Generalized Frobenius numbers: bounds and average behavior via geometric techniques

Lenny Fukshansky
Claremont McKenna College

International meeting on numerical semigroups with applications
Levico Terme 2016

Integer Knapsack Problem

Let $N \geq 2$ be an integer, $\boldsymbol{a} \in \mathbb{Z}_{>0}^N$ with

$$a_1 < \cdots < a_N, \quad \gcd(a_1, \ldots, a_N) = 1,$$

and $b \in \mathbb{Z}_{>0}$.

Integer Knapsack Problem

Let $N \geq 2$ be an integer, $\boldsymbol{a} \in \mathbb{Z}_{>0}^N$ with

$$a_1 < \cdots < a_N, \quad \gcd(a_1, \ldots, a_N) = 1,$$

and $b \in \mathbb{Z}_{>0}$.

The corresponding **knapsack polytope** is

$$P(\boldsymbol{a}, b) = \left\{ \boldsymbol{x} \in \mathbb{R}_{>0}^N : \sum_{i=1}^N a_i x_i = b \right\}.$$

Integer Knapsack Problem

Let $N \geq 2$ be an integer, $\boldsymbol{a} \in \mathbb{Z}_{>0}^N$ with

$$a_1 < \cdots < a_N, \quad \gcd(a_1, \ldots, a_N) = 1,$$

and $b \in \mathbb{Z}_{>0}$.

The corresponding **knapsack polytope** is

$$P(\boldsymbol{a}, b) = \left\{ \boldsymbol{x} \in \mathbb{R}_{>0}^N : \sum_{i=1}^{N} a_i x_i = b \right\}.$$

Integer Knapsack Problem: Is $P(\boldsymbol{a}, b) \cap \mathbb{Z}^N = \emptyset$?

Integer Knapsack Problem

Let $N \geq 2$ be an integer, $\boldsymbol{a} \in \mathbb{Z}_{>0}^N$ with

$$a_1 < \cdots < a_N, \quad \gcd(a_1, \ldots, a_N) = 1,$$

and $b \in \mathbb{Z}_{>0}$.

The corresponding **knapsack polytope** is

$$P(\boldsymbol{a}, b) = \left\{ \boldsymbol{x} \in \mathbb{R}_{>0}^N : \sum_{i=1}^N a_i x_i = b \right\}.$$

Integer Knapsack Problem: Is $P(\boldsymbol{a}, b) \cap \mathbb{Z}^N = \emptyset$?

This problem is known to be NP-complete.

Frobenius Problem

For $s \in \mathbb{Z}_{\geq 0}$, the s-**Frobenius number** of $\boldsymbol{a}$ is defined to be

$$g_s(\boldsymbol{a}) = \max\left\{ b \in \mathbb{Z}_{>0} : \left| P(\boldsymbol{a}, b) \cap \mathbb{Z}^N \right| = s \right\}.$$

This is well-defined, since $\gcd(a_1, ..., a_N) = 1$.

Frobenius Problem

For $s \in \mathbb{Z}_{\geq 0}$, the s-**Frobenius number** of $\boldsymbol{a}$ is defined to be

$$g_s(\boldsymbol{a}) = \max\left\{ b \in \mathbb{Z}_{>0} : \left| P(\boldsymbol{a}, b) \cap \mathbb{Z}^N \right| = s \right\}.$$

This is well-defined, since $\gcd(a_1, ..., a_N) = 1$. This was first defined for $s = 0$ in the lectures of G. Frobenius and for $s \geq 1$ by M. Beck & S. Robins (2003).

Frobenius Problem

For $s \in \mathbb{Z}_{\geq 0}$, the s-**Frobenius number** of $\boldsymbol{a}$ is defined to be

$$g_s(\boldsymbol{a}) = \max \left\{ b \in \mathbb{Z}_{>0} : \left| P(\boldsymbol{a}, b) \cap \mathbb{Z}^N \right| = s \right\}.$$

This is well-defined, since $\gcd(a_1, ..., a_N) = 1$. This was first defined for $s = 0$ in the lectures of G. Frobenius and for $s \geq 1$ by M. Beck & S. Robins (2003).

Frobenius Problem (FP): Given N and $\boldsymbol{a}$ as above, find $g_0(\boldsymbol{a})$.

Frobenius Problem

For $s \in \mathbb{Z}_{\geq 0}$, the s-**Frobenius number** of $\boldsymbol{a}$ is defined to be

$$g_s(\boldsymbol{a}) = \max\left\{ b \in \mathbb{Z}_{>0} : \left| P(\boldsymbol{a}, b) \cap \mathbb{Z}^N \right| = s \right\}.$$

This is well-defined, since $\gcd(a_1, \dots, a_N) = 1$. This was first defined for $s = 0$ in the lectures of G. Frobenius and for $s \geq 1$ by M. Beck & S. Robins (2003).

Frobenius Problem (FP): Given N and $\boldsymbol{a}$ as above, find $g_0(\boldsymbol{a})$.

Theorem 1 (Ramirez-Alfonsin, 1994)

Frobenius problem is NP-hard.

Frobenius Problem

For $s \in \mathbb{Z}_{\geq 0}$, the s-**Frobenius number** of $\boldsymbol{a}$ is defined to be

$$g_s(\boldsymbol{a}) = \max\left\{ b \in \mathbb{Z}_{>0} : \left| P(\boldsymbol{a}, b) \cap \mathbb{Z}^N \right| = s \right\}.$$

This is well-defined, since $\gcd(a_1, ..., a_N) = 1$. This was first defined for $s = 0$ in the lectures of G. Frobenius and for $s \geq 1$ by M. Beck & S. Robins (2003).

Frobenius Problem (FP): Given N and $\boldsymbol{a}$ as above, find $g_0(\boldsymbol{a})$.

Theorem 1 (Ramirez-Alfonsin, 1994)

Frobenius problem is NP-hard.

Theorem 2 (Kannan, 1992)

For each fixed N, the problem of finding the Frobenius number of a given N-tuple is P.

In terms of numerical semigroups...

For an integer $N \geq 2$ and $\boldsymbol{a} \in \mathbb{Z}_{>0}^N$ with

$$a_1 < \cdots < a_N, \quad \gcd(a_1, \ldots, a_N) = 1,$$

the sub-semigroup of $\mathbb{N}$ generated by $\boldsymbol{a} := (a_1, \ldots, a_N)$ is

$$S(\boldsymbol{a}) := \left\{ \sum_{i=1}^{N} a_i x_i : x_1, \ldots, x_N \in \mathbb{Z}_{\geq 0} \right\}.$$

In terms of numerical semigroups...

For an integer $N \geq 2$ and $\boldsymbol{a} \in \mathbb{Z}_{>0}^N$ with

$$a_1 < \cdots < a_N, \quad \gcd(a_1, \ldots, a_N) = 1,$$

the sub-semigroup of $\mathbb{N}$ generated by $\boldsymbol{a} := (a_1, \ldots, a_N)$ is

$$S(\boldsymbol{a}) := \left\{ \sum_{i=1}^{N} a_i x_i : x_1, \ldots, x_N \in \mathbb{Z}_{\geq 0} \right\}.$$

Set of gaps of $S(\boldsymbol{a})$ is $\mathbb{N} \setminus S(\boldsymbol{a})$, so $g_0(\boldsymbol{a})$ is the largest gap of $S(\boldsymbol{a})$.

In terms of numerical semigroups...

For an integer $N \geq 2$ and $\boldsymbol{a} \in \mathbb{Z}_{>0}^N$ with

$$a_1 < \cdots < a_N, \quad \gcd(a_1, \ldots, a_N) = 1,$$

the sub-semigroup of $\mathbb{N}$ generated by $\boldsymbol{a} := (a_1, \ldots, a_N)$ is

$$S(\boldsymbol{a}) := \left\{ \sum_{i=1}^{N} a_i x_i : x_1, \ldots, x_N \in \mathbb{Z}_{\geq 0} \right\}.$$

Set of gaps of $S(\boldsymbol{a})$ is $\mathbb{N} \setminus S(\boldsymbol{a})$, so $g_0(\boldsymbol{a})$ is the largest gap of $S(\boldsymbol{a})$. More generally, $g_s(\boldsymbol{a})$ is the largest $t \in S(\boldsymbol{a})$ that has *precisely s* different representations of the form

$$t = \sum_{i=1}^{N} a_i x_i \text{ for some } x_1, \ldots, x_N \in \mathbb{Z}_{\geq 0}.$$

Research Directions

When $N = 2$,

$$g_s(a_1, a_2) = (s+1)a_1 a_2 - a_1 - a_2.$$

This formula was obtained in 1884 for $s = 0$ and for $s \geq 1$ by M. Beck & S. Robins (2003).

Research Directions

When $N = 2$,

$$g_s(a_1, a_2) = (s + 1)a_1 a_2 - a_1 - a_2.$$

This formula was obtained in 1884 for $s = 0$ and for $s \geq 1$ by M. Beck & S. Robins (2003).

For $N \geq 3$ there currently are no known *elementary* formulas for the Frobenius numbers.

Research Directions

When $N = 2$,

$$g_s(a_1, a_2) = (s + 1)a_1 a_2 - a_1 - a_2.$$

This formula was obtained in 1884 for $s = 0$ and for $s \geq 1$ by M. Beck & S. Robins (2003).

For $N \geq 3$ there currently are no known *elementary* formulas for the Frobenius numbers.

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. Current research on FP includes algorithmic results, formulas for special sequences, theory of numerical semigroups, connections to operations research and discrete geometry, and many other directions.

Some Bounds

The two directions that we will focus on in this talk are:

- General bounds on the Frobenius numbers.

Some Bounds

The two directions that we will focus on in this talk are:

- General bounds on the Frobenius numbers.
- Average behavior of Frobenius numbers.

Some Bounds

The two directions that we will focus on in this talk are:

- General bounds on the Frobenius numbers.
- Average behavior of Frobenius numbers.

Lower bounds on g_0: Davison (1994) for $N = 3$ (sharp - $\sqrt{3}$ cannot be improved):

$$g_0(\boldsymbol{a}) \geq \sqrt{3a_1 a_2 a_3} - a_1 - a_2 - a_3$$

Aliev & Gruber (2007) for any N:

$$g_0(\boldsymbol{a}) > \left((N-1)! \prod_{i=1}^{N} a_i \right)^{\frac{1}{N-1}} - \sum_{i=1}^{N} a_i .$$

Upper bounds on g_0 for $N \geq 3$

Erdös, Graham (1972):

$$g_0(\boldsymbol{a}) \leq 2a_N \left[\frac{a_1}{N}\right] - a_1.$$

Vitek (1975):

$$g_0(\boldsymbol{a}) \leq \left[\frac{(a_2-1)(a_N-2)}{2}\right] - 1.$$

Selmer (1977):

$$g_0(\boldsymbol{a}) \leq 2a_{N-1} \left[\frac{a_N}{N}\right] - a_N.$$

Beck, Diaz, Robins (2002):

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

Kannan's geometric approach

We need some geometric notation.

Kannan's geometric approach

We need some geometric notation.

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

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

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

Kannan's geometric approach

We need some geometric notation.

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

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

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

Kannan (1992): $g_0(\boldsymbol{a}) = \mu(\mathcal{S}_{\boldsymbol{a}}, \mathcal{L}_{\boldsymbol{a}}) - \sum_{i=1}^{N} a_i$.

Kannan's geometric approach

We need some geometric notation.

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

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

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

Kannan (1992): $g_0(\boldsymbol{a}) = \mu(\mathcal{S}_{\boldsymbol{a}}, \mathcal{L}_{\boldsymbol{a}}) - \sum_{i=1}^{N} a_i$.

The simplex $\mathcal{S}_{\boldsymbol{a}}$ is not 0-symmetric, which makes explicit bounds on $\mu(\mathcal{S}_{\boldsymbol{a}}, \mathcal{L}_{\boldsymbol{a}})$ difficult to produce.

A related geometric approach

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

Convex body: $B(R)$ = ball of radius $R > 0$ centered at the origin in $V_{\boldsymbol{a}} = \operatorname{span}_{\mathbb{R}} \Lambda_{\boldsymbol{a}}$.

Covering radius: $R_{\boldsymbol{a}} = \inf \{ R \in \mathbb{R}_{>0} : B(R) + \Lambda_{\boldsymbol{a}} = V_{\boldsymbol{a}} \}.$

A related geometric approach

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

Convex body: $B(R)$ = ball of radius $R > 0$ centered at the origin in $V_{\boldsymbol{a}} = \operatorname{span}_{\mathbb{R}} \Lambda_{\boldsymbol{a}}$.

Covering radius: $R_{\boldsymbol{a}} = \inf \left\{ R \in \mathbb{R}_{>0} : B(R) + \Lambda_{\boldsymbol{a}} = V_{\boldsymbol{a}} \right\}.$

Theorem 3 (F., Robins, 2007)

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

A related geometric approach

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

Convex body: $B(R)$ = ball of radius $R > 0$ centered at the origin in $V_{\boldsymbol{a}} = \operatorname{span}_{\mathbb{R}} \Lambda_{\boldsymbol{a}}$.

Covering radius: $R_{\boldsymbol{a}} = \inf \left\{ R \in \mathbb{R}_{>0} : B(R) + \Lambda_{\boldsymbol{a}} = V_{\boldsymbol{a}} \right\}$.

Theorem 3 (F., Robins, 2007)

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

This bound is symmetric in all $a_1, \ldots, a_N$, unlike the previously known ones. The covering radius $R_{\boldsymbol{a}}$ can be bounded by standard techniques in the geometry of numbers.

Bounds on g_s for $s \geq 1$

Extending our previous method, we obtain:

Theorem 4 (F., Schürmann, 2011)

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

$$g_s(\boldsymbol{a}) \ll_N \max \left\{ \frac{R_{\boldsymbol{a}} \sum_{i=1}^{N} a_i \sqrt{\|\boldsymbol{a}\|^2 - a_i^2}}{\|\boldsymbol{a}\|}, \left(s \prod_{i=1}^{N-1} a_i \right)^{\frac{1}{N-2}} \right\},$$

where the lower bound holds for sufficiently large s.

Another s-Frobenius number g_s^*

Beck & Kifer (2011) defined a related generalized Frobenius number: $g_s^*(\boldsymbol{a})$ is the largest t that has *at most* s different representations of the form

$$t = \sum_{i=1}^{N} a_i x_i \text{ for some } x_1, \dots, x_N \in \mathbb{Z}_{\geq 0}.$$

Another s-Frobenius number g_s^*

Beck & Kifer (2011) defined a related generalized Frobenius number: $g_s^*(\boldsymbol{a})$ is the largest t that has *at most s* different representations of the form

$$t = \sum_{i=1}^{N} a_i x_i \text{ for some } x_1, \ldots, x_N \in \mathbb{Z}_{\geq 0}.$$

It is then clear that

$$g_s^*(\boldsymbol{a}) \geq g_s(\boldsymbol{a}),$$

and $g_0 = g_0^*$.

Another s-Frobenius number g_s^*

Beck & Kifer (2011) defined a related generalized Frobenius number: $g_s^*(\boldsymbol{a})$ is the largest t that has *at most s* different representations of the form

$$t = \sum_{i=1}^{N} a_i x_i \text{ for some } x_1, \ldots, x_N \in \mathbb{Z}_{\geq 0}.$$

It is then clear that

$$g_s^*(\boldsymbol{a}) \geq g_s(\boldsymbol{a}),$$

and $g_0 = g_0^*$.

This may be a more convenient definition of an s-Frobenius number – we will focus on it for the rest of the talk.

Bounds on g_s^*

We now present bounds on g_s^*, which have very similar order of magnitude as our previous bounds on g_s.

Theorem 5 (Aliev, F., Henk (2012))

Let $N \geq 3$, $s \geq 0$. *Then*

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

and

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

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).

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

$$\Sigma(\boldsymbol{a}) := a_1 + \cdots + a_N \to \infty.$$

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

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

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 Ω_N^1 be an ensemble of relatively prime positive integer N-tuples $\boldsymbol{a} = (a_1, \ldots, a_N)$ with

$$\Sigma(\boldsymbol{a}) := a_1 + \cdots + a_N \to \infty.$$

Arnold conjectured that for a "typical" N-tuple $\boldsymbol{a}$ from Ω_N^1,

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

Variants of Arnold's conjecture have been considered by a number of authors, including I. Aliev, J. Bourgain, M. Henk, A. Hinrichs, H. Li, J. Marklof, V. Shchur, W. M. Schmidt, Y. Sinai, A. Strömbergson, C. Ulcigrai, A. Ustinov.

Average value estimate for g_s^*

Theorem 6 (Aliev, F., Henk (2012))

Let $N \geq 3$, $s \geq 0$, and let

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

Let $D > 0$. Then there exists $T_0(D)$ such that for all $T \geq T_0(D)$, with respect to the uniform probability distribution on $\mathrm{G}(T)$,

$$\mathrm{Prob}\left(\frac{g_s^*(\boldsymbol{a})}{\left((s+1)\prod_{i=1}^{N-1} a_i\right)^{\frac{1}{N-1}}} \geq D \right) \ll_N \frac{1}{D^{N-1}}.$$

Average value estimate for g_s^*

Theorem 6 (Aliev, F., Henk (2012))

Let $N \geq 3$, $s \geq 0$, *and let*

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

Let $D > 0$. *Then there exists* $T_0(D)$ *such that for all* $T \geq T_0(D)$, *with respect to the uniform probability distribution on* $\mathrm{G}(T)$,

$$\mathrm{Prob}\left(\frac{g_s^*(\boldsymbol{a})}{\left((s+1)\prod_{i=1}^{N-1} a_i\right)^{\frac{1}{N-1}}} \geq D \right) \ll_N \frac{1}{D^{N-1}}.$$

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.

Proof Ingredients

- To prove Theorems 3 and 4, we relate Frobenius numbers to the number of integer lattice points in a certain simplex, and then apply techniques from the geometry of numbers to produce counting estimates.

Proof Ingredients

- To prove Theorems 3 and 4, we relate Frobenius numbers to the number of integer lattice points in a certain simplex, and then apply techniques from the geometry of numbers to produce counting estimates.
- To prove Theorem 5, we introduce the notion of s-**covering radius** for a convex body with respect to a lattice, generalizing the usual covering radius, and relate s-Frobenius numbers to $(s+1)$-covering radii, analogously to Kannan's formula.

Proof Ingredients

- To prove Theorems 3 and 4, we relate Frobenius numbers to the number of integer lattice points in a certain simplex, and then apply techniques from the geometry of numbers to produce counting estimates.
- To prove Theorem 5, we introduce the notion of s-**covering radius** for a convex body with respect to a lattice, generalizing the usual covering radius, and relate s-Frobenius numbers to $(s+1)$-covering radii, analogously to Kannan's formula.
- To prove Theorem 6, we use the bounds of Theorem 5 along with H. Li's result for g_0 and the fact that "reverse" arithmetic-geometric mean inequality holds with high probability.

Thank you!