{\mathbb{Z}}\{\mathbf{x}_1, \dots, \mathbf{x}_{N-1}\}$$

is WR and of the form $\Lambda_{\mathbf{a}}$ where \mathbf{a} is the vector with coordinates $a_i = (-1)^{N+1-i} \det(X_{I_i})$ for each $1 \leq i \leq N$.

- If we fix t_2, \dots, t_N in Corollary 6 above, and let $t_1 = t \in \mathbb{Z}_{>0}$ vary, we obtain infinite one-parameter families of WR lattices of the form Λ_a . For each such family bounds on \mathcal{F} given by (1) - (4) will in general be $O\left(t^{2(N-2)}\right)$, while our bound of Corollary 2 will be $O\left(t^{N-1}\right)$.
- WR lattices are essential in coding theory, sphere packings and coverings, kissing number, and related optimization problems.
- C. McMullen recently (2005, JAMS) studied the distribution of *unimodular* WR lattices, proving the six-dimensional case of a famous conjecture of Minkowski as a corollary of his results.
- Our work on the Frobenius problem provides additional motivation to study distribution of WR sublattices of \mathbb{Z}^N ; I have recently done this in case $N = 2$.