The average Frobenius number

Martin Henk

(joint works with Iskander Aliev and Aicke Hinrichs)

Otto-von-Guericke Universität Magdeburg

Toronto, September, 2010

The Frobenius Number

- Let $a = (a_1, \ldots, a_n) \in \mathbb{N}^n_{>0}$ with $\gcd(a) = 1$.
  The largest integer $\mathrm{F}(a)$ which cannot be written as a non-negative integral combination of $a_1, \ldots, a_n$ is called the *Frobenius number* of a, i.e.,

$$\mathrm{F}(a) = \max\{b \in \mathbb{Z} : b \neq \langle a, z\rangle \text{ for all } z \in \mathbb{N}^n\}.$$

The Frobenius Number

- Let $a = (a_1, \ldots, a_n) \in \mathbb{N}^n_{>0}$ with $\gcd(a) = 1$.
  The largest integer $\mathrm{F}(a)$ which cannot be written as a non-negative integral combination of $a_1, \ldots, a_n$ is called the *Frobenius number* of a, i.e.,

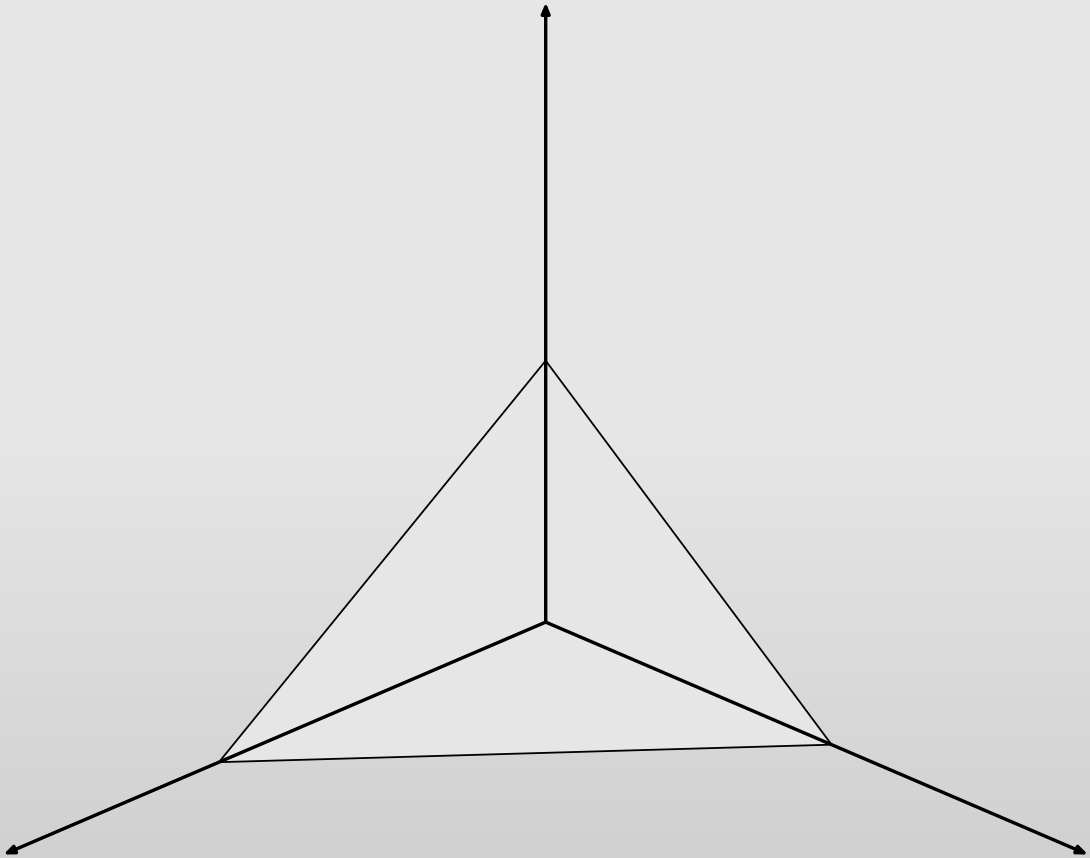
$$\mathrm{F}(a) = \max\{b \in \mathbb{Z} : b \neq \langle a, z\rangle \text{ for all } z \in \mathbb{N}^n\}.$$

- For instance, let $a = (3, 10)$. Then

$$\{\langle a, z\rangle : z \in \mathbb{N}^n\} = \{0,\ 3,\ 6,\ 9, 10,\ 12, 13,\ 15, 16,\ 18, 19, 20, \ldots\}.$$

  Hence $\mathrm{F}(a) = 17$.

- $P(a,b) = \left\{x \in \mathbb{R}^n_{\geq 0} : \langle a, x\rangle = b\right\}$.



- $n = 2$: Sylvester (*most likely*), 1884. $\mathrm{F}(a) = a_1\, a_2 - (a_1 + a_2)$.

- $n = 2$: Sylvester (*most likely*), 1884. $\mathrm{F}(a) = a_1\, a_2 - (a_1 + a_2)$.
- $n \geq 3$: "only" algorithmic solutions.

(Upper) **Bounds**

Let $n \geq 3$ and $a_1 \leq a_2 \leq \cdots \leq a_n$.

- Schur, 1935. $\mathrm{F}(a) \leq a_1\, a_n + a_2 + \cdots + a_{n-1}$.

(Upper) **Bounds**

Let $n \geq 3$ and $a_1 \leq a_2 \leq \cdots \leq a_n$.

- Schur, 1935. $\mathrm{F}(a) \leq a_1\, a_n + a_2 + \cdots + a_{n-1}$.
- A. Brauer, Erdős&Graham, Vitek, Selmer, Beck&Díaz&Robins, Fukshansky&Robins,...

(Upper) **Bounds**

Let $n \geq 3$ and $a_1 \leq a_2 \leq \cdots \leq a_n$.

- Schur, 1935. $\mathrm{F}(a) \leq a_1\, a_n + a_2 + \cdots + a_{n-1}$.
- A. Brauer, Erdős&Graham, Vitek, Selmer, Beck&Díaz&Robins, Fukshansky&Robins,...
- All known upper bounds are of order $|a|_\infty^2$, which is also best possible (Erdős&Graham, 1972; Schlage-Puchta, 2005; V.I. Arnol'd, 2006).

(Lower) **Bounds**

- Rödseth, 1990; Davison, 1994; Aliev&Gruber, 2007;...

$$\mathrm{F}(a) \geq c_n \, (a_1 \, a_2 \cdot \ldots \cdot a_n)^{\frac{1}{n-1}} - (a_1 + \cdots + a_n).$$

(Lower) **Bounds**

- Rödseth, 1990; Davison, 1994; Aliev&Gruber, 2007;...

$$\mathrm{F}(a) \geq c_n \, (a_1 \, a_2 \cdot \ldots \cdot a_n)^{\frac{1}{n-1}} - (a_1 + \cdots + a_n).$$

- If all a_i's are of the same size then all the known lower bounds are of order $|a|_\infty^{1+1/(n-1)}$, which is also best possible (Aliev&Gruber, 2007).

Typical behaviour of $\mathrm{F}(a)$?

- First systematic study by V.I. Arnol'd, 1999.
  He conjectures that $\mathrm{F}(a)$ grows like $T^{1+1/(n-1)}$ for a "typical" vector a with $|a|_1 = T$.

Typical behaviour of $\mathrm{F}(a)$?

- First systematic study by V.I. Arnol'd, 1999.
  He conjectures that $\mathrm{F}(a)$ grows like $T^{1+1/(n-1)}$ for a "typical" vector a with $|a|_1 = T$.

- Let $T > 0$ and let

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

  Bourgain&Sinaĭ, 2007.

$$\mathrm{Prob}\left(\mathrm{F}(a)/T^{1+1/(n-1)} \geq D\right) \leq \epsilon(D),$$

  where $\epsilon(D)$ does not depend on T and tends to 0 as D approaches infinity.

- Aliev&H., 2008.

$$\mathrm{Prob}\left(\mathrm{F}(a)/|a|_\infty^{1+1/(n-1)} \geq D\right) \ll_n D^{-2}.$$

- Aliev&H., 2008.

$$\mathrm{Prob}\left(\mathrm{F}(a)/|a|_\infty^{1+1/(n-1)} \geq D\right) \ll_n D^{-2}.$$

- Aliev&H., 2008.

$$\frac{\sum_{a\in \mathrm{G}(n,T)} \mathrm{F}(a)/|a|_\infty^{1+1/(n-1)}}{\#\mathrm{G}(n,T)} \ll_n 1.$$

- Aliev&H., 2008.

$$\mathrm{Prob}\left(\mathrm{F}(a)/|a|_\infty^{1+1/(n-1)} \geq D\right) \ll_n D^{-2}.$$

- Aliev&H., 2008.

$$\frac{\sum_{a\in \mathrm{G}(n,T)} \mathrm{F}(a)/|a|_\infty^{1+1/(n-1)}}{\#\mathrm{G}(n,T)} \ll_n 1.$$

So the "average" Frobenius number does not essentially exceed $|a|_\infty^{1+1/(n-1)}$.

- Problem. Can we replace $|a|_\infty^{1+1/(n-1)}$ by the "lower bound"

$$\sim (a_1\, a_2\, \cdot \ldots \cdot\, a_n)^{1/(n-1)}\, ?$$

Conjectured (in a stronger form) by Arnol'd, 1999/2003 and extensive computations by Beihoffer et al, 2005 suggest "Yes"!

- Problem. Can we replace $|a|_\infty^{1+1/(n-1)}$ by the "lower bound"

$$\sim (a_1\, a_2\, \cdot \ldots \cdot\, a_n)^{1/(n-1)}\, ?$$

Conjectured (in a stronger form) by Arnol'd, 1999/2003 and extensive computations by Beihoffer et al, 2005 suggest "Yes"!

- Marklof, 2009. (Shchur, Sinaĭ, Ustinov, 2008). Let $n \geq 3$. There exists a continuous non-increasing function $\Psi_n : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ with $\Psi_n(0) = 1$, such that

$$\lim_{T\to\infty} \mathrm{Prob}\left(\mathrm{F}(a)/\,(a_1\, a_2 \cdot \ldots \cdot\, a_n)^{\frac{1}{n-1}} \geq D\right) = \Psi_n(D).$$

- Problem. Can we replace $|a|_\infty^{1+1/(n-1)}$ by the "lower bound"

$$\sim (a_1\, a_2\, \cdot \ldots \cdot\, a_n)^{1/(n-1)}\, ?$$

Conjectured (in a stronger form) by Arnol'd, 1999/2003 and extensive computations by Beihoffer et al, 2005 suggest "Yes"!

- Marklof, 2009. (Shchur, Sinaĭ, Ustinov, 2008). Let $n \geq 3$. There exists a continuous non-increasing function $\Psi_n : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ with $\Psi_n(0) = 1$, such that

$$\lim_{T\to\infty} \mathrm{Prob}\left(\mathrm{F}(a)/\,(a_1\, a_2 \cdot \ldots \cdot\, a_n)^{\frac{1}{n-1}} \geq D\right) = \Psi_n(D).$$

Moreover, $\Psi_n(\cdot)$ is the probability distribution for the inhomogeneous minimum of the $(n-1)$-standard simplex with respect to a random lattice of determinant 1.

Observation

- $$\mathrm{Prob}\left(\mathrm{F}(a)/|a|_1^{1+1/(n-1)} \geq D\right) \ll_n D^{-2}.$$

Observation

- $$\mathrm{Prob}\left(\mathrm{F}(a)/|a|_1^{1+1/(n-1)} \geq D\right) \ll_n D^{-2}.$$

- All what is missing, is a (lattice) reverse Geometric-Arithmetic Mean Inequality (*with high probability*), i.e., for large γ, say, we want to show that

$$\mathrm{Prob}\left(\frac{|a|_1^{1+\frac{1}{n-1}}}{(a_1 \cdot \ldots \cdot a_n)^{\frac{1}{n-1}}} \geq \gamma\right) = \mathrm{Prob}\left(\frac{\frac{1}{n}|a|_1}{(a_1 \cdot \ldots \cdot a_n)^{\frac{1}{n}}} \geq \frac{1}{n}\gamma^{\frac{n-1}{n}}\right)$$

  is small.

Reverse (Lattice) Geometric-Arithmetic Mean Inequality

- Gluskin&Milman, 2003.

$$\mathrm{Prob}\left(x \in \mathbb{S}^{n-1} : \frac{\sqrt{\frac{1}{n}\sum_{i=1}^{n} x_i^2}}{\left(\prod_{i=1}^{n} |x_i|\right)^{1/n}} \geq \gamma : \right) \ll_n \gamma^{-n/2}.$$

Reverse (Lattice) Geometric-Arithmetic Mean Inequality

- Gluskin&Milman, 2003.

$$\mathrm{Prob}\left(x \in \mathbb{S}^{n-1} : \frac{\sqrt{\frac{1}{n}\sum_{i=1}^{n} x_i^2}}{\left(\prod_{i=1}^{n} |x_i|\right)^{1/n}} \geq \gamma :\right) \ll_n \gamma^{-n/2}.$$

- Aliev&H.&Hinrichs, 2009. Let $n \geq 3$. Then

$$\mathrm{Prob}\left(\frac{\frac{1}{n}|a|_1}{\left(\prod_{i=1}^{n} a_i\right)^{1/n}} \geq \gamma\right) \ll_n \gamma^{-(n-1)}.$$

Reverse (Lattice) Geometric-Arithmetic Mean Inequality

- Gluskin&Milman, 2003.

$$\mathrm{Prob}\left(x \in \mathbb{S}^{n-1} : \frac{\sqrt{\frac{1}{n}\sum_{i=1}^{n} x_i^2}}{\left(\prod_{i=1}^{n} |x_i|\right)^{1/n}} \geq \gamma :\right) \ll_n \gamma^{-n/2}.$$

- Aliev&H.&Hinrichs, 2009. Let $n \geq 3$. Then

$$\mathrm{Prob}\left(\frac{\frac{1}{n}|a|_1}{\left(\prod_{i=1}^{n} a_i\right)^{1/n}} \geq \gamma\right) \ll_n \gamma^{-(n-1)}.$$

- Aliev&H.&Hinrichs, 2009. Let $n \geq 3$. Then
  - $$\mathrm{Prob}\left(\frac{\mathrm{F}(a)}{(a_1\, a_2 \cdot \ldots \cdot a_n)^{\frac{1}{n-1}}} \geq D\right) \ll_n D^{-2\frac{n-1}{n+1}}.$$

Reverse (Lattice) Geometric-Arithmetic Mean Inequality

- Gluskin&Milman, 2003.

$$\mathrm{Prob}\left(x \in \mathbb{S}^{n-1} : \frac{\sqrt{\frac{1}{n}\sum_{i=1}^{n} x_i^2}}{\left(\prod_{i=1}^{n} |x_i|\right)^{1/n}} \geq \gamma :\right) \ll_n \gamma^{-n/2}.$$

- Aliev&H.&Hinrichs, 2009. Let $n \geq 3$. Then

$$\mathrm{Prob}\left(\frac{\frac{1}{n}|a|_1}{\left(\prod_{i=1}^{n} a_i\right)^{1/n}} \geq \gamma\right) \ll_n \gamma^{-(n-1)}.$$

- Aliev&H.&Hinrichs, 2009. Let $n \geq 3$. Then
  - $$\mathrm{Prob}\left(\frac{\mathrm{F}(a)}{(a_1\, a_2 \cdot \ldots \cdot a_n)^{\frac{1}{n-1}}} \geq D\right) \ll_n D^{-2\frac{n-1}{n+1}}.$$
  - $$\frac{\sum_{a \in \mathrm{G}(T)} \mathrm{F}(a)/\left(a_1\, a_2 \cdot \ldots \cdot a_n\right)^{\frac{1}{n-1}}}{\#\mathrm{G}(n,T)} \ll\gg_n 1.$$

Generalizations

- Let $A \in \mathbb{Z}^{m \times n}$ be a *generic* integral $(m \times n)$-matrix, and for $b \in \mathbb{Z}^m$ let $P(A, b) = \{x \in \mathbb{R}^n_{\geq 0} : A\,x = b\}$. We are interested in the structure of the set

$$\mathcal{F}(A) = \left\{b \in \mathbb{Z}^m : P(A, b) \cap \mathbb{Z}^n \neq \emptyset\right\}.$$

Generalizations

- Let $A \in \mathbb{Z}^{m\times n}$ be a *generic* integral $(m \times n)$-matrix, and for $b \in \mathbb{Z}^m$ let $P(A,b) = \{x \in \mathbb{R}^n_{\geq 0} : Ax = b\}$. We are interested in the structure of the set

$$\mathcal{F}(A) = \left\{b \in \mathbb{Z}^m : P(A,b) \cap \mathbb{Z}^n \neq \emptyset\right\}.$$

- Aliev&H., 2010. "Similar" results as in the case $m = 1$.

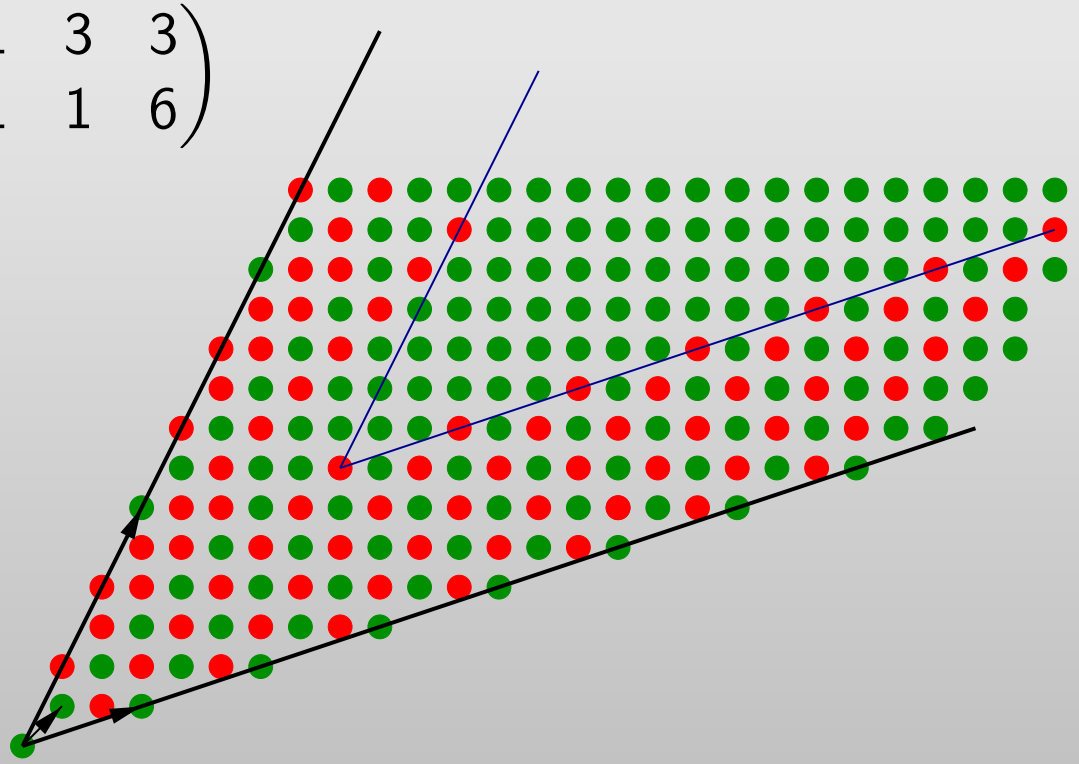
Generalizations

- Let $A \in \mathbb{Z}^{m\times n}$ be a *generic* integral $(m \times n)$-matrix, and for $b \in \mathbb{Z}^m$ let $P(A,b) = \{x \in \mathbb{R}^n_{\geq 0} : Ax = b\}$. We are interested in the structure of the set

$$\mathcal{F}(A) = \left\{b \in \mathbb{Z}^m : P(A,b) \cap \mathbb{Z}^n \neq \emptyset\right\}.$$

- Aliev&H., 2010. "Similar" results as in the case $m = 1$.

- $A = \begin{pmatrix} 1 & 3 & 3 \\ 1 & 1 & 6 \end{pmatrix}$



Idea(s) and ingredients of the proof

$$\mathrm{Prob}\left(\mathrm{F}(a)/|a|_\infty^{1+1/(n-1)} \geq D\right) \ll_n D^{-2}$$

Idea(s) and ingredients of the proof

$$\mathrm{Prob}\left(\mathrm{F}(a)/|a|_\infty^{1+1/(n-1)} \geq D\right) \ll_n D^{-2}$$

- Let

$$\Lambda_a = \frac{1}{\|a\|^{1/(n-1)}} \left\{x \in \mathbb{Z}^n : \langle a, x\rangle = 0\right\}.$$

Then $\det \Lambda_a = 1$, and let B_{n-1} be the $(n-1)$-dimensional unit ball in $\mathrm{lin}\, \Lambda_a$.

Idea(s) and ingredients of the proof

$$\mathrm{Prob}\left(\mathrm{F}(a)/|a|_\infty^{1+1/(n-1)} \geq D\right) \ll_n D^{-2}$$

- Let

$$\Lambda_a = \frac{1}{\|a\|^{1/(n-1)}} \{x \in \mathbb{Z}^n : \langle a, x\rangle = 0\}.$$

Then $\det \Lambda_a = 1$, and let B_{n-1} be the $(n-1)$-dimensional unit ball in $\mathrm{lin}\,\Lambda_a$.

- Based on results of Kannan, 1988, Fukshansky&Robins, 2007, (see also Arnol'd, 2006) one can show

$$\mathrm{F}(a) \leq n^3\ |a|_\infty^{1+1/(n-1)} \mu(\Lambda_a),$$

where $\mu(\Lambda_a) = \min\{\mu > 0 : \Lambda_a + \mu B_{n-1} = \mathrm{lin}\,\Lambda_a\}$ is called the inhomogeneous minimum of Λ_a.

- Jarnik's, 1941, inequality finally gives

$$\frac{\mathrm{F}(a)}{|a|_\infty^{1+1/(n-1)}} \leq n^4\, \lambda_{n-1}(\Lambda_a),$$

where

$$\lambda_i(\Lambda_a) = \min\{\lambda > 0 : \dim(\lambda\, B_{n-1} \cap \Lambda_a) \geq i\}$$

is called the i-th successive minimum of Λ_a.

- Jarnik's, 1941, inequality finally gives

$$\frac{\mathrm{F}(a)}{|a|_\infty^{1+1/(n-1)}} \leq n^4\, \lambda_{n-1}(\Lambda_a),$$

where

$$\lambda_i(\Lambda_a) = \min\{\lambda > 0 : \dim(\lambda\, B_{n-1} \cap \Lambda_a) \geq i\}$$

is called the i-th successive minimum of Λ_a.

- Since $\det \Lambda_a = 1$, and based on Minkowski's theorems on successive minima one can show that there exists an $i \in \{1, \ldots, n-2\}$ with

$$\frac{\mathrm{F}(a)}{|a|_\infty^{1+1/(n-1)}} < c_n \left(\frac{\lambda_{i+1}(\Lambda_a)}{\lambda_i(\Lambda_a)}\right)^{\frac{n-2}{2}}.$$

- Jarnik's, 1941, inequality finally gives

$$\frac{\mathrm{F}(a)}{|a|_\infty^{1+1/(n-1)}} \leq n^4\, \lambda_{n-1}(\Lambda_a),$$

where

$$\lambda_i(\Lambda_a) = \min\{\lambda > 0 : \dim(\lambda\, B_{n-1} \cap \Lambda_a) \geq i\}$$

is called the i-th successive minimum of Λ_a.

- Since $\det \Lambda_a = 1$, and based on Minkowski's theorems on successive minima one can show that there exists an $i \in \{1, \ldots, n-2\}$ with

$$\frac{\mathrm{F}(a)}{|a|_\infty^{1+1/(n-1)}} < c_n \left(\frac{\lambda_{i+1}(\Lambda_a)}{\lambda_i(\Lambda_a)}\right)^{\frac{n-2}{2}}.$$

- Based on results of W. Schmidt, 1998 on the distribution of primitive sublattices of $\mathbb{Z}^n$ one can show that the right hand side is small (with high probability).

The End

Thank you for your attention!