ON THE DISTRIBUTION OF LENGTHS OF SHORT VECTORS IN A RANDOM LATTICE

SEUNGKI KIM

ABSTRACT. We use an idea from sieve theory — specifically, an inclusion-exclusion argument inspired by Schmidt [4] — to estimate the distribution of the lengths of kth shortest vectors in a random lattice of covolume 1 in dimension n. This is an improvement of the results of Rogers [3] and Södergren [7] in that it allows k to increase with n.

1. Introduction

Let $X_n = SL_n\mathbb{Z}\backslash SL_n\mathbb{R}$ be the space of lattices[1] L of covolume 1 in $\mathbb{R}^n$. X_n admits a unique right $SL_n\mathbb{R}$-invariant probability measure μ_n, derived from a Haar measure of $SL_n\mathbb{R}$ (see [6]). This measure provides the standard notion of a random lattice.

In this paper, we are interested in investigating the statistics of short vectors of a random lattice. Instead of directly stating the mathematical formulation of this problem, we will present a couple of theorems in this direction to give the reader a flavor of this subject. One of the earliest theorems proved concerning lattice statistics is

Theorem 1 (Siegel [6]). *Let $\rho : \mathbb{R}^n \to \mathbb{R}$ be a compactly supported and bounded Borel measurable function. Then*

$$\int_{X_n} \sum_{x\in L\backslash\{0\}} \rho(x) d\mu_n = \int_{\mathbb{R}^n} \rho(x)dx.$$

In particular, if ρ is the characteristic function of the ball of radius r centered at the origin, then Siegel's theorem tells us that a random lattice on average has $V(r)$ nonzero vectors of length less than r, where $V(r)$ is the volume of a ball with radius r.

Later, C.A. Rogers, by using his own generalization of Siegel's theorem above, proved

Theorem 2 (Rogers [3]). *Let $\rho : \mathbb{R}^n \to \mathbb{R}$ be the characteristic function of a Borel set S with measure V that is symmetric at the origin (that is, $x \in S \Leftrightarrow -x \in S$). Fix a positive integer k. Provided $n \geq [k^2/4] + 3$, we have*

$$e^{-V/2}\sum_{i=0}^{\infty} \frac{i^k}{i!}(V/2)^i \leq \int \left(\frac{1}{2}\sum_{x\in L\backslash\{0\}} \rho(x)\right)^k d\mu_n(L) \leq e^{-V/2}\sum_{i=0}^{\infty} \frac{i^k}{i!}(V/2)^i + o_n(1).$$

Again let ρ be the characteristic function of the ball of radius r centered at the origin. Then this theorem says that the kth moment of

$$\frac{1}{2}\sum_{x\in L\backslash\{0\}} \rho(x) = (\text{the number of pairs of nonzero vectors } \pm x \text{ of a lattice } L \text{ of length } < r)$$

[1] In this paper, a lattice in $\mathbb{R}^n$ is simply a rank n $\mathbb{Z}$-submodule of $\mathbb{R}^n$ (with the standard addition structure).

converges to the kth moment of the Poisson distribution with mean $V(r)/2$ as n goes to infinity. In other words, the number of nonzero vectors (identified up to sign) of a random lattice with length less than r has a distribution that converges weakly to the Poisson distribution with mean $V(r)/2$ as dimension becomes large. This result is consistent with the intuition that the first few (relative to the dimension) shortest vectors of a random lattice should be nearly random, as the algebraic structure of a lattice would hardly interfere with the choices of those vectors.

It is clear that one could also convert this data into one about the statistics of the length of kth shortest vector (up to sign) of a random lattice, with k fixed and n arbitrarily large. In particular, the case $k = 1$, i.e. the statistics of the shortest nonzero vector of a random lattice is very closely related to finding the optimal density of lattice sphere packing.

These and other related theorems were all proved in 1940's and 50's. Since then, the field has come to its mysterious demise, despite much interest in short lattice vectors in computer science and applied mathematics in the latter half of the century. However, in a recent paper, Södergren proved that

Theorem 3 (Södergren [7])**.** *For a lattice L in $\mathbb{R}^n$ and $t \geq 0$, let $\tilde{N}_t^n(L)$ be the number of nonzero vectors (up to sign) of L in a ball of volume t. Taking L to be a random lattice, one may view $\tilde{N}_t^n$ as a stochastic process on the positive real line $\{t \in \mathbb{R} : t \geq 0\}$. As $n \to \infty$, $\tilde{N}_t^n$ weakly converges to a Poisson process on the positive real line with intensity $1/2$.*

This result has connections to some topics in analytic number theory, such as zeroes of the Epstein zeta function and to the Berry-Tabor conjecture; for more information see [7]. Södergren also investigates the joint distribution of the angles and the lengths of the first N shortest vectors of a random lattice; see [8].

The theorems of Rogers and Södergren above provide an insight over the "shape" of a random lattice. Namely, the lengths of the first k shortest vectors of a random lattice of dimension n converge in distribution to the first k points of a Poisson process on the positive real line with intensity $1/2$, with k fixed and as n goes to infinity. Naturally, we would like to remove the condition that k is fixed, and replace it with a weaker condition, such as that k grows with n at a certain rate, in order to understand more fully the statistics of lattice vectors. We expect that as the growth rate of k increases, the Poissonness of the length distribution exhibited in the case of fixed k will gradually fade away, as lattices come with the natural algebraic structure, which certainly plays a crucial role in determining their shape. Eventually we hope to grasp this entire picture—the interaction of the inherent structure on lattices (and their moduli space) and their fine quantitative properties—in rigorous terms.

It seems difficult, however, to directly employ Rogers' and Södergren's arguments to relax the condition on k. Both prove the convergence in distribution by proving the convergence in moments, and the precise quantitative relationship between convergence in moments and convergence in distribution is rather unclear. A more direct proof of their theorems would be helpful. This is the motivation for the present paper.

Using our main theorem, we will be able to obtain the following estimate

Theorem 4. *Let S be a Borel measurable set in $\mathbb{R}^n$ symmetric at the origin with Euclidean measure V. Fix $\varepsilon > 0$. Suppose that $0 \leq k \leq (n/2)^{\frac{1}{2}-\varepsilon}$ is a nonnegative integer, possibly depending on n, and suppose also that $8V \leq \sqrt{n/2} - k$. Let $P(S,k)$ be the probability that an n-dimensional random lattice has at most k nonzero vectors (up to sign) in S. Then*

$P(S,k)$ is close to $P_{V/2}(k)$ for n sufficiently large, where $P_{V/2}$ is the (left) cumulative distribution function of the Poisson distribution with mean $V/2$. More precisely,

$$P_{V/2}(k) - o_n(1) \leq P(S,k) \leq P_{V/2}(k) + o_n(1),$$

for all sufficiently large n (depending on ε).

Remark. Although $P_{V/2}(k)$ could also be $o_n(1)$ for certain choices of n, k, and V permitted by the theorem, it is still the main contribution in the above inequality in the sense that it is much larger than the implied error term. In fact, the expression $o_n(1)$ above may be replaced by

$$(\sqrt{n/2} - k)^{-1/2} P_{V/2}(k) + e(n, k+1, V)$$

(see Theorem 5 below for the definition of $e(n,k,V)$).

It is easily seen that Theorem 4 improves (the implications of) Theorems 2 and 3 upon letting S be a ball and an annulus, respectively. Its main selling point is that it allows k to increase with n to a certain extent.

We will delegate the proof of Theorem 4 to the last section of this paper. It is a rather crudely obtained bound from the following theorem, which is the main result of this paper:

Theorem 5. *Let S be as in Theorem 4. Let*

$$F_{S,k}(L) = \begin{cases} 1 & \textit{if } L \textit{ has} \geq k \textit{ nonzero vectors (mod } \pm\textit{) in } S \\ 0 & \textit{otherwise.} \end{cases}$$

For $k \leq \alpha, \beta \leq \sqrt{n/2}$ such that $\alpha - k$ is even and $\beta - k$ is odd,

$$\sum_{h=k}^{\beta} (-1)^{h-k} \frac{(V/2)^h}{h(h-k)!(k-1)!} - e(n,k,V) \leq \int_{X_n} F_{S,k}(L) d\mu_n$$
$$\leq \sum_{h=k}^{\alpha} (-1)^{h-k} \frac{(V/2)^h}{h(h-k)!(k-1)!} + e(n,k,V),$$

where the error term $e(n,k,V)$ has a bound

$$0 \leq e(n,k,V) \leq \frac{23}{k!} \sqrt{n/2} (0.999)^n (V/2+1)^{\sqrt{n/2}}.$$

Note that, for any k varying between 1 and $\min(\alpha,\beta)$ (e.g. k could grow with n at a rate comparable to $\sqrt{n}$), and a moderately increasing V (for instance, at the rate of $e^{n^{1/2-\varepsilon}}$ or slower[2]), the right-hand side goes to zero as $n \to \infty$.

The proof of Theorem 5 is in two steps. First we express $F_{S,k}$ as a series using an inclusion-exclusion argument, whose individual terms are integrable over X_n using Rogers' integration formula [2]. Then we estimate the tail of the series to show that we can "cut them off" and obtain an estimate. This is essentially an application of the idea of the Brun sieve.

The inspiration for this argument comes from the works of Wolfgang Schmidt [4], [5], another major contributor to the geometry of numbers in the 50's. In [4] Schmidt first introduces an inclusion-exclusion method on lattice vectors to prove a stronger version of the case $k = 0$ of Theorem 4, which he refines considerably in [5] (but neither says

[2] But of course, V must be of comparable magnitude to $\min(\alpha,\beta)$ in order for this estimate to be meaningful.

anything about the cases $k > 0$). It is worth comparing briefly the methods and the quality of the results in [4] and the present paper. The main theorem, Theorem 4, of [4] only requires $n \geq 13$, and more importantly, allows $V \leq n-1$. It would have been therefore desirable to give a straightforward generalization of Schmidt's argument to the cases $k > 0$. Yet this seems to be difficult to achieve, as the combinatorial identities exploited therein hold true only when $k = 0$, and fails irreparably otherwise (for example, Schmidt uses that the sign of $\sum_{i=0}^{m}(-1)^i\binom{n}{i}$ depends on the parity of m; this is not true if the summation starts from a nonzero number). Hence the inclusion-exclusion method we employed below is quite different from Schmidt's, admittedly more crude, but applicable to a much wider range of k.

It seems quite possible that further developments along this theme of sieve methods on lattice vectors will improve the bounds on both V and k to $O(n)$, which is probably the best result of its kind we can expect; I hope to return to this topic later.

2. Rogers' integration formula

The main technical tool in studying the statistics of lattice vectors is Rogers' integration formula [2], which gives an explicit expression for the integrals

$$\int_{X_n} \sum_{x_1,\ldots,x_k \in L\setminus\{0\}} \rho(x_1,\ldots,x_k)d\mu_n \tag{1}$$

$$\int_{X_n} \sum_{\substack{x_1,\ldots,x_k \in L\setminus\{0\} \\ \mathrm{rank}(\langle x_1,\ldots,x_k\rangle)=k}} \rho(x_1,\ldots,x_k)d\mu_n \tag{2}$$

or the like, where $k < n$ and ρ is a compactly supported and bounded Borel-measurable function on $(\mathbb{R}^n)^k$.

Theorem 6 (Rogers [2] Theorems 2 and 4)**.** *(1) equals*

$$\int_{\mathbb{R}^n}\cdots\int_{\mathbb{R}^n}\rho(x_1,\ldots,x_k)dx_1\ldots dx_k$$
$$+\sum_{(\nu,\mu)}\sum_{q=1}^{\infty}\sum_{D}\left(\frac{e_1}{q}\cdots\frac{e_m}{q}\right)^n\int_{\mathbb{R}^n}\cdots\int_{\mathbb{R}^n}\rho\left(\sum_{i=1}^{m}\frac{d_{i1}}{q}x_i,\ldots,\sum_{i=1}^{m}\frac{d_{ik}}{q}x_i\right)dx_1\ldots dx_m.$$

Here the first sum is over all partitions $(\nu,\mu) = (\nu_1,\ldots,\nu_m;\mu_1,\ldots,\mu_{k-m})$ of the numbers $1\ldots k$ into two sequences $1 \leq \nu_1 < \ldots < \nu_m \leq k$ and $1 \leq \mu_1 < \ldots < \mu_{k-m} \leq k$ with $1 \leq m \leq k-1$; of course $\nu_i \neq \mu_j$ for any i,j. The third sum is taken over all integral $m \times k$ matrices D, such that i) no column of D vanishes ii) the greatest common divisor of all entries is 1 iii) for all i,j, D satisfies $d_{i\nu_j} = q\delta_{ij}$ and $d_{i\mu_j} = 0$ if $\mu_j < \nu_i$. Finally, $e_i = (\varepsilon_i, q)$, where $\varepsilon_1,\ldots,\varepsilon_m$ are the elementary divisors of D.

Furthermore, (2) equals

$$\int_{\mathbb{R}^n}\cdots\int_{\mathbb{R}^n}\rho(x_1,\ldots,x_k)dx_1\ldots dx_k.$$

We will apply this theorem to the following situation. For $S \subseteq \mathbb{R}^n$ a Borel measurable set symmetric at the origin, define S' to be the set of elements $x \in S$ whose first nonzero coordinate is positive. In particular, S' does not contain the origin, and every nonzero pair $\{x, -x\}$ in S has only one element in S'. Clearly the mass of S' is half the mass of S. Let $\chi_{S'}$ be the characteristic function of S', and let

$$\rho_{S',h}(x_1, \dots, x_h) = \begin{cases} \prod_{i=1}^h \chi_{S'}(x_i) & \text{if } x_i \text{ are pairwise distinct} \\ 0 & \text{otherwise.} \end{cases}$$

Also define, for a lattice L,

$$\begin{aligned} \rho_{S',h}(L) &= (\text{the number of subsets of } L \cap S' \text{ of cardinality } h) \\ &= \frac{1}{h!} \sum_{x_1, \dots, x_h \in L \setminus \{0\}} \rho_{S',h}(x_1, \dots, x_h). \end{aligned}$$

We will be interested in estimating

$$\int_{X_n} \rho_{S',h}(L) d\mu_n. \tag{3}$$

Proposition 1. *Let V be the Euclidean volume of S. For $n \geq [h^2/4] + 3$, the integral (3) satisfies*

$$\begin{aligned} \frac{1}{h!} \left(\frac{V}{2}\right)^h &\leq \int_{X_n} \rho_{S',h}(L) d\mu_n \\ &\leq \frac{1}{h!} \left(\frac{V}{2}\right)^h + \frac{1}{h!} \left(2 \cdot 3^{[h^2/4]} (\sqrt{3}/2)^n + 21 \cdot 5^{[h^2/4]} (1/2)^n\right) \left(\frac{V}{2} + 1\right)^h. \end{aligned}$$

Proof. This is proved by applying Theorem 6 to $\rho_{S',h}$ and evaluating the following terms separately:

- The first integral $\int \dots \int \rho_{S',h}(x_1, \dots, x_h) dx_1 \dots dx_h$: This is clearly equal to $(V/2)^h$.
- Summations over $q = 1$ and D, whose entries are only $0, 1, -1$, and for each column of D exactly one of the entries is nonzero: In this case $x_l = \sum_{i=1}^m \frac{d_{i\nu_l}}{q} x_i = \pm \sum_{i=1}^m \frac{d_{i,\nu_l+l'}}{q} x_i = \pm x_l$ for some l and l'. If the sign in question is positive, the integral in the summation is zero because the ν_lth and $(\nu_l + l')$th entries coincide. If it is negative, the integral is still zero because either the ν_lth or $(\nu_l + l')$th entry is not in S'.
- Summations over $q = 1$ and D, whose entries are only $0, 1, -1$, and there exists a column of D in which at least two of the entries are nonzero: This is analyzed in [3], Section 4, and corresponds to the second term in the right-hand side of the above estimate.
- Summations over all the rest: This is analyzed in [1], Section 9, and corresponds to the last term above. This is where the condition that $n \geq [h^2/4] + 3$ is needed; Rogers had to use this assumption in order to show that the summation in question converges. It would be nice to improve this estimate, but I was unable to find a way to do so.

□

3. A formula for $F_{S,k}(L)$

We continue with the notation of the previous sections. Recall that we defined $F_{S,k}(L)$ so that it equals 1 if L has at least k vectors in S', and equals 0 otherwise. The goal of this section is to prove

Proposition 2.

$$F_{S,k}(L) = \sum_{h=k}^{\infty} (-1)^{h-k} \binom{h-1}{k-1} \rho_{S',h}(L). \tag{4}$$

Lemma 1. [3] *Let T be a finite set. For $R \subseteq S \subseteq T$, define*

$$\mu_S(R) = (-1)^{|S \setminus R|}.$$

Then for any positive integer k

$$\sum_{\substack{S \subseteq T \\ |S| \geq k}} \sum_{\substack{R \subseteq S \\ |R| \geq k}} \mu_S(R) = \begin{cases} 1 & \textit{if } |T| \geq k \\ 0 & \textit{otherwise.} \end{cases}$$

Remark. $\mu_S(R)$ as defined above is the Möbius function on the lattice (as an order) consisting of the subsets of T ordered by inclusion.

Proof.

$$\sum_{\substack{S \subseteq T \\ |S| \geq k}} \sum_{\substack{R \subseteq S \\ |R| \geq k}} \mu_S(R) = \sum_{\substack{R \subseteq T \\ |R| \geq k}} \sum_{\substack{S \subseteq T \\ R \subseteq S}} \mu_S(R) = \begin{cases} 1 & \text{if } |T| \geq k \\ 0 & \text{otherwise,} \end{cases}$$

because

$$\sum_{\substack{S \subseteq T \\ R \subseteq S}} \mu_S(R) = \begin{cases} 1 & \text{if } R = T \\ 0 & \text{if } R \neq T. \end{cases}$$

□

Proof of Proposition 2. Let $T = L \cap S'$.

$$\begin{aligned} \sum_{\substack{S \subseteq T \\ |S| \geq k}} \sum_{\substack{R \subseteq S \\ |R| \geq k}} \mu_S(R) &= \sum_{\substack{S \subseteq T \\ |S| \geq k}} \sum_{h=k}^{|T|} (-1)^{|S|-h} \binom{|S|}{h} \\ &= \sum_{\substack{S \subseteq T \\ |S| \geq k}} (-1)^{|S|-k} \binom{|S|-1}{k-1} \\ &= \sum_{h=k}^{\infty} (-1)^{h-k} \binom{h-1}{k-1} \binom{|T|}{h} \\ &= \sum_{h=k}^{\infty} (-1)^{h-k} \binom{h-1}{k-1} \rho_{S',h}(L). \end{aligned}$$

By Lemma 1 this completes the proof. □

4. Estimates

We are now ready to prove Theorem 5. Briefly speaking, the strategy is to first show that, for $\alpha \leq \sqrt{n/2}$, the integral of the partial sum of (4) over $h \leq \alpha$ converges to the intended main term, and then show that the remaining "tail" is either positive or negative depending on the parity of $\alpha - k$. We start by estimating the main term of $\int F_{S,k} d\mu_n$.

[3] This lemma is likely not a new observation, but we were unable to find a reference, so we provide a proof.

Proposition 3. *Let $k \le \alpha \le \sqrt{n/2}$. Then*

$$\left| \int \sum_{h=k}^{\alpha} (-1)^{h-k} \binom{h-1}{k-1} \rho_{S',h}(L) d\mu_n - \sum_{h=k}^{\alpha} (-1)^{h-k} \frac{(V/2)^h}{h(h-k)!(k-1)!} \right| \le e(n,k,V),$$

where the error term $e(n,k,V)$ has a bound

$$0 \le e(n,k,V) \le \frac{23}{k!} \sqrt{n/2} (0.999)^n (V/2+1)^{\sqrt{n/2}}.$$

Proof. By Proposition 1,

$$0 \le \int \rho_{S',h}(L) d\mu_n - \frac{1}{h!} \left(\frac{V}{2}\right)^h \le \frac{1}{h!} \left(2 \cdot 3^{[h^2/4]} (\sqrt{3}/2)^n + 21 \cdot 5^{[h^2/4]} (1/2)^n \right) \left(\frac{V}{2}+1\right)^h.$$

For $h \le \sqrt{n/2}$,

$$5^{[h^2/4]}(1/2)^n \le 3^{[h^2/4]}(\sqrt{3}/2)^n \le 3^{n/8}(\sqrt{3}/2)^n = (3^{5/8}/2)^n \le (0.994)^n$$

holds, so

$$0 \le \int \rho_{S',h}(L) d\mu_n - \frac{1}{h!} \left(\frac{V}{2}\right)^h \le (23/h!)(0.999)^n (V/2+1)^{\sqrt{n/2}}.$$

The proposition now follows easily from this inequality, by summing it up with alternating signs as h runs from k to α. □

It remains to estimate the "tail":

Proposition 4. *Let $k \le \alpha, \beta \le \sqrt{n/2}$, so that $\alpha - k$ is even and $\beta - k$ is odd. Then*

$$\int \sum_{h=\alpha+1}^{\infty} (-1)^{h-k} \binom{h-1}{k-1} \rho_{S',h}(L) d\mu_n \le 0 \tag{5}$$

and

$$\int \sum_{h=\beta+1}^{\infty} (-1)^{h-k} \binom{h-1}{k-1} \rho_{S',h}(L) d\mu_n \ge 0. \tag{6}$$

Proof. Let's prove (5) first. It suffices to show that for any lattice L with $|L \cap S'| > \alpha$,

$$\sum_{h=\alpha+1}^{\infty} (-1)^{h-k} \binom{h-1}{k-1} \rho_{S',h}(L) \le 0.$$

Write $M = |L \cap S'|$. Then the left-hand side equals

$$\begin{aligned} &\sum_{h=\alpha+1}^{M} (-1)^{h-k} \binom{h-1}{k-1} \binom{M}{h} \\ &= \sum_{h=\alpha+1}^{M} (-1)^{h-k} \frac{h-k+1}{h} \binom{h}{k-1} \binom{M}{h} \\ &= \sum_{h=\alpha+1}^{M} (-1)^{h-k} \frac{h-k+1}{h} \binom{M}{k-1} \binom{M-k+1}{h-k+1}. \end{aligned}$$

For convenience, let's denote the summand of the above series by A_h.

Case $M \ge 2\alpha - k$: In this case it is clear that $|A_h|$ is increasing for $h = k, \dots, \alpha$. Since $A_k > 0$ clearly, and $\alpha - k$ is even by assumption, $A_\alpha > 0$, so $A_\alpha + A_{\alpha-1} > 0$,

$A_{\alpha-2}+A_{\alpha-3}>0$, and so on. Since A_h's are all integers, this implies $\sum_{h=k}^{\alpha} A_h \geq 1$. Since $\sum_{h=k}^{M} A_h = 1$ by Proposition 2, this implies (5).

Case $\alpha+1 \leq M \leq 2\alpha-k-1$: In this case we want to show that $A_{\alpha+1}+A_{\alpha+2}<0$, $A_{\alpha+3}+A_{\alpha+4}<0$, and so on (if $M-\alpha$ is odd, then we also need $A_M<0$, but this is obvious). This is equivalent to showing

$$\frac{|A_{h+1}|}{|A_h|} = \frac{h}{h+1}\cdot\frac{h-k+2}{h-k+1}\cdot\frac{M-h}{h-k+2} = \frac{h}{h+1}\cdot\frac{M-h}{h-k+1} < 1$$

for $\alpha+1 \leq h \leq M$. $(M-h)/(h-k+1)$ is the largest when M is the largest and h is the smallest possible, namely when $M=2\alpha-k-1$ and $h=\alpha+1$. But even in this case $(M-h)/(h-k+1) = (\alpha-k-2)/(\alpha-k+2) < 1$, hence the desired conclusion.

The proof of (6) is more or less the same argument. It suffices to show that for any lattice L with $|L\cap S'|>\beta$,

$$\sum_{h=\beta+1}^{\infty} (-1)^{h-k}\binom{h-1}{k-1}\rho_{S',h}(L) \geq 0.$$

By the same argument as earlier we see that this equals

$$\sum_{h=\beta+1}^{M} (-1)^{h-k}\frac{h-k+1}{h}\binom{M}{k-1}\binom{M-k+1}{h-k+1}$$

whose summand we again denote by A_h.

Case $M \geq 2\beta-k$: Since $|A_h|$ is increasing for $h=k,\dots,\beta$ and $\beta-k$ is odd, $A_\beta+A_{\beta-1}<0$, $A_{\beta-2}+A_{\beta-3}<0$, and so on. By the same logic as earlier (6) follows.

Case $\beta+1 \leq M \leq 2\beta-k-1$: In this case we want to show that $A_{\beta+1}+A_{\beta+2}>0$, $A_{\beta+3}+A_{\beta+4}>0$, and so on. This follows from $|A_{h+1}|/|A_h|<1$ for $\beta+1\leq h\leq M$, which we have shown already. □

Theorem 5 now follows trivially from Propositions 3 and 4.

5. A proof of Theorem 4

From Theorem 5, and the relation $P(S,k) = 1-\int F_{S,k+1}(L)d\mu_n$, it follows that

$$1+\sum_{h=k+1}^{\alpha}\frac{(-1)^{h-k}}{h!}\binom{h-1}{k}(V/2)^h - e(n,k+1,V) \leq P(S,k)$$

$$\leq 1+\sum_{h=k+1}^{\beta}\frac{(-1)^{h-k}}{h!}\binom{h-1}{k}(V/2)^h + e(n,k+1,V)$$

for appropriate α,β, so it suffices to show that the expression

$$1+\sum_{h=k+1}^{\alpha}\frac{(-1)^{h-k}}{h!}\binom{h-1}{k}(V/2)^h$$

is close to $P_{V/2}(k)$ given the constraints in the statement of Theorem 4. In fact, by introducing the notation

$$e_\alpha(x) = \sum_{i=0}^{\alpha}\frac{x^i}{i!},$$

and writing $\lambda = V/2$, we can write

$$1 + \sum_{h=k+1}^{\alpha} \frac{(-1)^{h-k}}{h!} \binom{h-1}{k} (V/2)^h = \sum_{j=0}^{k} e_{\alpha-j}(-\lambda) \frac{\lambda^j}{j!}.$$

On the other hand, it is a standard fact that

$$P_\lambda(k) = e^{-\lambda} \sum_{j=0}^{k} \frac{\lambda^j}{j!}.$$

Therefore it is enough to ensure that $|e^{-\lambda} - e_{\alpha-j}(-\lambda)|$ is small for all $j = 0, \dots, k$. Writing $m = \alpha - j + 1$, and using Taylor's theorem and Stirling's approximation,

$$|e^{-\lambda} - e_{\alpha-j}(-\lambda)| \leq \frac{\lambda^{\alpha-j+1}}{(\alpha-j+1)!} \leq \frac{1}{\sqrt{m}} \left(\frac{\lambda e}{m}\right)^m.$$

It can be checked, by taking the log of the above line, that for $m \geq 16\lambda$ (the choice of 16 here is not optimal) we have,

$$\left(\frac{\lambda e}{m}\right)^m < e^{-\lambda}$$

so that

$$|e^{-\lambda} - e_{\alpha-j}(-\lambda)| < \frac{1}{\sqrt{m}} e^{-\lambda}. \tag{7}$$

Now take $\alpha = \lfloor \sqrt{n/2} \rfloor$ or $\lfloor \sqrt{n/2} \rfloor - 1$, so that $\alpha - k$ is even. Then, whenever $\sqrt{n/2} - k \geq 8V$, (7) holds for all $j = 0, \dots, k$. Choosing $k \leq \sqrt{n/2}^{1-\varepsilon}$ ensures that the right side of (7) is small compared to $e^{-\lambda}$. This completes the proof of Theorem 4.

References

[1] C.A. Rogers, The moments of the number of points of a lattice in a bounded set. Phil. Trans. R. Soc. London. A 248 (1955), 225-251.

[2] C.A. Rogers, Mean values over the space of lattices. Acta Math. 94 (1955), 249-287.

[3] C.A. Rogers, The number of lattice points in a set. Proc. Lond. Math. Soc. 6(3) (1956), 305-320.

[4] W. Schmidt, The measure of the set of admissable lattices. Proc. Amer. Math. Soc. 9 (1958), 390-403.

[5] W. Schmidt, Masstheorie in der Geometrie der Zahlen. Acta Math. 102 1959 159-224.

[6] C.L. Siegel, A mean value theorem in geometry of numbers. Ann. of Math. 46(2) (1945), 340-347.

[7] A. Södergren, On the Poisson distribution of lengths of lattice vectors in a random lattice. Math. Z. 269 (2011), 945-954.

[8] A. Södergren, On the distribution of angles between the N shortest vectors in a random lattice. J. London Math. Soc. (2) 84 (2011), 749-764.