Frobenius problem and the covering radius of a lattice

Lenny Fukshansky*
Texas A&M University

Sinai Robins
Temple University

December 2005

Introduction

- $N \geq 2$ an integer

- $a_1 < a_2 < \cdots < a_N$ positive relatively prime integers

Define the *Frobenius number*

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

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

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

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

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

Problem: Given N and $a_1, \ldots, a_N$ find $\mathcal{F}$.

This problem 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.

Explicit formula for the Frobenius number is only known in case $N = 2$:

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

For $N \geq 3$ there has been a number of upper bounds produced in the literature.

Upper bounds

Erdös, Graham (1972):

$$\mathcal{F} \leq 2a_N \left[\frac{a_1}{N}\right] - a_1. \tag{1}$$

Vitek (1975):

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

Selmer (1977):

$$\mathcal{F} \leq 2a_{N-1} \left[\frac{a_N}{N}\right] - a_N. \tag{3}$$

Beck, Diaz, Robins (2002):

$$\mathcal{F} \leq \frac{\sqrt{a_1a_2a_3(a_1+a_2+a_3)} - a_1 - a_2 - a_3}{2}. \tag{4}$$

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:

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

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:

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

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:

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

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 $V_{\boldsymbol{a}}$.

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

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

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

Not hard to prove:

$$2 \leq \lambda_1 \leq \cdots \leq \lambda_{N-1}. \tag{5}$$

Classical results of Jarnik and Minkowski, combined with (5), imply:

$$R_{\boldsymbol{a}} \leq \frac{(N-1)\|\boldsymbol{a}\|}{\omega_{N-1}},$$

where

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

Theorem 1 implies:

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

In the special case when

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

i.e. $\Lambda_{\boldsymbol{a}}$ is a lattice with *equal successive minima* (ESM), we obtain a better bound.

Corollary 2 (F., Robins (2005)). *If $\Lambda_{\boldsymbol{a}}$ is an ESM lattice, then*

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

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

ESM lattices

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

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

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

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

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

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

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

- The proof of Theorem 3 suggests an algorithm that appears to produce infinite one-parameter families of ESM lattices of the form $\Lambda_{\boldsymbol{a}}$ in higher dimensions as well.

- For each such family paramterized by $t \in \mathbb{Z}_{>0}$, 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 $O\left(t^{N-1}\right)$.

- ESM lattices are common in coding theory; they are also related to the shortest vector problem and some engineering applications, such as image processing.

- These results provide additional motivation to further study ESM lattices.