

Local Statistics of Lattice Points on the Sphere

Jean Bourgain, Peter Sarnak, and Zeév Rudnick

ABSTRACT. A celebrated result of Legendre and Gauss determines which integers can be represented as a sum of three squares, and for those it is typically the case that there are many ways of doing so. These different representations give collections of points on the unit sphere, and a fundamental result, conjectured by Linnik, is that under a simple condition these become uniformly distributed on the sphere. In this note we survey some of our recent work, which explores what happens beyond uniform distribution, giving evidence to randomness on smaller scales. We treat the electrostatic energy, local statistics such as the point pair statistic (Ripley's function), nearest neighbour statistics, minimum spacing and covering radius. We briefly discuss the situation in other dimensions, which is very different. In an appendix we compute the corresponding quantities for random points.

1. Statement of results

The set of integer solutions (x_1, x_2, x_3) to the equation

$$(1.1) \quad x_1^2 + x_2^2 + x_3^2 = n$$

has been much studied. However it appears that the spatial distribution of these solutions at small and critical scales as $n \rightarrow \infty$ have not been addressed. The main results announced below give strong evidence to the thesis that the solutions behave randomly. This is in sharp contrast to what happens with sums of two or four or more squares.

First we clarify what we mean by random. For a homogeneous space like the k -dimensional sphere S^k with its rotation-invariant probability measure $\hat{\sigma}$, the binomial process is what you get by placing N points P_1, \dots, P_N on S^k independently according to $\hat{\sigma}$. We are interested in statistics, that is functions $f(P_1, \dots, P_N)$, which have a given behaviour almost surely, as $N \rightarrow \infty$. If this happens we say that this behaviour of f is that of random points. We shall also contrast features of random points sets with those of "rigid" configurations, by which we mean points on a planar lattice, such as the honeycomb lattice.

2010 *Mathematics Subject Classification*. Primary 11K36; Secondary 11E12, 11E25.

The first author was supported in part by NSF grants DMS-1301619 and DMS 0835373.

The second author was partially supported by NSF grants DMS-0758299 and DMS 1302952.

The third author has received funding from the European Research Council under the European Union's Seventh Framework Programme (FP7/2007-2013) / ERC grant agreement n° 320755, and from the Israel Science Foundation (grant No. 1083/10).

A celebrated result of Legendre/Gauss asserts that n is a sum of three squares if and only if $n \neq 4^a(8b+7)$. Let $\mathcal{E}(n)$ be the set of solutions

$$(1.2) \quad \mathcal{E}(n) = \{\mathbf{x} \in \mathbb{Z}^3 : |\mathbf{x}|^2 = n\}$$

and set

$$(1.3) \quad N = N_n := \#\mathcal{E}(n).$$

The behaviour of N_n is very subtle and it was a fine achievement in the 1930's when it was shown that N_n goes to infinity with n (assuming say that n is square-free; if $n = 4^a$ then there are only six solutions). It is known that $N_n \ll n^{1/2+o(1)}$ and if there are *primitive* lattice points, that is $\mathbf{x} = (x_1, x_2, x_3)$ with $\gcd(x_1, x_2, x_3) = 1$ (which happens if and only if $n \not\equiv 0, 4, 7 \pmod{8}$) then there is a lower bound of $N_n \gg n^{1/2-o(1)}$. This lower bound is ineffective and indicates that the behaviour of N_n is still far from being understood [18].

The starting point of our investigation is the fundamental result conjectured by Linnik (and proved by him assuming the Generalized Riemann Hypothesis), that for $n \not\equiv 0, 4, 7 \pmod{8}$, the points

$$(1.4) \quad \widehat{\mathcal{E}}(n) := \frac{1}{\sqrt{n}}\mathcal{E}(n) \subset S^2$$

obtained by projecting to the unit sphere, become equidistributed on the unit sphere with respect to $\widehat{\sigma}$ as $n \rightarrow \infty$. This was proved unconditionally by Duke [5, 6] and Golubeva and Fomenko [9], following a breakthrough by Iwaniec [12]. Random points are equidistributed by definition and the above result says that on this crudest global scale the projected lattice points $\widehat{\mathcal{E}}(n)$ behave like random points. Figure 1 gives some visual support for random behaviour of $\widehat{\mathcal{E}}(n)$.

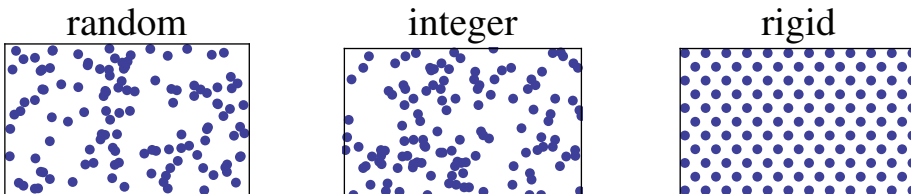


FIGURE 1. Lattice points coming from the prime $n = 1299709$ (center), versus random points (left) and rigid points (right). The plot displays an area containing about 120 points.

To make this precise we examine various statistics associated with the placement of points in S^2 . Our choice of these statistics is based on robustness tests for the random hypothesis, as well as quantities which are of interest in number theoretical and harmonic analysis applications. Our philosophy in what follows is that the behaviour of a quantity in question is easy to determine for random points (see Appendix A) while for $\widehat{\mathcal{E}}(n)$ we settle for estimates for them and also formulate conjectures, which are more precise. That one has to settle for such information for this kind of problem is to be expected given the problematic non-random behaviour of the number N_n itself. The proofs of our assertions on $\widehat{\mathcal{E}}(n)$ will appear in [2].

1.1. Electrostatic energy. The electrostatic energy of N points P_1, \dots, P_N on S^2 is given by

$$(1.5) \quad E(P_1, \dots, P_N) := \sum_{i \neq j} \frac{1}{|P_i - P_j|}.$$

Here and in the sequel, $|x - y|$ is the Euclidean distance in \mathbb{R}^3 . This energy E depends on both the global distribution of the points as well as a moderate penalty for putting the points too close to each other. The minimum energy configuration is known to satisfy [1, 22, 23]

$$(1.6) \quad N^2 - \beta N^{3/2} \leq \min_{P_1, \dots, P_N} E(P_1, \dots, P_N) \leq N^2 - \alpha N^{3/2}$$

for some $0 < \alpha \leq \beta < \infty$. The configurations which achieve this are rigid in various senses [4] and we will see below in Corollary 1.5 that our points $\widehat{\mathcal{E}}(n)$ are far from being rigid. For random points one has¹ that $E \sim N^2$ but the difference $E - N(N - 1)$ from the expected value has no definite sign. Our first result is that to leading order the points $\widehat{\mathcal{E}}(n)$ have the same energy as random or minimal energy configurations.

THEOREM 1.1. *There is some $\delta > 0$ so that*

$$(1.7) \quad E(\widehat{\mathcal{E}}(n)) = N^2 + O(N^{2-\delta})$$

as $n \rightarrow \infty$, $n \neq 0, 4, 7 \pmod 8$.

We have not been able to say anything about the sign of $E(\widehat{\mathcal{E}}(n)) - N(N - 1)$ which according to Table 1 appears to vary.

N	$E - N(N - 1)$	
	integer	random
1224	-282.	95.
3072	37732.	-4704.
4296	8380.	1747.

TABLE 1. The difference $E - N(N - 1)$ between the electrostatic energy and its expected value, for various values of N . In the column labeled “integer”, the energy for $\widehat{\mathcal{E}}(n)$ was computed for the primes $n = 104773, 104761$ and 1299763 with N_n listed in the left-most column. In the random case the result is a mean value of 20 runs.

¹Here and elsewhere, \sim is the usual asymptotic symbol denoting convergence to one of the ratio of the two sides.

1.2. Point pair statistics. The point pair statistic and its variants are at the heart of our investigation. It is a robust statistic as far as testing the randomness hypothesis and it is called Ripley’s function in the statistics literature [19]. For $P_1, \dots, P_N \in S^2$ and $0 < r < 2$, set

$$(1.8) \quad \widehat{K}_r(P_1, \dots, P_N) := \sum_{\substack{i \neq j \\ |P_i - P_j| < r}} 1$$

to be the number of ordered pairs of distinct points at (Euclidean) distance at most r apart. Note that we will allow r to vary with N so as to test randomness at different scales.

For fixed $\epsilon > 0$, uniformly for $N^{-1+\epsilon} \leq r \leq 2$, one has that for N random points chosen with respect to the binomial process

$$(1.9) \quad \widehat{K}_r(P_1, \dots, P_N) \sim \frac{1}{4}N(N-1)r^2 .$$

Based on the results below as well as some numerical experimentation, we conjecture that for n square-free the points $\widehat{\mathcal{E}}(n)$ behave randomly w.r.t. Ripley’s statistic at scales $N_n^{-1+\epsilon} \leq r \leq 2$; that is

$$(1.10) \quad \widehat{K}_r(\widehat{\mathcal{E}}(n)) \sim \frac{N^2 r^2}{4}, \quad \text{as } n \rightarrow \infty .$$

One of our main results is the following which shows that (1.10) is true at least in terms of an upper bound which is off only by a multiplicative constant.

THEOREM 1.2. *Assume the Generalized Riemann Hypothesis (GRH). Then for fixed $\epsilon > 0$ and $N^{-1+\epsilon} \leq r \leq 2$,*

$$\widehat{K}_r(\widehat{\mathcal{E}}(n)) \ll_{\epsilon} N^2 r^2$$

where the implied constant depends only on ϵ .

Remark: We do not need the full force of GRH here, but rather that there are no “Siegel zeros”.

We have not succeeded in giving individual lower bounds for $\widehat{K}_r(\widehat{\mathcal{E}}(n))$. What we can show is that at the smallest scale, that is r of order $N_n^{-1+o(1)} \approx n^{-1/2+o(1)}$, (1.10) holds for most n ’s:

THEOREM 1.3. *There is some $\delta_0 > 0$ such that for fixed $0 < \delta < \delta_0$ and $r = n^{\delta - \frac{1}{2}}$,*

$$\widehat{K}_r(\widehat{\mathcal{E}}(n)) \sim \frac{N^2 r^2}{4}$$

for almost all n .

The constant δ_0 can be determined explicitly, and is limited in our analysis by h having to be small in (2.1) below .

1.3. Nearest neighbour statistics. Closely connected to \widehat{K} is the distribution of nearest neighbour distances d_j , i. e. the distance from P_j to the remaining points. It is more convenient to work with these squares of the distances. Area considerations show that $\sum_j d_j^2 \leq 16$. For random points, the mean of d_j^2 is $4/N$. In order to space these numbers at a scale for which they have a limiting distribution in the random case, we rescale them by their mean for the random case, i.e.

replace d_j^2 by $\frac{N}{4}d_j^2$. Thus for $P_1, \dots, P_N \in S^2$ define the nearest neighbour spacing measure $\mu(P_1, \dots, P_N)$ on $[0, \infty)$ by

$$(1.11) \quad \mu(P_1, \dots, P_N) := \frac{1}{N} \sum_{j=1}^N \delta_{\frac{N}{4}d_j^2}$$

where δ_ξ is a delta mass at $\xi \in \mathbb{R}$. Note that the mean of μ is at most 1 and that for random points we have

$$(1.12) \quad \mu(P_1, \dots, P_N) \rightarrow e^{-x}dx, \quad \text{as } N \rightarrow \infty .$$

Based on this and numerical experiments (see figure 2) we conjecture:

CONJECTURE 1.4. *As $n \rightarrow \infty$ along square-free integers, $n \not\equiv 7 \pmod 8$,*

$$(1.13) \quad \mu(\widehat{\mathcal{E}}(n)) \rightarrow e^{-x}dx .$$

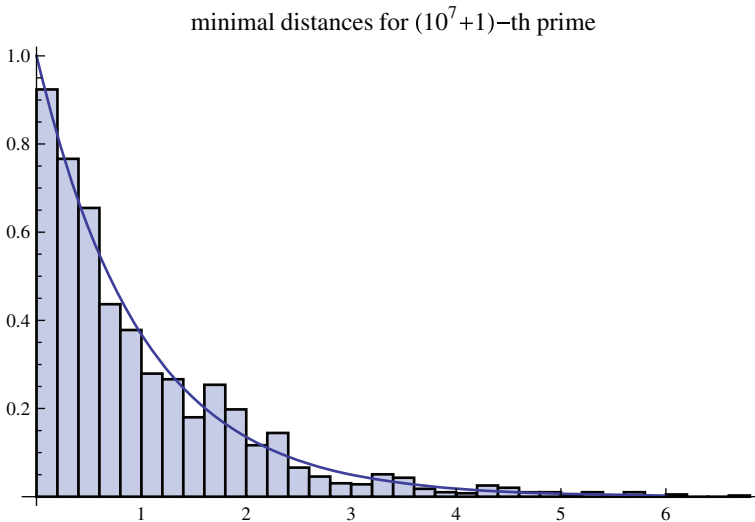


FIGURE 2. A histogram of the scaled minimal spacing between lattice points for for $n = 179424691$, the 10,000,001-th prime, where $N_n = 94536$, and modulo symmetries there are 1970 points. The smooth curve is the exponential distribution e^{-s} .

As a Corollary to Theorem 1.2 we have

COROLLARY 1.5. *Assume GRH. If ν is a weak limit of the $\mu(\widehat{\mathcal{E}}(n))$ then ν is absolutely continuous, in fact there is an absolute constant $c_4 > 0$ such that*

$$(1.14) \quad \nu \leq c_4 dx .$$

Corollary 1.5 implies that the $\widehat{\mathcal{E}}(n)$'s are not rigid for large n since for rigid configurations, $\mu_{P_1, \dots, P_N} \rightarrow \delta_{\pi/\sqrt{12}}$. Also in as much as it ensures that such a ν cannot charge $\{0\}$ positively, it follows that almost all the points of $\widehat{\mathcal{E}}(n)$ are essentially separated with balls of radius approximately $N^{-1/2}$ from the rest. Precisely, given a sequence η_N satisfying $\eta_N = o(N^{-1/2})$, all but $o(N)$ of the N points in $\widehat{\mathcal{E}}(n)$ have the ball of radius η_N about them free of any other points.

1.4. Minimum spacing and covering radius. Given $P_1, \dots, P_N \in S^2$ define the minimum spacing to be

$$(1.15) \quad m(P_1, \dots, P_N) := \min_{i \neq j} d_{i,j} = \min_j d_j .$$

This statistic is very sensitive to the placement of points and it is of arithmetic interest for $\widehat{\mathcal{E}}(n)$. From the area packing bound we have that

$$(1.16) \quad m(P_1, \dots, P_N) \leq 4/\sqrt{N}$$

for any configuration. In fact the rigid configuration of Figure 1 (coming from a planar lattice) maximizes m asymptotically

$$(1.17) \quad \max_{P_1, \dots, P_N} m(P_1, \dots, P_N) \sim \frac{2}{\sqrt{N}} \cdot 2\sqrt{\frac{\pi}{\sqrt{12}}} .$$

For random points the behaviour of the minimal spacing m is very different

$$(1.18) \quad m(P_1, \dots, P_N) = N^{-1+o(1)} .$$

Based on the random point model as well as number theoretic considerations which involve a nonlinear and shifted variation of Vinogradov’s least quadratic residue conjecture [21], we pose

CONJECTURE 1.6. $m(\widehat{\mathcal{E}}(n)) = N^{-1+o(1)}$ as $n \rightarrow \infty$.

The lower bound in Conjecture 1.6 is an immediate consequence of the integrality of the points in $\widehat{\mathcal{E}}(n)$ since that implies that for the projected points $P_i \neq P_j \in \widehat{\mathcal{E}}(n)$, we have $|P_i - P_j| \geq 1/\sqrt{n}$ and since $N \geq n^{1/2+o(1)}$ the lower bound follows. It is the upper bound that appears difficult even assuming GRH.

As with the previous statistics we can establish the conjecture for almost all n . Indeed it follows from Theorem 1.3 that

COROLLARY 1.7. *Given $\epsilon > 0$, $m(\widehat{\mathcal{E}}(n)) \ll_\epsilon N^{-1+\epsilon}$ for almost all n .*

Note that Conjecture 1.6 would follow from the stronger conjecture of Linnik [14], that for $\epsilon > 0$ and n odd and square-free (and $n \neq 7 \pmod{8}$) there are x_1, x_2, x_3 with $|x_3| \leq n^\epsilon$ and $x_1^2 + x_2^2 + x_3^2 = n$, as such a representation provides a pair of points $(x_1, x_2, \pm x_3)/\sqrt{n} \in \widehat{\mathcal{E}}(n)$ at distance $\leq n^{-1/2+o(1)} \ll N^{-1+\epsilon}$ from each other.

Finally we examine the covering radius for $\widehat{\mathcal{E}}(n)$ though there is little of substance that we can prove. Given $P_1, \dots, P_N \in S^2$, the covering radius $M(P_1, \dots, P_N)$ is the least $r > 0$ so that every point of S^2 is within distance at most r of some P_j . Again an area covering argument shows that for any configuration $M(P_1, \dots, P_N) \geq \frac{4}{\sqrt{N}}$.

As a statistic, the covering radius M is much more forgiving than the minimal spacing m in that the placement of a few bad points does not affect M drastically. In particular for random points, $M \leq N^{-1/2+o(1)}$.

Based on this we conjecture the following, though admittedly with much less evidence than the previous conjectures.

CONJECTURE 1.8. $M(\widehat{\mathcal{E}}(n)) = N^{-1/2+o(1)}$ as $n \rightarrow \infty$.

An effective version of the equidistribution of $\widehat{\mathcal{E}}(n)$ given in [6, 9], which is needed in the proof of Theorem 1.1, yields an $\alpha > 0$ such that $M(\widehat{\mathcal{E}}(n)) \ll N^{-\alpha}$.

1.5. Higher dimensions. The distribution of the solutions to

$$(1.19) \quad x_1^2 + x_2^2 + \dots + x_t^2 = n$$

for $t \neq 3$ is very different and certainly non-random. Firstly for $t = 2$ and say n a prime, $n = 1 \pmod 4$, there are exactly eight solutions to (1.19). So there is little to say about the distribution for individual such n 's. However for "generic" n 's which are sums of two squares, the projections of the solutions to the unit circle are uniformly distributed [8, 13], and for such n 's the local statistical questions certainly make sense.

For $t \geq 4$, the projections onto the unit sphere of the solutions to (1.19) can be examined using the same techniques that we use for $t = 3$, with the main differences being that the analysis is easier and the local behaviour is no longer random. We only discuss the last feature and since it is only enhanced with increasing t , we stick to $t = 4$. Let $\mathcal{E}_4(n)$ be the set of solutions to (1.19) and let $\widehat{\mathcal{E}}_4(n)$ be the projection of this set to S^3 , the unit sphere in \mathbb{R}^4 . The first difference from $t = 3$ is that $N_n^{(4)} := \#\widehat{\mathcal{E}}_4(n)$ is a regularly behaved function of n . When divided by 8 it is multiplicative and for $n = p$ an odd prime $\#\widehat{\mathcal{E}}_4(p) = 8(p + 1)$. Thus the number of points $N = N_n^{(4)}$ being placed on S^3 satisfies

$$(1.20) \quad N = n^{1+o(1)}$$

at least for odd n . For N random points on S^3 the two point function \widehat{K}_r defined as in (1.8) satisfies that for $\epsilon > 0$ and $N^{-2/3+\epsilon} \leq r \leq 2$

$$(1.21) \quad \widehat{K}_r(P_1, \dots, P_N) \sim N(N - 1)V(r)$$

where $V(r)$ is the relative volume of a cap $\{x \in S^3 : |x - x_0| < r\}$; for small r , $V(r) \sim \frac{2}{3\pi}r^3$.

On the other hand for $\widehat{\mathcal{E}}_4(n)$, the integrality of the corresponding points in $\mathcal{E}_4(n)$, implies that for $x \neq y$, $|x - y| \geq 1/\sqrt{n}$ and hence for $x \neq y \in \widehat{\mathcal{E}}_4(n)$

$$(1.22) \quad |x - y| \geq N^{-1/2+o(1)} .$$

In particular for $r \leq N^{-1/2-\epsilon}$,

$$(1.23) \quad \widehat{K}_r(\widehat{\mathcal{E}}_4(n)) = 0 .$$

Thus at the scales $N^{-2/3+\epsilon} \leq r \leq N^{-1/2-\epsilon}$, the point pair function for $\widehat{\mathcal{E}}_4(n)$ and that for random points are very different.

This difference is also reflected in the minimum spacing function $m(\widehat{\mathcal{E}}_4(n))$ for N points on S^3 . From (1.22) we have the lower bound $m(\widehat{\mathcal{E}}_4(n)) \geq N^{-1/2+o(1)}$ and on the other hand there is a similar upper bound, namely

PROPOSITION 1.9.

$$(1.24) \quad m(\widehat{\mathcal{E}}_4(n)) = N^{-1/2+o(1)} .$$

This is in sharp contrast to random points on S^3 for which

$$(1.25) \quad m(P_1, \dots, P_N) = N^{-2/3+o(1)} .$$

Thus the points $\widehat{\mathcal{E}}_4(n)$ are much more rigid than random points but they are far from being fully rigid as the latter satisfy (locally these points are placed at the

vertices of the face centered cubic lattice **[3]**):

$$(1.26) \quad \max_{P_1, \dots, P_N} m_4(P_1, \dots, P_N) \sim \frac{2}{N^{1/3}} c, \quad c = \frac{\pi^{2/3}}{\sqrt{2}}.$$

The nonrandom behaviour of the points $\widehat{\mathcal{E}}_4(n)$ manifests itself at a much larger scale as well, as is demonstrated by the minimum covering radius $M_4(P_1, \dots, P_N)$. While being very nonrigid, random points cover S^3 quite well. For them we have

$$(1.27) \quad M_4(P_1, \dots, P_N) = N^{-1/3+o(1)}.$$

Somewhat surprisingly the points $\widehat{\mathcal{E}}_4(n)$ which are more rigid than random points, are poorly distributed in terms of covering. This phenomenon of what might be called “big holes” was first observed in the context of approximations of 2×2 real matrices by certain rational ones, by Harman **[10]**. For $\widehat{\mathcal{E}}_4(n)$ we have

PROPOSITION 1.10.

$$(1.28) \quad M(\widehat{\mathcal{E}}_4(n)) \geq N^{-1/4+o(1)}.$$

2. Outline of the proofs

For n squarefree the general mass formula of Minkowski and Siegel, which in the following special case is due to Gauss, expresses N_n in terms of $L(1, \chi_{d_n})$ where χ_{d_n} is the quadratic character associated to the field $\mathbb{Q}(\sqrt{-n})$ of discriminant d_n . From this and Siegel’s lower bound on $L(1, \chi_d)$ it follows that $N_n \gg n^{1/2-\epsilon}$ for any $\epsilon > 0$ (ineffectively). The key tool in our analysis of the local point-pair functions is the mass formula applied to the representations of the binary form $nu^2 + 2tuv + nv^2$ by the ternary form $x_1^2 + x_2^2 + x_3^2 = \langle x, x \rangle$. Since this ternary form has one class in its genus, the mass formula gives the number $A(n, t)$ of pairs $(x, y) \in \mathcal{E}(n) \times \mathcal{E}(n)$ with $\langle x, y \rangle = t$, as a product of local densities. Again this is a special case of the mass formula, for which an elementary proof as well as an explicit form was given in **[20]**, and this was a critical ingredient in Linnik’s approach to the equidistribution of $\widehat{\mathcal{E}}(n)$ (see **[7]** for a recent exposition and extension of his method). The local to global formula allows us to give rather sharp upper bounds for $A(n, t)$. These are then used to control the contributions of nearby points in the sum (1.5) in the course of proving Theorem 1.1. For pairs of points that are not too close we use modular forms and in particular Duke’s theorem. Specifically we effectivise that analysis by giving a power saving (namely $N^{-\alpha}$, for some $\alpha > 0$) upper bound for the spherical cap discrepancy of the points $\widehat{\mathcal{E}}(n)$. Putting these two together leads to Theorem 1.1.

The proof of Theorem 1.2 also uses the local formula for $A(n, t)$, this time giving upper bounds for this quantity when summed over t in short intervals. It is critical that these upper bounds are sharp up to a universal factor and depend only on the subtle function N_n and not on n . We achieve this by adapting the upper bound sieve method of Nair **[16]** to our setting. This leads to an upper bound in terms of a product of local densities of primes connected with χ_{d_n} . It is here that we need to assume that there are no Siegel zeros in order to ensure that there is no dependence on n .

The “almost all” result in Theorem 1.3 is proven by computing the asymptotic mean and variance of $\widehat{K}_r(\widehat{\mathcal{E}}(n)) - N_n^2 r^2/4$, with $n \leq R$. This is approached by

analyzing similar asymptotics for

$$(2.1) \quad K_h(\mathcal{E}(n)) = \sum_{\substack{x,y \in \mathcal{E}(n) \\ x-y=h}} 1$$

and

$$(2.2) \quad K_{h,k}(\mathcal{E}(n)) = \sum_{\substack{x,y,z,w \in \mathcal{E}(n) \\ x-y=h, \quad z-w=k}} 1,$$

($0 \neq h, k \in \mathbb{Z}^3$).

The behaviour as $R \rightarrow \infty$ of $\sum_{n \leq R} K_h(\mathcal{E}(n))$ may be determined elementarily, while that of $\sum_{h \leq R} K_{h,k}(\mathcal{E}(n))$ can be derived using Kloosterman’s circle method for quadratic forms in 4 variables (see for example [15], [11]). The leading terms are given as products of Hardy-Littlewood local densities. The behaviour of $\sum_{n \leq R} \widehat{K}_r(\mathcal{E}(n))N_n$ and $\sum_{n \leq R} N_n^2$ may be determined using the Besicovich r -almost periodic properties of N_n/\sqrt{n} [17]. We rederive this almost periodicity directly using the circle method and this allows us to compare the various local densities directly.

The proof of Proposition 1.9 is immediate from Legendre and Gauss’ Theorem. Namely $n - a^2 = x_1^2 + x_2^2 + x_3^2$ has a solution for $a = 1$ or $a = 2$ (recall n is odd). Proposition 1.10 follows by considering annuli about the north pole $(1, 0, 0, 0)$.

Appendix A. Spatial statistics

We give proofs of the statements that were made about the placement of N random points on S^k and which were used to support the thesis that our points $\mathcal{E}(n)$ on S^2 behave like random points, while in higher dimension the corresponding points are non-random.

We first prove statements (1.9) and (1.21) concerning Ripley’s function. For $P_1, \dots, P_N \in S^k$,

$$(A.1) \quad \widehat{K}_r(P_1, \dots, P_N) = \sum_{i \neq j} I_r(P_i, P_j)$$

where $0 \leq r \leq 2$ and $I_r(P_i, P_j) = 1$ if $|P_i - P_j| \leq r$ and is zero otherwise. For such r let $B(P, r)$ denote the spherical cap about P consisting of all points $Q \in S^k$ such that $|P - Q| \leq r$. Let $V(r)$ denote the $\widehat{\sigma}$ -normalized surface measure of $B(P, r)$, which is independent of P . In particular, in dimension two, $V(r) = r^2/4$, and for S^k in general $V(r)$ scales like r^k for small r .

The claim is that for $N^{-2/k+\epsilon} \leq r \leq 2$, as $N \rightarrow \infty$

$$(A.2) \quad \widehat{K}_r(P_1, \dots, P_N) \sim N(N - 1)V(r)$$

in probability, by which we mean that for each fixed $\epsilon > 0$,

$$(A.3) \quad \text{Prob} \left\{ (P_1, \dots, P_N) : \left| \frac{\widehat{K}_r}{N(N - 1)V(r)} - 1 \right| > \epsilon \right\} \rightarrow 0$$

as $N \rightarrow \infty$.

This follows in a standard way from Chebyshev’s inequality once we show that the expected value of \widehat{K}_r is

$$(A.4) \quad \mathbb{E}(\widehat{K}_r) = N(N - 1)V(r)$$

and that its variance is

$$(A.5) \quad \text{Var}(\widehat{K}_r) = 2N(N - 1)V(r)(1 - V(r)) .$$

Indeed, then

$$(A.6) \quad \mathbb{E} \left(\left(\frac{\widehat{K}_r}{\mathbb{E}(\widehat{K}_r)} - 1 \right)^2 \right) = \frac{2(1 - V(r))}{N(N - 1)V(r)}$$

which tends to zero if and only if $N(N - 1)V(r) \rightarrow \infty$. Our lower bound for r ensures that the latter holds and if we allow r to be $N^{-2/k}$ or smaller then it is clear that (A.2) is no longer valid.

To see that (A.4) and (A.5) hold note that

$$(A.7) \quad \int_{S^k} \int_{S^k} I_r(P_1, P_2) d\widehat{\sigma}(P_1) d\widehat{\sigma}(P_2) = V(r) ,$$

while

$$(A.8) \quad \int_{S^k} \int_{S^k} \int_{S^k} I_r(P_1, P_2) I_r(P_2, P_3) d\widehat{\sigma}(P_1) d\widehat{\sigma}(P_2) d\widehat{\sigma}(P_3) = V(r)^2$$

and

$$(A.9) \quad \int_{S^k} \int_{S^k} \int_{S^k} \int_{S^k} I_r(P_1, P_2) I_r(P_3, P_4) d\widehat{\sigma}(P_1) d\widehat{\sigma}(P_2) d\widehat{\sigma}(P_3) d\widehat{\sigma}(P_4) = V(r)^2 .$$

Hence

$$(A.10) \quad \mathbb{E}(\widehat{K}_r) = \sum_{i \neq j} \mathbb{E} \left(I_r(P_i, P_j) \right) = N(N - 1)V(r) ,$$

which gives (A.4), and

$$\begin{aligned} \mathbb{E}(\widehat{K}_r^2) &= \mathbb{E} \left(\left(2 \sum_{i < j} I_r(P_i, P_j) \right)^2 \right) \\ &= 4 \sum_{i_1 < j_1} \sum_{i_2 < j_2} \mathbb{E} \left(I_r(P_{i_1}, P_{j_1}) I_r(P_{i_2}, P_{j_2}) \right) \\ (A.11) \quad &= 4 \sum_{\substack{i_1=i_2 \\ j_1=j_2 \\ i_1 < j_1}} V(r) + 4 \sum_{\substack{(i_1, j_1) \neq (i_2, j_2) \\ i_1 < j_1 \\ i_2 < j_2}} V(r)^2 \\ &= 4V(r) \frac{N(N - 1)}{2} + 4V(r)^2 \left(\left(\frac{N(N - 1)}{2} \right)^2 - \frac{N(N - 1)}{2} \right) \\ &= V(r)^2 \left(N(N - 1) \right)^2 + 2N(N - 1)V(r) \left(1 - V(r) \right) , \end{aligned}$$

which immediately gives (A.5).

Next, focusing on the two-dimensional case of S^2 , we compute the expected value of the average $\frac{1}{N} \sum_{j=1}^N d_j^2$ and show that it equals

$$(A.12) \quad \mathbb{E} \left(\frac{1}{N} \sum_{j=1}^N d_j^2 \right) = \frac{4}{N} .$$

Note that d_1, \dots, d_N are not *independent*, for instance for $N = 2$ we clearly have $d_1 = d_2$. However, they do have the same distribution and hence

$$(A.13) \quad \mathbb{E}\left(\frac{1}{N} \sum_{j=1}^N d_j^2\right) = \mathbb{E}(d_1^2) = \mathbb{E}\left(\min_{j=2, \dots, N} |P_1 - P_j|^2\right).$$

Now $|P_j - P_1|^2$ (for $j = 2, \dots, N$) are i.i.d. and take values in $[0, 4]$, and for $0 \leq x \leq 4$,

$$(A.14) \quad \begin{aligned} \text{Prob}\left(\min_{j=2, \dots, N} |P_1 - P_j|^2 > x\right) &= \text{Prob}\left(|P_2 - P_1|^2 > x\right)^{N-1} \\ &= \left(1 - V(\sqrt{x})\right)^{N-1} = \left(1 - \frac{x}{4}\right)^{N-1}. \end{aligned}$$

From general principles, if Y is non-negative then $\mathbb{E}(Y) = \int_0^\infty \text{Prob}(Y > y) dy$. Hence

$$(A.15) \quad \mathbb{E}\left(\min_{j=2, \dots, N} |P_1 - P_j|^2\right) = \int_0^4 \left(1 - \frac{x}{4}\right)^{N-1} dx = \frac{4}{N}$$

which in conjunction with (A.13) proves (A.12).

We turn to (1.12), the distribution of scaled nearest neighbour spacings

$$(A.16) \quad \mu_N(P_1, \dots, P_N) = \frac{1}{N} \sum_{j=1}^N \delta_{Nd_j^2/4}.$$

For $x \geq 0$ we examine the expectations

$$(A.17) \quad \mathbb{E}\left(\mu_N[0, x]\right) = \mathbb{E}\left(\frac{1}{N} \sum_{j=1}^N I\left(\frac{Nd_j^2}{4} \leq x\right)\right),$$

where $I(\bullet) = 1$ if the condition \bullet holds, and 0 otherwise. Setting $r = 2\sqrt{\frac{x}{N}}$ we have

$$(A.18) \quad \mu_N[0, x] = \frac{1}{N} \sum_j I\left(\min_{k \neq j} d(P_k, P_j) \leq r\right).$$

Hence

$$(A.19) \quad \mu_N[0, x] \leq A_1 := \frac{1}{N} \sum_j \sum_{k \neq j} I_r(P_j, P_k)$$

and

$$(A.20) \quad \mu_N[0, x] \geq A_1 - A_2,$$

where

$$(A.21) \quad A_2 := \frac{1}{N} \sum_j \sum_{\substack{k_1, k_2 \\ k_1 \neq k_2 \\ k_1, k_2 \neq j}} I_r(P_j, P_{k_1}) I_r(P_j, P_{k_2})$$

and continuing with inclusion/exclusion, defining A_k analogously,

$$(A.22) \quad \begin{aligned} \mu_N[0, x] &\leq A_1 - A_2 + A_3 + \dots + A_{2\ell+1} \\ \mu_N[0, x] &\geq A_1 - A_2 + A_3 + \dots - A_{2\ell+2}. \end{aligned}$$

Taking expectations we have from (A.19) and (A.21)

$$(A.23) \quad \mathbb{E}(\mu_N[0, x]) \leq \frac{1}{N}N(N-1)V(r) \rightarrow x, \quad \text{as } N \rightarrow \infty$$

and hence

$$(A.24) \quad \limsup_{N \rightarrow \infty} \mathbb{E}(\mu_N[0, x]) \leq x$$

while

$$(A.25) \quad \mathbb{E}(\mu_N[0, x]) \geq \frac{N(N-1)V(r)}{N} - \frac{1}{N} \frac{(N-1)(N-2)}{2} V(r)^2 \rightarrow x - \frac{x^2}{2}$$

and hence

$$(A.26) \quad \liminf_{N \rightarrow \infty} \mathbb{E}(\mu_N[0, x]) \geq x - \frac{x^2}{2}.$$

Continuing with (A.22) taking expectations and limit as $N \rightarrow \infty$ yields after a similar calculation that

$$(A.27) \quad \lim_{N \rightarrow \infty} \mathbb{E}(\mu_N[0, x]) = x - \frac{x^2}{2} + \frac{x^3}{3!} - \dots = 1 - e^{-x}$$

that is

$$(A.28) \quad \lim_{N \rightarrow \infty} \mathbb{E}(\mu_N) = e^{-t} dt.$$

One can compute variances as we did in (A.5) above, from which it follows that

$$(A.29) \quad \mu_N[0, x] \rightarrow 1 - e^{-x}$$

in probability, which is what is meant in (1.12).

We end this short appendix with proofs of (1.18), (1.25) and (1.27). The first two are concerned with the minimum spacing for random points in S^k . The probability of placing N independent points in S^k so that none are closer to each other than r is clearly

$$(A.30) \quad (1 - V(r))(1 - 2V(r)) \dots (1 - (N-1)V(r))$$

as long as $(N-1)V(r) < 1$ (otherwise the probability is zero). From this it is clear that if $r \geq N^{-2/k+\epsilon}$ so that $V(r)N^2 \geq N^{\epsilon'}$, then the product in (A.30) tends to 0. So that with probability tending to 1 the minimum spacing is at most $N^{-2/k+\epsilon}$. On the other hand if $r \leq N^{-2/k-\epsilon}$ then $V(r)N^2 \leq N^{-\epsilon'}$ and the product in (A.30) goes to 1, so that with probability tending to 1, the minimal spacing is at least $N^{-2/k-\epsilon}$. That is $m(P_1, \dots, P_N) = N^{-2/k+o(1)}$ with probability tending to 1, which establishes (1.18) and (1.25).

Finally we turn to (1.27), which is concerned with the covering radius $M(P_1, \dots, P_N)$ for random points. For any configuration of points on S^k , surface area considerations show that

$$(A.31) \quad M(P_1, \dots, P_N) \gg N^{-1/k}.$$

So to establish (1.27) we need to show that for $\epsilon > 0$ and random points P_1, \dots, P_N ,

$$(A.32) \quad M(P_1, \dots, P_N) \ll N^{-1/k+\epsilon}.$$

Given $x \in S^k$, the probability that the cap $B(x, r)$ does not contain any of the points P_1, \dots, P_N is

$$(A.33) \quad \left(1 - V(r)\right)^N.$$

Hence if x_1, \dots, x_L are L points in S^k , the probability that at least one of the caps $B(x_j, r)$ does not contain any of P_1, \dots, P_N is at most

$$(A.34) \quad L \left(1 - V(r)\right)^N.$$

In particular if $L = N$ and $r = N^{-1/k+\epsilon}$ then the probability in (A.34) goes to 0 as $N \rightarrow \infty$. Hence with probability tending to 1 each of the N caps $B(x_j, r)$ contains at least one of the P_j 's. Now choose the x_j 's to be a $c_k N^{-1/k}$ cover (i.e. each point of S^k is within $c_k N^{-1/k}$ of one of x_1, \dots, x_N). Since there is a P_i in each cap $B(x_j, r)$, it follows that the P_i 's form a $2N^{-1/k+\epsilon}$ covering of S^k . This completes the proof of (1.27).

References

- [1] J. S. Brauchart, D. P. Hardin, and E. B. Saff, *The next-order term for optimal Riesz and logarithmic energy asymptotics on the sphere*, Recent advances in orthogonal polynomials, special functions, and their applications, Contemp. Math., vol. 578, Amer. Math. Soc., Providence, RI, 2012, pp. 31–61, DOI 10.1090/conm/578/11483. MR2964138
- [2] V. A. Bykovskii, *A trace formula for the scalar product of Hecke series and its applications* (Russian, with Russian summary), Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI) **226** (1996), no. Anal. Teor. Chisel i Teor. Funktsii. 13, 14–36, 235–236, DOI 10.1007/BF02358528; English transl., J. Math. Sci. (New York) **89** (1998), no. 1, 915–932. MR1433344 (97k:11067)
- [3] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*, 3rd ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 290, Springer-Verlag, New York, 1999. With additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov. MR1662447 (2000b:11077)
- [4] B. E. J. Dahlberg, *On the distribution of Fekete points*, Duke Math. J. **45** (1978), no. 3, 537–542. MR507457 (80c:31003)
- [5] W. Duke, *Hyperbolic distribution problems and half-integral weight Maass forms*, Invent. Math. **92** (1988), no. 1, 73–90, DOI 10.1007/BF01393993. MR931205 (89d:11033)
- [6] W. Duke and R. Schulze-Pillot, *Representation of integers by positive ternary quadratic forms and equidistribution of lattice points on ellipsoids*, Invent. Math. **99** (1990), no. 1, 49–57, DOI 10.1007/BF01234411. MR1029390 (90m:11051)
- [7] J. S. Ellenberg, P. Michel, and A. Venkatesh, *Linnik's ergodic method and the distribution of integer points on spheres*, Automorphic representations and L -functions, Tata Inst. Fundam. Res. Stud. Math., vol. 22, Tata Inst. Fund. Res., Mumbai, 2013, pp. 119–185. MR3156852
- [8] P. Erdős and R. R. Hall, *On the angular distribution of Gaussian integers with fixed norm*, Discrete Math. **200** (1999), no. 1-3, 87–94, DOI 10.1016/S0012-365X(98)00329-X. Paul Erdős memorial collection. MR1692282 (2000m:11066)
- [9] E. P. Golubeva and O. M. Fomenko, *Asymptotic distribution of lattice points on the three-dimensional sphere* (Russian), Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) **160** (1987), no. Anal. Teor. Chisel i Teor. Funktsii. 8, 54–71, 297, DOI 10.1007/BF02342921; English transl., J. Soviet Math. **52** (1990), no. 3, 3036–3048. MR906844 (88m:11082)
- [10] G. Harman, *Approximation of real matrices by integral matrices*, J. Number Theory **34** (1990), no. 1, 63–81, DOI 10.1016/0022-314X(90)90053-T. MR1039768 (91a:11031)
- [11] D. R. Heath-Brown, *A new form of the circle method, and its application to quadratic forms*, J. Reine Angew. Math. **481** (1996), 149–206, DOI 10.1515/crll.1996.481.149. MR1421949 (97k:11139)

- [12] H. Iwaniec, *Fourier coefficients of modular forms of half-integral weight*, Invent. Math. **87** (1987), no. 2, 385–401, DOI 10.1007/BF01389423. MR870736 (88b:11024)
- [13] I. Kátai and I. Környei, *On the distribution of lattice points on circles*, Ann. Univ. Sci. Budapest. Eötvös Sect. Math. **19** (1976), 87–91 (1977). MR0506102 (58 #21985)
- [14] Yu. V. Linnik, *Ergodic properties of algebraic fields*, Translated from the Russian by M. S. Keane. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 45, Springer-Verlag New York Inc., New York, 1968. MR0238801 (39 #165)
- [15] A. V. Malyšev, *On the representation of integers by positive quadratic forms* (Russian), Trudy Mat. Inst. Steklov **65** (1962), 212. MR0142511 (26 #80)
- [16] M. Nair, *Multiplicative functions of polynomial values in short intervals*, Acta Arith. **62** (1992), no. 3, 257–269. MR1197420 (94b:11093)
- [17] M. Peter, *Almost periodicity of the normalized representation numbers associated to positive definite ternary quadratic forms*, J. Number Theory **77** (1999), no. 1, 122–144, DOI 10.1006/jnth.1998.2367. MR1695704 (2000m:11036)
- [18] C.L. Siegel, *Über die Klassenzahl quadratischen Zahlkörper* Acta Arithmetica 1 (1935) pp. 83–86.
- [19] D. Stoyan, W. S. Kendall, and J. Mecke, *Stochastic geometry and its applications*, Wiley Series in Probability and Mathematical Statistics: Applied Probability and Statistics, John Wiley & Sons, Ltd., Chichester, 1987. With a foreword by D. G. Kendall. MR895588 (88j:60034a)
- [20] B. A. Wenkov, *Über die Klassenanzahl positiver binärer quadratischer Formen* (German), Math. Z. **33** (1931), no. 1, 350–374, DOI 10.1007/BF01174358. MR1545216
- [21] I. M. Vinogradov, *Sur la distribution des résidus et des non-résidus des puissances*. Fiz.-Mat. Ob. Permsk. Gos. Univ. 1 (1918), pp. 94–98.
- [22] G. Wagner, *On means of distances on the surface of a sphere (lower bounds)*, Pacific J. Math. **144** (1990), no. 2, 389–398. MR1061328 (91e:52014)
- [23] G. Wagner, *On means of distances on the surface of a sphere. II. Upper bounds*, Pacific J. Math. **154** (1992), no. 2, 381–396. MR1159518 (93b:52007)

SCHOOL OF MATHEMATICS, INSTITUTE FOR ADVANCED STUDY, PRINCETON, NEW JERSEY 08540

E-mail address: bourgain@math.ias.edu

DEPARTMENT OF MATHEMATICS, PRINCETON UNIVERSITY, FINE HALL, WASHINGTON ROAD, PRINCETON, NJ 08544 AND SCHOOL OF MATHEMATICS, INSTITUTE FOR ADVANCED STUDY, EINSTEIN DRIVE, PRINCETON, NEW JERSEY 08540

E-mail address: sarnak@math.ias.edu

RAYMOND AND BEVERLY SACKLER SCHOOL OF MATHEMATICAL SCIENCES, TEL AVIV UNIVERSITY, TEL AVIV 69978, ISRAEL

E-mail address: rudnick@post.tau.ac.il