RANDOM EIGENFUNCTIONS ON FLAT TORI: UNIVERSALITY FOR THE NUMBER OF INTERSECTIONS

MEI-CHU CHANG, HOI NGUYEN, OANH NGUYEN, VAN VU

Abstract. We show that several statistics of the number of intersections between random eigenfunctions of general eigenvalues and a given smooth curve in flat tori are universal under various families of randomness.

1. Introduction

Let $\mathcal{M}$ be a smooth Riemannian manifold. Let F be a real-valued eigenfunction of the Laplacian on $\mathcal{M}$ with eigenvalue λ^2,

$$-\Delta F = \lambda^2 F.$$

The nodal set N_F is defined to be the zero set of F,

$$N_F := \{x \in \mathcal{M} : F(x) = 0\}.$$

The nodal set N_F has been studied intensively in analysis and differential geometry, see, for example, [17, 16, 11, 10, 5]. In this note we focus on the case when $\mathcal{M}$ is the flat tori $\mathbf{T}^d = \mathbf{R}^d/\mathbf{Z}^d$ with $d \geq 2$; more specifically we will be focusing on the intersection between N_F and a given reference curve.

Let $\mathcal{C} \subset \mathcal{M}$ be a curve assumed to have unit length with the arc-length parametrization $\gamma : [0,1] \to \mathcal{M}$. The number of nodal intersections $\mathcal{Z}(F)$ between F and $\mathcal{C}$ is defined to be the cardinality of the intersection $N_F \cap \mathcal{C}$.

1.1. Deterministic results in $\mathbf{T}^2$.

It is known that all eigenvalues λ^2 have the form $4\pi^2 m$ where $m = a^2 + b^2$ for some $a, b \in \mathbf{Z}$. Let $\mathcal{E}_\lambda$ be the collection of $\mu = (\mu_1, \mu_2) \in \mathbf{Z}^2$ such that

$$\mu_1^2 + \mu_2^2 = m.$$

The toral eigenfunctions $f(x) = e^{2\pi i \langle \mu, x\rangle}, \mu \in \mathcal{E}_\lambda$ form an orthonormal basis in the eigenspace corresponding to λ^2. In their beautiful paper [7], Bourgain and Rudnick provided uniform

2010 *Mathematics Subject Classification.* 15A52,11B25, 60C05, 60G50.

Key words and phrases. arithmetic random waves, universality phenomenon, arithmetic progressions.

M. C. Chang is partially supported by NSF grant DMS 1764081, the author thanks the Mathematics Department of University of California at Berkeley for its hospitality. H. Nguyen is partially supported by NSF grant DMS 1600782. O. Nguyen and V. Vu are partially supported by NSF grant DMS-1307797 and AFORS grant FA9550-12-1-0083.

upper and lower bounds for the L^2 norm of the restriction of F to a real analytic curve $\mathcal{C}$ with non-vanishing curvature ([7, Main Theorem])

$$\int_{\mathcal{C}} |F|^2 d\gamma = \Omega\left(\int_{\mathcal{M}} |F(x)|^2 dx\right) \tag{1.1}$$

where the implicit constants depend on $\mathcal{C}$ but not on λ.

Here we say that $f = O(g)$, or $g = \Omega(f)$, or $f \ll g$, if there exists a constant C such that $|f| \le C|g|$.

Using an argument from [5] (see also [38]), they showed that the lower bound in (1.1) implies an upper bound on the number of nodal intersections $\mathcal{Z}(F)$. Remarkably, they also obtained a lower bound on $\mathcal{Z}(F)$ from (1.1).

Theorem 1.1. [7, Theorem 1.1] *Let $\mathcal{C} \subset \mathbf{T}^2$ be a real analytic curve with nowhere vanishing curvature, then for any $\varepsilon > 0$,*

$$\lambda^{1-\varepsilon} \ll \mathcal{Z}(F) \ll \lambda,$$

where the implicit constants depend only on $\mathcal{C}$ and ε.

It was then conjectured by Bourgain and Rudnick that the lower bound is of order λ.

Conjecture 1.2. [7] *If $\mathcal{C} \subset \mathbf{T}^2$ is smooth with non-zero curvature, then*

$$\mathcal{Z}(F) \gg \lambda.$$

In a subsequent paper, to support this conjecture they showed

Theorem 1.3. [8, Theorem 1.1] *If $\mathcal{C} \subset \mathbf{T}^2$ is smooth with nowhere vanishing curvature, then*

$$\mathcal{Z}(F) \gg \frac{\lambda}{B_\lambda^{5/2}}$$

where B_λ denote the maximal number of lattice points which lie on an arc of size $\sqrt{\lambda}$ on the circle $|x| = \lambda$,

$$B_\lambda := \max_{|x|=\lambda} \# \left\{\mu \in \mathcal{E}_\lambda : |x - \mu| \le \sqrt{\lambda}\right\}.$$

In particular, as one can show that $B_\lambda \ll \log \lambda$ (see [8]), we have $\mathcal{Z}(F) \gg \lambda / \log^{5/2} \lambda$.

The above link between $\mathcal{Z}(F)$ and B_λ yields another interesting relationship between Bourgain-Rudnick conjecture 1.2 and Cilleruelo-Granville conjecture [12] which predicts that $B_\lambda = O(1)$ uniformly. This is known to hold for almost all λ^2, see for instance [6, Lemma 5]; we also refer the reader to Lemma 5.2 of Section 5 for a similar result (with a relatively short proof).

It's worth noting that when the curvature of $\mathcal{C}$ is zero, it could happen that $\liminf_\lambda \mathcal{Z}(F) = 0$. See [8].

1.2. **Arithmetic random wave model.** Denote by $N = N_m := \#\mathcal{E}_\lambda$ the dimension of the eigenspace corresponding to the eigenvalue λ^2. A probabilistic approach to the study of $\mathcal{Z}(F)$ was introduced in the pioneer paper of Rudnick and Wigman [34]. Consider the random Gaussian eigenfunction

$$F(x) = \frac{1}{\sqrt{N}} \sum_{\mu \in \mathcal{E}_\lambda} \varepsilon_\mu e^{2\pi i \langle \mu, x\rangle}, \tag{1.2}$$

for all $x \in \mathbf{T}^2$, where ε_μ are iid complex standard Gaussian with a saving

$$\varepsilon_{-\mu} = \bar{\varepsilon}_\mu.$$

This saving ensures that F is real-valued. The random function F is called *arithmetic random wave* [2, 27], which is a stationary Gaussian field because the correlation $\mathbb{E}(F(x)F(y))$ is invariant under translation. As we can also see, the law of this model is independent of the choice of the orthonormal basis of the eigenspaces.

Rudnick and Wigman showed that for all eigenvalues, *almost all* eigenfunctions satisfy Conjecture 1.2. More specifically, they showed the following.

Theorem 1.4. [34, Theorems 1.1, 1.2] *Let $\mathcal{C} \subset \mathbf{T}^2$ be a smooth curve on the torus, with nowhere vanishing curvature and of total length one. Then*

(1) *The expected number of nodal intersections is precisely*

$$\mathbb{E}_{\mathbf{g}} \mathcal{Z}(F) = \sqrt{2m}.$$

(2) *The variance is bounded from above as follows*

$$\mathrm{Var}_{\mathbf{g}}(\mathcal{Z}(F)) \ll \frac{m}{N}.$$

(3) *Furthermore, let $\{m\}$ be a sequence such that $N_m \to \infty$ and the Fourier coefficient $\{\widehat{\tau_m}(4)\}$ do not accumulate at ± 1, then*

$$\mathrm{Var}_{\mathbf{g}}(\mathcal{Z}(F)) = \frac{m}{N}\left(\int_{\mathcal{C}}\int_{\mathcal{C}} \sum_{\mu \in \mathcal{E}_\lambda} 4\frac{1}{N}\left\langle \frac{\mu}{|\mu|}, \dot{\gamma}(t_1)\right\rangle^2 \left\langle \frac{\mu}{|\mu|}, \dot{\gamma}(t_2)\right\rangle^2 - 1\right) dt_1 dt_2 + O\left(\frac{m}{N^{3/2}}\right).$$

Here the subscript $\mathbf{g}$ is used to emphasize standard Gaussian randomness, and τ_m is the probability measure on the unit circle $S^1 \subset \mathbf{R}^2$ associated with $\mathcal{E}_\lambda$,

$$\tau_m := \frac{1}{N} \sum_{\mu \in \mathcal{E}_\lambda} \delta_{\mu/\sqrt{m}}.$$

We also refer the reader to [35, Proposition 2.2] for a general estimate when the condition on $\{\widehat{\tau_m}(4)\}$ is lifted, and to [33, Theorem 1.3] for further extension when the first term in $\mathrm{Var}_{\mathbf{g}}(\mathcal{Z}(F))$ vanishes. By Markov's inequality, (1) and (2) in Theorem 1.4 imply that Conjecture (1.2) holds for the random wave F asymptotically almost surely. In fact, the statement of (2) and (3) show that the variance is much smaller than m, indicating a large number of cancellations in the formula of the variance.

1.3. **Partial results in $\mathbf{T}^3$.** Bourgain and Rudnick [4, 7, 8] also considered the number of nodal intersections $\mathcal{Z}(F)$ between the nodal set N_F and a smooth *hypersurface* σ for general $\mathbf{T}^d$. For $\mathbf{T}^3$, they obtained an analog of (1.1) for the L^2 restriction over σ (See [7, Main Theorem]). However, we are not aware of any deterministic results for $\mathbf{T}^3$ that are similar to Theorem 1.1. On the probabilistic side, Rudnick, Wigman and Yesha [35] have recently extended Theorem 1.4 to $\mathbf{T}^3$. Here, for $\lambda^2 = 4\pi^2 m$ with $m \neq 0, 4, 7 \mod 8$, let $\mathcal{E}_\lambda$ be the collection of $\mu = (\mu_1, \mu_2, \mu_3) \in \mathbf{Z}^3$ such that $\mu_1^2 + \mu_2^2 + \mu_3^2 = m$. Again denote $N = N_m = \#\mathcal{E}_\lambda$.

Consider the random Gaussian eigenfunction

$$F(x) = \frac{1}{\sqrt{N}} \sum_{\mu \in \mathcal{E}_\lambda} \varepsilon_\mu e^{2\pi i \langle \mu, x \rangle},$$

where ε_μ are iid complex standard Gaussian again with the saving

$$\varepsilon_{-\mu} = \bar{\varepsilon}_\mu.$$

Rudnick, Wigman and Yesha showed the following result.

Theorem 1.5. [35, Theorems 1.4, 1.5] *Let $\mathcal{C} \subset \mathbf{T}^3$ be a smooth curve on the torus of total length one with nowhere zero curvature. Assume further that either $\mathcal{C}$ has nowhere-vanishing torsion or $\mathcal{C}$ is planar. Let m be an integer with $m \not\equiv 0, 4, 7 \pmod 8$. Then*

(1) The expected number of nodal intersections is precisely

$$\mathbb{E}_{\mathbf{g}} \mathcal{Z}(F) = \frac{2}{\sqrt{3}} \sqrt{m}.$$

(2) There exists $c > 0$ such that

$$\mathrm{Var}_{\mathbf{g}}(\mathcal{Z}(F)) \ll \frac{m}{N^c}.$$

As pointed out in [35], the assumption $m \not\equiv 0, 4, 7 \pmod 8$ is natural because of the following two reasons.

- If $m \equiv 7 \pmod 8$, m cannot be written as a sum of three squares.
- If $m \equiv 0, 4 \pmod 8$, then $m = 4^a m'$ and any eigenfunction of the eigenvalue m is of the form $F(x) = F'(2^a x)$ where F' is an eigenfunction of m'.

The proof of Theorem 1.4 and Theorem 1.5 are based on Kac-Rice formula. To motivate the reader, let us sketch the computation of the expectation for $d \geq 2$

$$\mathbb{E}_{\mathbf{g}} \mathcal{Z}(F) = \frac{2\sqrt{m}}{\sqrt{d}}. \tag{1.3}$$

We follow the proof of [35, Lemma 2.3]. Let $r(t_1, t_2) = \mathbb{E}(F(\gamma(t_1))F(\gamma(t_2)))$. Let $K_1(t)$ be the Gaussian expectation (first intensity)

$$K_1(t) := \phi_t(0) \mathbb{E}\left(\left|(F \circ \gamma)'(t)\right| \middle| F(\gamma(t)) = 0 \right)$$

where ϕ_t is the density function of the random variable $F(\gamma(t))$, which is a standard Gaussian random variable. Thus, $\phi_t(0) = \frac{1}{\sqrt{2\pi}}$.

By the Kac-Rice formula

$$\mathbb{E}\mathcal{Z}(F)=\int_0^1 K_1(t)dt.$$

Let $\Gamma(t)$ be the covariance matrix of $((F\circ\gamma)(t),(F\circ\gamma)'(t))$,

$$\Gamma(t)=\begin{pmatrix} r(t,t) & r_1(t,t)\\ r_2(t,t) & r_{12}(t,t)\end{pmatrix},$$

where $r_1=\partial r/\partial t_1, r_2=\partial r/\partial t_2, r_{12}=\partial^2 r/\partial t_1\partial t_2$. It is not hard to show that $\Gamma(t)=\begin{pmatrix}1 & 0\\ 0 & \alpha\end{pmatrix}$, where $\alpha=r_{12}(t,t)=\frac{4\pi^2 m}{d}$. It thus follows

$$K_1(t)=\frac{1}{\pi}\sqrt{\alpha}=\frac{2\sqrt{m}}{\sqrt{d}}.$$

This proves (1.3).

For the variance, define $K_2(t_1,t_2)$ to be

$$K_2(t_1,t_2):=\phi_{t_1,t_2}(0,0)\mathbb{E}\left(\left|(F\circ\gamma)'(t_1)(F\circ\gamma)'(t_2)\right|\middle|F(\gamma(t_1))=0,F(\gamma(t_2))=0\right),$$

where ϕ_{t_1,t_2} is the density function of the random Gaussian vector $(F(\gamma(t_1)),F(\gamma(t_2)))$. It is known that for any measurable subsets $A,B\subset[0,1]$, if the covariance matrix $\Sigma(t_1,t_2)$ of the vectors $(F(\gamma(t_1)),F(\gamma(t_2)),(F\circ\gamma)'(t_1)(F\circ\gamma)'(t_2))$ is non-singular for all $(t_1,t_2)\in A\times B$, then

$$\mathbb{E}\left(\mathcal{Z}(F)\,|_A\mathcal{Z}(F)|_B\right)-\mathbb{E}\left(\mathcal{Z}(F)\big|_A\right)\mathbb{E}\left(\mathcal{Z}(F)\big|_B\right)=\int_{A\times B}K_2(t_1,t_2)dt_1dt_2.$$

The main problem here is that the matrix $\Sigma(t_1,t_2)$ is not always non-singular in $[0,1]^2$. Roughly speaking, to overcome this highly technical obstacle, basing on the Taylor expansion of the 2-point correlation function $K_2(t_1,t_2)$, Rudnick and Wigman [34] and Rudnick, Wigman and Yesha [35] divide $[0,1]$ into subintervals I_i of length of order $1/\sqrt{m}$ each, and then show that Kac-Rice's formula is available locally on most of the cells $I_i\times I_j$. We refer the reader to [34, 35] for more detailed treatment of these issues.

1.4. **More general random waves and our main results.**

With regard to the probabilistic approach to Conjecture 1.2, a natural question that one can ask is the behavior of $\mathcal{Z}(F)$ for other random eigenfunctions F beside the Gaussian arithmetic random waves described above. A special case of interest would be the case when the randomness comes from a discrete distribution, for example, when the random variables ε_i in (1.2) are random ± signs. More generally, we consider the random function

$$F(x)=\frac{1}{\sqrt{N}}\sum_{\mu\in\mathcal{E}_\lambda}\varepsilon_\mu e^{2\pi i\langle\mu,x\rangle}, \tag{1.4}$$

where $\varepsilon_\mu=\varepsilon_{1,\mu}+i\varepsilon_{2,\mu}$ and $\varepsilon_{1,\mu},\varepsilon_{2,\mu},\mu\in\mathcal{E}_\lambda$ are iid random variables with the saving constraint $\varepsilon_{-\mu}=\bar{\varepsilon}_\mu$. Note that the last constraint is again to make F a real-valued random eigenfunction.

We denote by $\mathbb{P}_{\varepsilon_\mu},\mathbb{E}_{\varepsilon_\mu}$, and $\mathrm{Var}_{\varepsilon_\mu}$ the probability, expectation, and variance with respect to the random variables $(\varepsilon_\mu)_{\mu\in\mathcal{E}_\lambda}$.

Question 1.6. *Are the statistics such as $\mathbb{E}_{\varepsilon_\mu}\mathcal{Z}(F)$ and $\mathrm{Var}_{\varepsilon_\mu}(\mathcal{Z}(F))$ with respect to the randomness of the random variables ε_μ universal? In other words, do the conclusions of Theorems 1.4 and 1.5 hold (asymptotically) when random variables ε_μ are non-Gaussian?*

Note that we can write F as

$$F(x) = \frac{1}{\sqrt{N}} \sum_{\mu\in\mathcal{E}_\lambda} \varepsilon_\mu e^{2\pi i\langle \mu, x\rangle} = \frac{1}{\sqrt{N}} \sum_{\mu\in\mathcal{E}_\lambda} \varepsilon_{1,\mu}\cos(2\pi\langle\mu,x\rangle) + \varepsilon_{2,\mu}\sin(2\pi\langle\mu,x\rangle). \tag{1.5}$$

We first restrict to $\mathbf{T}^2$ and describe our results when the random variables ε_μ can have discrete distribution. Consider the following conditions on the curves and the distributions.

Assumption on the reference curve. Let $\gamma(t), t \in [0,1]$ be a curve of unit length.

Condition 1.7. *Consider the following conditions*

(i) (Analyticity) The function $\gamma(t)$ is real analytic.

(ii) (Non-vanishing curvature) The curve $\gamma(t) : [0,1] \to \mathbf{T}^2$ has arc-length parametrization with positive curvature. More specifically, there exists a positive constant c such that $\|\gamma'(t)\| = 1$ and $\|\gamma''(t)\| > c$ for all t.

We also record a small remark below.

Remark 1.8. *For a fixed smooth curve γ as above, when $\lambda \to \infty$ and $N = N(\lambda) \to \infty$, for any constant $c_0 > 0$ there exists a constant $\alpha > 0$ such that for any interval $I \subset [0,1]$ of length c_0/λ, the segment $\{\gamma(t), t \in I\}$ cannot be contained in a ball of radius $N^{-\alpha}/\lambda$.*

Proof. We prove a slightly more general estimate. Let $M = \sup_{t\in[0,1]} \|\gamma''(t)\|$. Let $I = (a,b) \subset [0,1]$ be any interval with length $b - a \le 1/2M$. Let φ_a be the unit vector $\gamma'(a)$. Consider $f(t) = \langle\gamma(t), \varphi_a\rangle$ for $t \in I$. Then $f'(t) = \langle\gamma'(t), \varphi_a\rangle$ and particularly $f'(a) = 1$. Also, because $|f''(t)| \le M$ for all t, we have that $f'(t) \ge 1/2$ for all $t \in I$, and therefore by the mean value theorem $|f(b) - f(a)| \ge (b-a)/2$. This then implies that $\|\gamma(b) - \gamma(a)\| \ge |f(b) - f(a)| \ge (b-a)/2$. □

Assumption on the distribution.

Condition 1.9. *We will assume ε_μ to have mean zero, variance one, bounded $(2+\varepsilon)$-moment for some constant $\varepsilon > 0$ with the following properties. There is a fixed number K such that either*

(i) (Continuous distribution) ε_μ is absolutely continuous with bounded density function p, $\|p\|_\infty \le K$.

(ii) (Mixed distribution) There exist positive constants c_1, c_2, c_3 such that $\mathbb{P}(c_1 \le |\varepsilon_\mu - \varepsilon'_\mu| \le c_2) \ge c_3$ where ε'_μ is an independent copy of ε_μ and one of the following holds

- *either $|\varepsilon_\mu| > 1/K$ with probability one*
- *or $\varepsilon_\mu 1_{|\varepsilon_\mu|\le 1/K}$ is continuous with density bounded from above by K.*

The assumption that ε_μ stays away from zero (for discrete distribution) is necessary because otherwise the random function F might be vanishing with positive probability. As mentioned, one representative example of our consideration is Bernoulli random variable which takes values ±1 with probability 1/2, and this model does not have the nice invariance property of the Gaussian one. The assumption of bounded $(2+\varepsilon)$-moment is only for technical reasons and is mainly for Theorem 2.2.

We now state our main result for $\mathbf{T}^2$.

Theorem 1.10 (main result, universality of the moments in $\mathbf{T}^2$)**.** *Assume that γ satisfies Condition 1.7 and the random variables $\varepsilon_{1,\mu}, \varepsilon_{2,\mu}, \mu \in \mathcal{E}_\lambda$ are iid random variables satisfying Condition 1.9. Then for almost all m we have*

- $\mathbb{E}_{\varepsilon_\mu}\mathcal{Z}(F) = \mathbb{E}_{\mathbf{g}}\mathcal{Z}(F) + O\left(\lambda/N^{c'}\right)$;
- *More generally, for any fixed k, $\mathbb{E}_{\varepsilon_\mu}\mathcal{Z}(F)^k = \mathbb{E}_{\mathbf{g}}\mathcal{Z}(F)^k + O\left(\lambda^k/N^{c'}\right)$,*

where the subscript $\mathbf{g}$ stands for the distribution in which the $\varepsilon_{1,\mu}$ and $\varepsilon_{2,\mu}$ are independent standard Gaussian. Here c' and the implicit constants depend on the curve γ, k, and the constants in Conditions 1.7 and 1.9 but not on N and λ. In particular, for almost all m, we have

$$\mathbb{E}_{\varepsilon_\mu}\mathcal{Z}(F) = \sqrt{2m} + O\left(\lambda/N^{c'}\right) \qquad \text{and} \qquad \mathrm{Var}_{\varepsilon_\mu}(\mathcal{Z}(F)) \ll \frac{\lambda^2}{N^{c'}}.$$

The density of the sequence $\{m\}$ above can be worked out explicitly, but as this is not our main focus, we will omit the details. It is plausible to conjecture that the variance is indeed as small as in (iii) of Theorem 1.4. However, this seems to be an extremely delicate matter given the highly nontrivial analysis of the Gaussian case.

To prove Theorem 1.10, we will need to show that for almost all m the set $\mathcal{E}_\lambda$ satisfies the following property which is later proven in Section 6.

Lemma 1.11. *There exists a constant $\varepsilon_0 > 0$ such that for almost all m the following holds. For any vector $r \in \mathbf{R}^2$ with $|r| = \frac{1}{2\pi\lambda}$, the set $\{\langle r, \mu\rangle, \mu \in \mathcal{E}_\lambda\}$ can not be covered by less than $O\left(N^{\varepsilon_0}\right)$ intervals of length N^{-1} in $[-1, 1]$.*

Theorem 1.10 is stated for almost all m mainly because of the deterministic Lemma 5.2 of Section 5, which in turn is needed for the verification of one of our probabilistic conditions of the universality framework. We also need to pass to almost all m for a brief verification of Lemma 1.11.

Now we turn to $\mathbf{T}^d, d \geq 3$. While in this setting the cardinality N of $\mathcal{E}_\lambda$ is relatively large compared to λ, the situation is difficult by different reasons. Consider the following example from [35].

Example 1.12. *Let $F_0(x, y)$ be an eigenfunction on $\mathbf{T}^2$ with eigenvalue $4\pi^2 m$, and S_0 a curved segment length one contained in the nodal set, admitting an arc-length parameterization $\gamma_0 : [0, 1] \to S_0$ with curvature $\kappa_0(t) = |\gamma_0''(t)| > 0$. For $n > 0$, let $F_n(x, y, z) = F_0(x, y)\cos(2\pi n z)$, which is an eigenfunction on $\mathbf{T}^3$ with eigenvalue $4\pi^2(m + n^2)$. Let*

$\mathcal{C}$ be the curve $\gamma(t) = (\gamma_0(t/\sqrt{2}), t/\sqrt{2})$. Standard computation shows that the curvature $\kappa(t) = \kappa_0(t/\sqrt{2})/2 > 0$ and the torsion $\tau(t) = \pm\kappa_0(t/\sqrt{2})/2$ is non-zero. Note that $\mathcal{C}$ is contained in the nodal set of F_n for all n. Thus we can have a non-trivial curve contained in the nodal set for arbitrary large λ.

This example shows that the study of universality in $\mathbf{T}^d, d \geq 3$ in the case where the random variables ε_μ have discrete distribution can be highly complex (at least if we only assume γ to have non-vanishing curvature and torsion) as there is no deterministic upper bound for $\mathcal{Z}(F)$. If we are not careful with the choice of discrete distributions, our random function F from (1.4) might be one of the F_n in Example 1.12 with non-zero probability, and hence $\mathbb{E}\mathcal{Z}(F)$ is infinite. To avoid such type of singularity, in what follows we will assume that the random variables ε_μ are continuously distributed. More specifically, we assume Condition 1.9(i). Note that the following result also holds for $d = 2$, and here we don't need to assume Condition 1.7.

Theorem 1.13 (universality for the moments in $\mathbf{T}^d$, $d \geq 2$, continuous distributions)**.** *Assume that $\varepsilon_{1,\mu}, \varepsilon_{2,\mu}, \mu \in \mathcal{E}_\lambda$ are independent random variables satisfying Condition 1.9*(i). *Assume furthermore that the curve γ is real analytic. Then for any fixed k we have*

$$\mathbb{E}_{\varepsilon_\mu}\mathcal{Z}(F)^k = \mathbb{E}_{\mathbf{g}}\mathcal{Z}(F)^k + O\left(\lambda^k/N^{c'}\right).$$

In particular for $\mathbf{T}^3$, with γ and λ as in Theorem 1.5, we have

$$\mathbb{E}_{\varepsilon_\mu}\mathcal{Z}(F) = \frac{2}{\sqrt{3}}\sqrt{m} + O\left(\lambda/N^{c'}\right) \text{ and } \mathrm{Var}_{\varepsilon_\mu}(\mathcal{Z}(F)) \ll \frac{\lambda^2}{N^{c'}}.$$

Here c' and the implicit constants depend on the curve γ, k, and the constants in Condition 1.9(i) *but not on N and λ.*

All in all, our results support the striking conjecture (which cannot be observed from a deterministic point of view) that the statistics of the number of intersections between a random wave and a given non-degenerate curve is universal, *independently* of the random source used to generate the wave. We also refer the reader to [1] and [22] and the references therein for related issues.

1.5. **The method.** Our proof of the main results uses the *comparison* method: instead of directly computing the relevant statistics for each random wave, we compare them to those from the Gaussian wave and show that the differences are small. Roughly speaking, this comparison process itself contains many smaller comparisons as one goes over the random coefficients one by one to flip to Gaussian. So there are many types of differences (errors) to be taken care of. To this end, the "roughness" of the distributions has a huge affect, in analogy with the comparison between any random variable of mean zero and variance one with the standard Gaussian. Accordingly, our paper has two major components, one on the comparison method and its relation to previous developments, and one on the resolution of "roughness" associated to this complicated model.

The rest of the note is organized as follows. We first introduce in Section 2 a general scheme of the comparison method from [39], [15] and [32] gearing toward our universality result; a sketch of proof for these results will be discussed in Section 9 for the reader's convenience.

In the next phase, we prove Theorem 1.13 first in Section 3 as in this setting the error bounds are easier to control. The proof of Theorem 1.10 will be carried out throughout Section 4, 5, and 6 to check various regulatory conditions.

Further notation. We consider λ as an asymptotic parameter going to infinity and allow all other quantities to depend on λ unless they are explicitly declared to be fixed or constant. As mentioned earlier, we write $X = O(Y)$, $Y = \Omega(X)$, $X \ll Y$, or $Y \gg X$ if $|X| \leq CY$ for some fixed C; this C can depend on other fixed quantities such as the the parameter K of Condition 1.9 and the curve γ. If $X \ll Y$ and $Y \ll X$, we say that $Y = \Theta(X)$.

Throughout the note, if not specified otherwise, a property $p(\lambda)$ holds for *almost all* λ if the set of λ up to T that $p(\lambda)$ does not hold has cardinality much smaller than that of the set of λ for which $p(\lambda)$ holds, i.e. $|\{\lambda \leq T, \bar{p}(\lambda)\}| = o(|\{\lambda \leq T, p(\lambda)\}|)$ as $T \to \infty$.

Finally, all the norms $\|.\|$ in this note, if not specified, will be the usual ℓ_2-norm.

2. Supporting lemmas: general universality results

Our starting point uses the techniques developed by Do, Tao, and the last two authors [39, 15, 32] in the past several years. To put it in a more general context, we consider two random functions

$$H(x) = \sum_{\mu \in \mathcal{E}} \xi_\mu f_\mu(x), \quad \widetilde{H}(x) = \sum_{\mu \in \mathcal{E}} \tilde{\xi}_\mu f_\mu(x), \quad x \in$$

where $\mathcal{E}$ is a countable set and f_μ are deterministic functions with $f_\mu(\mathbf{R}) \subset \mathbf{R}$; the independent random variables ξ_μ satisfy Condition 1.9 and the independent random variables $\tilde{\xi}_\mu$ are standard Gaussian.

To introduce a general scheme to compare the number of roots of $H(x)$ and $\widetilde{H}(x)$ in a given set $\mathcal{B} \subset \mathbf{R}$, we first need some assumptions. As the reader will see, most of these requirements are very natural and easy to check.

Given positive constants $(k, C_1, \alpha_1, A, c_1, C)$, consider the following conditions where N is a positive number. (In applications, N is often set to be $|\mathcal{E}|$.)

Condition 2.1.

(1) *For any $x \in \mathcal{B}$, H is analytic on the ball $B(x, 1)$ with probability 1 and*

$$\mathbb{E}\mathcal{Z}^{k+2}_{B(x,1/2)} \mathbf{1}_{\mathcal{Z}_{B(x,1/2)} \geq N^{C_1}} \leq C$$

where $\mathcal{Z}_{B(x,1/2)}$ is the number of zeros of H in the complex ball $B(x, 1/2)$.

(2) *(Anti-concentration) For every $x \in \mathcal{B}$, with probability at least $1 - CN^{-A}$, there exists $x' \in B(x, 1/100)$ such that $|H(x')| \geq \exp(-N^{c_1})$.*

(3) *(Boundedness) For every $x \in \mathcal{B}$,*

$$\mathbb{P}\left(|H(z)| \leq \exp\left(N^{c_1}\right) \textit{ for all } z \in B(x, 1)\right) \geq 1 - CN^{-A}.$$

(4) (Delocalization) For every $z \in \mathcal{B} + B(0,1)$ and every $\mu \in \mathcal{E}$,

$$\frac{|f_\mu(z)|}{\sqrt{\sum_\mu |f_\mu(z)|^2}} \le N^{-c_1}.$$

(5) (Derivative growth) For any real number $x \in \mathcal{B} + [-1,1]$,

$$\sum_\mu |f'_\mu(x)|^2 \le C\left(N^{c_1} \sum_\mu |f_\mu(x)|^2\right), \tag{2.1}$$

as well as

$$\sup_{z \in B(x,1)} |f''_\mu(z)|^2 \le C\left(N^{c_1} \sum_\mu |f_\mu(x)|^2\right). \tag{2.2}$$

Note that the last conditions (4), (5) are about the deterministic functions f_μ, which automatically hold for trigonometric functions. Roughly speaking, the remaining Conditions 1, 2, and 3 guarantee that the number of roots in any local ball $B(x,1), x \in \mathcal{B}$ is not too large. Now we state the main result from [32].

Theorem 2.2 (Local universality of real roots)**.** [32, Theorem 2.5] *Let $k \ge 1$ be an integer constant and $\alpha_1, C_1, \varepsilon$ be positive constants. Assume that there exists a constant $C > 0$ such that the random functions H and $\widetilde{H}$ satisfy Condition 2.1 with parameters $(k, C_1, \alpha_1, A, c_1, C)$ for some constants $0 < c_1 \le \frac{\alpha_1 \varepsilon}{10^6 k^4}$ and $A \ge 2k(C_1+2) + \frac{\alpha_1\varepsilon}{6}$. Then there exists a constant c depending only on k and the constants in Conditions 1.9 and 2.1 (but not on $\mathcal{B}$ and N) such that the following holds. For any real numbers $x_1, \dots, x_k$ in $\mathcal{B}$, and for every smooth function G supported on $\prod_{j=1}^k [x_j - c, x_j + c]$ with $|\nabla^a G(z)| \le 1$ for $0 \le a \le 2k$ we have*

$$\left| \mathbb{E}_{\xi_\mu} \sum_{i_1,\dots,i_k} G(\zeta_{i_1}, \dots, \zeta_{i_k}) - \mathbb{E}_{\tilde{\xi}_\mu} \sum_{i_1,\dots,i_k} G(\tilde{\zeta}_{i_1}, \dots, \tilde{\zeta}_{i_k}) \right| \le \frac{1}{c} N^{-c}, \tag{2.3}$$

where the ζ_i are the roots of H, and the $\tilde{\zeta}_i$ are the roots of $\widetilde{H}$, the sums run over all possible assignments of $i_1, \dots, i_k$ which are not necessarily distinct.

Thus, heuristically, this theorem states that as long as the Condition 2.1 is satisfied, the k-wise correlation functions of the roots of H and $\tilde{H}$ in $\mathcal{B}$ are asymptotically the same.

We will provide a sketch of the proof of this theorem in Section 9 for the reader's convenience.

Now we consider F from (1.4). By the analyticity of the curve γ, there exists a constant $b > 0$ such that γ has analytic extension on $[0,1] + B(0,b)$. Let $b_\lambda = \max\{1/b, \lambda\}$. Set the scaled function $H : [0, b_\lambda] + B(0,1) \to$ to be

$$H(z) := F\left(\gamma\left(\frac{z}{b_\lambda}\right)\right) = \frac{1}{\sqrt{N}} \sum_{\mu \in \mathcal{E}_\lambda} \varepsilon_{1,\mu} g_\mu(z) + \varepsilon_{2,\mu} h_\mu(z) \tag{2.4}$$

where

$$g_\mu(z) := \cos\left(2\pi\left\langle \mu, \gamma\left(\frac{z}{b_\lambda}\right)\right\rangle\right) \quad \text{and} \quad h_\mu(z) := \sin\left(2\pi\left\langle \mu, \gamma\left(\frac{z}{b_\lambda}\right)\right\rangle\right) \tag{2.5}$$

To prove Theorems 1.10 and 1.13, the main task is to show that Condition 2.1 holds for H with an appropriate choice of the set $\mathcal{B}$. More specifically, for Theorem 1.13 we will show

Lemma 2.3. *Let k be a positive integer. Under the assumptions of Theorem 1.13, let $\mathcal{B}_1 = [0, b_\lambda]$. There exist positive constants c_k, A_k such that for any positive constants $c_1 < c_k$ and $A > A_k$, there exists a constant C for which the function H in* (2.4) *satisfies Condition 2.1 with $\mathcal{B} = \mathcal{B}_1, \alpha_1 = 1/2, C_1 = 1$, and $N = |\mathcal{E}_\lambda|$.*

(We would like to remind the reader that the constants in this manuscripts do not depend on $N, \mathcal{B}$, or λ.)

As the randomness here is smooth (i.e., the random variables have bounded, continuous density), our verification of this result (to be presented in Section 3) will be relatively short.

Next, for Theorem 1.10 we show

Lemma 2.4. *Under the assumptions of Theorem 1.10, let $\mathcal{B}_2 = [0, b_\lambda] \setminus \cup_{\varphi \in \mathcal{D}} (\lambda S_\varphi)$ where $\mathcal{D}$ is the set of directions*

$$\mathcal{D} = \left\{ \frac{\mu_1 - \mu_2}{\|\mu_1 - \mu_2\|}, \mu_1 \neq \mu_2, \mu_1, \mu_2 \in \mathcal{E}_\lambda \right\}$$

and

$$S_\varphi := \left\{ t \in [0,1], \angle(\gamma'(t), \varphi) < N^{-3} \right\}.$$

Then for any positive constants k, c_1, A, there exists a constant C for which the function H in (2.4) *satisfies Condition 2.1 with $\mathcal{B} = \mathcal{B}_2, \alpha_1 = 1/2, C_1 = 7$, and $N = |\mathcal{E}_\lambda|$.*

We refer the reader to Section 5 for the motivation of introducing $\mathcal{D}$ and S_φ as above. The verification of Lemma 2.4 (in Sections 4 and 5) will occupy the most technical part of our note: notably when we justify (1) and (2) from Condition 2.1.

Combining Theorem 2.2, Lemmas 2.3 and 2.4, we then show the following proposition, which in turn implies Theorems 1.10 and 1.13.

Proposition 2.5. *Let H be the function in* (2.4). *Under the assumptions of Theorem 1.13 (respectively Theorem 1.10), for any $k \geq 1$, there exists a constant $c > 0$ such that for any intervals $I_1, \dots, I_k \subset [0, b_\lambda]$ each belongs to $\mathcal{B}_1$ (respectively $\mathcal{B}_2$) and has length $O(1)$, we have*

$$\mathbb{E}_{\varepsilon_\mu} \prod_{j=1}^{k} \mathcal{Z}_j = \mathbb{E}_{\mathbf{g}} \prod_{j=1}^{k} \mathcal{Z}_j + O_k\left(N^{-c}\right)$$

where $N = |\mathcal{E}_\lambda|$ and $\mathcal{Z}_j$ is the number of roots of H in I_j.

The deduction of Proposition 2.5 from Lemmas 2.3 and 2.4 is given in Section 7. Theorems 1.10 and 1.13 are concluded from Proposition 2.5 in Section 8.

3. Proof of Lemma 2.3

In this section, we prove Lemma 2.3. Note that the random variables are assumed to satisfy Condition 1.9 (i), namely they are continuously distributed with bounded density. For notational convenience, we assume that λ is sufficiently large, and thus $b_\lambda = \lambda$. For small λ, the proof is similar. The analyticity of H on the ball $B(x, 1)$, $x \in \mathcal{B}$ in Condition 2.1(1) follows from our assumption on the analyticity of the curve γ.

3.1. **Verification of Condition 2.1**(2)**.** To prove Condition 2.1(2), it suffices to show that for any any $c_1, A > 0$, there exists a constant $C > 0$ such that for all $x_0 \in \mathcal{B}$, we have

$$\mathbb{P}\left(|H(x_0)| \geq \exp\left(-N^{c_1}\right)\right) \geq 1 - CN^{-A}. \tag{3.1}$$

For any $\delta > 0$ and any $\mu_0 \in \mathcal{E}_\lambda$, by conditioning on all other random variables except ε_{μ_0}, we can see that the probability that $|H(x_0)|$ is confined in an interval of size 2δ is bounded from above by the probability that $\varepsilon_{1,\mu_0} \cos(2\pi \langle \mu_0, \gamma(x_0/\lambda)\rangle) + \varepsilon_{2,\mu_0} \sin(2\pi\langle \mu_0, \gamma(x_0/\lambda)\rangle)$ is confined in an interval of size $2\sqrt{N}\delta$. From this and the continuity of ε_μ, we obtain

$$\mathbb{P}\left(|H(x_0)| \geq \delta\right) \quad \geq \quad 1 - O\left(\sqrt{N}\delta\right). \tag{3.2}$$

(Note that when $\sqrt{N}\delta$ is large, the last expression becomes negative and the inequality becomes trivial.) Let $\delta = \exp\left(-N^{c_1}\right)$, we obtain (3.1).

3.2. **Verification of Condition 2.1**(3)**.** For every $z \in [0, \lambda] \times [-1, 1]$, let $x = \mathrm{Re}(z)$. Since $\left\langle \mu, \gamma\left(\frac{x}{\lambda}\right)\right\rangle$ is real, we have

$$\left|\mathrm{Im}\left\langle \mu, \gamma\left(\frac{z}{\lambda}\right)\right\rangle\right| \leq \left|\left\langle \mu, \gamma\left(\frac{z}{\lambda}\right) - \gamma\left(\frac{x}{\lambda}\right)\right\rangle\right| = O(1), \tag{3.3}$$

and so

$$\left|\exp\left(i2\pi\left\langle \mu, \gamma\left(\frac{z}{\lambda}\right)\right\rangle\right)\right| = \exp\left(-2\pi \mathrm{Im}\left\langle \mu, \gamma\left(\frac{z}{\lambda}\right)\right\rangle\right) = O(1). \tag{3.4}$$

Thus,

$$|H(z)| = O(1) \sum_{\mu} |\varepsilon_\mu|.$$

By applying Markov's inequality to the random variable $\sum_\mu |\varepsilon_\mu|$, we obtain for any $M > 0$,

$$\mathbb{P}\left(|H(z)| \geq M \text{ for some } z \in [0, T] \times [-1, 1]\right) \leq \mathbb{P}\left(M = O\left(\sum_{\mu} |\varepsilon_\mu|\right)\right) = O\left(\frac{N}{M}\right). \tag{3.5}$$

Setting $M = e^{N^{c_1}}$, Condition 2.1(3) then follows. We remark that this condition holds even if the ε_μ have discrete distribution.

3.3. **Verification of Condition 2.1**(1)**.** Let $K = \max_{z \in B(x,1)} |H(z)|$. Recall the following Jensen's inequality for analytic functions (for a proof, see, for example, [32, Appendix 15.5]): for any $z \in, R > r > 0$, any analytic function ψ on an open domain that contains the closed disk $\bar{B}(z, R)$, the number of roots of ψ in the open disk $B(z, r)$ is bounded from above as follows.

$$\#\{w \in B(z, r) : \psi(w) = 0\} \leq \frac{\log \frac{M}{m}}{\log \frac{R^2 + r^2}{2Rr}} \tag{3.6}$$

where $M = \max_{w \in \bar{B}(z,R)} |\psi(w)|$, $m = \max_{w \in \bar{B}(z,r)} |\psi(w)|$.

By the Jensen's inequality (3.6), we obtain

$$\mathcal{Z}_{B(x,1/2)} = O(1) \log \frac{K}{|H(x)|}. \tag{3.7}$$

Let $\mathcal{A}$ be the event on which $\mathcal{Z}_{B(x,1/2)} \geq N^{C_1}$. By (3.7), the upper bound (3.5) on K and the lower bound (3.2) on H, we obtain

$$\mathbb{P}(\mathcal{A}) = O\left(N^{-10}\right).$$

Thus,

$$\mathbb{E}\mathcal{Z}^{k+2}_{B(x,1/2)} \mathbf{1}_{\mathcal{A}} \ll \mathbb{E}|\log K|^{k+2}\mathbf{1}_{\mathcal{A}} + \mathbb{E}|\log |H(x)||^{k+2}\mathbf{1}_{\mathcal{A}}. \tag{3.8}$$

By Hölder's inequality,

$$\mathbb{E}|\log K|^{k+2}\mathbf{1}_{\mathcal{A}} \leq \left(\mathbb{E}|\log K|^{2k+2}\right)^{1/2} \mathbb{P}(\mathcal{A})^{1/2}.$$

By the bound (3.5), we obtain $\mathbb{E}|\log K|^{k+2} = O_k(N)$ which yields

$$\mathbb{E}|\log K|^{k+2}\mathbf{1}_{\mathcal{A}} = O_k\left(N^{-9/2}\right). \tag{3.9}$$

We argue similarly for $\mathbb{E}|\log |H(x)||^{k+2}\mathbf{1}_{\mathcal{A}}$ using (3.2) (which is valid for all $\delta > 0$). From this and (3.8), (3.9), we obtain

$$\mathbb{E}\mathcal{Z}^{k+2}_{B(x,1/2)} \mathbf{1}_{\mathcal{Z}_{B(x,1/2)} \geq N^{C_1}} = O(1)$$

as claimed.

3.4. **Verification of Conditions 2.1**(4) **and 2.1**(5) **for** g_μ, h_μ**.** For Condition 2.1(4), note that for any $z \in (0, \lambda) + B(0,1)$ and g_μ, h_μ as in (2.5), we have

$$\sum_\mu (g_\mu(z))^2 + (h_\mu(z))^2 = N,$$

and so

$$\frac{|g_\mu(z)| + |h_\mu(z)|}{\sqrt{\sum_\mu |g_\mu(z)|^2 + |h_\mu(z)|^2}} = O\left(\frac{1}{\sqrt{N}}\right).$$

For (2.1) of Condition 2.1(5), we have

$$g'_\mu(z) = \frac{2\pi}{\lambda} \left\langle \mu, \gamma'\left(\frac{z}{\lambda}\right)\right\rangle \cos\left(2\pi \left\langle \mu, \gamma\left(\frac{z}{\lambda}\right)\right\rangle\right).$$

Thus

$$\sum_\mu |g'_\mu(z)|^2 + \sum_\mu |h'_\mu(z)|^2 \ll \sum_\mu \frac{1}{\lambda^2} \left\langle \mu, \gamma'\left(\frac{z}{\lambda}\right)\right\rangle^2 \ll N$$

where the implicit constant depends on $\max_{z\in[0,\lambda]} |\gamma'(\frac{z}{\lambda})|$. This proves (2.1). Finally, (2.2) of Condition 2.1(5) is proven similarly using the same argument together with (3.4).

4. Proof of Lemma 2.4: verification of Condition 2.1(2)

As the case when the random variables are continuously distributed has been treated in Section 3, here we will assume that

- there exist positive constants c_1, c_2, c_3 and K such that
$$\mathbb{P}\left(c_1 \le |\varepsilon_\mu - \varepsilon'_\mu| \le c_2\right) \ge c_3$$
- with probability one
$$|\varepsilon_\mu| > 1/K$$

where ε'_μ is an independent copy of ε_μ.

Since the verification of Conditions (3), (4) and (5) in Section 3 works automatically for this setting, it suffices to verify Conditions 2.1(1) and 2.1(2) only. In this section, we will verify Condition 2.1(2). In the next section, we will verify Condition 2.1(1).

Recall that $N = |\mathcal{E}_\lambda|$. Without scaling, we will show the following which implies Condition 2.1(2).

Theorem 4.1. *Let $A, \alpha, c_0 > 0$ be fixed constants, then there exists a constant C such that the following holds for $F(\gamma(t))$ from* (1.4)*: for any interval $I \subset [0,1]$ of length c_0/λ, for any $t_1, t_2 \in I$ with $\|\gamma(t_1) - \gamma(t_2)\| = \frac{N^{-\alpha}}{\lambda}$, we have*
$$\mathbb{P}\left(|F(\gamma(t_1))| \le N^{-C}\right) \le N^{-A} \quad \textit{or} \quad \mathbb{P}\left(|F(\gamma(t_2))| \le N^{-C}\right) \le N^{-A}.$$

Note that by Remark 1.8, for any interval I of length c_0/λ, there exist $t_1, t_2 \in I$ with $\|\gamma(t_1) - \gamma(t_2)\| = \frac{N^{-\alpha}}{\lambda}$.

Since $|F(\gamma(t))| \ge N^{-C}$ implies $|H(t)| \ge N^{-C} \gg \exp\left(-N^{-c_1}\right)$ for any positive constant c_1, Theorem 4.1 implies Condition 2.1(2). To prove Theorem 4.1 we will rely on two results on additive structures. For this we will need some definitions.

We say a set $S \subset \mathbb{C}$ is *δ-separated* if for any $s_1, s_2 \in S$, $|s_1 - s_2| \ge \delta$, and S is *ε-close* to a set P if for all $s \in S$, there exists $p \in P$ such that $|s - p| \le \varepsilon$.

Define a *generalized arithmetic progression* (or GAP) to be a finite subset Q of of the form
$$Q = \{g_0 + a_1 g_1 + \cdots + a_r g_r : a_i \in \mathbf{Z}, |a_i| \le N_i \text{ for all } i = 1, \ldots, r\}$$
where $r \ge 0$ is a natural number (the *rank* of the GAP), $N_1, \ldots, N_r > 0$ are positive integers (the *dimension lengths*, or *dimension* for short, of the GAP), and $g_0, g_1, \ldots, g_r \in$ are complex numbers (the *generators* of the GAP). We refer to the quantity $\prod_{i=1}^r (2N_i + 1)$ as the *volume* $\mathrm{vol}(Q)$ of Q; this is an upper bound for the cardinality $|Q|$ of Q. When $g_0 = 0$, we say that Q is *symmetric.* When $\sum_i a_i g_i$ are all distinct, we say that Q is *proper.*

Let ξ be a real random variable, and let $V = \{v_1, ..., v_n\}$ be a multi-set in $\mathbf{R}^d$. For any $r > 0$, we define the small ball probability as
$$\rho_{r,\xi}(V) := \sup_{x \in \mathbf{R}^d} \mathbb{P}\left(v_1 \xi_1 + \cdots + v_n \xi_n \in B(x, r)\right)$$

where $\xi_1, ..., \xi_n$ are iid copies of ξ, and $B(x, r)$ denotes the closed disk of radius r centered at x in $\mathbf{R}^d$.

We now cite the first useful ingredients.

Theorem 4.2. [30, Theorem 2.9] *Let $A > 0$ and $1/2 > \varepsilon_0 > 0$ be constants. Let $\beta > 0$ be a parameter that may depend on n. Suppose that $V = \{v_1, \dots, v_n\}$ is a (multi-) subset of $\mathbf{R}^d$ such that $\sum_{i=1}^n \|v_i\|^2 = 1$ and that V has large small ball probability*

$$\rho := \rho_{\beta,\xi}(V) \geq n^{-A},$$

where ξ is a real random variable satisfying Condition 1.9. Then the following holds: for any number $n^{\varepsilon_0} \leq n' \leq n$, there exists a proper symmetric GAP $Q = \{\sum_{i=1}^r x_i g_i : |x_i| \leq L_i\}$ such that

- *at least $n - n'$ elements of V are $O(\beta)$-close to Q,*
- *Q has constant rank $d \leq r = O(1)$, and cardinality*

$$|Q| = O\left(\rho^{-1} n'^{(-r+d)/2}\right).$$

Here the implicit constants are allowed to depend on the parameters A and ε_0.

Our second ingredient is a continuous analog of [13] by the first author, in connection with the "sum-product" phenomenon in additive combinatorics (see also [20].)

Theorem 4.3. *Let $P = \{g_0 + \sum_{i=1}^r n_i g_i : |n_i| < M\}$ be a generalized arithmetic progression of rank r on the complex plane. Then there exists an (explicit) constant C_r with the following property. Let $0 < \delta < 1$ and $\varepsilon < M^{-C_r}\delta^{C_r}$ and let $S \subset P$ be a subset consisting of elements which are δ-separated and ε-close to the unit circle, then*

$$S \leq \exp\left(C_r \log M / \log\log M\right).$$

We postpone the proof of Theorem 4.3 to the next subsection.

Proof of Theorem 4.1. First fix $t \in I$, and let $x = \gamma(t)$. Set $\beta = N^{-C}$, with C sufficiently large to be chosen, and assume that

$$\mathbb{P}\left(\left|\sum_{\mu\in\mathcal{E}_\lambda} \varepsilon_{1,\mu}\cos(2\pi\langle\mu, x\rangle) + \varepsilon_{2,\mu}\sin(2\pi\langle\mu, x\rangle)\right| \leq \beta\right) \geq N^{-A}. \tag{4.1}$$

We will choose ε_0 to be the constant in Lemma 1.11. Then by Theorem 4.2 (applied to the sequences $\{\cos(2\pi\langle\mu, x\rangle), \mu \in \mathcal{E}_\lambda\}$ and $\{\sin(2\pi\langle\mu, x\rangle), \mu \in \mathcal{E}_\lambda\}$ separately [1] with $n' = N^{\varepsilon_0}$), there exist proper GAPs $P_1, P_2 \subset \mathbf{R}$ and $|\mathcal{E}_\lambda| - 2n'$ indices $\mu \in \mathcal{E}_\lambda$ such that with $z_\mu(t) = \cos(2\pi\langle\mu, x\rangle) + i\sin(2\pi\langle\mu, x\rangle) = \exp(2\pi i\langle\mu, \gamma(t)\rangle)$,

$$\mathrm{dist}\left(z_\mu(t), P_1 + iP_2\right) \leq 2\beta$$

[1] We condition on $\varepsilon_{1,\mu}$ to obtain structure approximation for the sine sequence, and then condition on $\varepsilon_{2,\mu}$ to obtain structure approximation for the cosine sequence.

and such that the cardinalities of P_1 and P_2 are $O\left(N^{O_A(1)}\right)$ and the ranks are $O(1)$. The properness implies that the dimensions of the GAPs P_1 and P_2 are bounded by $O\left(N^{O_A(1)}\right)$.

For short, we denote the complex GAP $P_1 + iP_2$ by $P(t)$.

Now assume by contradiction that (4.1) holds for both $t = t_1$ and $t = t_2$. By applying the above process to t_1 and t_2, we obtain two GAPs $P(t_1)$ and $P(t_2)$ which are 2β-close to the points $z_\mu(t_1)$ and $z_\mu(t_2)$ respectively for at least $N - 4N^{\varepsilon_0}$ indices μ.

Since the $z_\mu(t_1)$ and $z_\mu(t_2)$ have magnitude 1, the product set

$$P(t_1)\bar{P}(t_2) = \{p_1\bar{p_2}, p_1 \in P_1(t), p_2 \in P_2(t)\}$$

will $O(\beta)$-approximate the points $z_\mu = z_\mu(t_1)\bar{z}_\mu(t_2) = \exp(2\pi\langle\mu, \gamma(t_1) - \gamma(t_2)\rangle)$ for at least $N - 4N^{\varepsilon_0}$ indices μ. Let $\mathcal{S}$ be the collection of these points z_μ.

By definition, $P = P(t_1)\bar{P}(t_2)$ is another GAP whose rank is $O(1)$ and dimensions are of order $O\left(N^{O_A(1)}\right)$.

Now we look at the set $\mathcal{S}$. On one hand, $\mathcal{S}$ is "closed" under multiplication in the sense that $|z_{\mu_1}z_{\mu_2}| = 1$ for all μ_1, μ_2. On the other hand, as z_μ can be well approximated by elements of a GAP of small size, the collection of sums $z_{\mu_1} + z_{\mu_2}$ can also be approximated by another GAP of small size. As such, we can apply Theorem 4.3 with $\varepsilon = O(\beta)$, $r = O_A(1)$, and $M = O\left(N^{O_A(1)}\right)$ to conclude that the set $\mathcal{S}$ can be covered by $\exp(C_r \log N/\log\log N)$ disks of radius δ with $\delta = M\varepsilon^{1/C_r}$. Taking into account at most $4N^{\varepsilon_0}$ elements z_μ not included in $\mathcal{S}$, the set $\{\langle\mu, \gamma(t_1) - \gamma(t_2)\rangle\}_{\mu\in\mathcal{E}}$ can be covered by $4N^{\varepsilon_0} + \exp(C_r \log N/\log\log N) \leq 5N^{\varepsilon_0}$ intervals of length $O(\delta)$. However, note that

$$\delta = M\varepsilon^{1/C_r} = O\left(N^{-C/C_r + O_A(1)}\right).$$

By choosing C sufficiently large, this would contradict with the equi-distribution Lemma 1.11 on $\mathcal{E}$. The proof of Theorem 4.1 is complete. □

4.1. **Proof of Theorem 4.3.** We will need some preparations. In this subsection C_r is a constant depending on r and may vary even within the same context. We denote the set of the coefficient vectors of S by

$$\mathcal{F} = \left\{\bar{n} = (n_1, \ldots, n_r) \in \mathbb{Z}^r : |n_i| < M, g_0 + \sum_{i=1}^r n_i g_i \in S\right\}.$$

Fix $\bar{m} \in \mathcal{F}$. Since $g_0 + \sum_{i=1}^r m_i g_i$ is ε-close to the unit circle, we have $|g_0 + \sum_{i=1}^r m_i g_i| \leq 1 + \varepsilon$ and

$$\left|\sum_{i=1}^r (n_i - m_i) g_i\right| \leq 2(1+\varepsilon) \quad \text{for all } \bar{n} \in \mathcal{F}. \tag{4.2}$$

Let $\langle\mathcal{F} - \bar{m}\rangle$ be the vector space generated by $\bar{n} - \bar{m}, \bar{n} \in \mathcal{F}$. We assume $\dim\langle\mathcal{F} - \bar{m}\rangle = r$, since otherwise we may reduce the rank of P without significantly changing the size of P (see [40, Chapter 3]).

Therefore, we can take r independent vectors $\bar{n}^{(1)}, \cdots, \bar{n}^{(r)} \in \mathcal{F}$ and use Cramer's rule to solve $g_1, \cdots, g_r$ in the following system of r equations.

$$\begin{gathered}(n_1^{(1)} - m_1)g_1 + \cdots + (n_r^{(1)} - m_r)g_r = c^{(1)} \\ \cdots \\ \cdots \\ \cdots \\ (n_1^{(r)} - m_1)g_1 + \cdots + (n_r^{(r)} - m_r)g_r = c^{(r)}\end{gathered}$$

where $|c^{(1)}|, \cdots, |c^{(r)}| \leq 2(1+\varepsilon) < 3$.

We obtain a bound

$$|g_1|, \ldots, |g_r| \leq 3.2^r r! M^{r-1}, \tag{4.3}$$

and hence

$$|g_0| < \sum_i |n_i g_i| + 1 + \varepsilon < (3r)2^r r! M^r. \tag{4.4}$$

Next, assume that $|\mathcal{F}| \geq 2$. Then the separation assumption means that for any $\bar{m}, \bar{n} \in \mathcal{F}$ with $\bar{m} \neq \bar{n}$ we have $|\sum_{i=1}^r (m_i - n_i) g_i| > \delta$. Thus,

$$\max \{|g_1|, \ldots, |g_r|\} > \frac{\delta}{2rM}. \tag{4.5}$$

Without loss of generality, assume that the maximum above is attained by $|g_1|$. We now introduce the key lemma toward the verification of Theorem 4.3.

Lemma 4.4. *There exist $z_0, z_1, \ldots, z_r, w_0, w_1, \ldots, w_r \in \mathbb{C}$ with $z_1 \neq 0$ such that for any $\bar{n} \in \mathcal{F}$*

$$\left(z_0 + \sum_{i=1}^r n_i z_i\right)\left(w_0 + \sum_{i=1}^r n_i w_i\right) = 1.$$

We now conclude Theorem 4.3 using this lemma.

Proof of Theorem 4.3. Let

$$\mathcal{A} = \left\{z_0 + \sum_{i=1}^r n_i z_i : \bar{n} \in \mathcal{F}\right\}.$$

Applying Proposition 3 in [13] to the mixed progression

$$\left\{n_0 z_0 + n_0 w_0 + \sum_{i=1}^r n_i z_i + \sum_{i=1}^r n_i' w_i : |n_0|, |n_0'| < 2 \text{ and } |n_i|, |n_i'| < M\right\},$$

we have

$$|\mathcal{A}| \leq \exp(D_r \log M / \log\log M),$$

for some positive constant D_r.

We next partition $\mathcal{F}$ as

$$\mathcal{F} = \bigcup_{a\in\mathcal{A}} \mathcal{F}_a, \text{ where } \mathcal{F}_a = \left\{ \bar{n} \in \mathcal{F} : z_0 + \sum_{i=1}^{r} n_i z_i = a \right\}.$$

Let S be as in Theorem 4.3, we write

$$S = \left\{ g_0 + \sum_{i=1}^{r} n_i g_i : \bar{n} \in \mathcal{F} \right\} = \bigcup_{a\in\mathcal{A}} S_a, \tag{4.6}$$

where

$$S_a := \left\{ g_0 + \sum_{i=1}^{r} n_i g_i : \bar{n} \in \mathcal{F}_a \right\}.$$

Notice that $S_a \subset P_a := \{g_0 + \sum_{i=1}^r n_i g_i \in P : z_0 + \sum_{i=1}^r n_i z_i = a\}$. The gain here is that P_a is contained in a progression of rank at most $r-1$, that is,

$$g_0 + \sum_{i=1}^{r} n_i g_i = \left(g_0 + \frac{a-z_0}{z_1} g_1 \right) + \sum_{i=2}^{r} n_i \left(g_i - \frac{z_i}{z_1} g_1 \right)$$

so by induction

$$|S_a| \le \exp(C_{r-1} \log M / \log\log M).$$

It thus follows from (4.6) that

$$|S| \le \exp(C_r \log M / \log\log M),$$

for some appropriately chosen constant sequence C_r, completing the proof of Theorem 4.3. □

It remains to verify Lemma 4.4. We will use the following effective form of Nullstellensatz from [26] (see also [14, Theorem 2]).

Theorem 4.5. *Let $q, f_1, \dots, f_s \in \mathbb{Z}[x_1, \dots, x_n]$ with $\deg q, \deg f_i \le d$ for all i such that q vanishes on the common zeros of $f_1, \cdots, f_s$ and $\mathbf{ht}(f_i) \le H$. Then there exist $q_1, \dots, q_s \in \mathbb{Z}[x_1, \dots, x_n]$ and positive integers b, l such that*

$$b\, q^l = \sum_{i=1}^{s} q_i f_i \tag{4.7}$$

where

$$l \le D = \max_{1\le i\le s} \{\deg q_i\} \le 4nd^n$$

as well as

$$\max_{1\le i\le s} \{\log|b|, \mathbf{ht}(q_i)\} \le 4n(n+1)d^n \left[H + \log s + (n+7)d\log(n+1)\right].$$

Here the height $\mathbf{ht}(f)$ of a polynomial $f \in \mathbf{Z}[x_1, \dots, x_n]$ is the logarithm of the maximum modulus of its coefficients.

Remark. Theorem 1 in [26] is stated for the case that $q = 1$ and that $f_1, \dots, f_s$ do not have common zeros. However, the standard proof of Nullstellensatz gives the above statement of Theorem 4.5.

Proof of Lemma 4.4. Define the polynomial P over $\bar{n} \in \mathcal{F}$ as

$$P_{\bar{n}}(z_0, z_1, \dots, z_r, w_0, w_1, \dots, w_r) = \left(z_0 + \sum_{i=1}^{r} n_i z_i\right)\left(w_0 + \sum_{i=1}^{r} n_i w_i\right) - 1.$$

Assume that the claim of Lemma 4.4 does not hold, thus the polynomials $P_{\bar{n}}, \bar{n} \in \mathcal{F}$ have no common zeros with $z_1 \neq 0$.

By Theorem 4.5, with $n = 2r+2, s = |\mathcal{F}| \leq (2M)^r, d = 2, H \leq 2\log M$ we have

$$b z_1^l = \sum_{\bar{n} \in \mathcal{F}} P_{\bar{n}} Q_{\bar{n}}, \tag{4.8}$$

where $b \in \mathbb{Z}\backslash\{0\}$, $Q_{\bar{n}} \in \mathbb{Z}[z_0, \dots, z_r, w_0, \dots, w_r]$ such that

- $\deg(Q_{\bar{n}}), l \leq D \leq C_r'$
- the coefficients of $Q_{\bar{n}}$ are bounded by $M^{C_r'}$.

Now replacing $z_0, \dots, z_r$ and $w_0, \dots, w_r$ by $g_0, \dots, g_r$ and $\bar{g}_0, \dots, \bar{g}_r$ in (4.8), we have

$$|g_1|^l \leq \sum_{\bar{n} \in \mathcal{F}} |P_{\bar{n}}(g_0, \dots, g_r, \bar{g}_0, \dots, \bar{g}_d)| \; |Q_{\bar{n}}(g_0, \dots, g_r, \bar{g}_0, \dots, \bar{g}_d)| \, .$$

By (4.3), (4.4), (4.5) we then have

$$\left(\frac{\delta}{2rM}\right)^l \leq D M^{C_r'} (3.2^r r! r M^r)^D \sum_{\bar{n} \in \mathcal{F}} |P_{\bar{n}}(g_0, \dots, g_r, \bar{g}_0, \dots, \bar{g}_r)|.$$

On the other hand, by definition, $|P_{\bar{n}}(g_0, \dots, g_r, \bar{g_0}, \dots, \bar{g}_r)| \leq \varepsilon$ for any $\bar{n} \in \mathcal{F}$. It thus follows that

$$\left(\frac{\delta}{2rM}\right)^l \leq \left(\frac{\delta}{2rM}\right)^D \leq M^{C_r''} \varepsilon.$$

However, this is impossible with the choice of ε from Theorem 4.3, completing the proof of Lemma 4.4. □

5. Proof of Lemma 2.4: verification of Condition 2.1(1)

Let $\kappa = N^{-3}$. We will verify Condition 2.1(1) through the following deterministic lemma, which seems to be of independent interest.

Theorem 5.1. *Suppose that $\gamma(t), t \in [0,1]$ is smooth and has non-vanishing curvature. Then there exist a constant c and a collection of at most N^2 intervals S_α each of length $O(\kappa)$ such that the following holds for almost all λ and for any eigenfunction $\Phi(x) = \sum_{\mu \in \mathcal{E}_\lambda} a_\mu e^{2\pi i \langle \mu, x \rangle}$ with $\sum_\mu |a_\mu|^2 = 1$.*

(1) The number of nodal intersections on $\cup S_\alpha$ is negligible

$$|N_\Phi \cap \cup\gamma(S_\alpha)| \ll \lambda N^{-1},$$

(2) Condition 2.1(1) on $[0,1] \setminus \cup S_\alpha$: for any $a \in [0,1] \backslash \cup_\alpha S_\alpha$, we have

$$|\left\{z \in B(a, N^7/\lambda) : \Phi(\gamma(z)) = 0\right\}| \ll N^7.$$

We will prove Theorem 5.1 by relying on Lemma 5.2, Lemma 5.3, and Lemma 5.4 below.

Lemma 5.2. *Let $\varepsilon_0 > 0$ be given. Then for almost all λ we have*

$$\min_{\mu_1 \neq \mu_2 \in \mathcal{E}_\lambda} \|\mu_1 - \mu_2\| \gg \frac{\lambda}{\log^{3/2+\varepsilon_0} \lambda}. \tag{5.1}$$

We also refer the reader to [6, Lemma 5]) for related estimates.

Proof of Lemma 5.2. Let R be a parameter and $M = R(\log R)^{-3/2-\varepsilon_0}$. Then

$$\begin{aligned}
&\left|\left\{(x,y) \in \mathbf{Z}^2 \times \mathbf{Z}^2 : \|x\| = \|y\| \leq R, 0 < \|x-y\| < M\right\}\right| \\
&= \sum_{v \in \mathbf{Z}^2 \backslash \{0\}, \|v\| < M} \left|\left\{x \in \mathbf{Z}^2 : \|x\| = \|x+v\| \leq R\right\}\right| \\
&= \sum_{v \in \mathbf{Z}^2 \backslash \{0\}, \|v\| < M} \left|\left\{\|x\| \leq R : 2\langle x, v\rangle + \|v\|^2 = 0\right\}\right| \\
&\leq \sum_{v \in \mathbf{Z}^2 \backslash \{0\}, \|v\| < M} \left|\{\|y\| \leq 3R : y_1 v_1 + y_2 v_2 = 0\}\right|, \qquad (5.2)
\end{aligned}$$

where $x = (x_1, x_2), v = (v_1, v_2)$ and $y = (y_1, y_2) = 2x + v$.

Now if $v_2 = 0$ then $y_1 = 0$. The contribution to the sum (5.2) is $O(MR)$. Similarly for $v_1 = 0$. For the other case that $v_1, v_2 \neq 0$, let $d = \gcd(v_1, v_2)$. Then $(v_1, v_2) = d(v_1', v_2')$ with $\gcd(v_1', v_2') = 1$. The equation $y_1 v_1' + y_2 v_2' = 0$ has $O\left(R/\|v'\|\right)$ solutions in y with $\|y\| < 3R$.

So by the Abel's summation formula, with $r_2(n)$ being the number of ways to represent n as a sum of two squares $a^2 + b^2, a, b \in \mathbf{Z}$, we have

$$\begin{aligned}
&\sum_{v \in \mathbf{Z}^2 \backslash \{0\}, \|v\| < M} \left|\{\|y\| \leq 3R : y_1 v_1 + y_2 v_2 = 0\}\right| \\
&\ll MR + \sum_{d < R} \sum_{v' \in \mathbf{Z}^2 \backslash \{0\}, \|v'\| < M/d} R/\|v'\| = MR + R \sum_{d<R} \sum_{n=1}^{M^2/d^2} \frac{r_2(n)}{\sqrt{n}} \\
&= MR + R \sum_{d<R} \left[\frac{\sum_{n=1}^{M^2/d^2} r_2(n)}{M/d} + \sum_{N=1}^{M^2/d^2-1} \left(\sum_{n=1}^{N} r_2(n)\right)\left(\frac{1}{\sqrt{N}} - \frac{1}{\sqrt{N+1}}\right)\right].
\end{aligned}$$

By Gauss' formula $\sum_{n=0}^{x} r_2(n) = (\pi + o(1))x$ we have

$$\sum_{v \in \mathbf{Z}^2 \backslash \{0\}, \|v\| < M} \left|\{\|y\| \leq 3R : y_1 v_1 + y_2 v_2 = 0\}\right| \ll R \sum_{d<R} \frac{M}{d} \ll MR \log R. \tag{5.3}$$

Combining Equations (5.2) and (5.3) we obtain

$$\left|\left\{(x,y) \in \mathbf{Z}^2 \times \mathbf{Z}^2 : \|x\| = \|y\| \leq R, 0 < \|x-y\| < M\right\}\right| \ll MR \log R.$$

On the other hand,

$$\left|\left\{(x,y) \in \mathbf{Z}^2 \times \mathbf{Z}^2 : \|x\| = \|y\| \leq R, 0 < \|x-y\| < M\right\}\right| \geq \sideset{}{'}\sum_{E < R^2} \mathbf{1}_{\min\{\|x-y\|, \|x\|^2 = \|y\|^2 = E, x \neq y\} < M},$$

where $\sum'$ is the sum over E of sum of two squares, and also note that by a classical result of Landau [28]

$$\left|\{E \in \mathbf{Z}, E < R^2, E = \text{sum of two squares}\}\right| = \Theta(R^2/\sqrt{\log R}).$$

Thus for almost all $E \leq R^2$ that are sum of two squares, with $M = R(\log R)^{-3/2-\varepsilon_0}$,

$$\min\left\{\|x-y\|, \|x\|^2 = \|y\|^2 = E, x \neq y\right\} \geq M \gg R(\log R)^{-3/2-\varepsilon_0} \gg \sqrt{E}(\log E)^{-3/2-\varepsilon_0}.$$

□

Now we consider Φ as in Theorem 5.1. Recall that by Condition 1.7(i), the curve γ has an analytic continuation to $[0,1] + B(0,\varepsilon) \subset$ for a sufficiently small ε. Arguing as in Sections 3.2 and 3.3, we get the following.

Lemma 5.3. *Let I be any interval with length $\delta = |I| < \varepsilon/2$. Then*

$$|\{z \in I + B(0,\delta) : \Phi(\gamma(z)) = 0\}| \leq C\lambda\delta + \log N - \log\max_{t\in I}|\Phi(\gamma(t))|.$$

Proof of Lemma 5.3. For $z \in I + B(0,2\delta), \exists t \in \mathbf{R}$ such that $|z-t| < 2\delta$,

$$|\gamma(z) - \gamma(t)| \leq c\delta.$$

Hence for $\mu \in \mathcal{E}_\lambda$,

$$\left|e^{i\langle\mu,\gamma(z)\rangle}\right| = \left|e^{i\langle\mu,\gamma(z)-\gamma(t)\rangle}\right| \leq e^{c\lambda\delta}.$$

Therefore

$$|\Phi(\gamma(z))| \leq \left(\sum_{\mu\in\mathcal{E}_\lambda}|a_\mu|\right)e^{c\lambda\delta} < \sqrt{N}e^{c\lambda\delta}.$$

The Jensen's inequality (3.6) then implies

$$\begin{aligned}|\{z \in I + B(0,\delta), \Phi(\gamma(z)) = 0\}| &\leq \log\left(\sqrt{N}e^{c\lambda\delta}\right) - \log\max_{t\in I}|\Phi(\gamma(t))| \\ &\leq c\lambda\delta + \log N - \log\max_{t\in I}|\Phi(\gamma(t))|.\end{aligned}$$

□

To make use of Lemma 5.3 we want to bound the quantity $\max_{t\in I}|\Phi(\gamma(t))|$.

Lemma 5.4. *We have*

$$\frac{1}{|I|}\int_I|\Phi(\gamma(t))|^2dt \geq 1/2,$$

provided that λ satisfies (5.1) *of Lemma 5.2 and*

$$|I| > \lambda^{-1/2}(\log\lambda)^{3/4+\varepsilon}N.$$

Proof of Lemma 5.4. We write

$$\int_I |\Phi(\gamma(t))|^2 \, dt = \int_I \left| \sum_\mu a_\mu e^{2\pi i \langle \mu, \gamma(t)\rangle} \right|^2 dt = |I| + \sum_{\mu \neq \mu'} a_\mu \bar{a}_{\mu'} \int_I e^{2\pi i \langle \mu - \mu', \gamma(t)\rangle}$$

$$\geq |I| - \sum_{\mu \neq \mu'} |a_\mu||a_{\mu'}| \left| \int_I e^{2\pi i \langle \mu - \mu', \gamma(t)\rangle} \right|.$$

By van der Corput's lemma on oscillatory integral (see for instance [37], and also [8] for related settings),

$$\left| \int_I e^{2\pi i \langle \mu - \mu', \gamma(t)\rangle} dt \right| \leq \frac{1}{\|\mu - \mu'\|^{1/2}}.$$

Hence

$$\int_I |\Phi(\gamma(t))|^2 \, dt \geq |I| - \frac{\log^{3/4+\varepsilon} \lambda}{\lambda^{1/2}} N \gg |I|/2.$$

□

Last but not least, we will need another elementary observation that will be useful for the proof of Theorem 5.1. Recall the set of directions from Lemma 2.4,

$$\mathcal{D} = \left\{ \frac{\mu_1 - \mu_2}{\|\mu_1 - \mu_2\|}, \mu_1 \neq \mu_2, \mu_1, \mu_2 \in \mathcal{E}_\lambda \right\}.$$

We partition $[0,1]$ as follows: for every unit direction φ, let S_φ be the interval of t where the angle between $\gamma'(t)$ and φ is smaller than κ

$$S_\varphi := \left\{ t \in [0,1], \angle(\gamma'(t), \varphi) < \kappa \right\}.$$

Lemma 5.5. *Assume that the arc-length parametrized curve $\gamma(t)$ has curvature bounded from below by some $c > 0$ for all t. Then for each φ, S_φ is an interval and has size $O(\kappa)$, where the implied constant depends on c.*

Proof of Lemma 5.5. Let $a(t)$ be the angle between $\gamma'(t)$ and φ. Then the curvature of γ at t is $|a'(t)|$ by definition. By continuity, the assumption that γ has curvature bounded from below by c implies that either $a'(t) \geq c$ for all t or $a'(t) \leq -c$ for all t. In either case, the claim follows. □

Let $J = [0,1] \setminus \cup_{\varphi \in \mathcal{D}} S_\varphi$. We note that J depends on $\mathcal{E}_\lambda$ and γ but not on Φ. We now prove the main result of this section.

Proof of Theorem 5.1. We first bound $|N_\Phi \cap \cup \gamma(S_\varphi)|$. As $\kappa > \lambda^{-1/2} (\log \lambda)^{3/4+\varepsilon} N$, the condition of Lemma 5.4 holds. Thus

$$\max_{t \in S_\varphi} |\Phi(\gamma(t))| \geq \frac{1}{|S_\varphi|} \int_{S_\varphi} |\Phi(\gamma(t))|^2 dt \geq 1/2.$$

Lemma 5.3 implies that

$$|N_\Phi \cap \gamma(S_\varphi)| \ll \kappa\lambda + \log N - c \ll \kappa\lambda.$$

Hence

$$|N_\Phi \cap \cup_\varphi \gamma(S_\varphi)| \ll N^2 \kappa \lambda \ll \lambda N^{-1}$$

proving (1) of Theorem 5.1.

Now for (2) of Theorem 5.1, let $a \in J$, and let $\delta = N^7/\lambda$, $M = N^7$. Denote also $\tilde{I} = [a-\delta, a+\delta]$. Our analysis again starts with Lemma 5.3, which in turn implies that for $\delta = M/\lambda \le \lambda^{-1+\varepsilon}$

$$\begin{aligned} |\{z \in B(a,\delta) : \Phi(\gamma(z)) = 0\}| &\le \left|\left\{z \in \tilde{I} + B(0,\delta) : \Phi(\gamma(z)) = 0\right\}\right| \\ &\le cM + \log N - \log \max_{t \in \tilde{I}} |\Phi(\gamma(t))|. \end{aligned} \tag{5.4}$$

In what follows we will bound $\max_{t\in\tilde{I}} |\Phi(\gamma(t))|$ from below. We are going to do this by an averaging argument.

First, with $\delta = M/\lambda \le \lambda^{-1+\varepsilon}$ and $t = a + \tau$, by Taylor's expansion

$$\langle \mu - \mu', \gamma(t)\rangle = \langle \mu - \mu', \gamma(a)\rangle + \langle \mu - \mu', \gamma'(a)\tau\rangle + O\left(\|\mu - \mu'\|\delta^2\right). \tag{5.5}$$

Since $a \in J, \angle(\gamma'(a), \varphi) \ge \kappa$ for all $\varphi \in \mathcal{D}$. So for any $\mu \neq \mu'$,

$$\left|\langle \mu - \mu', \gamma'(a)\rangle\right| \ge \kappa \|\mu - \mu'\| \gg \delta \|\mu - \mu'\|. \tag{5.6}$$

We thus have

$$\frac{1}{|\tilde{I}|}\left|\int_{\tilde{I}} e^{i\langle(\mu-\mu'),\gamma'(a)\tau\rangle} d\tau\right| \ll \frac{1}{\delta|\langle(\mu-\mu'),\gamma'(a)\rangle|} \ll \frac{1}{\delta\kappa\|\mu-\mu'\|} = \frac{\lambda}{M\kappa\|\mu-\mu'\|}.$$

On the other hand, Lemma 5.2 says that $\|\mu - \mu'\| \gg \frac{\lambda}{\log^{3/2+\varepsilon}\lambda}$. Therefore, with sufficiently large λ, and by (5.5) and (5.6)

$$\frac{1}{|\tilde{I}|}\left|\int_{\tilde{I}} e^{i\langle(\mu-\mu'),\gamma(t)\rangle} dt\right| \le \frac{1}{|\tilde{I}|}\left|\int_{\tilde{I}} e^{i\langle(\mu-\mu'),\gamma'(a)\tau\rangle} d\tau\right| + O\left(\|\mu-\mu'\|\delta^2\right) \le \frac{N^3 \log^{3/2+\varepsilon}\lambda}{M}.$$

This leads to the bound

$$\frac{1}{|\tilde{I}|}\left|\int_{\tilde{I}} |\Phi(\gamma(t))dt\right|^2 \ge 1 - \sum_{\mu\neq\mu'} |a_\mu||a'_\mu| \frac{1}{|\tilde{I}|}\left|\int_{\tilde{I}} e^{i\langle(\mu-\mu'),\gamma(t)\rangle} dt\right| \ge 1/2.$$

So

$$\max_{t\in\tilde{I}} |\Phi(\gamma(t))| > 1/\sqrt{2}.$$

Plugging this bound back to Equation (5.4), we then obtain (2) of Theorem 5.1. □

6. Proof of Lemma 1.11

As Lemma 1.11 is on the angles α_μ of the vectors $(\mu_1, \mu_2) = \sqrt{m}e^{2\pi i \alpha_\mu}$ in $\mathcal{E}_\lambda$, it suffices to restrict to the set $G(x)$ of m of prime factors congruent with 1 modulo 4 (see [19]). Indeed, let D^2 denote the product of prime factors that are congruent with 3 modulo 4 of m, then in any representation of m as $a^2 + b^2$, we have $D|a$ and $D|b$, so that D does not affect the angles. Moreover, none of these angles is influenced by the power of 2 dividing m because if this power is even, the angles are unchanged and if it is odd there is a rotation by $\pi/4$. We define the discrepancy of the angles α_μ of the vectors (μ_1, μ_2) in $\mathcal{E}_\lambda$ as follows

$$\Delta_m = \max\left\{\left|\#\left\{\alpha_\mu \in [\alpha_1, \alpha_2] \mod 1, \mu \in \mathcal{E}_\lambda\right\} - (\alpha_1 - \alpha_2) r_2(m)\right|, 0 \le \alpha_1 \le \alpha_2 \le 1\right\}.$$

Denote also

$$R_0(x) = (A + o(1))\,\frac{x}{\sqrt{\log x}} \quad \text{and} \quad A = \frac{1}{2\sqrt{2}} \prod_p \left(1 - \frac{1}{p^2}\right)^{1/2}.$$

Note that $R_0(x)$ is the number of $m \le x$ whose prime divisors are congruent with 1 mod 4 (see again [19]). Lemma 1.11 will easily follows from the following result by Erdős and Hall or Kátai and Környei.

Theorem 6.1. [19, 25] *Let $\varepsilon > 0$ be fixed. Then for all but $o\left(R_0(x)\right)$ integers $m \in G(x)$ we have*

$$\Delta_m < \frac{r_2(m)}{(\log x)^{\frac{1}{2}\log\frac{\pi}{2}-\varepsilon}}. \tag{6.1}$$

Proof of Lemma 1.11. Assume otherwise that for some $r \in \mathbf{R}^2$ with $|r| = \frac{1}{2\pi\lambda}$, the set $\{\langle \mu, r\rangle, \mu \in \mathcal{E}_\lambda\}$ can be covered by $k = O\left(N^{\varepsilon_0}\right)$ intervals $I_1, \dots, I_k$ of length $\beta = N^{-1}$ each in $[0,1]$. Consider the disjoint intervals $J_j = (j/3k, (j+1)/3k), 0 \le j \le 3k-1$. Let $\varepsilon_0 < 1$. As each interval $I_i, 1 \le i \le k$, intersects with at most two intervals J_{i_1}, J_{i_2}, there is one interval J_{j_0} which has no intersection with all $I_1, \dots, I_k$. Thus there is no $\mu \in \mathcal{E}_\lambda$ such that

$$\langle \mu, r\rangle \in J_{j_0}. \tag{6.2}$$

On the other hand, with $\varepsilon = .001$, Theorem 6.1 applied to a translation $[\alpha_1, \alpha_2]$ of J_{j_0} implies that the number of $\mu \in \mathcal{E}_\lambda$ with $\langle \mu, r\rangle \in J_{j_0}$ is at least

$$N|J_{j_0}| - \frac{r_2(m)}{(\log x)^{\frac{1}{2}\log\frac{\pi}{2}-\varepsilon}} = \frac{N}{3k} - \frac{N}{(\log x)^{\frac{1}{2}\log\frac{\pi}{2}-\varepsilon}}.$$

Moreover, since $\sum_{m \le x} r_2(m) = (\pi + o(1))x$, for almost all $m \in G(x)$ we have $N = r_2(m) \ll \log^{O(1)}(x)$. Hence automatically in this case $k = N^{\varepsilon_0} = o\left((\log x)^{\frac{1}{2}\log\frac{\pi}{2}-\varepsilon}\right)$, and so the above sum is strictly positive. In other words, J_{j_0} would contain at least one point of the set $\{\langle \mu, r\rangle, \mu \in \mathcal{E}_\lambda\}$, a contradiction with (6.2).

□

7. Proof of Proposition 2.5

Proof of Proposition 2.5. Under the assumptions of Theorem 1.13, we deduce Proposition 2.5 from Theorem 2.2 and Lemma 2.3. The deduction of Proposition 2.5 from Theorem 2.2 and Lemma 2.4 under the setting of Theorem 1.10 is completely analogous.

By Lemma 2.3, Theorem 2.2 holds for the random function H. Let $l_j = |I_j| = O(1)$. Let c be the constant in Theorem 2.2, and let α be a sufficiently small constant depending on c and k. Let G_j be a smooth function that approximates the indicator function $\mathbf{1}_{[-l_j/2, l_j/2]}$; in particular, let G_j be supported on $[-l_j/2 - N^{-\alpha}, l_j/2 + N^{-\alpha}]$ such that $0 \le G_j \le 1$, $G_j = 1$ on $[-l_j/2, l_j/2]$.

$$\|\nabla^a G_j\| \le C N^{C\alpha}, \quad \forall 0 \le a \le 2k. \tag{7.1}$$

Let x_j be the middle point of I_j. We will approximate $\mathcal{Z}_j$ by

$$\mathcal{T}_j := \sum G_j(\zeta - x_j)$$

where the sum runs over all roots ζ of H.

By Theorem 2.2, we have

$$\mathbb{E}_{\varepsilon_\mu} \prod_{j=1}^{k} \mathcal{T}_j - \mathbb{E}_{\mathbf{g}} \prod_{j=1}^{k} \mathcal{T}_j = O\left(N^{-c+C\alpha}\right) \tag{7.2}$$

where the term $C\alpha$ in the exponent comes from the fact that we have to rescale the functions G_j before applying Theorem 2.2 due to (7.1) (note that the constant C may change from line to line). By choosing α to be sufficiently small, we get from (7.2) that

$$\mathbb{E}_{\varepsilon_\mu} \prod_{j=1}^{k} \mathcal{T}_j - \mathbb{E}_{\mathbf{g}} \prod_{j=1}^{k} \mathcal{T}_j = O\left(N^{-\alpha}\right). \tag{7.3}$$

We will show that for each j and for arbitrarily small constant α',

$$\mathbb{E}_{\varepsilon_\mu} \mathcal{T}_j^k = O\left(N^{\alpha'}\right) \tag{7.4}$$

and

$$\mathbb{E}_{\varepsilon_\mu} |\mathcal{T}_j - \mathcal{Z}_j|^k = O\left(N^{-\alpha}\right). \tag{7.5}$$

Assuming (7.4) and (7.5), with $\alpha' = \alpha/2k$, by Hölder's inequality and the triangle inequality, we have

$$\mathbb{E}_{\varepsilon_\mu} \prod_{j=1}^{k} \mathcal{Z}_j - \mathbb{E}_{\varepsilon_\mu} \prod_{j=1}^{k} \mathcal{T}_j = O\left(N^{-\alpha/k+\alpha'}\right) = O\left(N^{-\alpha/2k}\right).$$

Combining this with the same bound for the Gaussian case and with (7.3), we obtain

$$\mathbb{E}_{\varepsilon_\mu} \prod_{j=1}^{k} \mathcal{Z}_j - \mathbb{E}_{\mathbf{g}} \prod_{j=1}^{k} \mathcal{Z}_j = O\left(N^{-\alpha/2k}\right),$$

completing the proof of Proposition 2.5. □

It remains to prove (7.4) and (7.5). The strategy is first to reduce to the Gaussian case using Theorem 2.2 and then work with the Gaussian case.

Proof of (7.4). By Theorem 2.2, we have

$$\mathbb{E}_{\varepsilon_\mu} \mathcal{T}_j^k - \mathbb{E}_{\mathbf{g}} \mathcal{T}_j^k = O\left(N^{-\alpha'}\right).$$

Therefore, it suffices for the rest of this proof of (7.4) to assume that the random variables $\varepsilon_{1,\mu}, \varepsilon_{2,\mu}$ are Gaussian and show that

$$\mathbb{E}_{\mathbf{g}} \mathcal{T}_j^k = O\left(N^{\alpha'}\right). \tag{7.6}$$

Note that $\mathcal{T}_j$ is bounded by X_j defined to be the number of roots of H in the interval $[x_j - l, x_j + l]$ for $l = l_j/2 + N^{-\alpha} = O(1)$. By Jensen's inequality (3.6), we have

$$X_j = O(1) \log \frac{K}{|H(x_j)|}$$

where $K = \max_{z \in B(x_j, 2l)} |H(z)|$. Thus,

$$\mathbb{E}_{\mathbf{g}} X_j^k = O(1) \mathbb{E}_{\mathbf{g}} |\log K|^k + O(1) \mathbb{E}_{\mathbf{g}} |\log |H(x_j)||^k. \tag{7.7}$$

Since $H(x_j)$ is standard Gaussian,

$$\mathbb{E}_{\mathbf{g}} |\log |H(x_j)||^k \le \frac{\sqrt{2}}{\sqrt{\pi}} \int_0^1 |\log x|^k dx + \frac{\sqrt{2}}{\sqrt{\pi}} \int_1^\infty |\log x|^k e^{-x^2/2} dx = O(1) \tag{7.8}$$

where the implicit constant depends on k. The first integral is bounded by integration by parts and second integral is bounded by $O\left(\int_1^\infty e^{-x^2/3} dx\right) = O(1)$.

Furthermore, as $|H(x_j)| \le K = O\left(\frac{1}{\sqrt{N}} \sum_\mu |\varepsilon_{1,\mu}| + |\varepsilon_{2,\mu}|\right)$, we have

$$\mathbb{E}_{\mathbf{g}} |\log |K||^k = O\left(\log^k N\right). \tag{7.9}$$

Combining the bounds (7.8) and (7.9) with (7.7), we obtain (7.6), and thus (7.4). □

Proof of (7.5). Note that $|\mathcal{T}_j - \mathcal{Z}_j|$ is less than the number of roots of H in a union of two intervals of length $N^{-\alpha}$. Approximating the indicator function of each of these intervals by a smooth test function supported on an interval of length $10N^{-\alpha}$ and applying Theorem 2.2 to this test function, it suffices to show that for any interval $J = [a, b]$ of length $b - a = O(N^{-\alpha})$, the number of roots of H in J, which is denoted by Y satisfies

$$\mathbb{E}_{\mathbf{g}} Y^k = O\left(N^{-\alpha}\right). \tag{7.10}$$

Assume that it holds for $k = 1$. That is $\mathbb{E}_{\mathbf{g}} Y = O(N^{-\alpha})$. We have

$$\mathbb{E}_{\mathbf{g}} Y^k \le \mathbb{E}_{\mathbf{g}} Y^k \mathbf{1}_{Y \ge 2} + \mathbb{E}_{\mathbf{g}} Y. \tag{7.11}$$

To control the event $Y \ge 2$, we use the following lemma which is a direct application of [32, Lemma 8.6] to our setting. We refer the interested reader to a sketch of the proof of [32, Lemma 8.6] in Section 9.

Lemma 7.1. *Under the assumptions of Theorem 1.13, for every $x \in \mathcal{B}_1$ and any sufficiently small constant α, the probability that H has at least 2 roots in $B(x, N^{-\alpha})$ is at most $O\left(N^{-3\alpha/2}\right)$.*

By Lemma 7.1,

$$\mathbb{P}_{\mathbf{g}}(Y \ge 2) = O\left(N^{-3\alpha/2}\right). \tag{7.12}$$

By Lemma 2.3, Conditions 2.1(2) and 2.1(3) hold which together with the Jensen's inequality (3.6) give

$$\mathbb{P}\left(Y \ge N^{\alpha/2k}\right) = O\left(N^{-A}\right) \tag{7.13}$$

for any constant A. We thus break up the first term on the right of (7.11) into

$$\mathbb{E}_{\mathbf{g}} Y^k \mathbf{1}_{Y\geq 2} = \mathbb{E}_{\mathbf{g}}\left(Y^k \mathbf{1}_{2\leq Y\leq N^{\alpha/2k}}\right) + \mathbb{E}_{\mathbf{g}}\left(Y^k \mathbf{1}_{N^{\alpha/2k}<Y\leq N}\right) + \mathbb{E}_{\mathbf{g}}\left(Y^k \mathbf{1}_{Y>N}\right) =: E_1 + E_2 + E_3. \tag{7.14}$$

To bound E_1, we use (7.12)

$$E_1 \leq \left(N^{\alpha/2k}\right)^k \mathbb{P}_{\mathbf{g}}(Y\geq 2) = O\left(N^{-\alpha}\right). \tag{7.15}$$

Similarly, by (7.13) with $A := k+\alpha$,

$$E_2 \leq N^k \mathbb{P}_{\mathbf{g}}\left(Y \geq N^{\alpha/2k}\right) = O\left(N^{-\alpha}\right). \tag{7.16}$$

For E_3, by Lemma 2.3, Condition 2.1(1) holds for $C_1 = 1$. We use this, (7.13) with $A = \alpha(k+2)/2$ and Hölder's inequality to get

$$E_3 \leq \left(\mathbb{E}_{\mathbf{g}}\left(Y^{k+2}\mathbf{1}_{Y>N}\right)\right)^{k/(k+2)} \mathbb{P}(Y>N)^{2/(k+2)} = O\left(N^{-2A/(k+2)}\right) = O\left(N^{-\alpha}\right). \tag{7.17}$$

Combining (7.15), (7.16) and (7.17), we obtain

$$\mathbb{E}_{\mathbf{g}} Y^k \mathbf{1}_{Y\geq 2} = O\left(N^{-\alpha}\right). \tag{7.18}$$

For the second term on the right of (7.11), by the Kac-Rice type formula (see Kac [24] or Edelman-Kostlan [18, Theorem 3.1]), one has for every $x \in \mathcal{B}_1$,

$$\mathbb{E}_{\mathbf{g}} Y \quad \leq \quad \int_a^b \sqrt{\frac{\mathcal{S}(t)}{\mathcal{P}(t)^2}} dt,$$

where $\mathcal{P}(t) = \mathrm{Var}_{\mathbf{g}}(H(t)) = 1$, $\mathcal{Q}(t) = \mathrm{Var}_{\mathbf{g}}(H'(t)) = \frac{1}{N}\sum_\mu \langle \mu, \frac{1}{\lambda}\gamma'(t)\rangle^2 = O(1)$, $\mathcal{R}(t) = \mathrm{Cov}_{\mathbf{g}}(H(t), H'(t)) = 0$, and $\mathcal{S} = \mathcal{P}\mathcal{Q} - \mathcal{R}^2 = \mathcal{P}\mathcal{Q}$. And so, for every t,

$$\frac{\mathcal{S}(t)}{\mathcal{P}(t)^2} = \frac{\mathcal{Q}(t)}{\mathcal{P}(t)} = O(1)$$

which leads to

$$\mathbb{E}_{\mathbf{g}} Y = O(1)\int_a^b 1 dt = O\left(N^{-\alpha}\right). \tag{7.19}$$

From (7.11), (7.18), and (7.19), we obtain (7.10), completing the proof of (7.5). □

8. Proof of Theorems 1.10 and 1.13

In this section, we deduce Theorems 1.10 and 1.13 from Proposition 2.5.

Proof of Theorem 1.10. We partition the set $\mathcal{B}_2$ into $M = O(\lambda)$ intervals $I_1, \dots, I_M$ each of length $O(1)$. Applying Proposition 2.5 to every k-tuple of these intervals, we get

$$\mathbb{E}_{\varepsilon_\mu} \mathcal{Z}_{\mathcal{B}_2}^k = \mathbb{E}_{\mathbf{g}} \mathcal{Z}_{\mathcal{B}_2}^k + O\left(\lambda^k / N^c\right) \tag{8.1}$$

where $\mathcal{Z}_{\mathcal{B}_2}$ is the number of zeros of H in $\mathcal{B}_2$.

Let $\mathcal{Z}$ be the number of zeros of H in $[0,\lambda]$ and $\mathcal{Z}' = \mathcal{Z} - \mathcal{Z}_{\mathcal{B}_2}$ be the number of zeros of H in $[0,\lambda] \setminus \mathcal{B}_2$. By (7.4), the number of roots $\mathcal{Z}_j$ of H in each interval I_j satisfies

$$\mathbb{E}_{\varepsilon_\mu} \mathcal{Z}_j^h = O\left(N^\alpha\right)$$

for any small constant α and any $h \le k$.

Thus, $\mathbb{E}_{\varepsilon_\mu} \mathcal{Z}^h_{\mathcal{B}_2} = O\left(\lambda^h N^\alpha\right)$. By Theorem 5.1, $\mathcal{Z}' = O\left(\lambda N^{-1}\right)$ a.e. Hence, by choosing $\alpha < 1 - c$

$$\mathbb{E}_{\varepsilon_\mu} \mathcal{Z}^k - \mathbb{E}_{\varepsilon_\mu} \mathcal{Z}^k_{\mathcal{B}_2} = O\left(\lambda^k N^{-1+\alpha}\right) = O\left(\lambda^k N^{-c}\right).$$

This together with (8.1) complete the proof of Theorem 1.10. □

Proof of Theorem 1.13. We partition the interval $[0,\lambda]$ into λ intervals $I_1, \dots, I_\lambda$ of length 1 and apply Proposition 2.5 to every k-tuple of these intervals. □

9. Sketch of the proof of Theorem 2.2

To make the note self-contained, we present here the main ideas of the proof; the reader is invited to consult [32] for a complete treatment. We first show universality of the complex roots and then deduce Theorem 2.2 from it.

Theorem 9.1 (Local universality for complex roots)**.** *Under the assumption of Theorem 2.2, there exists a constant c such that the following holds. For any numbers $z_1, \dots, z_k$ in $\mathcal{B}$ and for every smooth function $G : \mathbb{C}^k \to \mathbb{C}$ supported on $\prod_{j=1}^k B(z_j, c)$ with $|\nabla^a G(z)| \le 1$ for all $0 \le a \le 2k+4$ and $z \in^k$, we have*

$$\mathbb{E}_{\xi_\mu} \sum_{i_1,\dots,i_k} G\left(\zeta_{i_1}, \dots, \zeta_{i_k}\right) - \mathbb{E}_{\tilde{\xi}_\mu} \sum_{i_1,\dots,i_k} G\left(\tilde{\zeta}_{i_1}, \dots, \tilde{\zeta}_{i_k}\right) = O\left(N^{-c}\right), \tag{9.1}$$

where the ζ_i are the roots of H, the $\tilde{\zeta}_i$ are the roots of $\widetilde{H}$, the sums run over all possible assignments of $i_1, \dots, i_k$ which are not necessarily distinct.

Sketch of proof of Theorem 9.1. For simplicity, we assume $k = 1$.

Let $X = \sum G\left(\zeta_i\right)$ and $\tilde{X} = \sum G\left(\tilde{\zeta}_i\right)$. We need to show that

$$\mathbb{E}_{\xi_\mu} X - \mathbb{E}_{\tilde{\xi}_\mu} \tilde{X} = O\left(N^{-c}\right).$$

By the Green's formula,

$$X = \sum_i G(\zeta_i) = -\frac{1}{2\pi} \int_{B(z_1,c)} \log|H(z)| \triangle G(z) dz.$$

Let $K : \mathbf{R} \to \mathbf{R}$ be a smooth function supported on the interval $[-2N^{c_1}, 2N^{c_1}]$ that approximates the identity function. By Conditions 2.1 (1)-(3), we can approximate $\mathbb{E}_{\xi_\mu} X$ by $\mathbb{E}_{\xi_\mu} X'$ where

$$X' = -\frac{1}{2\pi} \int_{B(z_1,c)} K\left(\log|H(z)|\right) \triangle G(z) dz.$$

Let $\tilde{X}'$ be the corresponding identity for $\tilde{H}$. To show that $\mathbb{E}_{\xi_\mu} X' - \mathbb{E}_{\tilde{\xi}_\mu} \tilde{X}' = O\left(N^{-c}\right)$, it suffices to show that for each $z \in B(z_1, c)$,

$$\mathbb{E}_{\xi_\mu} K\left(\log|H(z)|\right) \triangle G(z) - \mathbb{E}_{\tilde{\xi}_\mu} K\left(\log|\widetilde{H}(z)|\right) \triangle G(z) = O\left(N^{-c}\right).$$

This can be done by the Lindeberg swapping argument. In particular, by smoothing the log function, we can further reduce the task to showing that for any $z \in B(z_1, c)$, and for any smooth function $L : \mathbb{C} \to \mathbb{C}$ having bounded derivatives up to order 3,

$$\mathbb{E}_{\xi_\mu} L\left(H(z)\right) - \mathbb{E}_{\tilde{\xi}_\mu} L\left(\widetilde{H}(z)\right) = O\left(N^{-c}\right).$$

The swapping method uses the triangle inequality to bound the above difference by a sum of $2N$ differences each of which involves changing only one random variable to Gaussian. For example, one of these differences is $\mathbb{E}L\left(H_0(z)\right) - \mathbb{E}L\left(H_1(z)\right)$ where $H_0(z) = H(z) = \sum_\mu \xi_\mu f_\mu(z)$ and $H_1(z) = \tilde{\xi}_{\mu_1} f_{\mu_1}(z) + \sum_{\mu \neq \mu_1} \xi_\mu f_\mu(z)$. We then Taylor expand the function $L\left(H_0(z)\right)$ (and $L\left(H_1(z)\right)$) as a function of one variable ξ_μ (and $\tilde{\xi}_\mu$ respectively). Making use of the assumption that the first and second moments of ξ_μ and $\tilde{\xi}_\mu$ are the same, one can see that upon taking expectation, the first three terms in the Taylor expansions cancel out, leaving us with a small error term. Adding up these errors terms, one obtains N^{-c} as desired. The reader may notice that this is quite similar to a classical proof of the Central Limit Theorem using the swapping argument. □

Sketch of proof of Theorem 2.2. For simplicity, we again assume that $k = 1$.

The idea is to reduce it to Theorem 9.1. This is done by showing that in a ball $B(x, N^{-\alpha})$ where $x \in \mathcal{B}$, the number of non-real roots of H is negligible with high probability. Since the non-real roots appear in conjugate pairs, if H has at least one non-real root in $B(x, N^{-\alpha})$, it indeed has at least 2. Thus, it reduces to proving the following version of Lemma 7.1 for the general setting of Theorem 2.2.

Lemma 9.2. *Under the assumptions of Theorem 2.2, for every $x \in \mathcal{B}$ and any sufficiently small constant α, the probability that H has at least 2 roots in $B(x, N^{-\alpha})$ is at most $O\left(N^{-3\alpha/2}\right)$.*

This key lemma together with some standard approximation arguments will finish the proof of Theorem 2.2. □

Sketch of proof of Lemma 9.2. Using Theorem 9.1, this lemma is reduced to the Gaussian case. Let $\gamma = N^{-\alpha}$. Let $g(z) = \widetilde{H}(x) + \widetilde{H}'(x)(z - x)$ and $p(z) = \widetilde{H}(z) - g(z)$. By Rouché's theorem,

$$\mathbb{P}_{\tilde{\xi}_\mu}\left(\tilde{H} \text{ has at least 2 roots in } B(x, 2\gamma)\right) \leq \mathbb{P}_{\tilde{\xi}_\mu}\left(\min_{z \in \partial B(x, 2\gamma)} |g(z)| \leq \max_{z \in \partial B(x, 2\gamma)} |p(z)|\right).$$

Both $g(z)$ and $p(z)$ have zero mean. The second part of Condition 2.1(5) shows that for all $z \in B(x, 2\gamma)$,

$$\mathrm{Var}(p(z)) = O\left(N^{-(4+\varepsilon)\alpha} \mathrm{Var}(\widetilde{H}(x))\right).$$

Thus with probability at least $1 - O\left(N^{-3\alpha/2}\right)$,

$$\max_{z \in \partial B(x,2\gamma)} |p(z)| = O\left(N^{-2\alpha}\sqrt{\mathrm{Var}(\widetilde{H}(x))}\right). \tag{9.2}$$

Now, for g, note that since g is a linear function with real coefficients, one has

$$\min_{z \in \partial B(x,2\gamma)} |g(z)| = \min |g(x \pm 2\gamma)|.$$

The first part of Condition 2.1(5) shows that $g(x \pm 2\gamma)$ is normally distributed with variance

$$\mathrm{Var}(g(x \pm 2\gamma)) \geq 1/2\mathrm{Var}(\widetilde{H}(x)).$$

Therefore, with probability at least $1 - O\left(N^{-3\alpha/2}\right)$,

$$|g(x \pm 2\gamma)| \geq N^{-3\alpha/2}\sqrt{\mathrm{Var}(\widetilde{H}(x))}.$$

Combining this with (9.2), we obtain Lemma 9.2. □

Acknowledgement. The authors would like to thank Zeev Rudnick and Igor Shparlinski for helpful comments. They are also grateful to the anonymous referees for valuable comments and suggestions that help substantially improve the presentation of the note.

References

[1] J. Angst and G. Poly, Universality of the nodal length of bivariate random trigonometric polynomials, to appear in Trans. Amer. Math. Soc., `arxiv.org/abs/1610.05360`.

[2] Berry, M. V. Regular and irregular semiclassical wave functions. J. Phys. A 10, no. 12 (1977), 2083-2091.

[3] E. Bombieri, J. Bourgain and S. V. Konyagin, Roots of Polynomials in Subgroups of formula and Applications to Congruences, Int. Math. Res. Not. IMRN, 5 (2009), 802-834.

[4] J. Bourgain and Z. Rudnick, Restriction of toral eigenfunctions to hypersurfaces, C. R. Acad. Sci. Paris, Ser. I 347 (2009), 1249-1253.

[5] J. Bourgain and Z. Rudnick. On the nodal sets of toral eigenfunctions. Invent. Math., 185 (2011), 199-237.

[6] J. Bourgain and Z. Rudnick, On the Geometry of the Nodal Lines of eigenfunctions of the Two-Dimensional Torus, Ann. Henri Poincaré 12 (2011), 1027-1053.

[7] J. Bourgain and Z. Rudnick, Restriction of toral eigenfunctions to hypersurfaces and nodal sets , Geom. Funct. Anal., Volume 22, Issue 4 (2012), Page 878-937.

[8] J. Bourgain and Z. Rudnick, Nodal intersections and L_p restriction theorems on the torus, Israel J. Math., 207(1) (2015), 479-505.

[9] J. Bourgain, Z. Rudnick and P. Sarnak, Spatial statistics for lattice points on the sphere I: Individual results, Bull. Iranian Math. Soc., 43 (2017), 361-386.

[10] N. Burq, P. G. Yerard, and N. Tzvetkov. Restrictions of the Laplace-Beltrami eigenfunctions to submanifolds, Duke Math. J., 138, no. 3 (2007), 445-486.

[11] J. Cilleruelo and A. Cordoba. Trigonometric polynomials and lattice points. Proc. Amer. Math. Soc., 115, no. 4 (1992), 899-905.

[12] J. Cilleruelo and A. Granville, Lattice points on circles, squares in arithmetic progressions and sumsets of squares, in Additive Combinatorics, CRM Proceedings & Lecture Notes, Vol. 43, American Mathematical Society, Providence, RI (2007), 241-262.

[13] M.C. Chang, Factorization in generalized arithmetic progressions and application to the Erdős-Szemerédi sum-product problems, Geom. Funct. Anal. 13, no. 4 (2003), 720-736.

[14] C. D'Andrea, T. Krick, and M. Sombra, Heights of varieties in multiprojective spaces and arithmetic Nullstellensatze, Ann. Sci. Ec. Norm. Super. (4) 46 (2013), no. 4 (2013), 549-627.

[15] Y. Do, O. Nguyen, and V. Vu, Roots of random polynomials with coefficients of polynomial growth, Ann. Probab., 46, no. 05 (2018), 2407–2494.

[16] H. Donnelly, and C. Fefferman. Nodal sets of eigenfunctions on Reimannian manifolds, Invent. Math., 93, no. 1 (1988), 161-183.

[17] W. Duke, Hyperbolic distribution problems and half-integral weight Maass forms, Invent. Math., 92, no. 1 (1988), 73-90.

[18] A. Edelman and E. Kostlan, How many zeros of a random polynomial are real?, Bull. Amer. Math. Soc., 32, no. 1 (1995), 1–37.

[19] P. Erdős and R. Hall, On the angular distribution of Gaussian integers with fixed norm, Discrete Math., 200 (1999), 87-94.

[20] P. Erdős and E. Szemerédi, On sums and products of integers, Studies in Pure Mathematics; To the memory of Paul Turán. P. Erdős, L. Alpár and G. Halász editors, Akadémiai Kiádó - Birkhauser Verlag, Budapest - Basel-Boston, Mass. 1983, 213-218.

[21] L. Fainsilber, P. Kurlberg and B. Wennberg, Lattice points on circles and discrete velocity models for the Boltzmann equation, SIAM J. Math. Anal. 37, no. 6 (2006), 1903-1922.

[22] A. Iksanov, Z. Kabluchko, and A. Marynych, Local universality for real roots of random trigonometric polynomials, Electron. J. Probab. Volume 21 (2016), paper no. 63.

[23] H. Iwaniec and E. Kowalski, Analytic number theory, American Mathematical Society, Colloquium publications, Volume 53.

[24] M. Kac, On the average number of real roots of a random algebraic equation, Bull. Amer. Math. Soc, 49, no. 1 (1943), 314–320.

[25] I. Katai and I. Kornyei. On the distribution of lattice points on circles. Ann. Univ. Sci. Budapest. Eotvos Sect. Math., 19 (1977), 87–91.

[26] T. Krick, L. M. Pardo and M. Sombra, Sharp estimates for the arithmetic Nullstellensatz, Duke Math. J., 109 (2001), 521-598.

[27] M. Krishnapur, P. Kurlberg and I. Wigman, Nodal length fluctuations for arithmetic random waves. Ann. of Math. 177, no. 2 (2013), 699-737.

[28] E. Landau, Uber die Einteilung der positiven ganzen Zahlen in vier Klassen nach der Mindestzahl der zu ihrer additiven Zusammensetzung erforderlichen Quadrate, Arch. der Math. u. Phys. 13, no. 3 (1908), 305-312.

[29] V. Jarnik, Uber die Gitterpunkte auf konvexen Kurven, Math. Z. 24, no. 1 (1926), 500-518.

[30] H. Nguyen and V. Vu, Optimal inverse Littlewood-Offord theorems, Adv. Math., Vol. 226 6 (2011), 5298–5319.

[31] H. Nguyen and V. Vu, Small probability, inverse theorems, and applications, Paul Erdős' 100th anniversary, Bolyai Society Mathematical Studies, Vol. 25 (2013).

[32] O. Nguyen and V. Vu, Roots of random functions: A general condition for local universality, submitted, arxiv:1711.03615.

[33] M. Rossi and I. Wigman, Asymptotic distribution of nodal intersections for arithmetic random waves, to appear in Nonlinearity, arxiv:1702.05179.

[34] Z. Rudnick and I. Wigman, Nodal Intersection for random eigenfunctions on the torus, Amer. J. Math., 138.6 (2016), 1605-1644.

[35] Z. Rudnick, I. Wigman and Nadav Yesha, Nodal intersections for random waves on the 3-dimensional torus, Ann. Inst. Fourier (Grenoble), 66(6) (2016), 2455-2484.

[36] J. Sally, Roots to research: a vertical development of mathematical problems. American Mathematical Soc., 2007.

[37] E. M. Stein, Oscillatory integrals in Fourier analysis, in Beijing Lectures in Harmonic Analysis (Beijing, 1984), Annals of Mathematics Studies, Vol. 112, Princeton University Press, Princeton, NJ, 1986, pp. 307-355.

[38] J. Toth and S. Zelditch, Counting nodal lines which touch the boundary of an analytic domain, J. Differential Geom., 81 (2009), 649-686.

[39] T. Tao and V. Vu, Local universality of zeroes of random polynomials, Int. Math. Res. Not. IMRN, (2014), 0-84.

[40] T. Tao and V. Vu, Additive Combinatorics, Cambridge Univ. Press, 2006.

Department of Mathematics, University of California, Riverside, CA 92521

Email address: mcc@math.ucr.edu

Department of Mathematics, The Ohio State University, Columbus, Ohio 43210

Email address: nguyen.1261@math.osu.edu

Department of Mathematics, Princeton University, Princeton, NJ 08544

Email address: onguyen@math.princeton.edu

Department of Mathematics, Yale University, New Haven, CT 06520

Email address: van.vu@yale.edu