

On the limit distribution of Frobenius numbers

by

ANDREAS STRÖMBERGSSON (Uppsala)

1. Introduction. We denote by $\widehat{\mathbb{N}}^d$ the set of integer vectors in \mathbb{R}^d with positive coprime coefficients (viz. the greatest common divisor of all coefficients is one). Given $\mathbf{a} = (a_1, \dots, a_d) \in \widehat{\mathbb{N}}^d$, the *Frobenius number* $g(\mathbf{a}) = g(a_1, \dots, a_d)$ is defined as the largest integer which is not representable as a non-negative integer combination of a_1, \dots, a_d . The problem of computing $g(\mathbf{a})$ is known as the *Frobenius problem* or the *coin exchange problem*, and it has been studied extensively (see, e.g., [23] and [16, Problem C7]).

In the majority of problems related to Frobenius numbers, it is more convenient to consider the function

$$(1.1) \quad f(\mathbf{a}) = f(a_1, \dots, a_d) = g(a_1, \dots, a_d) + a_1 + \dots + a_d.$$

Clearly, $f(\mathbf{a})$ is the largest integer which is not a *positive* integer combination of a_1, \dots, a_d .

In the case of two variables, $d = 2$, the Frobenius number is given by Sylvester's formula ([23, Theorem 2.1.1]),

$$(1.2) \quad g(a_1, a_2) = a_1 a_2 - a_1 - a_2 \quad (\text{viz., } f(a_1, a_2) = a_1 a_2).$$

For $d \geq 3$ no explicit formula is known. Arnold [4]–[6] asked about the behavior of $g(a_1, \dots, a_d)$ for a “random” large vector $(a_1, \dots, a_d) \in \mathbb{R}^d$. Davison had previously asked similar questions for $d = 3$, in [11, Sec. 5]. Recently Marklof [19] obtained a definitive result for arbitrary $d \geq 3$, generalizing previous results by Bourgain and Sinai [9] in the case $d = 3$ (cf. also Shchur, Sinai and Ustinov [32]):

THEOREM 1 (Marklof [19]). *Given $d \geq 3$, there exists a continuous non-increasing function $\Psi_d : \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}_{\geq 0}$ with $\Psi_d(0) = 1$, such that for any bounded set $\mathcal{D} \subset \mathbb{R}_{> 0}^d$ with non-empty interior and boundary of Lebesgue*

2010 *Mathematics Subject Classification*: Primary 11D07; Secondary 11H31.

Key words and phrases: Frobenius number, limit distribution, lattice covering.

measure zero, and any $R \geq 0$,

$$(1.3) \quad \lim_{T \rightarrow \infty} \frac{1}{\#(\widehat{\mathbb{N}}^d \cap T\mathcal{D})} \# \left\{ \mathbf{a} \in \widehat{\mathbb{N}}^d \cap T\mathcal{D} : \frac{f(\mathbf{a})}{(a_1 \cdots a_d)^{1/(d-1)}} > R \right\} = \Psi_d(R).$$

For arbitrary $d \geq 3$, Li [18, Thm. 1.3] has recently obtained an effective version of Theorem 1, where (1.3) is proved to hold with a power convergence rate (with respect to T).

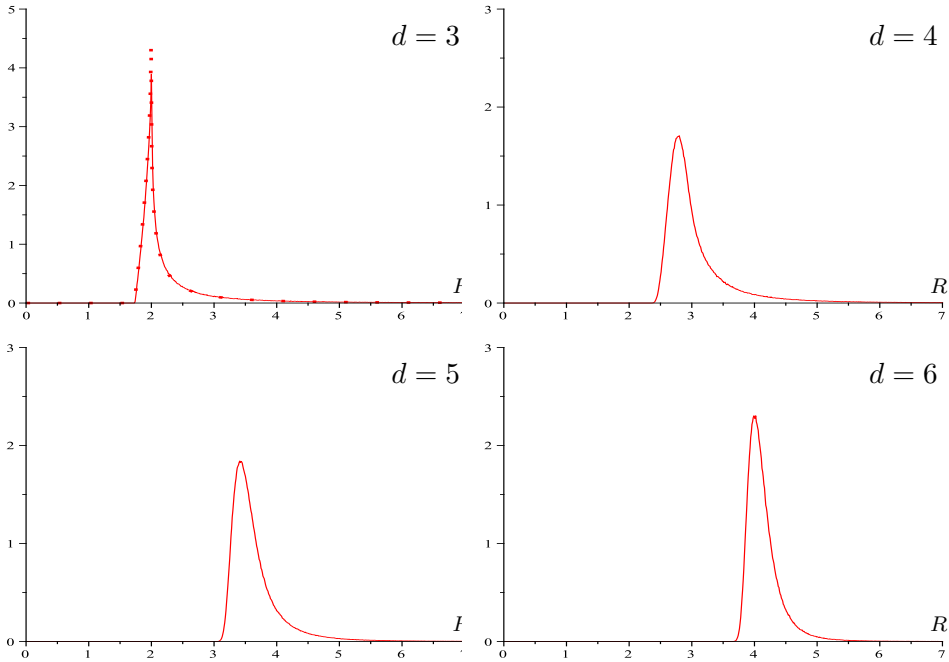


Fig. 1. Experimental graphs of the density functions $\psi_d(R) = -\frac{d}{dR}\Psi_d(R)$ of the limit distribution in Theorem 1, for $d = 3, 4, 5, 6$. The graphs were obtained by computing $(a_1 \cdots a_d)^{-1/(d-1)} f(\mathbf{a})$ for $1.2 \cdot 10^6$ integer vectors \mathbf{a} picked at random in $\widehat{\mathbb{N}}^d \cap [0, T]^d$ with $T = 10^{15}$, and collecting the results into bins of width 0.01 along the R -axis. The computations of $f(\mathbf{a})$ were performed using the Froby software package by Roune [28]; cf. also [29]. We repeated the computations using other random seeds and/or changing T to 10^{14} , as well as to $10^{13}, 10^{12}, 10^{11}$ in some cases, and the resulting graphs were consistently found to be practically indistinguishable, except for $d = 3$ and R very near 2. For $d = 3$ also the graph of the exact function in (1.7) is drawn (the dotted curve, which is distinguishable from the experimental graph only for R very near 2).

Marklof also proved an explicit formula for $\Psi_d(R)$, namely that $\Psi_d(R)$ equals the probability that the simplex

$$(1.4) \quad \Delta = \{ \mathbf{x} \in \mathbb{R}_{\geq 0}^{d-1} : \mathbf{x} \cdot \mathbf{e} \leq 1 \}, \quad \mathbf{e} := (1, \dots, 1),$$

has covering radius larger than R with respect to a random lattice $L \subset \mathbb{R}^{d-1}$ of covolume one. In other words ([19, Thm. 2]),

$$(1.5) \quad \Psi_d(R) = \mu_{d-1}(\{L \in X_{d-1} : \rho(L) > R\}),$$

where X_{d-1} is the set of all lattices $L \subset \mathbb{R}^{d-1}$ of covolume one, μ_{d-1} is Siegel’s measure ([33]) on X_{d-1} , normalized to be a probability measure, and $\rho(L)$ is the covering radius of Δ with respect to L , viz.

$$(1.6) \quad \rho(L) = \inf\{\rho > 0 : L + \rho\Delta = \mathbb{R}^{d-1}\}.$$

In the special case $d = 3$, Ustinov [37] (cf. also [36]) proved a more precise version of (1.3), where the averaging is performed over only two of the three arguments a_1, a_2, a_3 , and the limit is obtained with a power rate of convergence. Ustinov in fact gave a completely explicit formula for the limit density $\psi_3(R) = -\frac{d}{dR}\Psi_3(R)$ in terms of elementary functions:

$$(1.7) \quad \psi_3(R) = \begin{cases} 0 & (0 \leq R \leq \sqrt{3}), \\ \frac{12}{\pi} \left(\frac{R}{\sqrt{3}} - \sqrt{4 - R^2} \right) & (\sqrt{3} \leq R \leq 2), \\ \frac{12}{\pi^2} \left(R\sqrt{3} \arccos\left(\frac{R + 3\sqrt{R^2 - 4}}{4\sqrt{R^2 - 3}} \right) \right. \\ \quad \left. + \frac{3}{2} \sqrt{R^2 - 4} \log\left(\frac{R^2 - 4}{R^2 - 3} \right) \right) & (R > 2). \end{cases}$$

See also [22] for a derivation of (1.7) from (1.5).

Our purpose in the present note is to discuss the behavior of $\Psi_d(R)$ for d fixed and R large, as well as for d large. For fixed $d \geq 3$, it was proved by Li [18] that $\Psi_d(R) \ll_d R^{-(d-1)}$ for all $R > 0$, and Marklof in an unpublished note [20] pointed out that a corresponding lower bound also holds: $\Psi_d(R) \gg_d R^{-(d-1)}$ for all $R \geq 1$. Our first result, which we will prove in Section 2, is an asymptotic formula refining these bounds:

THEOREM 2. *Let $d \geq 3$. Then*

$$(1.8) \quad \Psi_d(R) = \frac{d}{2\zeta(d-1)} R^{-(d-1)} + O_d(R^{-d-1/(d-2)}) \quad \text{as } R \rightarrow \infty.$$

Here the error term is sharp; in fact there exists a constant $c > 0$ which only depends on d , such that for all sufficiently large R ,

$$(1.9) \quad \Psi_d(R) > \frac{d}{2\zeta(d-1)} R^{-(d-1)} + cR^{-d-1/(d-2)}.$$

In particular we may note that (1.7) implies $\Psi_3(R) = \frac{9}{\pi^2} R^{-2} + \frac{33}{2\pi^2} R^{-4} + O(R^{-6})$ as $R \rightarrow \infty$, which is consistent with Theorem 2.

Combining Theorems 1 and 2 we conclude that if R is large, and if \mathbf{a} is picked at random from a set of the type $\widehat{\mathbb{N}}^d \cap T\mathcal{D}$ with T sufficiently large—where the notion of “sufficiently large” may depend on R —then the

probability that the normalized Frobenius number $\frac{f(\mathbf{a})}{(a_1 \cdots a_d)^{1/(d-1)}}$ is greater than R is approximately $\frac{d}{2\zeta(d-1)}R^{-(d-1)}$. It is an interesting problem to try to get a more uniform control on the probability of $\frac{f(\mathbf{a})}{(a_1 \cdots a_d)^{1/(d-1)}}$ being large, i.e. to give bounds from above and below, *uniformly with respect to large T and R* , on

$$(1.10) \quad P_d(T, R) := \frac{1}{\#\widehat{\mathbb{N}}^d \cap T\mathcal{D}} \#\left\{ \mathbf{a} \in \widehat{\mathbb{N}}^d \cap T\mathcal{D} : \frac{f(\mathbf{a})}{(a_1 \cdots a_d)^{1/(d-1)}} > R \right\}.$$

Results related to this question have recently been obtained by Aliev and Henk [2] and Aliev, Henk and Hinrichs [3], by making use of Schmidt's results on the distribution of similarity classes of sublattices of \mathbb{Z}^m [31]. We will show that the application of [31] can be refined—using in particular the strong uniform error bounds which Schmidt provides for his asymptotic formulas—so as to give a uniform bound which significantly improves upon the bounds obtained in [2], [3], and which can be viewed as a T -uniform version of Li's upper bound $\Psi_d(R) \ll_d R^{-(d-1)}$.

For technical reasons we will consider the Frobenius number normalized not with the factor $(a_1 \cdots a_d)^{-1/(d-1)}$, but with $s(\mathbf{a})^{-1}$, where

$$(1.11) \quad s(\mathbf{a}) := \frac{\sum_{j=1}^d a_j \sqrt{\|\mathbf{a}\|^2 - a_j^2}}{\|\mathbf{a}\|^{1-1/(d-1)}},$$

with $\|\mathbf{a}\|$ denoting the standard Euclidean norm of \mathbf{a} . Thus, we set

$$(1.12) \quad \tilde{P}_d(T, R) := \frac{1}{\#\widehat{\mathbb{N}}^d \cap T\mathcal{D}} \#\left\{ \mathbf{a} \in \widehat{\mathbb{N}}^d \cap T\mathcal{D} : \frac{f(\mathbf{a})}{s(\mathbf{a})} > R \right\}.$$

Note that $P_d(T, R)$ and $\tilde{P}_d(T, R)$ are defined for any $T > 0$ such that $\widehat{\mathbb{N}}^d \cap T\mathcal{D} \neq \emptyset$; in particular, for any fixed $\mathcal{D} \subset \mathbb{R}_{\geq 0}^d$ with non-empty interior, $P_d(T, R)$ and $\tilde{P}_d(T, R)$ are defined for all $T \gg_{\mathcal{D}} 1$.

The normalizing factor $s(\mathbf{a})$ was used also in Aliev and Henk [2]; cf. also Fukshansky and Robins [13]. Note that if we assume that the coefficients of \mathbf{a} are ordered so that $a_1 \leq \cdots \leq a_d$ then $s(\mathbf{a}) \asymp_d a_{d-1} a_d^{1/(d-1)}$; in particular we have

$$(1.13) \quad (a_1 \cdots a_d)^{1/(d-1)} \ll_d s(\mathbf{a}) \ll_d \|\mathbf{a}\|^{d/(d-1)}, \quad \forall \mathbf{a} \in \mathbb{R}_{>0}^d.$$

Hence there exists a constant $c_1 > 0$ which only depends on d such that

$$(1.14) \quad \tilde{P}_d(T, c_1 R) \leq P_d(T, R)$$

for any $R > 0$ and any $\mathcal{D} \subset \mathbb{R}_{\geq 0}^d$ and $T > 0$ such that $\widehat{\mathbb{N}}^d \cap T\mathcal{D} \neq \emptyset$. On the other hand, if \mathcal{D} is bounded and satisfies $\overline{\mathcal{D}} \subset \mathbb{R}_{>0}^d$, then $s(\mathbf{a}) \asymp$

$(a_1 \cdots a_d)^{1/(d-1)}$ holds uniformly over all $\mathbf{a} \in \mathbb{R}_{>0}\mathcal{D}$, and thus we have $P_d(T, R) \leq \tilde{P}_d(T, c_2 R)$ for all $T, R > 0$ with $\widehat{\mathbb{N}}^d \cap T\mathcal{D} \neq \emptyset$, where $c_2 > 0$ is a constant which only depends on \mathcal{D} . Hence for any such region \mathcal{D} , any of the two functions $P_d(T, R)$ and $\tilde{P}_d(T, R)$ can essentially be bounded in terms of the other, as long as we allow an implied constant which may depend on \mathcal{D} .

Our main result on $\tilde{P}_d(T, R)$ is the following bound, which we will prove in Section 3.

THEOREM 3. *Let $d \geq 3$, and let $\mathcal{D} \subset \mathbb{R}_{\geq 0}^d$ be bounded with non-empty interior. Then*

$$(1.15) \quad \tilde{P}_d(T, R) \ll_{d, \mathcal{D}} R^{-(d-1)}$$

uniformly over all $T > 0$ with $\widehat{\mathbb{N}}^d \cap T\mathcal{D} \neq \emptyset$, and all $R > 0$. Furthermore, for any such T ,

$$(1.16) \quad \tilde{P}_d(T, R) = 0 \quad \text{whenever} \quad R \geq (T \sup_{\mathbf{x} \in \mathcal{D}} \|\mathbf{x}\|)^{1-1/(d-1)}.$$

Theorem 3 strengthens the bound $\tilde{P}_d(T, R) \ll R^{-2}$ which was given in [2, Thm. 1.1]. Note also that if the set \mathcal{D} satisfies $\overline{\mathcal{D}} \subset \mathbb{R}_{>0}^d$, then by the previous discussion Theorem 3 implies $P_d(T, R) \ll_{d, \mathcal{D}} R^{-(d-1)}$.

From many points of view, the normalization factor $(a_1 \cdots a_d)^{-1/(d-1)}$ is the most natural one to use in the Frobenius problem. A clear indication of this is for example the fact that the limit distribution obtained in Theorem 1 is independent of the choice of \mathcal{D} . Hence it is interesting to ask whether the bound in Theorem 3 is valid also for $P_d(T, R)$, *without* the extra assumption $\overline{\mathcal{D}} \subset \mathbb{R}_{>0}^d$. We conjecture that this is so. However in the present paper we will content ourselves with pointing out a weaker bound, which follows fairly directly from Theorem 3 by an argument along the lines of [3], and which strengthens the bound ⁽¹⁾ $P_d(T, R) \ll R^{-2\frac{d-1}{d+1} + \varepsilon}$ obtained in [3].

COROLLARY 1. *Let $d \geq 3$, and let $\mathcal{D} \subset \mathbb{R}_{\geq 0}^d$ be bounded with non-empty interior. Then*

$$(1.17) \quad P_d(T, R) \ll_{d, \mathcal{D}} R^{-(d-1)/2} (\log(R+2))^{(d-3)/2}$$

uniformly over all $T > 0$ with $\widehat{\mathbb{N}}^d \cap T\mathcal{D} \neq \emptyset$, and all $R > 0$. Furthermore,

$$(1.18) \quad P_d(T, R) = 0 \quad \text{whenever} \quad R \geq d(T \sup_{\mathbf{x} \in \mathcal{D}} \|\mathbf{x}\|)^{1-1/(d-1)}.$$

⁽¹⁾ We here correct a mistake in [3, p. 530, lines 5–6] by adding ε in the exponent: In the notation of [3], the choice of $t = \frac{n-1}{n+1}$ yields the bound $\beta^{-2\frac{(n-1)^2}{n(n+1)}}$ and not $\beta^{-2\frac{n-1}{n+1}}$ as claimed; choosing t optimally yields the bound $\beta^{-2\frac{(n-1)^2}{n^2+1}}$, and using also [3, p. 529, Remark 1] brings the bound down to $\beta^{-2\frac{n-1}{n+1} + \varepsilon}$.

We remark that in the special case $d = 3$, it follows from Ustinov [37, pp. 1025, 1044] that the stronger bound $P_3(T, R) \ll_{\mathcal{D}} R^{-2}$ is valid at least so long as we keep $T \gg R^{22+\varepsilon}$.

It is also interesting to consider the *moments* of the (normalized) Frobenius number; in particular the *expected value* has been considered by many authors (cf., e.g., [3]–[6], [11, Sec. 5], [36]). Note that it follows from Theorem 2 (or just from the upper and lower bounds by Li [18] and Marklof [20]) that the limit distribution described by $\Psi_d(R)$ possesses q th moment for $0 < q < d - 1$ (q not necessarily an integer), and for no larger q . Let us write $M_{d,q}$ for this moment:

$$(1.19) \quad M_{d,q} := - \int_0^\infty R^q d\Psi_d(R) = q \int_0^\infty R^{q-1} \Psi_d(R) dR, \quad 0 < q < d - 1.$$

Now the following is an easy consequence of Theorem 1 combined with Theorem 3 and Corollary 1.

COROLLARY 2. *Let $d \geq 3$, and let $\mathcal{D} \subset \mathbb{R}_{\geq 0}^d$ be a bounded set with non-empty interior and boundary of Lebesgue measure zero. Then for any q in the interval $0 < q < \frac{1}{2}(d - 1)$, we have convergence of moments:*

$$(1.20) \quad \lim_{T \rightarrow \infty} \frac{1}{\#(\widehat{\mathbb{N}}^d \cap T\mathcal{D})} \sum_{\mathbf{a} \in \widehat{\mathbb{N}}^d \cap T\mathcal{D}} \left(\frac{f(\mathbf{a})}{(a_1 \cdots a_d)^{1/(d-1)}} \right)^q = M_{d,q}.$$

If furthermore $\overline{\mathcal{D}} \subset \mathbb{R}_{> 0}^d$, then (1.20) holds for all $0 < q < d - 1$.

We expect that (1.20) should hold for all $0 < q < d - 1$ also without the extra assumption $\overline{\mathcal{D}} \subset \mathbb{R}_{> 0}^d$ (indeed this would follow from our previous conjecture that $P_d(T, R) \ll_{d, \mathcal{D}} R^{-(d-1)}$ holds for general \mathcal{D}). We note that in the special case $d = 3$ and $q = 1$, (1.20) *does* hold for general $\mathcal{D} \subset \mathbb{R}_{\geq 0}^d$ (bounded with non-empty interior); this follows from Ustinov [36, Thm. 1]. We also remark that for $d \geq 4$ and $q = 1$, (1.20) was proved in [3].

Finally let us turn to a slightly different question: What can be said about the limit distribution of Frobenius numbers for d large? Let ρ_{d-1} be the absolute inhomogeneous minimum of Δ , viz.

$$(1.21) \quad \rho_{d-1} = \inf\{\rho(L) : L \in X_{d-1}\}.$$

Using (1.5) and the fact that Ψ_d is continuous ([19, Lemma 7]), one easily shows that

$$(1.22) \quad \Psi_d(R) = 1 \quad \text{for } 0 \leq R \leq \rho_{d-1}, \quad \text{and} \quad \Psi_d(R) < 1 \quad \text{for } R > \rho_{d-1},$$

i.e. the limit distribution described by $\Psi_d(R)$ has support exactly in the interval $[\rho_{d-1}, \infty)$. In fact ρ_{d-1} is not only a lower bound for the support of the limit distribution, but also a lower bound on the normalized Frobenius number for *any* input vector; we have

$$(1.23) \quad \frac{f(\mathbf{a})}{(a_1 \cdots a_d)^{1/(d-1)}} \geq \rho_{d-1}, \quad \forall \mathbf{a} \in \widehat{\mathbb{N}}^d$$

(cf. Aliev and Gruber [1, Thm. 1.1(i)] as well as Rödseth [24]). It was noted in [1, (7)] that

$$(1.24) \quad \rho_{d-1} > (d-1)!^{1/(d-1)}.$$

On the other hand the number ρ_{d-1} is quite near $(d-1)!^{1/(d-1)}$ for d large: It follows from a bound by Rogers [27] on lattice coverings by general convex bodies, refined by Gritzmann [14] in the case of convex bodies satisfying a mild symmetry condition (cf. also [12, Sec. 9], and use the fact that Δ can be mapped to a regular $(d-1)$ -simplex by a volume preserving linear map), that

$$(1.25) \quad \rho_{d-1} \leq (d-1)!^{1/(d-1)} \left(1 + O\left(\frac{\log d}{d}\right) \right) \quad \text{as } d \rightarrow \infty.$$

When computing the Frobenius numbers for modest d and several random large vectors \mathbf{a} , one notes that the normalized values $f(\mathbf{a})/(a_1 \cdots a_d)^{1/(d-1)}$ most often do not exceed the experimental value for the lower bound ρ_{d-1} by more than a constant factor < 2 . This is seen in Figure 1 above in the cases $d = 3, 4, 5, 6$; the same phenomenon was also noted in [7, Sec. 5 (esp. Fig. 17)] for $d = 4$ and $d = 8$. The following result shows that this behavior continues as $d \rightarrow \infty$; indeed, for d large, the distribution described by $\Psi_d(R)$ has almost all of its mass concentrated in the interval between $(d-1)!^{1/(d-1)}$ and $1.757 \cdot (d-1)!^{1/(d-1)}$.

THEOREM 4. *Let $\eta_0 = 0.756 \dots$ be the unique real root of $e \log \eta + \eta = 0$. Then for any $\alpha > 1 + \eta_0$ we have*

$$(1.26) \quad \Psi_d(\alpha(d-1)!^{1/(d-1)}) \rightarrow 0 \quad \text{as } d \rightarrow \infty.$$

We remark that the proof will show that (1.26) holds with an exponential rate, for any fixed $\alpha > 1 + \eta_0$.

Combining Theorem 4 with Theorem 1 and (1.24) implies that for large d , the normalized Frobenius number $f(\mathbf{a})/(a_1 \cdots a_d)^{1/(d-1)}$ is very likely to lie between $(d-1)!^{1/(d-1)}$ and $1.757 \cdot (d-1)!^{1/(d-1)}$. In precise terms, for any fixed $\alpha > \eta_0$ we have

$$(1.27) \quad \lim_{d \rightarrow \infty} \liminf_{T \rightarrow \infty} \frac{1}{\#\{\widehat{\mathbb{N}}^d \cap [0, T]^d\}} \# \left\{ \mathbf{a} \in \widehat{\mathbb{N}}^d \cap [0, T]^d : \right. \\ \left. (d-1)!^{1/(d-1)} < \frac{f(\mathbf{a})}{(a_1 \cdots a_d)^{1/(d-1)}} < \alpha(d-1)!^{1/(d-1)} \right\} = 1.$$

Theorem 4 follows from a modification of a general bound by Rogers on lattice coverings of space with convex bodies [25], further improved by Schmidt [30]. We carry this out in Section 4 below.

REMARK 1. It is an interesting question whether the bound on α in Theorem 4 can be further improved. Could it be that the limit distribution of Frobenius numbers in fact concentrates near $(d-1)!^{1/(d-1)}$ as $d \rightarrow \infty$, in the sense that (1.26) holds for *all* $\alpha > 1$?

It is also an interesting task to try to prove a good *uniform* bound on $\Psi_d(R)$ valid for all large d and R , uniting Theorem 4 and the fact that $\Psi_d(R) \ll_d R^{-(d-1)}$ as $R \rightarrow \infty$. Even more generally, we may ask for a good uniform bound on $P_d(T, R)$ valid for all large d, T, R .

2. The asymptotic behavior of $\Psi_d(R)$ as $R \rightarrow \infty$. In this section we will prove Theorem 2.

2.1. Preliminaries. Let us write $n = d - 1$. Recall that Δ denotes the standard n -dimensional simplex defined in (1.4). Given $L \in X_n$ and $\rho > 0$, we have $L + \rho\Delta = \mathbb{R}^n$ if and only if $\zeta - \rho\Delta$ has non-empty intersection with L for each $\zeta \in \mathbb{R}^n$. Thus, since $L = -L$,

$$(2.1) \quad \rho(L) = \sup\{\rho > 0 : \text{there is } \zeta \in \mathbb{R}^n \text{ such that } L \cap (\rho\Delta - \zeta) = \emptyset\}.$$

It follows that the formula for $\Psi_d(R)$, (1.5), may be rewritten as

$$(2.2) \quad \Psi_d(R) = \mu_n(\{L \in X_n : \text{there is } \zeta \in \mathbb{R}^n \text{ such that } L \cap (R\Delta - \zeta) = \emptyset\}).$$

Let us write $G = G^{(n)} = \mathrm{SL}(n, \mathbb{R})$ and $\Gamma = \Gamma^{(n)} = \mathrm{SL}(n, \mathbb{Z})$. For any $M \in G$, $\mathbb{Z}^n M$ is an n -dimensional lattice of covolume one, and this gives an identification of the space X_n with the homogeneous space $\Gamma \backslash G$. Note that μ_n is the measure on X_n coming from Haar measure on G , normalized to be a probability measure; we write μ_n also for the corresponding Haar measure on G . Let $A = A^{(n)}$ be the subgroup of G consisting of the diagonal matrices with positive entries

$$(2.3) \quad \mathbf{a}(a) = \begin{pmatrix} a_1 & & & \\ & \ddots & & \\ & & \ddots & \\ & & & a_n \end{pmatrix} \in G, \quad a_j > 0,$$

and let $N = N^{(n)}$ be the subgroup of upper triangular matrices

$$(2.4) \quad \mathbf{n}(u) = \begin{pmatrix} 1 & u_{12} & \cdots & u_{1n} \\ & \ddots & \ddots & \vdots \\ & & \ddots & u_{n-1,n} \\ & & & 1 \end{pmatrix} \in G.$$

Every element $M \in G$ has a unique Iwasawa decomposition

$$(2.5) \quad M = \mathfrak{n}(u)\mathfrak{a}(a)\mathfrak{k}$$

with $\mathfrak{k} \in \mathrm{SO}(n)$. We set

$$(2.6) \quad \mathcal{F}_N = \{u : u_{jk} \in (-1/2, 1/2], 1 \leq j < k \leq n\};$$

then $\{\mathfrak{n}(u) : u \in \mathcal{F}_N\}$ is a fundamental region for $(\Gamma \cap N) \backslash N$. We define the following Siegel set:

$$(2.7) \quad \mathcal{S}_n := \{\mathfrak{n}(u)\mathfrak{a}(a)\mathfrak{k} \in G : u \in \mathcal{F}_N, \\ 0 < a_{j+1} \leq \frac{2}{\sqrt{3}}a_j \ (j = 1, \dots, n-1), \mathfrak{k} \in \mathrm{SO}(n)\}.$$

It is known that \mathcal{S}_n contains a fundamental region for $X_n = \Gamma \backslash G$, and on the other hand \mathcal{S}_n is contained in a finite union of fundamental regions for X_n (cf. [8]).

LEMMA 1. *If $R > 0$ and $M = \mathfrak{n}(u)\mathfrak{a}(a)\mathfrak{k} \in \mathcal{S}_n$ satisfy $\mathbb{Z}^n M \cap (R\Delta - \zeta) = \emptyset$ for some $\zeta \in \mathbb{R}^n$, then $a_1 \gg_d R$.*

Proof. Note that $R\Delta$ contains a ball of radius $\gg_d R$. Now the lemma follows from [35, Lemma 2.1]. ■

Alternatively, Lemma 1 follows from Jarník’s inequalities (cf., e.g., [15, p. 99]) together with the fact that $a_1 \asymp_d \lambda_n$, where λ_n is the last successive minimum of the lattice $\mathbb{Z}^n M$ (cf. (3.6) below).

Using the above lemma together with (2.2) and the bound

$$(2.8) \quad \mu_n(\{M \in \mathcal{S}_n : a_1 > A\}) \ll_d A^{-n}, \quad \forall A > 0$$

(cf. the proof of [35, Lemma 2.4]), we immediately deduce the upper bound

$$(2.9) \quad \Psi_d(R) \ll_d R^{-n},$$

which was proved by Li [18, Thm. 1.2] in a different (but closely related) way.

We next recall the parametrization of $G = G^{(n)}$ by $\mathbb{R}_{>0} \times \mathrm{S}_1^{n-1} \times \mathbb{R}^{n-1} \times G^{(n-1)}$ introduced in [35, (2.9)–(2.11)]. Let us fix a function f (smooth except possibly at one point, say) $\mathrm{S}_1^{n-1} \rightarrow \mathrm{SO}(n)$ such that $\mathbf{e}_1 f(\mathbf{v}) = \mathbf{v}$ for all $\mathbf{v} \in \mathrm{S}_1^{n-1}$ (where $\mathbf{e}_1 = (1, 0, \dots, 0)$). Given $M = \mathfrak{n}(u)\mathfrak{a}(a)\mathfrak{k} \in G$, the matrices $\mathfrak{n}(u)$, $\mathfrak{a}(a)$ and \mathfrak{k} can be split uniquely as

$$(2.10) \quad \mathfrak{n}(u) = \begin{pmatrix} 1 & \mathbf{u} \\ \mathfrak{t}\mathbf{0} & \mathfrak{n}(u) \end{pmatrix}, \quad \mathfrak{a}(a) = \begin{pmatrix} a_1 & \mathbf{0} \\ \mathfrak{t}\mathbf{0} & a_1^{-1/(n-1)}\mathfrak{a}(a) \end{pmatrix}, \quad \mathfrak{k} = \begin{pmatrix} 1 & \mathbf{0} \\ \mathfrak{t}\mathbf{0} & \mathfrak{k} \end{pmatrix} f(\mathbf{v}),$$

where $\mathbf{u} \in \mathbb{R}^{n-1}$, $\mathfrak{n}(u) \in N^{(n-1)}$, $a_1 > 0$, $\mathfrak{a}(a) \in A^{(n-1)}$, $\mathfrak{k} \in \mathrm{SO}(n-1)$ and

$\mathbf{v} \in S_1^{n-1}$. We set

$$(2.11) \quad \widetilde{M} = \mathfrak{n}(\underline{u})\mathfrak{a}(\underline{a})\mathfrak{k} \in G^{(n-1)}.$$

In this way we get a bijection between G and $\mathbb{R}_{>0} \times S_1^{n-1} \times \mathbb{R}^{n-1} \times G^{(n-1)}$; we write $M = [a_1, \mathbf{v}, \mathbf{u}, \widetilde{M}]$ for the element in G corresponding to the 4-tuple $\langle a_1, \mathbf{v}, \mathbf{u}, \widetilde{M} \rangle \in \mathbb{R}_{>0} \times S_1^{n-1} \times \mathbb{R}^{n-1} \times G^{(n-1)}$. The Haar measure μ_n takes the following form in the parametrization $M = [a_1, \mathbf{v}, \mathbf{u}, \widetilde{M}]$:

$$(2.12) \quad d\mu_n(M) = \zeta(n)^{-1} d\mu_{n-1}(\widetilde{M}) d\mathbf{u} d\mathbf{v} \frac{da_1}{a_1^{n+1}},$$

where $d\mathbf{u}$ is standard Lebesgue measure on \mathbb{R}^{n-1} and $d\mathbf{v}$ is the $(n-1)$ -dimensional volume measure on S_1^{n-1} ([35, (2.12)]). Note that all of the above claims are valid also for $n=2$, with the natural interpretation that $S_1 = \mathrm{SL}(1, \mathbb{R}) = \{1\}$ with $\mu_1(\{1\}) = 1$.

2.2. On the intersection of Δ and a hyperplane orthogonal to \mathbf{v} .

For $M = [a_1, \mathbf{v}, \mathbf{u}, \widetilde{M}]$, the points in the lattice $\mathbb{Z}^n M$ are given by the formula

$$(2.13) \quad (k, \mathbf{m})M = ka_1\mathbf{v} + a_1^{-1/(n-1)}(0, k\mathbf{u}\mathfrak{a}(\underline{a})\mathfrak{k} + \mathbf{m}\widetilde{M})f(\mathbf{v}) \\ (\forall k \in \mathbb{Z}, \mathbf{m} \in \mathbb{Z}^{n-1}).$$

In particular $\mathbb{Z}^n M$ is contained in the union of the (parallel) hyperplanes $ka_1\mathbf{v} + \mathbf{v}^\perp$:

$$(2.14) \quad \mathbb{Z}^n M \subset \bigcup_{k \in \mathbb{Z}} (ka_1\mathbf{v} + \mathbf{v}^\perp).$$

Note that for each k , the $(n-1)$ -dimensional affine lattice $\mathbb{Z}^n M \cap (ka_1\mathbf{v} + \mathbf{v}^\perp)$ has covolume a_1^{-1} inside $ka_1\mathbf{v} + \mathbf{v}^\perp$. Hence if a_1 is large then this point set typically covers $ka_1\mathbf{v} + \mathbf{v}^\perp$ well in the sense that the maximal distance from $\mathbb{Z}^n M \cap (ka_1\mathbf{v} + \mathbf{v}^\perp)$ to any point in $ka_1\mathbf{v} + \mathbf{v}^\perp$ is small.

Given $\mathbf{v} = (v_1, \dots, v_n) \in S_1^{n-1}$ we let $P_{\mathbf{v}} : \mathbb{R}^n \rightarrow \mathbb{R}^n$ be the orthogonal projection onto the line $\mathbb{R}\mathbf{v}$, viz.

$$(2.15) \quad P_{\mathbf{v}}(\mathbf{x}) := (\mathbf{x} \cdot \mathbf{v})\mathbf{v}.$$

Note that $P_{\mathbf{v}}(\Delta)$ is a closed line segment; let $\ell(\mathbf{v})$ denote its length. In other words, $\ell(\mathbf{v})$ is the width of Δ in the direction \mathbf{v} . Since Δ is the convex hull of $\{\mathbf{0}, \mathbf{e}_1, \dots, \mathbf{e}_n\}$, where \mathbf{e}_j is the j th standard basis vector of \mathbb{R}^n , $P_{\mathbf{v}}(\Delta)$ is the convex hull of $\{P_{\mathbf{v}}(\mathbf{0}), P_{\mathbf{v}}(\mathbf{e}_1), \dots, P_{\mathbf{v}}(\mathbf{e}_n)\}$, and here $P_{\mathbf{v}}(\mathbf{0}) = \mathbf{0}$ and $P_{\mathbf{v}}(\mathbf{e}_j) = v_j\mathbf{v}$. Hence

$$(2.16) \quad \ell(\mathbf{v}) = \ell_+(\mathbf{v}) - \ell_-(\mathbf{v}),$$

where

$$(2.17) \quad \ell_+(\mathbf{v}) := \max(0, v_1, \dots, v_n), \quad \ell_-(\mathbf{v}) := \min(0, v_1, \dots, v_n).$$

In particular $1/\sqrt{n} \leq \ell(\mathbf{v}) \leq \sqrt{2}$.

LEMMA 2. *If $R > 0$, $M = [a_1, \mathbf{v}, \mathbf{u}, \widetilde{M}]$ and $a_1 > \ell(\mathbf{v})R$, then there exists $\zeta \in \mathbb{R}^n$ such that $\mathbb{Z}^n M \cap (R\Delta - \zeta) = \emptyset$.*

Proof. Because of (2.14), $\mathbb{Z}^n M \cap (R\Delta - \zeta) = \emptyset$ certainly holds whenever $R\Delta - \zeta$ lies completely inside the open strip contained between the two parallel hyperplanes \mathbf{v}^\perp and $a_1\mathbf{v} + \mathbf{v}^\perp$, and this holds if and only if $P_{\mathbf{v}}(R\Delta - \zeta) \subset \{t\mathbf{v} : 0 < t < a_1\}$. There exist vectors ζ satisfying the last inclusion if and only if $\ell(\mathbf{v})R < a_1$. ■

We next seek to obtain restrictions on those lattices $\mathbb{Z}^n M$ with $M = [a_1, \mathbf{v}, \mathbf{u}, \widetilde{M}]$ and $a_1 \leq \ell(\mathbf{v})R$ which still satisfy $\mathbb{Z}^n M \cap (R\Delta - \zeta) = \emptyset$ for some $\zeta \in \mathbb{R}^n$. We first prove the following simple geometric fact.

LEMMA 3. *For any $\mathbf{v} \in S_1^{n-1}$ and $x \in \mathbb{R}$, the hyperplane $x\mathbf{v} + \mathbf{v}^\perp$ intersects Δ if and only if $x \in [\ell_-(\mathbf{v}), \ell_+(\mathbf{v})]$, and furthermore when this happens, $(x\mathbf{v} + \mathbf{v}^\perp) \cap \Delta$ contains an $(n-1)$ -dimensional ball of radius*

$$(2.18) \quad r := (2\sqrt{n} + n)^{-1} \min(x - \ell_-(\mathbf{v}), \ell_+(\mathbf{v}) - x).$$

Proof. The first statement follows since $x\mathbf{v} + \mathbf{v}^\perp$ intersects Δ if and only if $x\mathbf{v} \in P_{\mathbf{v}}(\Delta)$, and $P_{\mathbf{v}}(\Delta) = \{t\mathbf{v} : \ell_-(\mathbf{v}) \leq t \leq \ell_+(\mathbf{v})\}$.

To prove the second statement we will prove the stronger fact that if $x \in [\ell_-(\mathbf{v}), \ell_+(\mathbf{v})]$ then there is some $\mathbf{y} \in x\mathbf{v} + \mathbf{v}^\perp$ such that $\mathbf{y} + \mathcal{B}_r^n \subset \Delta$, where \mathcal{B}_r^n denotes the closed n -dimensional ball of radius r centered at $\mathbf{0}$ (thus $\mathbf{y} + \mathcal{B}_r^n$ is the ball of radius r centered at \mathbf{y}).

For an arbitrary point $\mathbf{y} = (y_1, \dots, y_n) \in \mathbb{R}^n$ we note that $\mathbf{y} + \mathcal{B}_r^n \subset \Delta$ holds if and only if $y_1, \dots, y_n \geq r$ and $y_1 + \dots + y_n \leq 1 - \sqrt{nr}$, which is equivalent to saying that $(\sqrt{n} + n)r \leq 1$ and $\mathbf{y} - r\mathbf{e} \in (1 - (\sqrt{n} + n)r)\Delta$. The condition $(\sqrt{n} + n)r \leq 1$ is clearly met for our r , since $\min(x - \ell_-(\mathbf{v}), \ell_+(\mathbf{v}) - x) \leq \frac{1}{2}\ell(\mathbf{v}) \leq 2^{-1/2}$.

Hence, since Δ is the convex hull of $\{\mathbf{0}, \mathbf{e}_1, \dots, \mathbf{e}_n\}$, it follows that there exists a point $\mathbf{y} \in x\mathbf{v} + \mathbf{v}^\perp$ with $\mathbf{y} + \mathcal{B}_r^n \subset \Delta$ if and only if x lies in the (1-dimensional) convex hull of the $n+1$ numbers

$$(2.19) \quad r\mathbf{v} \cdot \mathbf{e} \quad \text{and} \quad r\mathbf{v} \cdot \mathbf{e} + (1 - (\sqrt{n} + n)r)v_j \quad \text{for } j = 1, \dots, n.$$

Recalling (2.17) we see that this holds if and only if $x \in [\alpha_-, \alpha_+]$, where

$$(2.20) \quad \alpha_\pm := r\mathbf{v} \cdot \mathbf{e} + (1 - (\sqrt{n} + n)r)\ell_\pm(\mathbf{v}).$$

However

$$(2.21) \quad |\alpha_\pm - \ell_\pm(\mathbf{v})| \leq r|\mathbf{v} \cdot \mathbf{e}| + (\sqrt{n} + n)r|\ell_\pm(\mathbf{v})| \leq r(\sqrt{n} + \sqrt{n} + n).$$

Hence $x \in [\alpha_-, \alpha_+]$ certainly holds whenever

$$(2.22) \quad \ell_-(\mathbf{v}) + (2\sqrt{n} + n)r \leq x \leq \ell_+(\mathbf{v}) - (2\sqrt{n} + n)r,$$

and this condition is clearly fulfilled for our r in (2.18). ■

LEMMA 4. *If $R > 0$, $M = [a_1, \mathbf{v}, \mathbf{u}, \underline{M}] \in \mathcal{S}_n$ and $a_1 \leq \ell(\mathbf{v})R$, and if $\mathbb{Z}^n M \cap (R\Delta - \zeta) = \emptyset$ for some $\zeta \in \mathbb{R}^n$, then $a_1 \gg_d (\ell(\mathbf{v})R - a_1)a_1^{1/(n-1)}$ in $\underline{M} = \mathfrak{n}(\underline{u})\mathfrak{a}(\underline{a})\underline{k} \in G^{(n-1)}$.*

Proof. Set $X = \ell(\mathbf{v})R - a_1 \geq 0$. Since $P_{\mathbf{v}}(R\Delta - \zeta)$ is a closed line segment in $\mathbb{R}\mathbf{v}$ of length $\ell(\mathbf{v})R$, there exists some $k \in \mathbb{Z}$ such that $ka_1\mathbf{v} \in P_{\mathbf{v}}(R\Delta - \zeta)$ and furthermore such that $ka_1\mathbf{v}$ has distance $\geq \frac{1}{2}X$ to both the endpoints of $P_{\mathbf{v}}(R\Delta - \zeta)$. Hence by Lemma 3, $(ka_1\mathbf{v} + \mathbf{v}^\perp) \cap (R\Delta - \zeta)$ contains an $(n-1)$ -dimensional ball B of radius $\gg_d X$. Now $\mathbb{Z}^n M \cap (R\Delta - \zeta) = \emptyset$ implies that the $(n-1)$ -dimensional affine lattice $(ka_1\mathbf{v} + \mathbf{v}^\perp) \cap \mathbb{Z}^n M$ must be disjoint from B . In view of (2.13) it follows that the $(n-1)$ -dimensional lattice $a_1^{-1/(n-1)}(0, \mathbb{Z}^{n-1}\underline{M})f(\mathbf{v}) \subset \mathbf{v}^\perp$ is disjoint from a certain translate of B inside \mathbf{v}^\perp . Hence $\mathbb{Z}^{n-1}\underline{M}$ is disjoint from a ball of radius $\gg_d a_1^{1/(n-1)}X$ in \mathbb{R}^{n-1} , and so $a_1 \gg_d a_1^{1/(n-1)}X$ by [35, Lemma 2.1]. ■

2.3. The main computation. Recall that by Lemma 1, if $M = \mathfrak{n}(u)\mathfrak{a}(a)\mathfrak{k} \in \mathcal{S}_n$ satisfies $\mathbb{Z}^n M \cap (R\Delta - \zeta) = \emptyset$ for some $\zeta \in \mathbb{R}^n$, then $a_1 \geq \kappa R$, where $\kappa > 0$ is a constant which only depends on d . We set

$$(2.23) \quad A := \kappa R,$$

and from now on we keep $R > \kappa^{-1}$, so that $A > 1$.

We next recall some definitions and facts from [21, Sec. 3.2]. We fix a subset $S_\pm^{n-1} \subset S_1^{n-1} \cap \{v_1 \geq 0\}$ which contains exactly one of the vectors \mathbf{v} and $-\mathbf{v}$ for every $\mathbf{v} \in S_1^{n-1}$. Let us also fix a (set-theoretical, measurable) fundamental region $\mathcal{F}_{n-1} \subset \mathcal{S}_{n-1}$ for $\Gamma^{(n-1)} \backslash G^{(n-1)}$. We set (cf. [21, (3.15), (3.18)])

$$(2.24) \quad \mathcal{G}_A := \{[a_1, \mathbf{v}, \mathbf{u}, \underline{M}] \in G : a_1 > A, \mathbf{v} \in S_\pm^{n-1}, \\ \mathbf{u} \in (-1/2, 1/2]^{n-1}, \underline{M} \in \mathcal{F}_{n-1}\}$$

and

$$(2.25) \quad \mathcal{S}'_n := \{[a_1, \mathbf{v}, \mathbf{u}, \underline{M}] \in \mathcal{S}_n : \mathbf{v} \in S_\pm^{n-1}\}.$$

LEMMA 5. *There exists a (set-theoretical, measurable) fundamental region $\mathcal{F}_n \subset \mathcal{S}'_n$ for $X_n = \Gamma \backslash G$ and a (measurable) subset $\mathcal{C} \subset \mathcal{S}'_n \cup \mathcal{G}_A$ such that*

$$(2.26) \quad \mathcal{G}_A \setminus \mathcal{C} \subset \{M \in \mathcal{F}_n : a_1 > A\} \subset \mathcal{G}_A \cup \mathcal{C}$$

and $\mu_n(\mathcal{C}) \ll_d A^{-2n}$ if $n \geq 3$, while $\mathcal{C} = \emptyset$ if $n = 2$.

Proof. For $n \geq 3$ this follows from [21, Lemma 3.4], together with the computation in [21, (3.23), (3.24)]. In the remaining case $n = 2$ we use the well-known fact that a fundamental region for $X_2 = \Gamma^{(2)} \backslash G^{(2)}$ is provided by

$$(2.27) \quad \mathcal{F}_2 := \{\mathfrak{n}(u)\mathfrak{a}(a)f(\mathbf{v}) \in G^{(2)} : u + a_1^2 i \in \mathcal{F}_{\mathbb{H}}, \mathbf{v} \in \mathbb{S}_{\pm}^1\},$$

where $\mathcal{F}_{\mathbb{H}}$ is the usual fundamental region for the action of $\Gamma^{(2)}$ on the upper half-plane $\mathbb{H} = \{z = x + iy \in \mathbb{C} : y > 0\}$, viz.

$$(2.28) \quad \mathcal{F}_{\mathbb{H}} := \{z = x + iy \in \mathbb{H} : -1/2 < x \leq 1/2, |z| \geq 1, (x < 0 \Rightarrow |z| > 1)\}.$$

In particular for this choice of \mathcal{F}_2 we have $\mathcal{F}_2 \subset \mathcal{S}'_2$ and $\{M \in \mathcal{F}_2 : a_1 > A\} = \mathcal{G}_A$, since $A > 1$. ■

It follows from Lemma 5 and (2.2) that

$$(2.29) \quad \Psi_d(R) = \int_{\mathcal{G}_A} I(\exists \zeta \in \mathbb{R}^n : \mathbb{Z}^n M \cap (R\Delta - \zeta) = \emptyset) d\mu_n(M) + O(\mu_n(\mathcal{C})),$$

where the error term is $\ll_d A^{-2n} \ll_d R^{-2n}$ if $n \geq 3$, while if $n = 2$ then the error term vanishes. Hence, using (2.24) and (2.12), we obtain

$$(2.30) \quad \Psi_d(R) = \frac{1}{\zeta(n)} \int_{\mathbb{S}_{\pm}^{n-1}} \int_{(-1/2, 1/2)^{n-1}} \int_{\mathcal{F}_{n-1}} I(\exists \zeta \in \mathbb{R}^n :$$

$$\mathbb{Z}^n [a_1, \mathbf{v}, \mathbf{u}, \underline{M}] \cap (R\Delta - \zeta) = \emptyset) d\mu_{n-1}(\underline{M}) d\mathbf{u} d\mathbf{v} \frac{da_1}{a_1^{n+1}} + O_d(I(n \geq 3) \cdot R^{-2n}).$$

Here it follows from Lemma 2 that the right hand side is

$$(2.31) \quad \geq \frac{1}{\zeta(n)} \int_{\mathbb{S}_{\pm}^{n-1}} \int_{\ell(\mathbf{v})R} \frac{da_1}{a_1^{n+1}} d\mathbf{v} = \frac{R^{-n}}{n\zeta(n)} \int_{\mathbb{S}_{\pm}^{n-1}} \ell(\mathbf{v})^{-n} d\mathbf{v}.$$

(Note here that by Lemma 2 and our definition of A we have $A \leq \ell(\mathbf{v})R$ for all $\mathbf{v} \in \mathbb{S}_1^{n-1}$.) On the other hand it follows from Lemma 4 that there is a constant $\kappa' > 0$ which only depends on d such that the difference between the integral in (2.30) and the right hand side of (2.31) is

$$(2.32) \quad \leq \frac{1}{\zeta(n)} \int_{\mathbb{S}_{\pm}^{n-1}} \int_A^{\ell(\mathbf{v})R} \mu_{n-1}(\{\underline{M} \in \mathcal{F}_{n-1} : a_1 \geq \kappa'(\ell(\mathbf{v})R - a_1)a_1^{1/(n-1)}\}) \frac{da_1}{a_1^{n+1}} d\mathbf{v}.$$

Here $A = \kappa R$; hence $R \ll_d a_1 \ll_d R$ in the integral, and we get, with a new constant $\kappa'' > 0$ which only depends on d ,

$$\begin{aligned}
(2.33) \quad & \ll_d R^{-(n+1)} \int_{\mathbb{S}_{\pm}^{n-1}} \int_{\kappa R}^{\ell(\mathbf{v})R} \mu_{n-1}(\{\underline{M} \in \mathcal{F}_{n-1} : \\
& \qquad \qquad \qquad \underline{a}_1 \geq \kappa''(\ell(\mathbf{v})R - a_1)R^{1/(n-1)}\}) da_1 d\mathbf{v} \\
& \leq R^{-(n+1)} \int_{\mathbb{S}_{\pm}^{n-1}} \int_0^{\ell(\mathbf{v})R} \mu_{n-1}(\{\underline{M} \in \mathcal{F}_{n-1} : \underline{a}_1 \geq \kappa''tR^{1/(n-1)}\}) dt d\mathbf{v} \\
& \ll_d R^{-(n+1)} \int_0^{\sqrt{2}R} \mu_{n-1}(\{\underline{M} \in \mathcal{F}_{n-1} : \underline{a}_1 \geq \kappa''tR^{1/(n-1)}\}) dt.
\end{aligned}$$

Now if $n \geq 3$ then by a computation as in the proof of [35, Lemma 2.4] we get

$$(2.34) \quad \ll_d R^{-(n+1)} \int_0^{\sqrt{2}R} (1 + tR^{1/(n-1)})^{-(n-1)} dt \ll_d R^{-n-1-1/(n-1)}.$$

On the other hand if $n = 2$ then $\mathcal{F}_{n-1} = \{1\}$ and hence the last line of (2.33) equals $R^{-3} \cdot \min(\sqrt{2}R, \kappa''^{-1}R^{-1})$, which is $\ll R^{-4}$. Hence we conclude that

$$(2.35) \quad \Psi_d(R) = \frac{R^{-n}}{n\zeta(n)} \int_{\mathbb{S}_{\pm}^{n-1}} \ell(\mathbf{v})^{-n} d\mathbf{v} + O_d(R^{-n-1-1/(n-1)}).$$

Now to prove the asymptotic formula for $\Psi_d(R)$ stated in Theorem 2, it only remains to compute the integral $\int_{\mathbb{S}_{\pm}^{n-1}} \ell(\mathbf{v})^{-n} d\mathbf{v}$.

2.4. Computing the constant in the main term

LEMMA 6. *For every $n \geq 2$ we have*

$$(2.36) \quad \int_{\mathbb{S}_{\pm}^{n-1}} \ell(\mathbf{v})^{-n} d\mathbf{v} = \frac{n(n+1)}{2}.$$

Proof. Set

$$(2.37) \quad K = \{r\mathbf{v} : \mathbf{v} \in \mathbb{S}_1^{n-1}, 0 \leq r \leq \ell(\mathbf{v})^{-1}\} \subset \mathbb{R}^n;$$

then clearly

$$(2.38) \quad \int_{\mathbb{S}_{\pm}^{n-1}} \ell(\mathbf{v})^{-n} d\mathbf{v} = \frac{1}{2} \int_{\mathbb{S}_1^{n-1}} \ell(\mathbf{v})^{-n} d\mathbf{v} = \frac{n}{2} \text{vol}(K).$$

But for any $\mathbf{x} = r\mathbf{v}$ with $r > 0$ and $\mathbf{v} \in \mathbb{S}_1^{n-1}$ we have

$$(2.39) \quad \ell(\mathbf{v}) = \|\mathbf{x}\|^{-1}(\max(0, x_1, \dots, x_n) - \min(0, x_1, \dots, x_n)),$$

so that $r \leq \ell(\mathbf{v})^{-1}$ if and only if $\max(0, x_1, \dots, x_n) - \min(0, x_1, \dots, x_n) \leq 1$. In other words,

$$(2.40) \quad K = \{\mathbf{x} \in [-1, 1]^n : |x_j - x_k| \leq 1, \forall j, k\}.$$

Hence by easy symmetry considerations we have

$$(2.41) \quad \begin{aligned} \text{vol}(K) &= \text{vol}(K \cap [0, 1]^n) + \text{vol}(K \cap [-1, 0]^n) \\ &\quad + n(n-1) \text{vol}(\{\mathbf{x} \in K : x_1 < 0 < x_2 \text{ and} \\ &\quad \quad \quad x_1 < x_j < x_2 \text{ for } j = 3, \dots, n\}) \\ &= 2 + n(n-1) \int_{-1}^0 \int_0^{1+x_1} (x_2 - x_1)^{n-2} dx_2 dx_1 = n + 1. \end{aligned}$$

The lemma follows from (2.38) and (2.41). ■

2.5. Bound from below. Finally we will prove the lower bound (1.9) in Theorem 2.

The key step is the following lemma, which says that for “good” directions $\mathbf{v} = (v_1, \dots, v_n) \in S_1^{n-1}$, we may weaken the restriction $a_1 > \ell(\mathbf{v})R$ in Lemma 2 by a small but uniform amount, and still be sure to have $\mathbb{Z}^n M \cap (R\Delta - \zeta) = \emptyset$ for some $\zeta \in \mathbb{Z}^n$.

LEMMA 7. *Let c be a fixed number in the interval $(0, n^{-1/2})$, and set*

$$(2.42) \quad c' = (n-1)!^{1/(n-1)} c^{n/(n-1)}.$$

Then for any $R \geq (2c'\sqrt{n})^{1-1/n}$ and any $M = [a_1, \mathbf{v}, \mathbf{u}, \tilde{M}]$ with $a_1 > \ell(\mathbf{v})R - c'R^{-1/(n-1)}$ and $v_j > c$ (for all j), there exists $\zeta \in \mathbb{R}^n$ such that $\mathbb{Z}^n M \cap (R\Delta - \zeta) = \emptyset$.

Proof. Let R and $M = [a_1, \mathbf{v}, \mathbf{u}, \tilde{M}]$ satisfy the given assumptions. If $a_1 > \ell(\mathbf{v})R$ then the desired statement is in Lemma 2; hence from now on we may assume $a_1 \leq \ell(\mathbf{v})R$. We will choose

$$(2.43) \quad \zeta = c'R^{-1/(n-1)}\mathbf{v} + \mathbf{w}$$

for some $\mathbf{w} \in \mathbf{v}^\perp$ which will be fixed at the end of the proof. Then for every $\mathbf{x} \in R\Delta - \zeta$ we have

$$(2.44) \quad \mathbf{x} \cdot \mathbf{v} \leq \ell_+(\mathbf{v})R - \zeta \cdot \mathbf{v} = \ell(\mathbf{v})R - c'R^{-1/(n-1)}$$

and

$$(2.45) \quad \mathbf{x} \cdot \mathbf{v} \geq -\zeta \cdot \mathbf{v} = -c'R^{-1/(n-1)} \geq -(\ell(\mathbf{v})R - c'R^{-1/(n-1)}),$$

where we used the assumption $R \geq (2c'\sqrt{n})^{1-1/n}$ in the last step. Using (2.44), (2.45) and $a_1 > \ell(\mathbf{v})R - c'R^{-1/(n-1)}$ we conclude that

$$(2.46) \quad (R\Delta - \zeta) \cap (ka_1\mathbf{v} + \mathbf{v}^\perp) = \emptyset, \quad \forall k \in \mathbb{Z} \setminus \{0\}.$$

Hence, using also (2.14), we get

$$(2.47) \quad (R\Delta - \zeta) \cap \mathbb{Z}^n M = (R\Delta - \zeta) \cap L_{M, \mathbf{v}},$$

where $L_{M, \mathbf{v}}$ is the $(n-1)$ -dimensional lattice $L_{M, \mathbf{v}} = \mathbb{Z}^n M \cap \mathbf{v}^\perp$. Recall that $L_{M, \mathbf{v}}$ has covolume a_1^{-1} in \mathbf{v}^\perp . Using also $R\Delta \subset \mathbb{R}_{\geq 0}^n$ and $\zeta = c'R^{-1/(n-1)}\mathbf{v} + \mathbf{w}$, $\mathbf{w} \in \mathbf{v}^\perp$, we obtain

$$(2.48) \quad \begin{aligned} (R\Delta - \zeta) \cap \mathbb{Z}^n M &\subset (\mathbb{R}_{\geq 0}^n - c'R^{-1/(n-1)}\mathbf{v} - \mathbf{w}) \cap L_{M, \mathbf{v}} \\ &= ((\mathbb{R}_{\geq 0}^n - c'R^{-1/(n-1)}\mathbf{v}) \cap \mathbf{v}^\perp) - \mathbf{w}) \cap L_{M, \mathbf{v}}. \end{aligned}$$

Here $(\mathbb{R}_{\geq 0}^n - c'R^{-1/(n-1)}\mathbf{v}) \cap \mathbf{v}^\perp$ is a closed $(n-1)$ -dimensional simplex, and a simple computation yields for its volume (cf. [13, (17)], or the simpler computation in [5, Lemma 1])

$$(2.49) \quad \begin{aligned} \text{vol}_{n-1}((\mathbb{R}_{\geq 0}^n - c'R^{-1/(n-1)}\mathbf{v}) \cap \mathbf{v}^\perp) \\ = \frac{\prod_{j=1}^n v_j^{-1}}{(n-1)!} (c'R^{-1/(n-1)})^{n-1} < R^{-1}. \end{aligned}$$

In the last step we used $v_j > c$ (for all j) and (2.42). However the covolume of $L_{M, \mathbf{v}}$ in \mathbf{v}^\perp is, since we assumed $a_1 \leq \ell(\mathbf{v})R$ from the start,

$$(2.50) \quad \text{vol}_{n-1}(\mathbf{v}^\perp / L_{M, \mathbf{v}}) = a_1^{-1} \geq (\ell(\mathbf{v})R)^{-1} > R^{-1}.$$

(Indeed $\ell(\mathbf{v}) = \ell_+(\mathbf{v}) < 1$ since all v_j are positive.) The above shows that the volume of $(\mathbb{R}_{\geq 0}^n - c'R^{-1/(n-1)}\mathbf{v}) \cap \mathbf{v}^\perp$ is smaller than the covolume of $L_{M, \mathbf{v}}$, and hence there is some $\mathbf{w} \in \mathbf{v}^\perp$ such that the intersection in (2.48) is empty. ■

We now return to the computation in Section 2.3. We will bound the difference between the integral in (2.30) and the right hand side of (2.31) from *below*. Fix a constant $c \in (0, n^{-1/2})$ as in Lemma 7, let $c' > 0$ be as in (2.42), and let Ω be the non-empty, relatively open subset of S_{\pm}^{n-1} consisting of all $\mathbf{v} = (v_1, \dots, v_n) \in S_1^{n-1}$ with $v_j > c$ (for all j). It now follows from Lemma 7 that, for any $R \geq (2c'\sqrt{n})^{1-1/n}$, the difference between the integral in (2.30) and the right hand side of (2.31) is

$$(2.51) \quad \geq \frac{1}{\zeta(n)} \int_{\ell(\mathbf{v})R - c'R^{-1/(n-1)}}^{\ell(\mathbf{v})R} \int_{\Omega} d\mathbf{v} \frac{da_1}{a_1^{n+1}} \gg_d R^{-n-1-1/(n-1)}.$$

In particular note that this contribution is asymptotically larger than the error term in (2.30). Hence we conclude that there exist constants $c, c' > 0$ which only depend on n such that for all $R > c'$,

$$(2.52) \quad \Psi_d(R) > \frac{R^{-n}}{n\zeta(n)} \int_{S_{\pm}^{n-1}} \ell(\mathbf{v})^{-n} d\mathbf{v} + cR^{-n-1-1/(n-1)}.$$

In view of Lemma 6 we have thus proved (1.9) in Theorem 2. Since the asymptotic relation (1.8) follows from (2.35) and Lemma 6, this concludes the proof of Theorem 2. ■

3. Uniform bounds on $\tilde{P}_d(T, R)$ and $P_d(T, R)$. In this section we will prove Theorem 3 and Corollary 1.

3.1. Proof of Theorem 3. Let us first note that the claim (1.16), i.e.

$$(3.1) \quad \tilde{P}_d(T, R) = 0 \quad \text{whenever } R \geq \kappa_{\mathcal{D}}^{1-1/(d-1)} T^{1-1/(d-1)}$$

where

$$(3.2) \quad \kappa_{\mathcal{D}} := \sup_{\mathbf{x} \in \mathcal{D}} \|\mathbf{x}\|,$$

is a direct consequence of any among several known bounds on the Frobenius number (cf., e.g., [23]). For example, the classical bound by Schur (cf. [10]) asserts that for any $\mathbf{a} \in \widehat{\mathbb{N}}^d$ satisfying $a_1 \leq \dots \leq a_d$,

$$(3.3) \quad g(\mathbf{a}) \leq a_1 a_d - a_1 - a_d \quad (\text{thus } f(\mathbf{a}) \leq a_1 a_d + a_2 + \dots + a_{d-1} < d a_1 a_d).$$

Using this together with the fact that $s(\mathbf{a}) \geq d a_1 a_d \|\mathbf{a}\|^{-1+1/(d-1)}$ for any such \mathbf{a} , we deduce

$$(3.4) \quad \frac{f(\mathbf{a})}{s(\mathbf{a})} < \|\mathbf{a}\|^{1-1/(d-1)}.$$

Here both the left and the right hand sides are invariant under permutations of the coefficients of \mathbf{a} ; hence (3.4) in fact holds for *all* $\mathbf{a} \in \widehat{\mathbb{N}}^d$. Finally, (3.1) follows from (3.4).

We next turn to the proof of (1.15) in Theorem 3. As in the previous section we write $n = d - 1$. Given $\mathbf{a} \in \widehat{\mathbb{N}}^d$ we set

$$(3.5) \quad \Lambda_{\mathbf{a}} = \mathbb{Z}^d \cap \mathbf{a}^{\perp} = \{\mathbf{x} \in \mathbb{Z}^d : \mathbf{a} \cdot \mathbf{x} = 0\}.$$

This is an n -dimensional sublattice of \mathbb{Z}^d of determinant $\det(\Lambda_{\mathbf{a}}) = \|\mathbf{a}\|$. (By the determinant, $\det(\Lambda)$, of a lattice Λ of not necessarily full rank in \mathbb{R}^d , we mean the covolume of Λ in $\text{span}_{\mathbb{R}} \Lambda$.) Given any n -dimensional lattice $\Lambda \subset \mathbb{R}^d$ we write $0 < \lambda_1(\Lambda) \leq \dots \leq \lambda_n(\Lambda)$ for the Minkowski successive minima of Λ , i.e.

$$(3.6) \quad \lambda_j(\Lambda) = \inf\{r > 0 : \dim \text{span}_{\mathbb{R}}(\mathcal{B}_r^d \cap \Lambda) \geq j\}.$$

(Recall that \mathcal{B}_r^d is the closed d -dimensional ball of radius r centered at $\mathbf{0}$.) Then by Aliev and Henk [2, (14)] ⁽²⁾ (cf. also Kannan [17, Thm. 2.5]) we have

⁽²⁾ Note that λ_j in [2] equals $\|\mathbf{a}\|^{-1/n} \lambda_j(\Lambda_{\mathbf{a}})$ in our notation.

$$(3.7) \quad \frac{f(\mathbf{a})}{s(\mathbf{a})} \leq \frac{1}{2}n\|\mathbf{a}\|^{-1/n}\lambda_n(\Lambda_{\mathbf{a}}).$$

Note also that we have $\#(\widehat{\mathbb{N}}^d \cap T\mathcal{D}) \asymp_{d,\mathcal{D}} T^d$ uniformly over all $T > 0$ for which $\widehat{\mathbb{N}}^d \cap T\mathcal{D} \neq \emptyset$, since \mathcal{D} is bounded with non-empty interior. From these facts together with the fact that $\Lambda_{\mathbf{a}} \neq \Lambda_{\mathbf{b}}$ for all $\mathbf{a} \neq \mathbf{b} \in \widehat{\mathbb{N}}^d$ (since $\text{span}_{\mathbb{R}} \Lambda_{\mathbf{a}} = \mathbf{a}^\perp \neq \mathbf{b}^\perp = \text{span}_{\mathbb{R}} \Lambda_{\mathbf{b}}$), it follows that

$$(3.8) \quad \widetilde{P}_d(T, R) \ll_{d,\mathcal{D}} T^{-d} \#\{\Lambda \in \mathcal{L}_n : \det(\Lambda) \leq \kappa_{\mathcal{D}}T, \lambda_n(\Lambda) > 2n^{-1} \det(\Lambda)^{1/n}R\},$$

where \mathcal{L}_n is the set of all n -dimensional sublattices of \mathbb{Z}^d .

Let us set

$$(3.9) \quad \rho_j(\Lambda) := \lambda_{j+1}(\Lambda)/\lambda_j(\Lambda) \quad \text{for } j = 1, \dots, n-1.$$

(Thus $\rho_j(\Lambda) \geq 1$ for all Λ .) Also, for any $\mathbf{r} = (r_1, \dots, r_{n-1}) \in \mathbb{R}_{\geq 1}^{n-1}$, we set

$$(3.10) \quad \mathcal{L}_n(\mathbf{r}) := \{\Lambda \in \mathcal{L}_n : \rho_j(\Lambda) \geq r_j \ (\forall j)\}.$$

Now as a special case of Schmidt's [31, Thm. 5], the number of lattices in $\mathcal{L}_n(\mathbf{r})$ with determinant at most T is given by the following asymptotic formula with a precise error term. Let us write $\rho_j(L) = \lambda_{j+1}(L)/\lambda_j(L)$ also for an n -dimensional lattice $L \subset \mathbb{R}^n$, with $\lambda_1(L) \leq \dots \leq \lambda_n(L)$ being the successive minima of L .

THEOREM 5 ([31, Thm. 5]). *For any $\mathbf{r} \in \mathbb{R}_{\geq 1}^{n-1}$ and $T > 0$ we have*

$$(3.11) \quad \#\{\Lambda \in \mathcal{L}_n(\mathbf{r}) : \det(\Lambda) \leq T\} \\ = \frac{\pi^{d/2}}{2\Gamma(1+d/2)} \left(\prod_{j=2}^n \zeta(j) \right) \mu_n(\{L \in X_n : \rho_j(L) \geq r_j \ (\forall j)\}) \cdot T^d \\ + O_d\left(\left(\prod_{j=1}^{n-1} r_j^{-(j-1/n)(n-j)} \right) T^{d-1/n} \right).$$

Furthermore,

$$(3.12) \quad \mu_n(\{L \in X_n : \rho_j(L) \geq r_j \ (\forall j)\}) \asymp_d \prod_{j=1}^{n-1} r_j^{-j(n-j)}.$$

For our argument we will only make use of the upper bound which follows from the above theorem, viz.

$$(3.13) \quad \#\{\Lambda \in \mathcal{L}_n(\mathbf{r}) : \det(\Lambda) \leq T\} \\ \ll_d T^d \prod_{j=1}^{n-1} r_j^{-j(n-j)} \left(1 + T^{-1/n} \prod_{j=1}^{n-1} r_j^{(n-j)/n} \right).$$

We will now form a finite union of sets $\mathcal{L}_n(\mathbf{r})$ which contains the set on the right hand side of (3.8).

For any n -dimensional lattice Λ we have

$$(3.14) \quad \lambda_n(\Lambda)^n = \prod_{j=1}^n \lambda_j(\Lambda) \prod_{j=1}^{n-1} \rho_j(\Lambda)^j \asymp_d \det(\Lambda) \prod_{j=1}^{n-1} \rho_j(\Lambda)^j,$$

where in the last step we used Minkowski's Second Theorem (cf., e.g., [34, Lectures 3–4]). Hence there exists a constant $c > 0$ which only depends on n (viz., only on d) such that for any n -dimensional lattice Λ and any $R > 0$,

$$(3.15) \quad \lambda_n(\Lambda) > 2n^{-1} \det(\Lambda)^{1/n} R \Rightarrow \prod_{j=1}^{n-1} \rho_j(\Lambda)^j > cR^n.$$

Note that (1.15) is trivial when $R \ll 1$ (since $\tilde{P}_d(T, R) \leq 1$ always); hence from now on we may keep $R \geq ec^{-1/n}$ without loss of generality. Set

$$(3.16) \quad B := \lfloor \log(cR^n) - n \rfloor \in \mathbb{Z}_{\geq 0}$$

and

$$(3.17) \quad \mathcal{R}(n, R) := \left\{ \mathbf{r} = (e^{b_1}, e^{b_2/2}, e^{b_3/3}, \dots, e^{b_{n-1}/(n-1)}) : \right. \\ \left. \mathbf{b} \in \mathbb{Z}_{\geq 0}^{n-1}, \sum_{j=1}^{n-1} b_j = B \right\}.$$

Note that if Λ is any n -dimensional lattice satisfying $\prod_{j=1}^{n-1} \rho_j(\Lambda)^j > cR^n$, then if we set $b_j := \lfloor j \log \rho_j(\Lambda) \rfloor$ we have

$$(3.18) \quad \sum_{j=1}^{n-1} b_j > \sum_{j=1}^{n-1} (j \log \rho_j(\Lambda) - 1) \\ > \log(cR^n) - (n-1) > \log(cR^n) - n \geq B.$$

Hence there is a way to decrease some of the b_j 's so as to make $\sum_{j=1}^{n-1} b_j = B$, while keeping $\mathbf{b} = (b_1, \dots, b_{n-1}) \in \mathbb{Z}_{\geq 0}^{n-1}$. Of course the new vector $\mathbf{b} = (b_1, \dots, b_{n-1})$ still satisfies $b_j \leq j \log \rho_j(\Lambda)$ for each j , i.e. $\rho_j(\Lambda) \geq e^{b_j/j}$. We have thus proved that for any n -dimensional lattice Λ satisfying $\prod_{j=1}^{n-1} \rho_j(\Lambda)^j > cR^n$, there exists some $\mathbf{r} \in \mathcal{R}(n, R)$ such that $r_j \leq \rho_j(\Lambda)$ for $j = 1, \dots, n-1$. This fact together with (3.15) implies that the set on the right hand side of (3.8) is contained in the union of $\mathcal{L}_n(\mathbf{r})$ over all $\mathbf{r} \in \mathcal{R}(n, R)$. So, by (3.8), for all $T > 0$ with $\widehat{\mathbb{N}}^d \cap T\mathcal{D} \neq \emptyset$ and all $R \geq ec^{-1/n}$ we have

$$(3.19) \quad \tilde{P}_d(T, R) \ll_{d, \mathcal{D}} T^{-d} \sum_{\mathbf{r} \in \mathcal{R}(n, R)} \#\{\Lambda \in \mathcal{L}_n(\mathbf{r}) : \det(\Lambda) \leq \kappa_{\mathcal{D}} T\}.$$

Therefore, via (3.13),

$$(3.20) \quad \tilde{P}_d(T, R) \ll_{d, \mathcal{D}} \sum_{\substack{\mathbf{b} \in \mathbb{Z}_{\geq 0}^{n-1} \\ b_1 + \dots + b_{n-1} = B}} \exp\left\{-\sum_{j=1}^{n-1} (n-j)b_j\right\} \\ + T^{-1/n} \sum_{\substack{\mathbf{b} \in \mathbb{Z}_{\geq 0}^{n-1} \\ b_1 + \dots + b_{n-1} = B}} \exp\left\{-\sum_{j=1}^{n-1} (1 - (nj)^{-1})(n-j)b_j\right\}.$$

If $n = 2$ then each sum above has exactly one term, and we conclude

$$(3.21) \quad \tilde{P}_3(T, R) \ll_{\mathcal{D}} R^{-2} + T^{-1/2} R^{-1}.$$

If $R < \kappa_{\mathcal{D}}^{1/2} T^{1/2}$ then this gives $\tilde{P}_3(T, R) \ll_{\mathcal{D}} R^{-2}$. On the other hand if $R \geq \kappa_{\mathcal{D}}^{1/2} T^{1/2}$ then $\tilde{P}_3(T, R) = 0$ by (3.1). Hence the proof of (1.15) is complete in the case $n = 2$.

We now assume $n \geq 3$. We set

$$(3.22) \quad \gamma_1(j) := n - j, \\ \gamma_2(j) := (1 - (nj)^{-1})(n - j) = n + n^{-1} - (j + j^{-1}).$$

Now for any $\mathbf{b} \in \mathbb{Z}_{\geq 0}^{n-1}$ with $b_1 + \dots + b_{n-1} = B$ and $b_1 + \dots + b_{n-2} =: s$ we have, since $\gamma_1(j)$ is a decreasing function of j ,

$$(3.23) \quad \sum_{j=1}^{n-1} \gamma_1(j)b_j \geq \gamma_1(n-2) \sum_{j=1}^{n-2} b_j + \gamma_1(n-1)b_{n-1} \\ = 2s + (B - s) = B + s.$$

Similarly, since also $\gamma_2(j)$ is a decreasing function of j for $j \geq 1$,

$$(3.24) \quad \sum_{j=1}^{n-1} \gamma_2(j)b_j \geq \gamma_2(n-2)s + \gamma_2(n-1)(B - s) \\ = \left(1 - \frac{1}{n(n-1)}\right)B + \left(1 - \frac{1}{(n-1)(n-2)}\right)s.$$

Note also that for any $s \in \{0, 1, \dots, B\}$ there are exactly $\binom{s+n-3}{n-3}$ vectors $\mathbf{b} \in \mathbb{Z}_{\geq 0}^{n-1}$ satisfying $b_1 + \dots + b_{n-1} = B$ and $b_1 + \dots + b_{n-2} = s$. Hence

$$\begin{aligned}
 (3.25) \quad \tilde{P}_d(T, R) & \ll_{d, \mathcal{D}} \sum_{s=0}^B \binom{s+n-3}{n-3} e^{-B-s} \\
 & \quad + T^{-1/n} \sum_{s=0}^B \binom{s+n-3}{n-3} e^{-(1-\frac{1}{n(n-1)})B - (1-\frac{1}{(n-1)(n-2)})s} \\
 & \ll_{d, \mathcal{D}} e^{-B} + T^{-1/n} e^{-(1-\frac{1}{n(n-1)})B} \ll_d R^{-n} (1 + T^{-1/n} R^{1/(n-1)}).
 \end{aligned}$$

If $R < \kappa_{\mathcal{D}}^{1-1/n} T^{1-1/n}$ then this gives $\tilde{P}_d(T, R) \ll_{d, \mathcal{D}} R^{-n}$. On the other hand if $R \geq \kappa_{\mathcal{D}}^{1-1/n} T^{1-1/n}$ then $\tilde{P}_d(T, R) = 0$ by (3.1). Hence the proof of (1.15) is complete. ■

REMARK 2. Note that our proof makes crucial use of the precise error terms which Schmidt has worked out for the asymptotic formulas in [31, Sec. 2]. In this vein, note that the proof of the bound $\tilde{P}_d(T, R) \ll_d R^{-2}$ in [2, Thm. 1.1] is correct as it stands only when T is sufficiently large in a way which may depend on R (as well as d); this is because the proof in [2] uses Schmidt’s [31, Thm. 2], in which the rate of convergence may depend in an unspecified way on the chosen set \mathcal{D} of lattice similarity classes.

3.2. Proof of Corollary 1. Let us first note that (1.18) is again a direct consequence of the classical bound by Schur, (3.3). Indeed, for any $\mathbf{a} \in \hat{\mathbb{N}}^d$ satisfying $a_1 \leq \dots \leq a_d$, by (3.3) we have

$$\begin{aligned}
 (3.26) \quad \frac{f(\mathbf{a})}{(a_1 \cdots a_d)^{1/(d-1)}} & < d \cdot \frac{a_1}{(a_1 \cdots a_{d-1})^{1/(d-1)}} \cdot a_d^{1-1/(d-1)} \\
 & \leq d a_d^{1-1/(d-1)} < d \|\mathbf{a}\|^{1-1/(d-1)},
 \end{aligned}$$

and this implies (1.18).

The following lemma refines [3, Thm. 2 and Remark 1]. Recall that $n = d - 1 \geq 2$. Let us write $\|\mathbf{x}\|_\infty := \max(|x_1|, \dots, |x_n|)$ for the maximum norm of a vector $\mathbf{x} \in \mathbb{R}^n$.

LEMMA 8. *For any $T > 0$ and $\alpha > 0$ we have*

$$\begin{aligned}
 \#\left\{ \mathbf{x} = (x_1, \dots, x_n) \in \mathbb{N}^n : \|\mathbf{x}\|_\infty \leq T, \frac{\|\mathbf{x}\|_\infty}{(x_1 \cdots x_n)^{1/n}} > \alpha \right\} \\
 \ll_n T^n \alpha^{-n} (\log(2 + \alpha))^{n-2}.
 \end{aligned}$$

REMARK 3. For any fixed $\varepsilon > 0$ the above bound is in fact sharp in the range $1 \leq \alpha \leq T^{1-1/n-\varepsilon}$, in the sense that the cardinality on the left hand side is also $\gg_{n, \varepsilon} T^n \alpha^{-n} (\log(2 + \alpha))^{n-2}$ uniformly over all $T \geq T_0(n, \varepsilon)$ and all $1 \leq \alpha \leq T^{1-1/n-\varepsilon}$. However we do not need this fact and we will not prove it here.

Proof of Lemma 8. It suffices to prove

$$(3.27) \quad \#\left\{\mathbf{x} \in \mathbb{N}^n : \frac{1}{2}T < \|\mathbf{x}\|_\infty \leq T, \frac{\|\mathbf{x}\|_\infty}{(x_1 \cdots x_n)^{1/n}} > \alpha\right\} \\ \ll_n T^n \alpha^{-n} (\log(2 + \alpha))^{n-2},$$

since the lemma then follows by dyadic decomposition in the T -variable. Of course we may assume $T \geq 1$ since otherwise the set on the left hand side is empty. We may also assume $\alpha \geq 1$ since otherwise the right hand side is $\gg_n T^n$ and (3.27) is trivial. Now note that if \mathbf{x} belongs to the set on the left hand side of (3.27) then for every real vector \mathbf{y} in the unit box $\mathbf{x} + [0, 1]^n$ we have $\frac{1}{2}T < \|\mathbf{y}\|_\infty \leq T + 1 \leq 2T$ and (since all $x_j \geq 1$)

$$(3.28) \quad \prod_{j=1}^n y_j \leq \prod_{j=1}^n (x_j + 1) \leq \prod_{j=1}^n (2x_j) = 2^n \prod_{j=1}^n x_j \\ < 2^n (\|\mathbf{x}\|_\infty)^n \alpha^{-n} \leq 2^n T^n \alpha^{-n}.$$

Hence the left hand side of (3.27) is

$$(3.29) \quad \leq \text{vol}\left(\left\{\mathbf{y} \in \mathbb{R}_{\geq 1}^n : T/2 < \|\mathbf{y}\|_\infty \leq 2T, \prod_{j=1}^n y_j < 2^n T^n \alpha^{-n}\right\}\right) \\ \leq n \int_1^{2T} \cdots \int_1^{2T} \int_{T/2}^{2T} I\left(\prod_{j=1}^n y_j < 2^n T^n \alpha^{-n}\right) dy_n dy_{n-1} \cdots dy_1 \\ \leq 2nT \int_1^{2T} \cdots \int_1^{2T} I\left(\prod_{j=1}^{n-1} y_j < 2^{n+1} T^{n-1} \alpha^{-n}\right) dy_{n-1} \cdots dy_1 \\ = 2^n n T^n \int_0^{\log(2T)} \cdots \int_0^{\log(2T)} I\left(\sum_{j=1}^{n-1} u_j > \log(\alpha^n/4)\right) e^{-\sum_{j=1}^{n-1} u_j} du_{n-1} \cdots du_1,$$

where in the last step we substituted $y_j = 2T e^{-u_j}$. If $n = 2$ then the last expression is clearly $\ll T^2 \alpha^{-2}$, as desired. From now on we assume $n \geq 3$. Set $u_{n-1} = s + \log(\alpha^n/4) - \sum_{j=1}^{n-2} u_j$; then the conditions $\sum_{j=1}^{n-1} u_j > \log(\alpha^n/4)$ and $u_{n-1} > 0$ are equivalent to $s > 0$ and $\sum_{j=1}^{n-2} u_j < s + \log(\alpha^n/4)$, respectively. Hence the last expression in (3.29) is

$$(3.30) \quad \leq 2^{n+2} n T^n \alpha^{-n} \int_0^\infty e^{-s} \left(\int_0^\infty \cdots \int_0^\infty I\left(\sum_{j=1}^{n-2} u_j < s + \log(\alpha^n/4)\right) \right. \\ \left. \times du_{n-2} \cdots du_1 \right) ds$$

$$\leq \frac{2^{n+2}n}{(n-2)!} T^n \alpha^{-n} \int_0^\infty e^{-s} (s+n \log \alpha)^{n-2} ds \ll_n T^n \alpha^{-n} (\log(2+\alpha))^{n-2},$$

where we used $\alpha \geq 1$. ■

We now give the proof of (1.17) in Corollary 1. We may assume $R \geq 10$ since otherwise (1.17) follows immediately from $P_d(T, R) \leq 1$. We keep $R' \in [1, R]$, to be fixed later. Now

$$\begin{aligned} (3.31) \quad P_d(T, R) &\ll_{d, \mathcal{D}} T^{-d} \# \left\{ \mathbf{a} \in \widehat{\mathbb{N}}^d \cap T\mathcal{D} : \frac{f(\mathbf{a})}{s(\mathbf{a})} > R' \text{ or } \frac{s(\mathbf{a})}{(a_1 \cdots a_d)^{1/(d-1)}} > \frac{R}{R'} \right\} \\ &\leq T^{-d} \# \left\{ \mathbf{a} \in \widehat{\mathbb{N}}^d \cap T\mathcal{D} : \frac{f(\mathbf{a})}{s(\mathbf{a})} > R' \right\} \\ &\quad + T^{-d} \# \left\{ \mathbf{a} \in \mathbb{N}^d : \|\mathbf{a}\|_\infty \leq \kappa'_\mathcal{D} T, \frac{s(\mathbf{a})}{(a_1 \cdots a_d)^{1/(d-1)}} > \frac{R}{R'} \right\}, \end{aligned}$$

where $\kappa'_\mathcal{D} := \sup_{\mathbf{x} \in \mathcal{D}} \|\mathbf{x}\|_\infty$. In the last term, at the price of an extra factor d we may impose the extra assumption $a_d = \max(a_1, \dots, a_d)$. For such vectors \mathbf{a} , we have

$$\begin{aligned} (3.32) \quad \frac{s(\mathbf{a})}{(a_1 \cdots a_d)^{1/(d-1)}} &< \frac{d^{3/2} a_d \max(a_1, \dots, a_n)}{\|\mathbf{a}\|^{1-1/n} (a_1 \cdots a_d)^{1/n}} \\ &< \frac{d^{3/2} a_d \max(a_1, \dots, a_n)}{a_d^{1-1/n} (a_1 \cdots a_d)^{1/n}} = d^{3/2} \frac{\|(a_1, \dots, a_n)\|_\infty}{(a_1 \cdots a_n)^{1/n}}. \end{aligned}$$

Hence for any $T > 0$ with $\widehat{\mathbb{N}}^d \cap T\mathcal{D} \neq \emptyset$,

$$\begin{aligned} (3.33) \quad P_d(T, R) &\ll_{d, \mathcal{D}} T^{-d} \# \left\{ \mathbf{a} \in \widehat{\mathbb{N}}^d \cap T\mathcal{D} : \frac{f(\mathbf{a})}{s(\mathbf{a})} > R' \right\} \\ &\quad + T^{-n} \# \left\{ \mathbf{a} \in \mathbb{N}^n : \|\mathbf{a}\|_\infty \leq \kappa'_\mathcal{D} T, \frac{\|(a_1, \dots, a_n)\|_\infty}{(a_1 \cdots a_n)^{1/n}} > \frac{1}{d^{3/2}} \frac{R}{R'} \right\} \\ &\ll_{d, \mathcal{D}} R'^{-n} + R^{-n} R'^n \left(\log \left(2 + \frac{R}{R'} \right) \right)^{n-2}, \end{aligned}$$

where we used Theorem 3 and Lemma 8. The bound in (1.17) now follows by choosing $R' = \sqrt{R}(\log(R+2))^{1/n-1/2}$. ■

4. Lattice coverings of space with convex bodies. According to a theorem of Schmidt ([30, Thm. 11*]), sharpening a previous result by Rogers ([25, Thm. 2]), if n is sufficiently large, then for any n -dimensional convex body K of volume

$$(4.1) \quad \text{vol}_n(K) \geq (1 + \eta_0)^n \quad (\text{with } \eta_0 = 0.756\dots \text{ as in Theorem 4}),$$

there exists a lattice $L \in X_n$ such that the translates of K by L cover \mathbb{R}^n , viz. $K + L = \mathbb{R}^n$. The lower bound (4.1) was shortly afterwards improved by Rogers to a subexponential bound, in [27]. However, our purpose in this section is to point out that the argument in [30], [25] can fairly easily be modified to show that $K + L = \mathbb{R}^n$ holds not just for *some* lattice $L \in X_n$, but in fact for a subset of large measure in X_n :

THEOREM 6. *Let $\eta_0 = 0.756\dots$ be the unique real root of $e \log \eta + \eta = 0$. For every dimension n larger than a certain absolute constant, if a is any real number satisfying*

$$(4.2) \quad n\eta_0^{n/2} \leq a < 1,$$

and K is any n -dimensional convex body of volume

$$(4.3) \quad \text{vol}_n(K) \geq n(1 + \eta_0 a^{-1/n})^n,$$

then

$$(4.4) \quad \mu_n(\{L \in X_n : K + L = \mathbb{R}^n\}) \geq 1 - a.$$

In particular, for any given constant $\alpha > 1 + \eta_0$ there exists $c < 1$ such that for any sufficiently large n , and for any convex body $K \subset \mathbb{R}^n$ of volume $\geq \alpha^n$, the probability that K fails to give a covering with respect to a random lattice $L \in X_n$ is $\leq c^n$, i.e. exponentially small in n .

We obtain Theorem 4 as a special case of this by taking $n = d - 1$ and $K = \alpha(d - 1)!^{1/(d-1)} \Delta$.

4.1. Proof of Theorem 6. We start by recalling another result of Rogers ([26]) which is used in the proof of [30, Thm. 11*]. For any (Lebesgue) measurable set $M \subset \mathbb{R}^n$ and any lattice $L \in X_n$ we write $\epsilon(M, L)$ for the density of the set of points in \mathbb{R}^n left uncovered by the translates of M by the vectors of L . In other words,

$$(4.5) \quad \epsilon(M, L) = 1 - \text{vol}_n((M + L)/L).$$

(Note that $(M+L)/L$ is a well-defined measurable subset of the torus \mathbb{R}^n/L .)

THEOREM 7 ([26, Thm. 1] ⁽³⁾). *For any measurable set $M \subset \mathbb{R}^n$ ($n \geq 2$) of volume V ,*

$$(4.6) \quad \int_{X_n} \epsilon(M, L) d\mu_n(L) \leq 1 - V + \frac{1}{2}V^2.$$

Let us note the following corollary.

⁽³⁾ The boundedness assumption in Rogers' statement of [26, Thm. 1] can be disposed of, cf. [26, p. 211]. Note also that we do not have to require $V \leq 1$, although if $V > 1$ then the bound in (4.6) is subsumed by the bound $\int \epsilon(M, L) d\mu_n \leq 1/2$, which follows by applying Theorem 7 to an arbitrary subset $M' \subset M$ of volume 1.

COROLLARY 3. For any $C > 0$ and any measurable set $M \subset \mathbb{R}^n$ ($n \geq 2$) of volume V ,

$$(4.7) \quad \mu_n(\{L \in X_n : \epsilon(M, L) \geq 1 - V + CV^2\}) \leq \frac{1}{2C}.$$

Proof. Clearly, for any lattice $L \in X_n$ we have $\text{vol}_n((M + L)/L) \leq V$, and thus

$$(4.8) \quad \epsilon(M, L) \geq 1 - V.$$

Hence if p denotes the measure on the left hand side of (4.7) then

$$(4.9) \quad \int_{X_n} \epsilon(M, L) d\mu_n(L) \geq p(1 - V + CV^2) + (1 - p)(1 - V) \\ = 1 - V + pCV^2,$$

and thus Theorem 7 implies $pC \leq 1/2$. ■

Proof of Theorem 6. Let a and K be as in the statement of the theorem. Let $r = 0.278\dots$ be the root of the equation $1 + r + \log r = 0$; then $\eta_0 = e^{-r}$. We set $K' = \rho K$, where $\rho > 0$ is chosen so that the volume of K' is

$$(4.10) \quad V = \text{vol}_n(K') = rn.$$

We also set

$$(4.11) \quad \eta = e^{-r} a^{-1/n} = \eta_0 a^{-1/n}.$$

Now by Schmidt [30, Thm. 10*] (applied with $\varepsilon = 1$), if n is larger than a certain absolute constant then

$$(4.12) \quad \int_{X_n} \epsilon(K', L) dL \leq 2(1 + V^{n-1}n^{-n+1}e^{V+n})e^{-V} = 2(1 + r^{-1})e^{-rn},$$

and thus

$$(4.13) \quad \mu_n(\{L \in X_n : \epsilon(K', L) \geq 4(1 + r^{-1})e^{-rn}a^{-1}\}) \leq \frac{1}{2}a.$$

Also, by Corollary 3,

$$(4.14) \quad \mu_n(\{L \in X_n : \epsilon(\eta K', L) \geq 1 - \eta^n V + a^{-1}\eta^{2n}V^2\}) \leq \frac{1}{2}a.$$

Note that $e^{-rn}a^{-1}/(\eta^n V) = 1/V = r^{-1}n^{-1} \rightarrow 0$ as $n \rightarrow \infty$, and also

$$(4.15) \quad \frac{a^{-1}\eta^{2n}V^2}{\eta^n V} = a^{-1}\eta^n V = a^{-2}e^{-rn}rn \leq rn^{-1} \rightarrow 0 \quad \text{as } n \rightarrow \infty,$$

where we used (4.2). Hence for n larger than a certain absolute constant,

$$(4.16) \quad 1 - \eta^n V + a^{-1}\eta^{2n}V^2 + 4(1 + r^{-1})e^{-rn}a^{-1} < 1.$$

It follows from (4.13), (4.14) and (4.16) that

$$(4.17) \quad \mu_n(\{L \in X_n : \epsilon(\eta K', L) + \epsilon(K', L) < 1\}) \geq 1 - a.$$

However, for any $L \in X_n$ that satisfies $\epsilon(\eta K', L) + \epsilon(K', L) < 1$ we have $(1 + \eta)K' + L = \mathbb{R}^n$, since K' is convex (cf. [25, Sec. 1.3]), and thus also $\alpha K' + L = \mathbb{R}^n$ for any $\alpha \geq 1 + \eta$. In particular, since $K = \rho^{-1}K'$, we have $K + L = \mathbb{R}^n$ for any such L , provided that $\rho^{-1} \geq 1 + \eta$. But $\text{vol}_n(K) = \rho^{-n}V$; hence $\rho^{-1} \geq 1 + \eta$ is equivalent to $\text{vol}_n(K) \geq (1 + \eta)^n V$, and this inequality certainly holds, because of $V < n$ and our assumption (4.3). Hence (4.4) follows from (4.17). ■

Acknowledgements. I am grateful to Jens Marklof for inspiring and helpful discussions.

The author is a Royal Swedish Academy of Sciences Research Fellow supported by a grant from the Knut and Alice Wallenberg Foundation, and is furthermore supported by the Swedish Research Council Grant 621-2007-6352.

References

- [1] I. M. Aliev and P. M. Gruber, *An optimal lower bound for the Frobenius problem*, J. Number Theory 123 (2007), 71–79.
- [2] I. Aliev and M. Henk, *Integer knapsacks: Average behavior of the Frobenius numbers*, Math. Oper. Res. 34 (2009), 698–705.
- [3] I. Aliev, M. Henk and A. Hinrichs, *Expected Frobenius numbers*, J. Combin. Theory Ser. A 118 (2011), 525–531.
- [4] V. I. Arnold, *Weak asymptotics of the numbers of solutions of Diophantine equations*, Funct. Anal. Appl. 33 (1999), 292–293.
- [5] —, *Geometry and growth rate of Frobenius numbers of additive semigroups*, Math. Phys. Anal. Geom. 9 (2006), 95–108.
- [6] —, *Arithmetical turbulence of selfsimilar fluctuations statistics of large Frobenius numbers of additive semigroups of integers*, Moscow Math. J. 7 (2007), 173–193.
- [7] D. Beihoffer, J. Hendry, A. Nijenhuis and S. Wagon, *Faster algorithms for Frobenius numbers*, Electron. J. Combin. 12 (2005), res. paper 27, 38 pp.
- [8] A. Borel, *Introduction aux groupes arithmétiques*, Hermann, Paris, 1969.
- [9] J. Bourgain and Ya. G. Sinai, *Limit behavior of large Frobenius numbers*, Russian Math. Surveys 62 (2007), 713–725.
- [10] A. Brauer, *On a problem of partitions*, Amer. J. Math. 64 (1942), 299–312.
- [11] J. L. Davison, *On the linear Diophantine problem of Frobenius*, J. Number Theory 48 (1994), 353–363.
- [12] R. Dougherty and V. Faber, *The degree-diameter problem for several varieties of Cayley graphs I: The Abelian case*, SIAM J. Discrete Math. 17 (2004), 478–519.
- [13] L. Fukshansky and S. Robins, *Frobenius problem and the covering radius of a lattice*, Discrete Comput. Geom. 37 (2007), 471–483.
- [14] P. Gritzmann, *Lattice covering of space with symmetric convex bodies*, Mathematika 32 (1985), 311–315.
- [15] P. M. Gruber and C. G. Lekkerkerker, *Geometry of Numbers*, North-Holland, Amsterdam, 1987.
- [16] R. K. Guy, *Unsolved Problems in Number Theory*, Problem Books in Math., Springer, New York, 2004.

- [17] R. Kannan, *Lattice translates of a polytope and the Frobenius problem*, *Combinatorica* 12 (1992), 161–177.
- [18] H. Li, *Effective limit distribution of the Frobenius numbers*, arXiv:1101.3021.
- [19] J. Marklof, *The asymptotic distribution of Frobenius numbers*, *Invent. Math.* 181 (2010), 179–207.
- [20] —, *Tail estimates for the limit distribution of Frobenius numbers*, unpublished note, 2010.
- [21] J. Marklof and A. Strömbergsson, *The periodic Lorentz gas in the Boltzmann–Grad limit: Asymptotic estimates*, *Geom. Funct. Anal.* 21 (2011), 560–647.
- [22] —, —, *Diameters of random circulant graphs*, arXiv:1103.3152.
- [23] J. L. Ramírez Alfonsín, *The Diophantine Frobenius Problem*, Oxford Lecture Ser. Math. Appl. 30, Oxford Univ. Press, Oxford, 2005.
- [24] Ö. J. Rödseth, *An upper bound for the h -range of the postage stamp problem*, *Acta Arith.* 54 (1990), 301–306.
- [25] C. A. Rogers, *Lattice coverings of space: The Minkowski–Hlawka theorem*, *Proc. London Math. Soc.* 8 (1958), 447–465.
- [26] —, *Lattice coverings of space with convex bodies*, *J. London Math. Soc.* 33 (1958), 208–212.
- [27] —, *Lattice coverings of space*, *Mathematika* 6 (1959), 33–39.
- [28] B. H. Roune, *Frobby—a software package for computing Frobenius numbers and irreducible decompositions of monomial ideals*, 2006; <http://www.broune.com/frobby/>.
- [29] —, *Solving thousand-digit Frobenius problems using Gröbner bases*, *J. Symbolic Comput.* 43 (2008), 1–7.
- [30] W. M. Schmidt, *Masstheorie in der Geometrie der Zahlen*, *Acta Math.* 102 (1959), 159–224.
- [31] —, *The distribution of sublattices of \mathbb{Z}^m* , *Monatsh. Math.* 125 (1998), 37–81.
- [32] V. Shchur, Ya. Sinai and A. Ustinov, *Limiting distribution of Frobenius numbers for $n = 3$* , *J. Number Theory* 129 (2009), 2778–2789.
- [33] C. L. Siegel, *A mean value theorem in geometry of numbers*, *Ann. of Math.* 46 (1945), 340–347.
- [34] —, *Lectures on the Geometry of Numbers*, Springer, Berlin, 1989.
- [35] A. Strömbergsson, *On the probability of a random lattice avoiding a large convex set*, *Proc. London Math. Soc.*, to appear.
- [36] A. V. Ustinov, *The solution of Arnold’s problem on the weak asymptotics of Frobenius numbers with three arguments*, *Sb. Math.* 200 (2009), 597–627.
- [37] —, *On the distribution of Frobenius numbers with three arguments*, *Izv. Math.* 74 (2010), 1023–1049.

Andreas Strömbergsson
Department of Mathematics, Box 480
Uppsala University
SE-75106 Uppsala, Sweden
E-mail: astrombe@math.uu.se

Received on 1.4.2011
and in revised form on 15.6.2011

(6659)

