

Lattice Points in High-Dimensional Spheres

J. E. Mazo
A. M. Odlyzko

AT&T Bell Laboratories
Murray Hill, New Jersey 07974

1. Introduction

A general principle, dating back to Gauss, that is widely used in estimating the number of integer lattice points in nice sets S in \mathbb{R}^n is that this number equals the volume of S with a small error term [4,5,13]. This approach is very useful, and can be proved to be rigorous, for example, if one considers the number of lattice points in sets rT , where the dimension n is fixed, T is a given nice set, and $r \rightarrow \infty$. However, we will show below that this principle fails completely if one considers the dimension $n \rightarrow \infty$, and the sets S to be spheres of radii proportional to $n^{1/2}$. That this general principle cannot be justified rigorously in this case is not surprising, since (i) the surface area of the sphere of radius $(\alpha n)^{1/2}$ is larger than the volume by a factor of $(n/\alpha)^{1/2}$, and (ii) the diameter of the unit cube is comparable to the diameter of the sphere. However, it is rather interesting that it is not just the proof, but the principle itself, that fails.

At the end of this section we will mention some applications of our results. At this point we remark that the problem of estimating the number of lattice points in an n -dimensional sphere is in some ways most delicate when the radius $r = (\alpha n)^{1/2}$ for a constant α . If $r \leq n^{1/2-\varepsilon}$ for some fixed $\varepsilon > 0$, then for most locations of the center of the sphere, there will be no lattice points inside it. If $r \geq n^{1/2+\varepsilon}$, then it can be shown by methods similar to those of this paper that the classical principle does apply, and the number of lattice points inside the sphere is asymptotic to the volume, no matter where the center is located.

For $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{R}^n$, and $\alpha > 0$, let $S(\mathbf{x}, n, \alpha)$ denote the n -dimensional sphere of radius $(\alpha n)^{1/2}$ centered at \mathbf{x} ,

$$S(\mathbf{x}, n, \alpha) = \left\{ \mathbf{z} \in \mathbb{R}^n : \sum_{i=1}^n (z_i - x_i)^2 \leq \alpha n \right\}. \quad (1.1)$$

Further, let $N(\mathbf{x}, n, \alpha)$ denote the number of lattice points in $S(\mathbf{x}, n, \alpha)$,

$$N(\mathbf{x}, n, \alpha) = \left\{ \mathbf{z} \in \mathbb{Z}^n : \sum_{i=1}^n (z_i - x_i)^2 \leq \alpha n \right\}. \quad (1.2)$$

We will study the dependence of $N(\mathbf{x}, n, \alpha)$ on \mathbf{x} for α fixed and $n \rightarrow \infty$. The average value of $N(\mathbf{x}, n, \alpha)$ as \mathbf{x} runs over the unit cube $0 \leq x_1, \dots, x_n \leq 1$ is just the volume of the sphere $S(\mathbf{x}, n, \alpha)$, which equals

$$\frac{\pi^{n/2} (\alpha n)^{n/2}}{\Gamma(n/2 + 1)} \sim (\pi n)^{-1/2} (2\pi e \alpha)^{n/2} \quad \text{as } n \rightarrow \infty. \quad (1.3)$$

This paper shows that the maximal and minimal values of $N(\mathbf{x}, n, \alpha)$, as \mathbf{x} varies, differ from the mean value by multiplicative factors of the form $\exp(cn)$, where c is a constant depending on α . Table 1 shows the growth rates of $N(\mathbf{x}, n, \alpha)$. The entry labeled $\lim n^{-1} \log (1 + \min N)$ denotes

$$\lim_{n \rightarrow \infty} n^{-1} \log \left[1 + \min_{\mathbf{x}} N(\mathbf{x}, n, \alpha) \right],$$

for example. Natural logarithms are used in the table, as in the rest of the paper. The values in the table are all obtained by truncation, not rounding, so that π , for example, might be represented as 3.141592. Table 1 was computed using the estimates of Section 2, and the transcendental equations that arise were solved numerically. Table 1 shows that as $\alpha \rightarrow \infty$, the difference between the minimal and maximal values of $N(\mathbf{x}, n, \alpha)$ decreases, which was to be expected.

The precise results are stated and proved in Section 2. They give the (asymptotically) minimal and maximal values of $N(\mathbf{x}, n, \alpha)$ to within multiplicative factors of $\exp(c' n^{1/2})$, where c' is another constant depending on α . (Section 3 mentions possible ways to improve on these estimates.) The main terms in the asymptotic estimates come from solutions of certain

transcendental equations.

The results of Section 2 show that (at least to within multiplicative factors of $\exp(c' n^{1/2})$) $N(\mathbf{x}, n, \alpha)$ is maximized at $\mathbf{x}=(0, 0, \dots, 0)$ and minimized at $\mathbf{x}=(1/2, 1/2, \dots, 1/2)$. (Note that $N((1/2, \dots, 1/2), n, \alpha)=0$ for any $\alpha < 1/4$.) While the best possible result is probably much better (perhaps with the maximum of $N(\mathbf{x}, n, \alpha)$ only a constant times $N((0, \dots, 0), n, \alpha)$, for example), there are infinitely many values of α for each n for which

$$\max_{\mathbf{x}} N(\mathbf{x}, n, \alpha) > N((0, 0, \dots, 0), n, \alpha) .$$

To see this, fix n and consider a sphere of radius α centered at $(0, 0, \dots, 0)$. Increase α until there are lattice points just outside the sphere. If we now move the sphere, we will capture about half of those lattice points. By using the very precise saddle-point estimate sketched in Section 3, it is possible to show a stronger result, namely that for any $0 < c_1 < c_2 < \infty$, there is a $\delta > 0$ such that

$$\max_{\mathbf{x}} N(\mathbf{x}, n, \alpha_n) > (1 + \delta) N((0, 0, \dots, 0), n, \alpha_n)$$

for a sequence of values $\alpha_n, n \geq n_0$, with $c_1 < \alpha_n < c_2$.

Most of the published works on lattice points have concentrated on the difference between the number of lattice points inside a sphere and the volume of the sphere as the radius of the sphere increases and the dimension is held constant (see [5,7,13] and the references given there). Most of these results have also concentrated on spheres with centers at the origin. The few papers we are aware of that deal with variable centers also consider fixed dimensions and radii going to infinity [1,3,12,15].

The main results of this paper were obtained in 1982, prompted by a question posed by J. Ziv in connection with his work on universal quantization [16]. (Our results could be used to obtain another proof of his main technical results.) Afterwards, similar problems turned up in

connection with an algorithm for solving low-density subset-sum problems [9], where a crucial role in evaluating the performance of the algorithm is played by an estimate for $N((0, \dots, 0), n, \alpha)$. This same estimate is also used in [6], which presents a simplified analysis of the algorithm of [9].

2. Main results and proofs

We define

$$f(s, y) = \sum_{k=-\infty}^{\infty} e^{-s(k-y)^2}, \quad y \in \mathbf{R}, \quad s \in \mathbf{C}, \quad \operatorname{Re}(s) > 0. \quad (2.1)$$

Our results will be phrased in terms of $f(s, y)$. In the standard terminology of theta functions [2,14] we have

$$f(s, y) = e^{-sy^2} \theta_3(iys, is/\pi), \quad (2.2)$$

where

$$\theta_3(z, t) = \sum_{k=-\infty}^{\infty} e^{\pi i t k^2} \cos(2kz), \quad (2.3)$$

a result that will be used extensively, since it will allow us to utilize a variety of results about theta functions. (See [10] for other recent applications of classical theta function results.)

We next define $F(s) = F(x_1, \dots, x_n, s)$ by

$$F(s) = \prod_{j=1}^n f(s, x_j). \quad (2.4)$$

By (2.1), we have

$$F(s) = \sum_r N_r e^{-sr}, \quad (2.5)$$

where $N_r = N_r(\mathbf{x}, n)$ is the number of lattice points at distance $r^{1/2}$ from \mathbf{x} , and r runs over all the (countably many) nonnegative values that can occur this way. We first obtain a very easy upper bound.

Lemma 1. For any $s \in \mathbb{R}^+$,

$$N(\mathbf{x}, n, \alpha) \leq e^{s\alpha n} \prod_{j=1}^n f(s, x_j) . \quad (2.6)$$

Proof. By (2.4) and (2.5), we have

$$\begin{aligned} e^{s\alpha n} \prod_{j=1}^n f(s, x_j) &= \sum_r N_r e^{s(\alpha n - r)} \\ &\geq \sum_{r \leq \alpha n} N_r = N(\mathbf{x}, n, \alpha) , \end{aligned}$$

which is the desired result. ■

The bound of Lemma 1 is optimized by choosing s appropriately. We next show that there is basically a unique best choice for s . We let $\|y\|$ denote the distance from y to the nearest integer,

$$\|y\| = \min_k |y - k| ,$$

and note that

$$N((x_1, \dots, x_n), n, \alpha) = N((\|x_1\|, \dots, \|x_n\|), n, \alpha) . \quad (2.7)$$

Lemma 2. For $y \in \mathbb{R}$, let $g(s) = f(s, y)$. Then for all $s \in \mathbb{R}^+$,

$$g(s) > 0 , \quad (2.8)$$

$$\frac{g'}{g}(s) < 0 , \quad (2.9)$$

$$\left[\frac{g'}{g} \right]'(s) > 0 , \quad (2.10)$$

and

$$\frac{g'}{g}(s) \rightarrow -\infty \quad \text{as } s \rightarrow 0^+ , \quad (2.11)$$

$$\frac{g'}{g}(s) \rightarrow -\|y\|^2 \quad \text{as } s \rightarrow \infty . \quad (2.12)$$

Furthermore, for any constants $0 < c_1 < c_2 < \infty$, there is a constant $c_3 > 0$ depending on c_1 and c_2 only, but not on y , such that for $c_1 \leq s \leq c_2$,

$$\left[\frac{g'}{g} \right]'(s) \geq c_3 . \quad (2.13)$$

Also, $g(s)$, $(g'/g)(s)$, $(g'/g)'(s)$, and $(g'/g)''(s)$ are all bounded for $c_1 \leq s \leq c_2$ by constants independent of y .

Proof. Inequalities (2.8) and (2.9) are obvious from the definition (2.1) of $g(s)=f(s, y)$. To prove (2.10), note that we need to prove

$$g''(s)g(s) > (g'(s))^2 ,$$

which is equivalent to

$$\begin{aligned} & \left[\sum_k (k-y)^4 e^{-s(k-y)^2} \right] \left[\sum_m e^{-s(m-y)^2} \right] \\ & > \left[\sum_k (k-y)^2 e^{-s(k-y)^2} \right]^2 . \end{aligned} \quad (2.14)$$

However, (2.14) follows by the Cauchy-Schwarz inequality, with strict inequality holding because the terms in the sums cannot be proportional. In fact, if we use the identity

$$2 \sum_i a_i^2 \sum_j b_j^2 - 2 \left[\sum_i a_i b_i \right]^2 = \sum_{i,j} (a_i b_j - a_j b_i)^2 , \quad (2.15)$$

we see that for $0 < c_1 \leq s \leq c_2 < \infty$,

$$g''(s)g(s) > (g'(s))^2 + \eta \quad (2.16)$$

for some $\eta=\eta(c_1, c_2) > 0$ that does not depend on y , and this (together with the trivial boundedness claims in the last section of the lemma) establishes (2.13) for some effectively computable constant c_3 . (To simply prove the existence of c_3 , we can use a compactness

argument.)

This limit (2.11) follows from comparing the series for $g'(s)$ and $g(s)$, while (2.12) follows by noting that only the leading terms in the series for $g'(s)$ and $g(s)$ are involved in determining the asymptotic behavior as $s \rightarrow \infty$. ■

We now proceed to prove our main results. Note that as $s \rightarrow \infty$,

$$f(s, y) \sim \begin{cases} 1 & \text{if } \|y\| = 0, \\ e^{-s\|y\|^2} & \text{if } 0 < \|y\| < 1/2, \\ 2e^{-s/4} & \text{if } \|y\| = 1/2. \end{cases} \quad (2.17)$$

Therefore if

$$\sum_{j=1}^n \|x_j\|^2 > \alpha n, \quad (2.18)$$

then Lemma 1 implies that $N(\mathbf{x}, n, \alpha) = 0$. This result is obvious anyway, but it is interesting to see that it can be obtained by our analytic method.

Theorem 1. *Suppose that α and δ are positive constants. For any $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{R}^n$ that satisfies*

$$\alpha n > \delta n + \sum_{j=1}^n \|x_j\|^2 \quad (2.19)$$

there is a unique $s = s(\alpha) = s(\alpha; \mathbf{x})$ that satisfies the equation

$$\sum_{j=1}^n \frac{\partial}{\partial s} \log f(s, x_j) + \alpha n = 0. \quad (2.20)$$

For this $s = s(\alpha)$, we have

$$N(\mathbf{x}, n, \alpha) \leq e^{s(\alpha)\alpha n} \prod_{j=1}^n f(s(\alpha), x_j) \quad (2.21)$$

and also

$$N(\mathbf{x}, n, \alpha) \geq e^{s(\alpha)\alpha n - cn^{1/2}} \prod_{j=1}^n f(s(\alpha), x_j) \quad (2.22)$$

for a constant $c > 0$ that depends only on α and δ .

Proof. The existence and uniqueness of $s(\alpha)$ follow from Lemma 2. The upper bound (2.21) holds with any s , not just $s(\alpha)$, as we already noted in Lemma 1. Thus it only remains to prove the lower bound (2.22).

We choose

$$0 < s_1 < s_2 < s_3 = s(\alpha)$$

and define α_k , $1 \leq k \leq 3$, by

$$\alpha_k = -\frac{1}{n} \sum_{j=1}^n \frac{\partial}{\partial s} \log f(s_k, x_j). \quad (2.23)$$

By Lemma 2, we have $\alpha_1 > \alpha_2 > \alpha_3 > 0$.

We next let $F(s)$ be defined by (2.4), and consider

$$H = e^{\alpha_2 s_2 n} F(s_2) - e^{\alpha_1 s_1 n} F(s_1) e^{(\alpha_2 - \alpha_1) s_2 n} - e^{\alpha_3 s_3 n} F(s_3) e^{(\alpha_2 - \alpha_3) s_2 n}. \quad (2.24)$$

If we write

$$H = \sum_r N_r w_r, \quad (2.25)$$

then we see that $w_r \leq 0$ for $r \geq \alpha_1 n$, since in that range

$$\alpha_2 s_2 n - s_2 r \leq \alpha_1 s_1 n - s_1 r + (\alpha_2 - \alpha_1) s_2 n,$$

so just subtracting the second term on the right side in (2.25) from the first gives $w_r \leq 0$.

Similarly, we find $w_r \leq 0$ for $r \leq \alpha_3 n$. Now for $\alpha_3 n < r < \alpha_1 n$,

$$w_r \leq \exp(\alpha_2 s_2 n - s_2 r) \leq \exp((\alpha_2 - \alpha_3) s_2 n), \quad (2.27)$$

so

$$N(\mathbf{x}, n, \alpha) \geq H \exp(-(\alpha_2 - \alpha_3) s_2 n) . \quad (2.28)$$

Thus we basically have to prove that H is positive and large.

Let us consider

$$V_1 = \alpha_2 s_2 n + \log F(s_2) - \alpha_1 s_1 n - \log F(s_1) - (\alpha_2 - \alpha_1) s_2 n . \quad (2.29)$$

By Lemma 2,

$$\log F(s_1) = \log F(s_2) + (s_1 - s_2) \frac{F'}{F}(s_2) + \frac{1}{2} (s_1 - s_2)^2 \left[\frac{F'}{F} \right]'(s_2) + O(n |s_1 - s_2|^3) ,$$

where the constant implied by the O -notation depends only on α and δ . Also,

$$\begin{aligned} \alpha_1 n &= - \frac{F'}{F}(s_1) = - \frac{F'}{F}(s_2) + (s_2 - s_1) \left[\frac{F'}{F} \right]'(s_2) + O(n |s_1 - s_2|^3) \\ &= \alpha_2 n + (s_2 - s_1) \left[\frac{F'}{F} \right]'(s_2) + O(n |s_1 - s_2|^3) . \end{aligned}$$

Therefore

$$V_1 = \frac{1}{2} (s_1 - s_2)^2 \left[\frac{F'}{F} \right]'(s_2) + O(n |s_1 - s_2|^3) . \quad (2.30)$$

Similarly, if we let

$$V_3 = \alpha_2 s_2 n + \log F(s_2) - \alpha_3 s_3 n - \log F(s_3) - (\alpha_2 - \alpha_3) s_2 n , \quad (2.31)$$

then we find that

$$V_3 = \frac{1}{2} (s_3 - s_2)^2 \left[\frac{F'}{F} \right]'(s_2) + O(n |s_3 - s_2|^3) . \quad (2.32)$$

Therefore, if we choose

$$\begin{aligned} s_2 &= s_3 - C n^{-1/2} , \\ s_1 &= s_3 - 2C n^{-1/2} , \end{aligned} \quad (2.33)$$

for any $C > 0$, then by Lemma 2 we will have

$$V_1, V_3 \geq C^2 \sigma - O(n^{-1/2}) \quad \text{as } n \rightarrow \infty \quad (2.34)$$

for some $\sigma > 0$, and so if C is chosen large enough, then for large n we will have

$$V_1, V_3 \geq 2, \quad (2.35)$$

and so

$$H \geq \frac{1}{2} e^{\alpha_2 s_2 n} F(s_2), \quad (2.36)$$

which together with (2.28) proves (2.22), since by the same arguments as were used to estimate V_1 and V_3 ,

$$\alpha_2 s_2 n + \log F(s_2) \geq \alpha_3 s_3 n + \log F(s_3) - c' n^{1/2}. \quad (2.37)$$

This completes the proof of Theorem 1. ■

Theorem 1 determines $N(\mathbf{x}, n, \alpha)$ to within a multiplicative factor of $\exp(cn^{1/2})$ for all \mathbf{x} if $\alpha > 1/4$, and also for many values of \mathbf{x} (in particular for $\mathbf{x} = (0, 0, \dots, 0)$) if $0 < \alpha \leq 1/4$. However, the determination is in terms of solutions to complicated transcendental equations. We next use the results of Theorem 1 to show that up to factors of $\exp(cn^{1/2})$, $N(\mathbf{x}, n, \alpha)$ is maximized at $\mathbf{x}=(0, 0, \dots, 0)$ and minimized at $\mathbf{x}=(1/2, 1/2, \dots, 1/2)$.

Theorem 2. *For any $\alpha > 0$, there is a constant $c'(\alpha) > 0$ such that for all $\mathbf{x} \in \mathbb{R}^n$,*

$$N(\mathbf{x}, n, \alpha) \leq \exp(c'(\alpha)n^{1/2}) N(\mathbf{x}_0, n, \alpha), \quad (2.38)$$

where $\mathbf{x}_0=(0, 0, \dots, 0)$. *For any $\alpha > 1/4$, there is a constant $c''(\alpha) > 0$ such that for all $\mathbf{x} \in \mathbb{R}^n$,*

$$N(\mathbf{x}, n, \alpha) \geq \exp(-c''(\alpha)n^{1/2}) N(\mathbf{x}_1, n, \alpha), \quad (2.39)$$

where $\mathbf{x}_1=(1/2, 1/2, \dots, 1/2)$. (For $0 < \alpha < 1/4$, $N(\mathbf{x}_1, n, \alpha)=0$, so (2.39) is trivially valid there also.)

Proof. By Eq. (2.2) and the fundamental transformation formula for theta functions [2,14]

$$\theta_3(z, t) = (-it)^{-1/2} \exp(z^2/(\pi it)) \theta_3(z/t, -i/t) , \quad (2.40)$$

we have, for any $s \in \mathbf{R}^+$,

$$\begin{aligned} f(s, y) &= (\pi/s)^{1/2} \theta_3(\pi y, i\pi/s) \\ &= (\pi/s)^{1/2} \sum_{k=-\infty}^{\infty} \exp(-\pi^2 k^2/s) \cos(2ky\pi) \\ &\leq (\pi/s)^{1/2} \sum_{k=-\infty}^{\infty} \exp(-\pi^2 k^2/s) \\ &= f(s, 0) . \end{aligned} \quad (2.41)$$

Therefore for any $s > 0, \alpha > 0$,

$$e^{s\alpha n} F(x_1, \dots, x_n, s) \leq e^{s\alpha n} F(0, \dots, 0, s) , \quad (2.42)$$

and so by Lemma 1 and Theorem 1 we obtain the inequality (2.38).

To prove (2.39), we use a similar argument, but this time we utilize the infinite product for theta functions [2; Eq. (32.1)]. We find, for $q = \exp(-\pi^2/s)$, that

$$\begin{aligned} f(s, y) &= (\pi/s)^{1/2} \theta_3(\pi y, i\pi/s) \\ &= (\pi/s)^{1/2} \theta_4(\pi y + \pi/2, i\pi/s) \\ &= (\pi/s)^{1/2} \prod_{k=1}^{\infty} \{(1 + 2q^{2k-1} \cos(2\pi y) + q^{4k-2})(1 - q^{2k})\} \\ &\geq (\pi/s)^{1/2} \prod_{k=1}^{\infty} \{(1 - 2q^{2k-1} + q^{4k-2})(1 - q^{2k})\} \\ &= f(s, 1/2) , \end{aligned} \quad (2.43)$$

which shows that for all $s > 0, \alpha > 0$,

$$e^{s\alpha n} F(x_1, \dots, x_n, s) \geq e^{s\alpha n} F(1/2, \dots, 1/2, s) , \quad (2.44)$$

and this gives the inequality (2.39). ■

To conclude our series of technical results, we show that the extremal values of $N(\mathbf{x}, n, \alpha)$ differ from the mean value by exponential factors.

Theorem 3. *For any $\alpha > 0$, there is a constant $\omega > 0$ such that for $n \geq n_0(\alpha)$,*

$$N((1/2, \dots, 1/2), n, \alpha) e^{\omega n} \leq (2\pi e \alpha)^{n/2} \leq N((0, \dots, 0), n, \alpha) e^{-\omega n}. \quad (2.45)$$

Proof. In view of previous results, it suffices to show that if (in the notation of Theorem 1)

$$s_1 = s(\alpha; (0, \dots, 0)), \quad (2.46)$$

then

$$s_1 \alpha + \log f(s_1, 0) > \frac{1}{2} \log (2\pi e \alpha), \quad (2.47)$$

and that if $\alpha > 1/4$ and

$$s_2 = s(\alpha; (1/2, \dots, 1/2)), \quad (2.48)$$

then

$$s_2 \alpha + \log f(s_2, 1/2) < \frac{1}{2} \log (2\pi e \alpha). \quad (2.49)$$

(Note that for $0 < \alpha \leq 1/4$, the inequality on the left side of (2.45) is trivial, as $N((1/2, \dots, 1/2), n, \alpha) = 0$ for $0 < \alpha < 1/4$, and $= 2^n$ for $\alpha = 1/4$.) It is easy to see (using the transformation formula (2.40), as in the first part of (2.41)) that

$$s_1 \alpha + \log f(s_1, 0) - \frac{1}{2} \log (2\pi e \alpha) \rightarrow 0 \quad \text{as } \alpha \rightarrow \infty, \quad (2.50)$$

and so to prove (2.47) it suffices to show that for $0 < \alpha < \infty$,

$$\frac{\partial}{\partial \alpha} \left[s_1 \alpha + \log f(s_1, 0) - \frac{1}{2} \log (2\pi e \alpha) \right] < 0. \quad (2.51)$$

Since

$$\alpha = - \frac{\partial}{\partial s_1} \log f(s_1, 0) , \quad (2.52)$$

inequality (2.51) will follow if we show that

$$- \frac{\partial}{\partial s} \log f(s, 0) < \frac{1}{2s}, \quad 0 < s < \infty . \quad (2.53)$$

As in inequality (2.41), we have

$$f(s, 0) = (\pi/s)^{1/2} \theta_3(0, i\pi/s) ,$$

and so we only have to show that

$$\frac{\partial}{\partial s} \theta_3(0, i\pi/s) > 0 \quad \text{for } 0 < s < \infty , \quad (2.54)$$

which is obvious from the infinite sum (2.3) defining θ_3 . This proves (2.47).

To prove (2.48), we use a similar argument. Again,

$$s_2 \alpha + \log f(s_2, 1/2) - \frac{1}{2} \log (2\pi e \alpha) \rightarrow 0 \quad \text{as } \alpha \rightarrow \infty , \quad (2.55)$$

so it suffices to show that for $0 < \alpha < \infty$,

$$\frac{\partial}{\partial \alpha} \left[s_2 \alpha + \log f(s_2, 1/2) - \frac{1}{2} \log (2\pi e \alpha) \right] > 0 . \quad (2.56)$$

Since

$$\alpha = - \frac{\partial}{\partial s_2} \log f(s_2, 1/2) , \quad (2.57)$$

we need to show that

$$- \frac{\partial}{\partial s} \log f(s, 1/2) > \frac{1}{2s}, \quad 0 < s < \infty , \quad (2.58)$$

which reduces to showing that

$$\frac{\partial}{\partial s} \theta_4(0, i\pi/s) < 0 \quad \text{for} \quad 0 < s < \infty. \quad (2.59)$$

This, however, follows from the infinite product for $\theta_4(0, i\pi/s)$. As in (2.43), we find that for $q = \exp(-\pi^2/s)$,

$$\theta_4(0, i\pi/s) = \prod_{k=1}^{\infty} \{(1-q^{2k-1})^2(1-q^{2k})\}, \quad (2.60)$$

and so (2.59) follows. This completes the proof of the theorem. ■

A different proof of Theorem 3 could be given based more directly on the proofs of Theorems 1 and 2. It would rely on the fact that

$$\exp(n\alpha s(\alpha; \mathbf{x})) F(x_1, \dots, x_n, s)$$

is not constant as \mathbf{x} varies, and so minimal and maximal values have to differ from the mean.

3. Concluding remarks

Theorem 2 leaves open the question whether the inequality (2.39) of Theorem 2 holds for $\alpha=1/4$. It seems very likely that it does, and this might be provable by extensions of our methods. (By Theorem 1, inequality (2.39) definitely holds if $\sum \|x_j\|^2$ stays away from $n/4$.)

The lower bound of Theorem 2 can be obtained fairly easily basically because it estimates partial sums of coefficients of generating functions. When one deals with a single fixed generating function, it is often possible to get very precise information about the asymptotic behavior of sums of coefficients with indices $\leq x$ as $x \rightarrow \infty$ by using Tauberian theorems. Since Tauberian theorems require very little information about the generating function, such a method is very convenient to use. Unfortunately, it is not applicable to our problem, since we do not deal with a single fixed generating function, but a sequence of functions.

The method used to obtain the lower bound of Theorem 2 is very simple, and can be extended to many other problems in number theory, analysis, and combinatorial enumeration. For

example, it can be used to show that the Rush-Sloane packing results [11] hold for general σ , not just for integers.

The essence of the lower bound method of Theorem 2 is the use of a weighted sum of the quantities whose cumulative sums are being sought. In our case it gives estimates accurate to within multiplicative factors of $\exp(cn^{1/2})$. One can improve on this method and obtain more accurate estimates by using more complicated weights (which might also require using an integral of $\exp(s\alpha n) F(s)$ times a weight function instead of the simple three-term sum of (2.24)).

In some cases it is possible to obtain very precise estimates by using the saddle-point method. For example, to estimate $N(\mathbf{x}_0, n, \alpha)$, where $\mathbf{x}_0 = (0, \dots, 0)$, let

$$z = e^{-s} ,$$

so that $f(s, 0) = h(z)$, with

$$h(z) = 1 + 2 \sum_{k=1}^{\infty} z^{k^2} . \quad (3.1)$$

Then $N_r = 0$ for $r \neq m^{1/2}$, $m \in \mathbb{Z}$, $m \geq 0$, and if $r = m^{1/2}$, then N_r is the coefficient of z^m in the Taylor series expansion of $h(z)^n$. Therefore for $r = m^{1/2}$ (so $\alpha = m/n$)

$$N((0, \dots, 0), n, \alpha) = \frac{1}{2\pi i} \oint \frac{h(z)^n}{z^m} \frac{dz}{z(1-z)} , \quad (3.2)$$

where the integral is taken over any circle $|z|=w$, $0 < w < 1$. If we let $m, n \rightarrow \infty$ so that $\alpha = m/n \in (c_1, c_2)$ for some fixed $0 < c_1 < c_2 < \infty$, then it is easy to show that the integrand in (3.2) has an approximate saddle point at $z = z_0$, where z_0 is the unique real solution in $(0, 1)$ to

$$z \frac{h'}{h} (z) = \alpha \quad (3.3)$$

(this corresponds to the point determined by Theorem 1), and that

$$N((0, \dots, 0), n, \alpha) \sim \frac{1}{(1-z_0)\sqrt{2b\pi n}} \frac{h(z_0)^n}{z_0^m}, \quad (3.4)$$

where

$$b = \frac{d}{dz} \left[\frac{h'(z)}{n} - \frac{m}{nz} \right] \Bigg|_{z=z_0}. \quad (3.5)$$

This estimate shows that the bound of Lemma 1 is off only by a factor of $n^{1/2}$ for $\mathbf{x}=(0, \dots, 0)$, and suggests that the same is true for other \mathbf{x} .

The estimate (3.4) applies only for $\alpha=m/n$, $m, n \in Z^+$. If we wish to apply it for a fixed α , with $n \rightarrow \infty$, we do not obtain a simple solution, since for each n we need to take $m = \lfloor n\alpha \rfloor$ (the integer part of $n\alpha$) and compute the bound for this m . This gives rise to slight oscillations, reflecting the fact that the number of lattice points in a sphere of radius $(m+1)^{1/2}$ is larger than the number in a sphere of radius $m^{1/2}$ by a constant > 1 .

The saddle-point method can be extended to a few points other than $\mathbf{x}=(0, \dots, 0)$. However, to obtain precise bounds by analytic method, it seems that one needs to go back to using the functions $f(s, y)$, but this time allowing s to be complex. Perron-type integral formulas can then be used to evaluate the $N(\mathbf{x}, n, \alpha)$, but to estimate them effectively one needs to use kernels that lead to problems similar to those one encounters when using weighted sums of the form mentioned at the beginning of this section.

REFERENCES

1. J. Beck, On a lattice point problem of L. Moser. I, *Combinatorica* **8** (1989), 21-47.
2. R. Bellman, *A Brief Introduction to Theta Functions*, Holt, Rinehart, and Winston, 1961.
3. K. Chandrasekharan and R. Narasimhan, On lattice-points in a random sphere, *Bull. Amer. Math. Soc.* **73** (1967), 68-71.
4. P. Erdős, P. M. Gruber, and J. Hammer, *Lattice Points*, Longman, 1989.
5. F. Fricker, *Einführung in die Gitterpunktlehre*, Birkhäuser, 1982.
6. A. M. Frieze, On the Lagarias-Odlyzko algorithm for the subset sum problem, *SIAM J. Comp.* **15** (1986), 536-539.
7. E. Grosswald, *Representations of Integers as Sums of Squares*, Springer, 1985.
8. J. Hammer, *Unsolved Problems Concerning Lattice Points*, Pitman 1977.
9. J. C. Lagarias and A. M. Odlyzko, Solving low-density subset sum problems, *J. Assoc. Comp. Mach.* **32** (1985), 229-246. (Preliminary version in *Proc. 24th IEEE Found. Computer Sci. Symp.*, 1983, pp. 1-10.)
10. H. L. Montgomery, Minimal theta functions, *Glasgow Math. J.* **30** (1988), 75-85.
11. J. Rush and N. J. A. Sloane, An improvement to the Minkowski-Hlawka bound for packing superballs, *Mathematika* **34** (1987), 8-18.
12. A. I. Vinogradov and M. M. Skriyanov, The number of lattice points inside the sphere with variable center, analytic number theory and the theory of functions, 2, *Zap. Nančn. Sem. Leningrad Otdal. Mat. Inst. Steklov (LOMI)* **91** (1979), 25-30, 180.
13. A. Walfisz, *Gitterpunkte in mehrdimensionalen Kugeln*, Polish Scientific Publishers,

Warsaw, 1957.

14. E. T. Whittaker and G. N. Watson, *A Course of Modern Analysis*, 4th ed., Cambridge Univ. Press, 1927.
15. A. A. Yudin, On the number of integer points in the displaced circles, *Acta Arith.* **14** (1967/68), 141-152.
16. J. Ziv, On universal quantization, *IEEE Trans. Information Theory* **IT-31** (1985), 344-347.

Table 1. Number of lattice points, N , in an n -dimensional sphere of radius $(\alpha n)^{1/2}$ as the center of the sphere varies.

α	$\lim n^{-1} \log (1 + \min N)$	$\lim n^{-1} \log (\text{mean } N)$	$\lim n^{-1} \log (\max N)$
0.1	0.0	0.267645986	0.394414813
0.2	0.0	0.614219576	0.639415756
0.3	0.810070417	0.816952131	0.821516167
0.4	0.960010601	0.960793167	0.961505491
0.5	1.072260430	1.072364942	1.072467359
0.6	1.163511322	1.163525721	1.163540062
0.7	1.240599064	1.240601061	1.240603056
0.8	1.307366480	1.307366757	1.307367034
0.9	1.366258236	1.366258275	1.366258313
1.0	1.418938527	1.418938533	1.418938538

Lattice Points in High-Dimensional Spheres

J. E. Mazo
A. M. Odlyzko

AT&T Bell Laboratories
Murray Hill, New Jersey 07974

ABSTRACT

Let $N(\mathbf{x}, n, \alpha)$ denote the number of integer lattice points inside the n -dimensional sphere of radius $(\alpha n)^{1/2}$ with center at \mathbf{x} . This number $N(\mathbf{x}, n, \alpha)$ is studied for α fixed, $n \rightarrow \infty$, and \mathbf{x} varying. The average value (as \mathbf{x} varies) of $N(\mathbf{x}, n, \alpha)$ is just the volume of the sphere, which is roughly of the form $(2\pi e \alpha)^{n/2}$. It is shown that the maximal and minimal values of $N(\mathbf{x}, n, \alpha)$ differ from the average by factors exponential in n , which is in contrast to the usual lattice point problems in bounded dimensions. This lattice point problem arose separately in universal quantization and in low density subset sum problems.