

A MODEL PROBLEM FOR MULTIPLICATIVE CHAOS IN NUMBER THEORY

KANNAN SOUNDARARAJAN AND ASIF ZAMAN

ABSTRACT. Resolving a conjecture of Helson, Harper recently established that partial sums of random multiplicative functions typically exhibit more than square-root cancellation. Harper's work gives an example of a problem in number theory that is closely linked to ideas in probability theory connected with multiplicative chaos; another such closely related problem is the Fyodorov–Hiary–Keating conjecture on the maximum size of the Riemann zeta function in intervals of bounded length on the critical line. In this paper we consider a problem that might be thought of as a simplified function field version of Helson's conjecture. We develop and simplify the ideas of Harper in this context, with the hope that the simplified proof would be of use to readers seeking a gentle entry-point to this fascinating area.

1. INTRODUCTION

The aim of this article is to describe, in a simple setting, some recent work of Harper [24] on the distribution of random multiplicative functions. The study of random multiplicative functions has been very active in recent years, and turns out to be closely related to problems of “multiplicative chaos” which have recently received attention in the probability literature. On the number theory side, the study of mean values of random multiplicative functions is closely related to problems involving the size of the Riemann zeta function in short intervals of the critical line, a line of investigation originating in the conjectures of Fyodorov, Hiary and Keating [14]. Let us begin by quickly describing the model problem that we study here, and then giving its connections with the problem of random multiplicative functions.

Consider a sequence $(X(k))_{k \geq 1}$ of independent standard complex Gaussians; thus the real and imaginary parts of $X(k)$ are distributed like independent real Gaussian random variables with mean 0 and variance $\frac{1}{2}$. Define a sequence of random variables $(A(N))_{N \geq 0}$ by the formal power series identity

$$(1.1) \quad \exp \left(\sum_{k=1}^{\infty} \frac{X(k)}{\sqrt{k}} z^k \right) = \sum_{n=0}^{\infty} A(n) z^n.$$

The random variables $A(n)$ are naturally determined by the independent random variables $X(k)$; for example, $A(0) = 1$, $A(1) = X(1)$, $A(2) = X(1)^2/2 + X(2)/\sqrt{2}$, and so on. With this notation, the main result that we wish to explain is the following.

Corollary 1.1. *For all $N \geq 1$,*

$$(1.2) \quad \mathbb{E}[|A(N)|^2] = 1.$$

However there are positive constants C_1 and C_2 such that for $N \geq 2$

$$(1.3) \quad \frac{C_1}{(\log N)^{\frac{1}{4}}} \leq \mathbb{E}[|A(N)|] \leq \frac{C_2}{(\log N)^{\frac{1}{4}}}.$$

In particular, $\mathbb{E}[|A(N)|] \rightarrow 0$ as $N \rightarrow \infty$.

Date: November 6, 2021.

As mentioned already, the result above is motivated by a breakthrough of Harper on the partial sums of random multiplicative functions. A random Steinhaus multiplicative function $f : \mathbb{N} \rightarrow \{|z| = 1\}$ is obtained by picking independent random variables $f(p)$ (for prime numbers p) distributed uniformly on the unit circle, and extending this to all natural numbers by (complete) multiplicativity. Thus if $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ then $f(n)$ is the random variable $f(p_1)^{\alpha_1} \cdots f(p_k)^{\alpha_k}$. Given such a random multiplicative function, an important goal is to understand the partial sums $\sum_{n \leq x} f(n)$. Since $\mathbb{E}[f(m)\overline{f(n)}] = 1$ if $m = n$ and 0 otherwise it follows that

$$(1.4) \quad \mathbb{E} \left[\left| \sum_{n \leq x} f(n) \right|^2 \right] = [x] = x + O(1).$$

Harper showed that even though the variance is about x , surprisingly the typical size of $\sum_{n \leq x} f(n)$ is smaller than $\sqrt{x}$:

$$(1.5) \quad \mathbb{E} \left[\left| \sum_{n \leq x} f(n) \right| \right] \asymp \frac{\sqrt{x}}{(\log \log x)^{\frac{1}{4}}}.$$

Here the relation $A \asymp B$ means that $C_1 B \leq A \leq C_2 B$ for some absolute positive constants C_1 and C_2 . Harper's result established the conjecture of Helson [26] that partial sums of random multiplicative functions typically exhibit more than square-root cancellation; the truth of Helson's conjecture seemed far from clear at the time, and indeed earlier work of Harper, Nikeghbali and Radziwiłł [25] had suggested the opposite of Helson's conjecture.

Identifying N with $\log x$, we see a strong parallel between the variances given in (1.2) and (1.4), and the estimates for the first moment in (1.3) and (1.5). For large k , the quantity $\sum_{e^k < p \leq e^{k+1}} f(p)$ behaves like a complex Gaussian with mean 0 and variance $\sum_{e^k < p \leq e^{k+1}} 1$, which by the prime number theorem is on the scale of $e^k(e-1)/k$. After normalization, the sum over primes behaves analogously to $X(k)/\sqrt{k}$. Then the random variable $A(N)$ is analogous to $e^{-N/2} \sum_{n \leq e^N} f(n)$. The key relation of the generating functions (1.1) is paralleled by the Euler product formula

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_p \left(1 - \frac{f(p)}{p^s} \right)^{-1} = \exp \left(\sum_{p^k} \frac{f(p^k)}{kp^{ks}} \right).$$

The analogy between our model problem and Harper's work is perhaps clearer in the "function field setting." Consider the polynomial ring $\mathbb{F}_q[t]$ where q is a prime power, and $\mathbb{F}_q$ is a finite field with q elements. Many problems in the integers have close parallels in this polynomial ring, and for example a study of multiplicative functions in this framework may be found in [17]. The role of positive integers is played by $\mathcal{M}$, the set of monic polynomials. Let $\mathcal{M}_n$ denote the monic polynomials of degree n , so that $|\mathcal{M}_n| = q^n$, which mirrors integers of size about x . The role of primes is played by $\mathcal{P}$, the set of irreducible monic polynomials. Letting $\mathcal{P}_n$ denote the monic irreducibles of degree n , there is also a well-known analogue of the prime number theorem (indeed of the Riemann hypothesis): $|\mathcal{P}_n| = q^n/n + O(q^{n/2}/n)$. We can model Steinhaus multiplicative functions in this setting by considering (for monic irreducibles P) independent random variables $f(P)$ uniformly distributed on the unit circle, and then extending these to $\mathcal{M}$ by complete multiplicativity: if $F = P_1^{\alpha_1} \cdots P_k^{\alpha_k}$ then put $f(F) = f(P_1)^{\alpha_1} \cdots f(P_k)^{\alpha_k}$.

In the function field context, our goal is to understand $\sum_{F \in \mathcal{M}_N} f(F)$. If we set $A(n) = q^{-n/2} \sum_{F \in \mathcal{M}_n} f(F)$, then

$$\sum_{n=0}^{\infty} A(n) z^n = \sum_{F \in \mathcal{M}} f(F) (q^{-1/2} z)^{\deg(F)} = \prod_P \left(1 - f(P) (q^{-1/2} z)^{\deg(P)} \right)^{-1}.$$

Writing

$$X(k) = \frac{\sqrt{k}}{q^{k/2}} \sum_{\substack{\deg(P) | k \\ r = k/\deg(P)}} \frac{f(P)^r}{r},$$

we may see that the generating function above equals

$$\exp \left(\sum_P \sum_{r=1}^{\infty} \frac{1}{r} f(P)^r (q^{-1/2} z)^{\deg(P^r)} \right) = \exp \left(\sum_{k=1}^{\infty} \frac{X(k)}{\sqrt{k}} z^k \right).$$

This relation mirrors (1.1). Moreover, note that if q^k is large then $X(k)$ is a (normalized) sum of about q^k/k independent random variables uniformly distributed on the unit circle, so that $X(k)$ is distributed very nearly like a standard complex Gaussian. In this manner we see that our model problem corresponds approximately to the study of Steinhaus multiplicative functions in the $\mathbb{F}_q[t]$ setting, and corresponds exactly to the limiting case when $q \rightarrow \infty$.

Perhaps one of the earliest occurrences of the model (1.1) is in the work of Hughes, Keating, O’Connell [28] where it arises as a prototypical example of a log-correlated field. Our interest arose in trying to simplify and understand Harper’s work, and while we lectured on these results earlier (see for example [8]), we have been slow with writing up this version. In the meantime, independent work of Najnudel, Paquette and Simm [31] (1.14) and Lemma 7.5] motivated by random matrix theory studies more general versions of this model (which they term “holomorphic multiplicative chaos”), establishing the upper bounds in Corollary 1.1 (and Theorem 2.1 below).

We conclude our introduction with a brief discussion of related work. In addition to the Steinhaus model of random multiplicative functions mentioned above, another natural model is the Rademacher class of random multiplicative functions taking values ± 1 (independently and with equal probability) on the primes, and extended multiplicatively to all square-free numbers. Harper [24] also established the analogue of (1.5) in this class. Indeed as we shall discuss in the next section, Harper [24] determined the order of magnitude of the $2q$ -th moment of partial sums for all $0 \leq q \leq 1$, with the key feature being that the low moments exhibit more cancellation than what would be obtained by using Hölder’s inequality with the second moment. The complementary range of high moments is studied by Harper in [21]. While the partial sums of random multiplicative functions are typically smaller than expected, there are variant problems where the behavior follows expected Gaussian laws. For example, the sums of random multiplicative functions over suitable short intervals or suitable arithmetic progressions [9], or when restricted to integers without too many prime factors [20], [27], exhibit Gaussian behavior.

Given a random Steinhaus multiplicative function f , one can ask whether almost surely one has $\sum_{n \leq x} f(n) = O(\sqrt{x})$ for all x . That is, here we are choosing the multiplicative function f at random, and asking about the behavior of partial sums as x varies, in contrast with our earlier discussion where x is first fixed and the random multiplicative function varies. This problem, which is an analogue of the law of the iterated logarithm, was raised by Halász [18],

and investigated further in [19] and [29]. Recently Halász's problem was answered in the negative by Harper [23], who established that almost surely there are arbitrarily large x with $|\sum_{n \leq x} f(n)| \geq \sqrt{x}(\log \log x)^{\frac{1}{4}-\varepsilon}$ for any $\varepsilon > 0$. The law of the iterated logarithm shows that sums of independent random variables (for example taking values ± 1 with equal probability) attain values as large as $\sqrt{x \log \log x}$ occasionally, and Harper's result differs from this by about the same amount $(\log \log x)^{-\frac{1}{4}}$ that appears in (1.5). Harper's result suggests that in our model problem, almost surely there exist arbitrarily large N with $|A(N)| \geq (\log N)^{\frac{1}{4}-\varepsilon}$. It would be of interest to make this precise, and perhaps obtain a more accurate law of the iterated logarithm in this context.

Another problem in number theory that is closely related to this circle of ideas concerns the distribution of the Riemann zeta function over typical intervals of length 1 on the critical line $\text{Re}(s) = 1/2$. One vague connection between these problems is that $\zeta(\frac{1}{2} + it)$ may be thought of as $\sum n^{-\frac{1}{2}-it}$ for suitable ranges of n , and if t is chosen randomly, the function n^{it} behaves in some ways like a random Steinhaus multiplicative function. More precisely, a conjecture of Fyodorov, Hiary, and Keating (see [14], [15]) states that if t is chosen uniformly from $[T, 2T]$ then

$$(1.6) \quad \log \log T - \frac{3}{4} \log \log \log T - g(T) \leq \max_{t \leq u \leq t+1} \log |\zeta(\frac{1}{2} + iu)| \leq \log \log T - \frac{3}{4} \log \log \log T + g(T),$$

holds with probability tending to 1 as $g(T)$ tends to infinity with T . The key feature of this conjecture is the secondary term $-\frac{3}{4} \log \log \log T$, which is smaller than the answer $-\frac{1}{4} \log \log \log T$ that may be suggested by a crude application of Selberg's classical theorem that $\log |\zeta(\frac{1}{2} + it)|$ is distributed like a normal random variable with mean 0 and variance $\sim \frac{1}{2} \log \log T$. Another closely related conjecture states that

$$(1.7) \quad \frac{1}{T} \int_T^{2T} \left(\frac{1}{\log T} \int_0^1 |\zeta(\frac{1}{2} + it + ih)|^2 dh \right)^{\frac{1}{2}} \asymp \frac{1}{(\log \log T)^{\frac{1}{4}}}.$$

Since $\int_T^{2T} |\zeta(\frac{1}{2} + it)|^2 dt \sim T \log T$, the Cauchy–Schwarz inequality shows that the above quantity is $\ll 1$, and the interest above is that it is still smaller, and by a factor very similar to that arising in (1.5). Indeed there is a very strong analogy between (1.7) and Propositions 3.2 and 8.2 below. There has been a lot of recent progress towards the conjectures in (1.6) and (1.7) and other related questions, see [2], [3], [4], [5], [16], [23], [30]. Most notably, the upper bound portion of (1.7) has been established by Harper [22], who also established a slightly weaker version of the upper bound in (1.6). An even more precise version of the upper bound in (1.6) has been established by Arguin, Bourgade and Radziwiłł [4]. For a recent comprehensive survey on this topic see [6].

The multiplication table problem (which asks for the number of integers n up to N^2 that may be written as $n = ab$ with $a, b \leq N$) exhibits some features in common with these problems, although the link here is perhaps less clearly defined. We content ourselves with referring the reader to [13], and pointing out also the interesting analogous problem of counting permutations in S_{2N} that leave some N -element set fixed (so that such permutations may be thought of as the product of two permutations on N element sets) [12].

Lastly, we mention that there is an extensive literature in probability where related problems are studied under “critical multiplicative chaos”; a few sample references are [7], [10], [11], [33].

Acknowledgments. K.S. is partially supported through a grant from the National Science Foundation, and a Simons Investigator Grant from the Simons Foundation. Part of this work was written while K.S. was a senior Fellow at the ETH Institute for Theoretical Studies, whom he thanks for their warm and generous hospitality. Part of this work was written while A.Z. was a postdoctoral fellow at Stanford University supported by an NSERC Postdoctoral Fellowship. A.Z. is grateful to both institutions for their financial support and to the university for providing excellent working conditions. A.Z. also thanks Valeriya Kovaleva for helpful comments and sharing reference [31] with him. We are also grateful to the referee for a careful reading and some helpful comments.

2. PRELIMINARIES

In this section we set up some convenient notation, and make preliminary observations for our analysis of $A(N)$.

By a partition λ we mean a non-increasing sequence of non-negative integers $\lambda_1 \geq \lambda_2 \geq \dots$, with $\lambda_n = 0$ from some point onwards. We denote by $|\lambda|$ the sum of the parts $\lambda_1 + \lambda_2 + \dots$, and for an integer $k \geq 1$ we denote by $m_k = m_k(\lambda)$ the number of parts in λ that are equal to k . Given a partition λ , define

$$(2.1) \quad a(\lambda) = a(\lambda; X) = \prod_k \left(\frac{X(k)}{\sqrt{k}} \right)^{m_k} \frac{1}{m_k!},$$

where, as in the introduction, $X(k)$ is a sequence of independent standard complex Gaussians. With this notation, we have

$$\exp \left(\sum_{k=1}^{\infty} \frac{X(k)}{\sqrt{k}} z^k \right) = \sum_{\lambda} a(\lambda) z^{|\lambda|},$$

so that

$$(2.2) \quad A(N) = \sum_{|\lambda|=N} a(\lambda).$$

Recall that a standard complex Gaussian Z satisfies

$$\mathbb{E} \left[Z^m \overline{Z}^n \right] = \begin{cases} n! & \text{if } m = n, \\ 0 & \text{if } m \neq n. \end{cases}$$

It follows that if λ and λ' are two different partitions then

$$(2.3) \quad \mathbb{E} [a(\lambda) \overline{a(\lambda')}] = 0,$$

while if $\lambda = \lambda'$ then

$$(2.4) \quad \mathbb{E} [|a(\lambda)|^2] = \prod_k \frac{1}{m_k!^2 k^{m_k}} \mathbb{E} [|X(k)|^{2m_k}] = \prod_k \frac{1}{m_k! k^{m_k}},$$

where we again use the notation that the partition λ contains m_k parts equal to k . We deduce that

$$\mathbb{E} [|A(N)|^2] = \sum_{|\lambda|=N} \mathbb{E} [|a(\lambda)|^2] = \sum_{|\lambda|=N} \prod_k \frac{1}{m_k! \cdot k^{m_k}} = 1,$$

where the last step follows from the familiar formula for the number of permutations in S_N whose cycle decomposition corresponds to the partition λ . This establishes (1.2), and our main task is to bound the first moment in (1.3).

In fact we will determine the order of magnitude of all low moments $\mathbb{E}[|A(N)|^{2q}]$ for $0 \leq q \leq 1$, following Harper who determined the order of magnitude for such moments for random multiplicative functions.

Theorem 2.1. *Uniformly for any integer $N \geq 1$ and any $0 \leq q \leq 1$,*

$$\mathbb{E}[|A(N)|^{2q}] \asymp \left(\frac{1}{(1-q)\sqrt{\log N + 1}} \right)^q.$$

In particular (1.3) holds.

Naturally one can study $A(N)$ through the generating function $\sum_{n=0}^{\infty} A(n)z^n$, which converges almost surely for $|z| < 1$. For example, by Cauchy's theorem we have for $r < 1$ the almost sure identity

$$A(N) = \frac{1}{2\pi i} \int_{|z|=r} \sum_{n=0}^{\infty} A(n)z^n \frac{dz}{z^{N+1}}.$$

Indeed since $A(N)$ depends only on the random variables $X(k)$ for $k \leq N$, we can avoid all issues of convergence and write (for any $K \geq N$ and any $r > 0$)

$$A(N) = \frac{1}{2\pi i} \int_{|z|=r} \exp \left(\sum_{k \leq K} \frac{X(k)}{\sqrt{k}} z^k \right) \frac{dz}{z^{N+1}}.$$

We will not use this relation, but it motivates us to define (for any real number $K \geq 1$)

$$(2.5) \quad F_K(z) = \exp \left(\sum_{k \leq K} \frac{X(k)}{\sqrt{k}} z^k \right).$$

When the parameter K is clear from context, we shall abbreviate $F_K(z)$ to $F(z)$.

We shall relate the problem of bounding $\mathbb{E}[|A(N)|^{2q}]$ to that of estimating

$$(2.6) \quad \mathbb{E} \left[\left(\frac{1}{2\pi} \int_0^{2\pi} |F_K(re^{i\theta})|^2 d\theta \right)^q \right].$$

Here K will be a parameter of size about N , and r will be a parameter close to 1.

Lemma 2.2. *For any $K \geq 1$, any $r > 0$, and any $\theta \in \mathbb{R}$, we have*

$$\mathbb{E}[|F_K(re^{i\theta})|^2] = \exp \left(\sum_{k \leq K} \frac{r^{2k}}{k} \right).$$

Proof. Since the complex Gaussian is rotationally symmetric, the variables $X(k)$ and $X(k)e^{ik\theta}$ are identically distributed and therefore $|F_K(re^{i\theta})|^2$ is distributed identically as $|F_K(r)|^2$. Now $\operatorname{Re} \sum_{k \leq K} X(k)r^k/\sqrt{k}$ is a sum of independent Gaussians, and therefore is distributed like a real Gaussian with mean 0 and variance $\frac{1}{2} \sum_{k \leq K} r^{2k}/k$. The lemma follows upon recalling that if Z is a real Gaussian with mean zero and variance σ^2 then $\mathbb{E}[e^{tZ}] = e^{t^2\sigma^2/2}$. $\square$

From Lemma 2.2 and Hölder's inequality it follows that

$$(2.7) \quad \mathbb{E} \left[\left(\frac{1}{2\pi} \int_0^{2\pi} |F_K(re^{i\theta})|^2 d\theta \right)^q \right] \leq \left(\mathbb{E} \left[\frac{1}{2\pi} \int_0^{2\pi} |F_K(re^{i\theta})|^2 d\theta \right] \right)^q = \exp \left(q \sum_{k \leq K} \frac{r^{2k}}{k} \right).$$

Thinking of $r = 1$ and $K = N$ for simplicity (this is the most relevant range of the parameters) this furnishes an upper bound of size N^q above. The true size of the quantity on the left side above turns out to be a little bit smaller, by a factor $(1 + (1 - q)\sqrt{\log N})^q$ exactly as in [Theorem 2.1](#). We point out that there are close parallels between the moment in [\(2.7\)](#) (for $q = 1/2$) and the corresponding problem for $|\zeta(\frac{1}{2} + it)|$ considered in [\(1.7\)](#).

Ultimately the smaller size of the left side of [\(2.7\)](#) can be traced to the “ballot problem” in probability theory; see [\[1\]](#), [\[32\]](#) for introductions to this classical problem. We will borrow from Harper the following extension of classical results on Gaussian random walks.

Lemma 2.3 (Harper). *Let $a \geq 1$. For any integer $n \geq 1$, let $G_1, \dots, G_n$ be independent real Gaussian random variables, each having mean zero and variance between $\frac{1}{20}$ and 20, say. Let h be a function such that $|h(j)| \leq 10 \log j$. Then*

$$\mathbb{P}\left(\sum_{m=1}^j G_m \leq a + h(j), \forall 1 \leq j \leq n\right) \asymp \min\left(1, \frac{a}{\sqrt{n}}\right).$$

Proof. This is [\[24\]](#) Probability Result 1, p. 29]. Harper states the result with a and n being large, but this may be relaxed by adjusting the implied constants suitably. $\square$

The term $h(j)$ in [Lemma 2.3](#) is needed, for example, in the upper bound part of our argument to obtain convergence of some sums. It should be thought of as largely harmless, since a sum of j independent Gaussian variables would typically exhibit fluctuations on the scale of $\sqrt{j}$ and $h(j)$ is negligible in comparison to this natural scale.

With the one exception of [Lemma 2.3](#) above, we have kept the proof of [Theorem 2.1](#) self-contained. For convenience, we have split the paper into two parts, focussing first on the upper bound implicit in [Theorem 2.1](#) (see Sections [3](#) to [7](#)) and then dealing with the lower bound (see Sections [8](#) to [11](#)). Note that the relation $A \ll B$ means that $A \leq CB$ for some absolute positive constant C .

Part I: The upper bound of [Theorem 2.1](#)

3. DEDUCING THE UPPER BOUND FROM TWO PROPOSITIONS

It is enough to prove the upper bound in the range $\frac{1}{2} \leq q \leq 1$, since by Hölder’s inequality the bound would then hold for all smaller q as well. As mentioned earlier, the problem of bounding $\mathbb{E}[|A(N)|^{2q}]$ may be related to the problem of bounding moments of the generating function $F_K(re^{i\theta})$ as in [\(2.6\)](#). We make this link precise here, and reduce the upper bound part of the main theorem to two propositions that will be established in the following sections.

Proposition 3.1. *For $1/2 \leq q \leq 1$ and any integer $N \geq 1$, we have*

$$\left(\mathbb{E}[|A(N)|^{2q}]\right)^{\frac{1}{2q}} \ll \frac{1}{\sqrt{N}} \sum_{j=1}^J \left(\mathbb{E}\left[\left(\frac{1}{2\pi} \int_0^{2\pi} |F_{N/2^j}(\exp(j/N + i\theta))|^2 d\theta\right)^q\right]\right)^{\frac{1}{2q}} + \frac{1}{N},$$

where $J = \lceil 4 \log \log(4N) \rceil$.

Proposition 3.2. *Let $K \geq 1$ be a real number and let $F(z) = F_K(z)$ be as in [\(2.5\)](#). Uniformly for $1/2 \leq q \leq 1$ and $1 \leq r \leq e^{1/K}$ we have*

$$\mathbb{E}\left[\left(\frac{1}{2\pi} \int_0^{2\pi} |F(re^{i\theta})|^2 d\theta\right)^q\right] \ll \left(\frac{K}{(1-q)\sqrt{\log K} + 1}\right)^q.$$

Applying the estimate of [Proposition 3.2](#) in [Proposition 3.1](#) it follows that for $1/2 \leq q \leq 1$

$$\left(\mathbb{E}[|A(N)|^{2q}]\right)^{\frac{1}{2q}} \ll \frac{1}{\sqrt{N}} \sum_{j=1}^J \left(\frac{N/2^j}{(1-q)\sqrt{\log N} + 1}\right)^{\frac{1}{2}} + \frac{1}{N} \ll \left(\frac{1}{(1-q)\sqrt{\log N} + 1}\right)^{\frac{1}{2}}.$$

This establishes the upper bound in [Theorem 2.1](#) in the range $1/2 \leq q \leq 1$.

4. PROOF OF [PROPOSITION 3.1](#)

Our starting point is the representation of $A(N)$ as a sum over partitions λ of N , recall [\(2.1\)](#) and [\(2.2\)](#). Group these partitions according to the size of their largest part λ_1 . For $1 \leq j \leq J$ write

$$A_j(N) = \sum_{\substack{|\lambda|=N \\ N/2^j < \lambda_1 \leq N/2^{j-1}}} a(\lambda),$$

and put

$$\tilde{A}_J(N) = \sum_{\substack{|\lambda|=N \\ \lambda_1 \leq N/2^J}} a(\lambda),$$

so that we have the natural decomposition

$$A(N) = \sum_{j=1}^J A_j(N) + \tilde{A}_J(N).$$

Minkowski's inequality gives, for $1/2 \leq q \leq 1$,

$$(4.1) \quad \left(\mathbb{E}[|A(N)|^{2q}]\right)^{\frac{1}{2q}} \leq \sum_{j=1}^J \left(\mathbb{E}[|A_j(N)|^{2q}]\right)^{\frac{1}{2q}} + \left(\mathbb{E}[|\tilde{A}_J(N)|^{2q}]\right)^{\frac{1}{2q}}.$$

We begin by estimating the last term in the right side of [\(4.1\)](#), showing that it is $\ll 1/N$. By Hölder's inequality, we find that

$$(4.2) \quad \left(\mathbb{E}[|\tilde{A}_J(N)|^{2q}]\right)^{\frac{1}{q}} \leq \mathbb{E}[|\tilde{A}_J(N)|^2] = \sum_{\substack{|\lambda|=N \\ \lambda_1 \leq N/2^J}} \prod_k \frac{1}{m_k! k^{m_k}}.$$

The right side of [\(4.2\)](#) is the proportion of elements in the symmetric group S_N whose cycle decomposition has largest cycle $\leq N/2^J$ in length, and it is a familiar fact that such permutations are rare (corresponding to the rarity of integers all of whose prime factors are small). We may supply a quick bound (corresponding to Rankin's trick with Dirichlet series) on this quantity as follows. The right side of [\(4.2\)](#) is the coefficient of z^N in the generating function $\exp(\sum_{k \leq N/2^J} z^k/k)$. Since the coefficients of this generating function are all non-negative, for any $r > 0$ we conclude that the right side of [\(4.2\)](#) is

$$\leq r^{-N} \exp\left(\sum_{k \leq N/2^J} \frac{r^k}{k}\right) \ll \exp(-2^J) \frac{N}{2^J} \ll \frac{1}{N^2},$$

upon choosing $r = \exp(2^J/N)$. Inserting this into [\(4.1\)](#) we conclude that the last term in [\(4.1\)](#) is $\ll 1/N$.

We now focus on bounding the contribution of the j -th term of the sum in [\(4.1\)](#). Recall that the term $A_j(N)$ sums over partitions λ of N with largest part λ_1 lying between $N/2^j$

and $N/2^{j-1}$. Decompose the partition λ into ρ and σ , where ρ consists of those non-zero parts in λ that lie between $N/2^j$ and $N/2^{j-1}$, and σ consists of those non-zero parts of λ that are $\leq N/2^j$; note that ρ must have at least one non-zero term. It follows from (2.1) that $a(\lambda) = a(\rho)a(\sigma)$. Thus, with the above understanding,

$$A_j(N) = \sum_{\substack{\rho, \sigma \\ |\rho|+|\sigma|=N \\ |\rho|>0}} a(\rho)a(\sigma).$$

Observe that $a(\sigma)$ depends only on the random variables $X(k)$ for $k \leq N/2^j$, while $a(\rho)$ depends only on the random variables $X(k)$ with $N/2^j < k \leq N/2^{j-1}$.

We shall bound the expected value of $|A_j(N)|$ by first conditioning on the variables $X(k)$ for $k \leq N/2^j$ (so that $a(\sigma)$ is fixed in the notation above), and then bounding the expectation over these small variables $X(k)$. Let $\mathbb{E}_j$ denote the conditional expectation when the variables $X(k)$ for $k \leq N/2^j$ are fixed. We shall show that

$$(4.3) \quad \mathbb{E}_j \left[|A_j(N)|^{2q} \right] \ll \left(\frac{1}{2\pi N} \int_0^{2\pi} |F_{N/2^j}(\exp(j/N + i\theta))|^2 d\theta \right)^q,$$

so that, upon now taking the expectation over the variables $X(k)$ with $k \leq N/2^j$, we may conclude that

$$\mathbb{E} \left[|A_j(N)|^{2q} \right] \ll \mathbb{E} \left[\left(\frac{1}{2\pi N} \int_0^{2\pi} |F_{N/2^j}(\exp(j/N + i\theta))|^2 d\theta \right)^q \right].$$

This would complete the proof of our proposition.

It remains now to establish (4.3). By Hölder's inequality,

$$\mathbb{E}_j \left[|A_j(N)|^{2q} \right] \leq \mathbb{E}_j \left[|A_j(N)|^2 \right]^q,$$

so that (4.3) follows from the estimate

$$(4.4) \quad \mathbb{E}_j \left[|A_j(N)|^2 \right] \ll \left(\frac{1}{2\pi N} \int_0^{2\pi} |F_{N/2^j}(\exp(j/N + i\theta))|^2 d\theta \right).$$

Expanding out the expression for $A_j(N)$ in terms of $a(\rho)$ and $a(\sigma)$, we find

$$\mathbb{E}_j \left[|A_j(N)|^2 \right] = \sum_{\substack{\rho_1, \sigma_1 \\ |\rho_1|+|\sigma_1|=N \\ |\rho_1|>0}} \sum_{\substack{\rho_2, \sigma_2 \\ |\rho_2|+|\sigma_2|=N \\ |\rho_2|>0}} a(\sigma_1)\overline{a(\sigma_2)} \mathbb{E}_j \left[a(\rho_1)\overline{a(\rho_2)} \right].$$

Now note (2.3) implies that $\mathbb{E}_j[a(\rho_1)\overline{a(\rho_2)}] = 0$ unless $\rho_1 = \rho_2$. Thus, writing $n = |\rho_1| = |\rho_2|$ with $N/2^j < n \leq N$ (and so $|\sigma_1| = |\sigma_2| = N - n$), we obtain

$$(4.5) \quad \mathbb{E}_j \left[|A_j(N)|^2 \right] = \sum_{N/2^j < n \leq N} \left| \sum_{|\sigma|=N-n} a(\sigma) \right|^2 \sum_{|\rho|=n} \mathbb{E}_j \left[|a(\rho)|^2 \right].$$

To proceed further, we must estimate the sum over the partitions ρ above. Recall that all parts of ρ must be between $N/2^j$ and $N/2^{j-1}$, and denote (as before) by m_k the number of parts of size k in ρ (so $N/2^j < k \leq N/2^{j-1}$). Then by (2.4), we have that

$$\mathbb{E}_j \left[|a(\rho)|^2 \right] = \prod_{N/2^j < k \leq N/2^{j-1}} \frac{1}{m_k! k^{m_k}} \leq \left(\frac{2^j}{N} \right)^r,$$

where r denotes the number of parts in ρ (so that $2^{j-1}n/N \leq r < 2^j n/N$). Thus

$$\sum_{|\rho|=n} \mathbb{E}_j \left[|a(\rho)|^2 \right] \leq \sum_{2^{j-1}n/N \leq r < 2^j n/N} \#\{\rho : |\rho| = n, \rho \text{ has } r \text{ parts}\} \left(\frac{2^j}{N} \right)^r.$$

The number of partitions ρ of n with r parts (all between $N/2^j$ and $N/2^{j-1}$) is at most $\binom{[N/2^j]+r}{r-1}$, since $r-1$ parts may be freely chosen among the integers in $(N/2^j, N/2^{j-1}]$ and the final part has at most one possibility. Thus, using $r \leq 2^j \leq N/2^j$ for large N ,

$$\sum_{|\rho|=n} \mathbb{E}_j \left[|a(\rho)|^2 \right] \leq \sum_{2^{j-1}n/N \leq r < 2^j n/N} \left(\frac{2^j}{N} \right)^r \frac{(N/2^j + r)^{r-1}}{(r-1)!} \leq \frac{2^j}{N} \sum_{2^{j-1}n/N \leq r < 2^j n/N} \frac{2^{r-1}}{(r-1)!}.$$

If $n \leq N/2$ then the sum over r above is $\ll 1$, while if $n > N/2$ we may bound the sum over r above by $\ll 2^{-j}$. Thus in both cases we may conclude that

$$\sum_{|\rho|=n} \mathbb{E}_j \left[|a(\rho)|^2 \right] \ll \frac{1}{N} \exp \left(2^j \frac{N-n}{N} \right).$$

Inserting the above in (4.5) it follows that

$$\mathbb{E}_j \left[|A_j(N)|^2 \right] \ll \frac{1}{N} \sum_{N/2^j < n \leq N} \left| \sum_{|\sigma|=N-n} a(\sigma) \right|^2 \exp \left(2^j \frac{N-n}{N} \right).$$

Now

$$F_{N/2^j}(z) = \sum_r \left(\sum_{|\sigma|=r} a(\sigma) \right) z^r,$$

and so by Parseval

$$\frac{1}{N} \sum_{N/2^j < n \leq N} \left| \sum_{|\sigma|=N-n} a(\sigma) \right|^2 \exp \left(2^j \frac{N-n}{N} \right) \leq \frac{1}{2\pi N} \int_0^{2\pi} |F_{N/2^j}(\exp(j/N + i\theta))|^2 d\theta.$$

This establishes (4.4) and completes the proof of the proposition. $\square$

5. PLAN FOR THE PROOF OF PROPOSITION 3.2

The proof of the upper bound portion of Theorem 2.1 has now been reduced to establishing Proposition 3.2. By Lemma 2.2 we conclude that for $1 \leq r \leq e^{1/K}$,

$$(5.1) \quad \mathbb{E} \left[\frac{1}{2\pi} \int_0^{2\pi} |F(re^{i\theta})|^2 d\theta \right] = \exp \left(\sum_{k \leq K} \frac{r^{2k}}{k} \right) \asymp K.$$

By Hölder's inequality it follows that for $0 < q \leq 1$ and $1 \leq r \leq e^{1/K}$,

$$\mathbb{E} \left[\left(\frac{1}{2\pi} \int_0^{2\pi} |F(re^{i\theta})|^2 d\theta \right)^q \right] \ll K^q,$$

so that in Proposition 3.2 we are looking for a small improvement over this easy upper bound. As mentioned earlier, the source of this improvement is connected to the ballot problem in probability.

Definition 5.1. Let $K \geq 3$. Suppose $1 \leq r \leq e^{1/K}$ and $1 \leq A \leq \sqrt{\log K}$. Define $\mathcal{G}_r(A, \theta; K)$ to be the following event: for each $1 \leq n \leq \log K$, one has

$$\sum_{k < e^n} \left(\operatorname{Re} \frac{X(k) r^k e^{ik\theta}}{\sqrt{k}} - \frac{r^{2k}}{k} \right) \leq A + 10 \log n.$$

Further, define $\mathcal{G}_r(A; K)$ to be the event where $\mathcal{G}_r(A, \theta; K)$ holds for all $\theta \in [0, 2\pi)$.

We shall deduce [Proposition 3.2](#) from the following two propositions concerning $\mathcal{G}_r(A; K)$.

Proposition 5.2. For all $1 \leq r \leq e^{1/K}$ and all $1 \leq A \leq \sqrt{\log K}$ we have

$$\mathbb{P}[\mathcal{G}_r(A; K) \text{ fails}] \ll \exp(-A).$$

Thus the event $\mathcal{G}_r(A; K)$ is very likely for large A . The crucial point is that on this large set, we can improve upon the upper bound [\(5.1\)](#) for the mean square of $F(re^{i\theta})$.

Proposition 5.3. With notations as above, we have

$$\mathbb{E} \left[\mathbf{1}_{\mathcal{G}_r(A, \theta; K)} |F(re^{i\theta})|^2 \right] \asymp \frac{A}{\sqrt{\log K}} K,$$

and therefore

$$\mathbb{E} \left[\mathbf{1}_{\mathcal{G}_r(A; K)} \int_0^{2\pi} |F(re^{i\theta})|^2 d\theta \right] \ll \frac{A}{\sqrt{\log K}} K.$$

Deducing [Proposition 3.2](#) from [Propositions 5.2](#) and [5.3](#). Assume without loss that $K \geq e^4$. Partition the whole probability space into the events $\mathcal{G}_r(1; K)$, $\mathcal{G}_r(2^j; K) \setminus \mathcal{G}_r(2^{j-1}; K)$ for $1 \leq j \leq J := \lfloor (\log \log K) / (2 \log 2) \rfloor$, and $\mathcal{G}_r(2^J; K)^c$. [Proposition 5.3](#) and Hölder's inequality give

$$\mathbb{E} \left[\mathbf{1}_{\mathcal{G}_r(1; K)} \left(\int_0^{2\pi} |F(re^{i\theta})|^2 d\theta \right)^q \right] \leq \left(\mathbb{E} \left[\mathbf{1}_{\mathcal{G}_r(1; K)} \int_0^{2\pi} |F(re^{i\theta})|^2 d\theta \right] \right)^q \ll \left(\frac{K}{\sqrt{\log K}} \right)^q.$$

For $1 \leq j \leq J$, the event $\mathcal{G}_r(2^j; K) \setminus \mathcal{G}_r(2^{j-1}; K)$ means that $\mathcal{G}_r(2^j; K)$ holds but $\mathcal{G}_r(2^{j-1}; K)$ fails. Thus Hölder's inequality gives

$$\begin{aligned} & \mathbb{E} \left[\mathbf{1}_{\mathcal{G}_r(2^j; K) \setminus \mathcal{G}_r(2^{j-1}; K)} \left(\int_0^{2\pi} |F(re^{i\theta})|^2 d\theta \right)^q \right] \\ & \leq \left(\mathbb{P}[\mathcal{G}_r(2^{j-1}; K) \text{ fails}] \right)^{1-q} \left(\mathbb{E} \left[\mathbf{1}_{\mathcal{G}_r(2^j; K)} \int_0^{2\pi} |F(re^{i\theta})|^2 d\theta \right] \right)^q. \end{aligned}$$

Using [Propositions 5.2](#) and [5.3](#), we see that this is

$$\ll \exp(-(1-q)2^{j-1}) \left(\frac{2^j K}{\sqrt{\log K}} \right)^q \leq \left(\frac{K}{\sqrt{\log K}} \right)^q \left(2^j \exp(-(1-q)2^{j-1}) \right).$$

Similarly we find that

$$\mathbb{E} \left[\mathbf{1}_{\mathcal{G}_r(2^J; K)^c} \left(\int_0^{2\pi} |F(re^{i\theta})|^2 d\theta \right)^q \right] \ll K^q \exp \left(-(1-q)2^J \right).$$

Adding up these estimates, we deduce [Proposition 3.2](#). □

6. PROOF OF PROPOSITION 5.2

We prove that the event $\mathcal{G}_r(A; K)$ is very likely by showing that $\sum_{k < e^n} \operatorname{Re} X(k) r^k e^{ik\theta} / \sqrt{k}$ is unlikely to exceed the stated barrier for any single $1 \leq n \leq \log K$ and any single $\theta \in [0, 2\pi]$. From Definition 5.1, the union bound gives

$$(6.1) \quad \begin{aligned} \mathbb{P}[\mathcal{G}_r(A; K) \text{ fails}] &\leq \sum_{n \leq \log K} \mathbb{P} \left[\max_{\theta} \sum_{k < e^n} \operatorname{Re} \frac{X(k) r^k e^{ik\theta}}{\sqrt{k}} \geq A + 10 \log n + \sum_{k < e^n} \frac{r^{2k}}{k} \right] \\ &=: \sum_{n \leq \log K} \mathcal{P}_n. \end{aligned}$$

To estimate $\mathcal{P}_n$ we discretize the possible values of $\theta \in [0, 2\pi)$, setting $\theta_j = 2\pi j / \lceil ne^n \rceil$ for $0 \leq j < \lceil ne^n \rceil$. Roughly speaking, $\sum_{k < e^n} X(k) r^k e^{ik\theta} / \sqrt{k}$ varies with θ on the scale $1/e^n$, and the finer discretization into intervals of length about $1/(ne^n)$ allows for a precise understanding of this sum. If the maximum over θ in the definition of $\mathcal{P}_n$ satisfies the corresponding inequality, then we must have

$$(6.2) \quad \sum_{k < e^n} \operatorname{Re} \frac{X(k) r^k e^{ik\theta_j}}{\sqrt{k}} \geq \frac{A}{2} + 5 \log n + \sum_{k < e^n} \frac{r^{2k}}{k}, \quad \text{for some } 0 \leq j < \lceil ne^n \rceil,$$

or for some $0 \leq j < \lceil ne^n \rceil$, and some $\theta_j < \theta \leq \theta_{j+1}$ we must have

$$\operatorname{Re} \int_{\theta_j}^{\theta} \sum_{k < e^n} X(k) r^k (i\sqrt{k} e^{iky}) dy = \operatorname{Re} \sum_{k < e^n} \frac{X(k) r^k}{\sqrt{k}} (e^{i\theta k} - e^{i\theta_j k}) \geq \frac{A}{2} + 5 \log n.$$

This second case only happens if

$$(6.3) \quad \int_{\theta_j}^{\theta_{j+1}} \left| \sum_{k < e^n} X(k) r^k \sqrt{k} e^{iky} \right| dy \geq \frac{A}{2} + 5 \log n, \quad \text{for some } 0 \leq j < \lceil ne^n \rceil.$$

Since the random variables $X(k)$ are independent and rotationally invariant, it follows that

$$(6.4) \quad \mathcal{P}_n \leq ne^n (\mathcal{P}'_n + \mathcal{P}''_n),$$

where $\mathcal{P}'_n$ is the probability that the inequality in (6.2) holds for $j = 0$, and $\mathcal{P}''_n$ is the probability that the inequality in (6.3) holds for $j = 0$.

Since $\operatorname{Re} \sum_{k < e^n} X(k) r^k / \sqrt{k}$ is a real Gaussian with mean 0 and variance $\frac{1}{2} \sum_{k < e^n} r^{2k} / k$, it follows that

$$\mathcal{P}'_n \ll \exp \left(- \left(\sum_{k < e^n} \frac{r^{2k}}{k} + \frac{A}{2} + 5 \log n \right)^2 / \sum_{k < e^n} \frac{r^{2k}}{k} \right) \leq \exp \left(- \sum_{k < e^n} \frac{r^{2k}}{k} - A - 10 \log n \right),$$

where we used that $\int_t^\infty e^{-x^2/2} dx \ll e^{-t^2/2}$ for $t \geq 0$. Thus, as $1 \leq r \leq e^{1/K}$,

$$(6.5) \quad \mathcal{P}'_n \ll \frac{e^{-n-A}}{n^{10}}.$$

Now we turn to the task of estimating $\mathcal{P}''_n$. By Hölder's inequality, it follows that if (6.3) holds (with $j = 0$ there) then for any integer $\ell \geq 1$ we must have

$$\theta_1^{2\ell-1} \int_0^{\theta_1} \left| \sum_{k < e^n} X(k) r^k \sqrt{k} e^{iky} \right|^{2\ell} dy \geq \left(\frac{A}{2} + 5 \log n \right)^{2\ell}.$$

Therefore, by Chebyshev's inequality,

$$\begin{aligned}\mathcal{P}_n'' &\leq \left(\frac{A}{2} + 5 \log n\right)^{-2\ell} \theta_1^{2\ell-1} \int_0^{\theta_1} \mathbb{E} \left[\left| \sum_{k < e^n} X(k) r^k \sqrt{k} e^{iky} \right|^{2\ell} \right] dy \\ &= \left(\frac{A}{2} + 5 \log n\right)^{-2\ell} \theta_1^{2\ell} \ell! \left(\sum_{k < e^n} k r^{2k} \right)^\ell,\end{aligned}$$

since $\sum_{k < e^n} X(k) r^k \sqrt{k} e^{iky}$ is distributed like a complex Gaussian with variance $\sum_{k < e^n} k r^{2k}$. Since $\ell! \leq \ell^\ell$, $\theta_1 \leq 2\pi/(ne^n)$ and $\sum_{k \leq e^n} k r^{2k} \leq e^{2+2n}$ (as $r \leq e^{1/K}$) it follows that

$$\mathcal{P}_n'' \leq \left(\frac{A}{2} + 5 \log n\right)^{-2\ell} \ell^\ell \left(\frac{2\pi e}{n}\right)^{2\ell}.$$

Upon choosing ℓ to be an integer around $n(A/2 + 5 \log n)$, we see that $\mathcal{P}_n'' \ll e^{-n-A}/n^{10}$; indeed $\mathcal{P}_n''$ is much smaller than this, but we have just matched our earlier bound in (6.5). Combining this with (6.4) and (6.5), it follows that $\mathcal{P}_n \ll e^{-A}/n^9$, which when inserted in (6.1) yields Proposition 5.2. Note that the factor $1/n^9$ ensures that the sum in (6.1) converges, and it is for this reason that the “safety valve” term $10 \log n$ was introduced in Definition 5.1 (and one of the reasons why Lemma 2.3 has the flexible term $h(j)$). $\square$

7. PROOF OF PROPOSITION 5.3

The proof of the upper bound in Theorem 2.1 has finally been reduced to Proposition 5.3, which we shall now obtain as an application of Lemma 2.3. We focus on showing that

$$(7.1) \quad \mathbb{E} \left[\mathbf{1}_{\mathcal{G}_r(A, \theta; K)} |F(re^{i\theta})|^2 \right] \asymp \frac{A}{\sqrt{\log K}} K.$$

Since $\mathcal{G}_r(A; K)$ is the event where $\mathcal{G}_r(A, \theta; K)$ holds for all θ , it then follows that

$$\mathbb{E} \left[\mathbf{1}_{\mathcal{G}_r(A; K)} \int_0^{2\pi} |F(re^{i\theta})|^2 d\theta \right] \leq \int_0^{2\pi} \mathbb{E} \left[\mathbf{1}_{\mathcal{G}_r(A, \theta; K)} |F(re^{i\theta})|^2 \right] d\theta \ll \frac{A}{\sqrt{\log K}} K,$$

completing the proof of the proposition. By rotational symmetry it is enough to establish (7.1) in the case $\theta = 0$.

Put $x_k = \operatorname{Re}(X(k))$ so that the x_k are independent real normal variables with mean 0 and variance $1/2$. Then we may write

$$(7.2) \quad \mathbb{E} \left[\mathbf{1}_{\mathcal{G}_r(A, 0; K)} |F(r)|^2 \right] = \frac{1}{\pi^{\lfloor K \rfloor / 2}} \int \cdots \int_{\mathcal{R}} \exp \left(\sum_{k \leq K} \left(\frac{2x_k r^k}{\sqrt{k}} - x_k^2 \right) \right) dx_1 dx_2 \cdots dx_{\lfloor K \rfloor},$$

where $\mathcal{R} \subseteq \mathbb{R}^{\lfloor K \rfloor}$ is the region given by $(x_k)_{k=1}^{\lfloor K \rfloor} \in \mathbb{R}^{\lfloor K \rfloor}$ satisfying

$$\sum_{k < e^n} \left(\frac{x_k r^k}{\sqrt{k}} - \frac{r^{2k}}{k} \right) \leq A + 10 \log n$$

for all $1 \leq n \leq \log K$. Write $y_k = x_k - r^k/\sqrt{k}$, which completes the square and allows us to express the integral in (7.2) as

$$\exp \left(\sum_{k \leq K} \frac{r^{2k}}{k} \right) \frac{1}{\pi^{\lfloor K \rfloor / 2}} \int \cdots \int_{\mathcal{R}'} \exp \left(- \sum_{k \leq K} y_k^2 \right) dy_1 \cdots dy_{\lfloor K \rfloor},$$

where $\mathcal{R}' \subseteq \mathbb{R}^{[K]}$ is the region given by $\sum_{k < e^n} y_k r^k / \sqrt{k} \leq A + 10 \log n$ for all $1 \leq n \leq \log K$. Since $1 \leq r \leq e^{1/K}$, it follows that

$$(7.3) \quad \mathbb{E} \left[\mathbf{1}_{\mathcal{G}_r(A, 0; K)} |F(r)|^2 \right] = \exp \left(\sum_{k \leq K} \frac{r^{2k}}{k} \right) \mathbb{P}[\mathcal{B}] \asymp K \mathbb{P}[\mathcal{B}],$$

where $\mathcal{B}$ is the event that, for all $1 \leq n \leq \log K$, one has

$$(7.4) \quad \sum_{k < e^n} \frac{y_k r^k}{\sqrt{k}} \leq A + 10 \log n,$$

for independent normal random variables y_k with mean 0 and variance $\frac{1}{2}$.

To complete the proof, we are now ready to apply [Lemma 2.3](#) with the random variables $G_m = \sum_{e^{m-1} \leq k < e^m} y_k r^k / \sqrt{k}$ for $1 \leq m \leq \log K$. Note that the variables G_m are Gaussians with variance $\frac{1}{2} \sum_{e^{m-1} \leq k < e^m} r^{2k}/k$ which lies between $1/20$ and 20 as required in [Lemma 2.3](#). Thus, we deduce that $\mathbb{P}[\mathcal{B}] \asymp A/\sqrt{\log K}$. Using this estimate in [\(7.3\)](#) now finishes the proof of [\(7.1\)](#) in the case $\theta = 0$. This completes the proof of the proposition, and hence the upper bound of [Theorem 2.1](#). $\square$

Part II: The lower bound of [Theorem 2.1](#)

8. DEDUCING THE LOWER BOUND FROM TWO PROPOSITIONS

Now, we turn our focus to the lower bound portion of [Theorem 2.1](#). If $0 \leq q \leq \frac{1}{2}$ then by Hölder's inequality it follows that

$$\mathbb{E}[|A(N)|] \leq (\mathbb{E}[|A(N)|^{3/2}])^{\frac{2-4q}{3-4q}} (\mathbb{E}[|A(N)|^{2q}])^{\frac{1}{3-4q}}.$$

The upper bound $\mathbb{E}[|A(N)|^{3/2}] \ll (\log N)^{-3/8}$ in [Theorem 2.1](#) has already been established. If we knew the lower bound $\mathbb{E}[|A(N)|] \gg (\log N)^{-1/4}$, then the desired lower bound for $\mathbb{E}[|A(N)|^{2q}]$ would follow. Thus, it is enough to prove the lower bound in the range $\frac{1}{2} \leq q \leq 1$.

Here we shall reduce the lower bound part of the main theorem to propositions involving bounds for the second moment of $F_K(z)$ defined by [\(2.1\)](#) for any real number $K \geq 1$.

Proposition 8.1. *For $\frac{1}{2} \leq q \leq 1$ and $0 < r < 1$ we have*

$$\mathbb{E}[|A(N)|^{2q}] \geq \frac{1}{4} \left(\mathbb{E} \left[\left(\frac{1}{2\pi N} \int_0^{2\pi} |F_{N/2}(re^{i\theta})|^2 d\theta \right)^q \right] - \mathbb{E} \left[\left(\frac{r^N}{2\pi N} \int_0^{2\pi} |F_{N/2}(e^{i\theta})|^2 d\theta \right)^q \right] \right).$$

Proposition 8.2. *Let $K \geq 100$ be a real number, and let $F(z) = F_K(z)$ be as in [\(2.5\)](#). Uniformly for $\frac{1}{2} \leq q \leq 1$ and $e^{-1/400} \leq r < 1$ we have*

$$\mathbb{E} \left[\left(\int_0^{2\pi} |F_K(re^{i\theta})|^2 d\theta \right)^q \right] \gg \left(\frac{K_r}{(1-q)\sqrt{\log K_r + 1}} \right)^q,$$

where $\log K_r$ is the largest integer such that $K_r \leq \min\{\frac{-1}{4\log r}, K\}$.

With $r = e^{-V/N}$ for a suitably large, but fixed, constant V , [Proposition 8.2](#) gives

$$\mathbb{E} \left[\left(\frac{1}{2\pi N} \int_0^{2\pi} |F_{N/2}(re^{i\theta})|^2 d\theta \right)^q \right] \gg \left(\frac{1}{V(1 + (1-q)\sqrt{\log N})} \right)^q,$$

while [Proposition 3.2](#) gives

$$\mathbb{E}\left[\left(\frac{r^N}{2\pi N} \int_0^{2\pi} |F_{N/2}(e^{i\theta})|^2 d\theta\right)^q\right] \ll \left(\frac{e^{-V}}{1 + (1-q)\sqrt{\log N}}\right)^q.$$

Combining these estimates with [Proposition 8.1](#), and choosing V to be a large enough constant, we obtain the lower bound in [Theorem 2.1](#) in the range $\frac{1}{2} \leq q \leq 1$.

9. PROOF OF [PROPOSITION 8.1](#)

As with the upper bound in [Section 4](#), we begin by decomposing the definition of $A(N)$ in terms of $a(\lambda)$ for partitions λ (see [\(2.1\)](#) and [\(2.2\)](#)), grouping terms according to the size of the largest part λ_1 . Define

$$A_1(N) = \sum_{\substack{|\lambda|=N \\ N/2 < \lambda_1 \leq N}} a(\lambda) = \sum_{N/2 < n \leq N} \frac{X(n)}{\sqrt{n}} A(N-n) \quad \text{and} \quad \tilde{A}_1(N) = \sum_{\substack{|\lambda|=N \\ \lambda_1 \leq N/2}} a(\lambda),$$

so that $A(N) = A_1(N) + \tilde{A}_1(N)$. Using that $X(n)$ is distributed identically to $-X(n)$ for $N/2 < n \leq N$, we see that

$$(9.1) \quad \mathbb{E}[|A(N)|^{2q}] = \frac{1}{2} \mathbb{E}[|A_1(N) + \tilde{A}_1(N)|^{2q} + |-A_1(N) + \tilde{A}_1(N)|^{2q}] \geq \frac{1}{2} \mathbb{E}[|A_1(N)|^{2q}],$$

where the last inequality holds because $\max(|-z+w|, |z+w|) \geq |z|$ for any two complex numbers z and w .

To obtain a lower bound on $\mathbb{E}[|A_1(N)|^{2q}]$, we first condition on the variables $X(k)$ for all $k \leq N/2$. Note that $A(N-n)$ is then determined for all $N/2 < n \leq N$. Therefore

$$A_1(N) = \sum_{N/2 < n \leq N} \frac{X(n)}{\sqrt{n}} A(N-n),$$

being a linear combination of the independent standard complex Gaussians $X(n)$, is distributed like a complex Gaussian with mean 0 and variance $\sum_{N/2 < n \leq N} |A(N-n)|^2/n$. With $\mathbb{E}_1$ denoting the conditional expectation (fixing $X(k)$ for $k \leq N/2$), it follows that

$$\mathbb{E}_1[|A_1(N)|^{2q}] = C_q \left(\sum_{N/2 < n \leq N} \frac{|A(N-n)|^2}{n} \right)^q,$$

where $C_q = \mathbb{E}[|Z|^{2q}]$ is the $2q$ -th moment of a standard complex Gaussian Z with mean 0 and variance 1. Hölder's inequality gives

$$\mathbb{E}[|Z|^{2q}] \geq \frac{(\mathbb{E}[|Z|^2])^{2-q}}{(\mathbb{E}[|Z|^4])^{1-q}} = \frac{1}{2^{1-q}},$$

and so we obtain

$$\mathbb{E}_1[|A_1(N)|^{2q}] \geq \frac{1}{2^{1-q}} \left(\sum_{N/2 < n \leq N} \frac{|A(N-n)|^2}{n} \right)^q \geq \frac{1}{2} \left(\frac{1}{N} \sum_{n < N/2} |A(n)|^2 \right)^q.$$

Now taking the full expectation and using [\(9.1\)](#), we deduce that

$$(9.2) \quad \mathbb{E}[|A(N)|^{2q}] \geq \frac{1}{4} \mathbb{E} \left[\left(\frac{1}{N} \sum_{n < N/2} |A(n)|^2 \right)^q \right].$$

Write

$$F_{N/2}(z) = \exp \left(\sum_{k \leq N/2} \frac{X(k)}{\sqrt{k}} z^k \right) = \sum_{n=0}^{\infty} \tilde{A}_1(n) z^n,$$

and note that $\tilde{A}_1(n) = A(n)$ for $n \leq N/2$. Note that Parseval's identity gives, for any $0 < r \leq 1$,

$$\begin{aligned} \sum_{n < N/2} |A(n)|^2 &= \sum_{n < N/2} |\tilde{A}_1(n)|^2 \geq \sum_{n=0}^{\infty} |\tilde{A}_1(n)|^2 r^{2n} - r^N \sum_{n=0}^{\infty} |\tilde{A}_1(n)|^2 \\ &= \frac{1}{2\pi} \int_0^{2\pi} |F_{N/2}(re^{i\theta})|^2 d\theta - \frac{r^N}{2\pi} \int_0^{2\pi} |F_{N/2}(e^{i\theta})|^2 d\theta. \end{aligned}$$

Since $|z + w|^q \leq |z|^q + |w|^q$ for $q \leq 1$, it follows that

$$\left(\sum_{n < N/2} |A(n)|^2 \right)^q \geq \left(\frac{1}{2\pi} \int_0^{2\pi} |F_{N/2}(re^{i\theta})|^2 d\theta \right)^q - \left(\frac{r^N}{2\pi} \int_0^{2\pi} |F_{N/2}(e^{i\theta})|^2 d\theta \right)^q,$$

and inserting this in (9.2), we obtain Proposition 8.1. □

10. PLAN FOR THE PROOF OF PROPOSITION 8.2

The proof of the lower bound in Theorem 2.1 has now been reduced to establishing Proposition 8.2. Let $\mathcal{L} = \mathcal{L}(X)$ denote any (random) subset of $\theta \in [0, 2\pi)$ with the random subset depending possibly on the instantiation of the random variables X . Using Hölder's inequality, we obtain

$$\begin{aligned} \mathbb{E} \left[\left(\frac{1}{2\pi} \int_0^{2\pi} |F(re^{i\theta})|^2 d\theta \right)^q \right] &\geq \mathbb{E} \left[\left(\frac{1}{2\pi} \int_{\mathcal{L}(X)} |F(re^{i\theta})|^2 d\theta \right)^q \right] \\ (10.1) \quad &\geq \frac{\left(\mathbb{E} \left[\frac{1}{2\pi} \int_{\mathcal{L}(X)} |F(re^{i\theta})|^2 d\theta \right] \right)^{2-q}}{\left(\mathbb{E} \left[\left(\frac{1}{2\pi} \int_{\mathcal{L}(X)} |F(re^{i\theta})|^2 d\theta \right)^2 \right] \right)^{1-q}}. \end{aligned}$$

We apply this idea to a carefully chosen random subset $\mathcal{L}(X)$ where the second and fourth moments will be of comparable size so that there is no loss involved in applying Hölder's inequality in (10.1). The random set $\mathcal{L}(X)$ is defined similarly to Definition 5.1, keeping once again the ballot problem in mind.

Definition 10.1. Let $K \geq 100$. Suppose $e^{-1/400} \leq r < 1$ and define $\log K_r$ to be the largest integer such that $K_r \leq \min \left\{ \frac{-1}{4 \log r}, K \right\}$. Let A be a real number with $1 \leq A \leq \sqrt{\log K_r}$. Define $\mathcal{L}(\theta) = \mathcal{L}_r(A, \theta; K)$ to be the following event: For each $1 \leq n \leq \log K_r$ one has

$$\sum_{k < e^n} \left(\operatorname{Re} \frac{X(k) r^k e^{ik\theta}}{\sqrt{k}} - \frac{r^{2k}}{k} \right) \leq A - 5 \log n.$$

Define $\mathcal{L} = \mathcal{L}_r(A; K)$ to be the random subset of $\theta \in [0, 2\pi]$ such that $\mathcal{L}(\theta)$ holds.

With this choice of the random subset $\mathcal{L}$, we seek a lower bound for the numerator in (10.1) and an upper bound for the denominator there. We start with the easier case of the lower bound. Since $\mathcal{L}$ denotes the subset of θ for which $\mathcal{L}(\theta)$ holds, we find that

$$\mathbb{E}\left[\frac{1}{2\pi} \int_{\mathcal{L}} |F(re^{i\theta})|^2 d\theta\right] = \mathbb{E}\left[\frac{1}{2\pi} \int_0^{2\pi} \mathbf{1}_{\mathcal{L}(\theta)} |F(re^{i\theta})|^2 d\theta\right] = \frac{1}{2\pi} \int_0^{2\pi} \mathbb{E}[\mathbf{1}_{\mathcal{L}(\theta)} |F(re^{i\theta})|^2] d\theta,$$

and by the rotational symmetry of the random variables X , this equals

$$\mathbb{E}[\mathbf{1}_{\mathcal{L}(0)} |F(r)|^2].$$

Arguing as in Section 7 we may see that

$$\mathbb{E}[\mathbf{1}_{\mathcal{L}(0)} |F(r)|^2] = \exp\left(\sum_{k \leq K} \frac{r^{2k}}{k}\right) \mathbb{P}[\mathcal{B}],$$

where $\mathcal{B}$ is the event that, for all $1 \leq n \leq \log K_r$, one has

$$\sum_{k < e^n} \frac{y_k r^k}{\sqrt{k}} \leq A - 5 \log n,$$

for independent normal random variables y_k with mean 0 and variance $\frac{1}{2}$. We now invoke Lemma 2.3 with the random variables $G_m = \sum_{e^{m-1} \leq k < e^m} y_k r^k / \sqrt{k}$ for $1 \leq m \leq \log K_r$. Note that these variables G_m are Gaussian with variance $\frac{1}{2} \sum_{e^{m-1} \leq k < e^m} r^{2k}/k$ which lies between $1/20$ and 20 as required in Lemma 2.3. Therefore it follows that $\mathbb{P}(\mathcal{B}) \asymp A/\sqrt{\log K_r}$, and we conclude that

$$(10.2) \quad \mathbb{E}\left[\frac{1}{2\pi} \int_{\mathcal{L}} |F(re^{i\theta})|^2 d\theta\right] \gg \frac{A}{\sqrt{\log K_r}} \exp\left(\sum_{k \leq K} \frac{r^{2k}}{k}\right) \gg \frac{AK_r}{\sqrt{\log K_r}}.$$

Now we turn to the harder problem of obtaining satisfactory upper bounds for the denominator in (10.1). Expanding out we see that

$$\mathbb{E}\left[\left(\frac{1}{2\pi} \int_{\mathcal{L}} |F(re^{i\theta})|^2 d\theta\right)^2\right] = \frac{1}{(2\pi)^2} \mathbb{E}\left[\int_0^{2\pi} \int_0^{2\pi} \mathbf{1}_{\mathcal{L}(\theta_1)} |F(re^{i\theta_1})|^2 \mathbf{1}_{\mathcal{L}(\theta_2)} |F(re^{i\theta_2})|^2 d\theta_1 d\theta_2\right],$$

and upon writing $\theta = \theta_2 - \theta_1$ (and taking θ to be in $[-\pi, \pi)$) and using rotational symmetry this equals

$$\frac{1}{2\pi} \int_{-\pi}^{\pi} \mathbb{E}[\mathbf{1}_{\mathcal{L}(0)} |F(r)|^2 \mathbf{1}_{\mathcal{L}(\theta)} |F(re^{i\theta})|^2] d\theta.$$

Proposition 10.2. *With notations as above, and any $\theta \in [-\pi, \pi)$ we have*

$$\mathbb{E}[\mathbf{1}_{\mathcal{L}(0)} |F(r)|^2 \mathbf{1}_{\mathcal{L}(\theta)} |F(re^{i\theta})|^2] \ll A^2 e^{2A} \frac{K_r^2}{\log K_r} \frac{\min(K_r, 2\pi/|\theta|)}{(\log \min(K_r, 2\pi/|\theta|))^8}.$$

We postpone the proof of Proposition 10.2 to the next section, and assuming this bound now finish our proof of Proposition 8.2. Applying Proposition 10.2 we obtain

$$\mathbb{E}\left[\left(\frac{1}{2\pi} \int_{\mathcal{L}} |F(re^{i\theta})|^2 d\theta\right)^2\right] \ll A^2 e^{2A} \frac{K_r^2}{\log K_r} \int_{-\pi}^{\pi} \frac{\min(K_r, 2\pi/|\theta|)}{(\log \min(K_r, 2\pi/|\theta|))^8} d\theta \ll A^2 e^{2A} \frac{K_r^2}{\log K_r}.$$

Using this upper bound for the denominator in (10.1) together with the lower bound for the numerator (given in (10.2)) we conclude that

$$\mathbb{E}\left[\left(\frac{1}{2\pi} \int_0^{2\pi} |F(re^{i\theta})|^2 d\theta\right)^q\right] \gg e^{-2A(1-q)} \left(\frac{AK_r}{\sqrt{\log K_r}}\right)^q.$$

Selecting $A = \sqrt{\log K_r}/((1-q)\sqrt{\log K_r} + 1)$ completes the proof of Proposition 8.2. Note that $\log K_r \geq 4$ in Definition 10.1, and so $A \geq 1$.

11. PROOF OF PROPOSITION 10.2

Given $\theta \in [-\pi, \pi)$, define $M = M(r, \theta)$ to be the smallest integer such that

$$(11.1) \quad e^M \geq \min\{10^3/|\theta|, K_r/e\}.$$

Note that $\log K_r \geq 4$ in Definition 10.1, and so $M \geq 1$. Set

$$(11.2) \quad A_0(M) = \operatorname{Re} \sum_{k < e^M} \left(\frac{X(k)r^k}{\sqrt{k}} - \frac{r^{2k}}{k} \right), \quad A_\theta(M) = \operatorname{Re} \sum_{k < e^M} \left(\frac{X(k)r^k e^{ik\theta}}{\sqrt{k}} - \frac{r^{2k}}{k} \right),$$

and define for $M+1 \leq m \leq \log K_r$,

$$(11.3) \quad Z_0(m) = \operatorname{Re} \sum_{e^{m-1} \leq k < e^m} \frac{X(k)}{\sqrt{k}} r^k, \quad Z_\theta(m) = \operatorname{Re} \sum_{e^{m-1} \leq k < e^m} \frac{X(k)}{\sqrt{k}} r^k e^{ik\theta}.$$

Our goal is to bound the expected value of $|F(r)|^2 |F(re^{i\theta})|^2$ when restricted to the event $\mathcal{L}(0) \cap \mathcal{L}(\theta)$. Recall that $\mathcal{L}(0) \cap \mathcal{L}(\theta)$ is the event satisfying the inequalities (for $1 \leq n \leq \log K_r$)

$$\sum_{k < e^n} \left(\operatorname{Re} \frac{X(k)}{\sqrt{k}} r^k - \frac{r^{2k}}{k} \right) \leq A - 5 \log n, \quad \sum_{k < e^n} \left(\operatorname{Re} \frac{X(k)}{\sqrt{k}} r^k e^{ik\theta} - \frac{r^{2k}}{k} \right) \leq A - 5 \log n.$$

Since our goal is to obtain upper bounds, we replace the event $\mathcal{L}(0) \cap \mathcal{L}(\theta)$ with a less restrictive event which is easier to handle. This less restrictive event $\tilde{\mathcal{L}}$ is defined by the constraints

$$(11.4) \quad A_0(M), A_\theta(M) \leq A - 5 \log M,$$

together with, for $M+1 \leq m \leq \log K_r$

$$(11.5) \quad \sum_{e^M \leq k < e^m} \left(\operatorname{Re} \frac{X(k)}{\sqrt{k}} r^k - \frac{r^{2k}}{k} \right), \quad \sum_{e^M \leq k < e^m} \left(\operatorname{Re} \frac{X(k)}{\sqrt{k}} r^k e^{ik\theta} - \frac{r^{2k}}{k} \right) \leq A - \min(A_0(M), A_\theta(M), 0).$$

Before entering into the details, let us give a loose description of the argument. The values k below e^M are thought of as small, and here $e^{ik\theta}$ may be thought of as close to 1. The constraints imposed by $\mathcal{L}(0)$ and $\mathcal{L}(\theta)$ are strongly correlated for such k , and so are the quantities $A_0(M)$ and $A_\theta(M)$. The “barrier events” in (11.4) prevent the contribution of these small k from getting too large. In the range $e^M \leq k \leq K_r$, the oscillation of $e^{ik\theta}$ becomes significant, and the terms $Z_0(m)$ and $Z_\theta(m)$ behave almost independently of each other. This allows us to think of the constraints in (11.5) as corresponding to two independent applications of the ballot problem, leading eventually to the saving of $\log K_r$ in Proposition 10.2. Lastly the terms with $K \geq k > K_r$ contribute a negligible amount as they are weighted down by the factor r^k which is small in this range.

Returning to the proof, in the notation just introduced, we have

$$\mathbb{E}[\mathbf{1}_{\mathcal{L}(0) \cap \mathcal{L}(\theta)} |F(r)F(re^{i\theta})|^2] \leq \exp\left(4 \sum_{k < e^M} \frac{r^{2k}}{k}\right) \mathbb{E}[\mathbf{1}_{\tilde{\mathcal{L}}} \exp(2A_0(M) + 2A_\theta(M)) \prod_{M+1 \leq m \leq \log K_r} \exp(2Z_0(m) + 2Z_\theta(m)) \exp\left(2 \sum_{K_r \leq k \leq K} \frac{r^k}{\sqrt{k}} \operatorname{Re}(X(k) + X(k)e^{ik\theta})\right)].$$

We make a few initial simplifications to this quantity, before getting to the crux of the proof. Note that the terms involving $X(k)$ with $K_r \leq k \leq K$ are independent of the random variables with $k < K_r$, and are not constrained by (11.4) or (11.5). So we may separate these terms from our expression above, and they contribute

$$\leq \frac{1}{2} \mathbb{E}\left[\exp\left(4 \sum_{K_r \leq k \leq K} \operatorname{Re} X(k) \frac{r^k}{\sqrt{k}}\right) + \exp\left(4 \sum_{K_r \leq k \leq K} \operatorname{Re}(X(k)e^{ik\theta}) \frac{r^k}{\sqrt{k}}\right)\right] = \exp\left(4 \sum_{K_r \leq k \leq K} \frac{r^{2k}}{k}\right),$$

since $\sum_{K_r \leq k \leq K} \operatorname{Re}(X(k))r^k/\sqrt{k}$ and $\sum_{K_r \leq k \leq K} \operatorname{Re}(X(k)e^{ik\theta})r^k/\sqrt{k}$ are distributed like Gaussian random variables with mean 0 and variance $\frac{1}{2} \sum_{K_r \leq k \leq K} r^{2k}/k$ (compare with Lemma 2.2). Noting that

$$\sum_{k < e^M} \frac{r^{2k}}{k} \leq \sum_{k < e^M} \frac{1}{k} = M + O(1), \quad \text{and} \quad \sum_{K_r \leq k \leq K} \frac{r^{2k}}{k} = O(1),$$

we conclude that

$$(11.6) \quad \mathbb{E}[\mathbf{1}_{\mathcal{L}(0) \cap \mathcal{L}(\theta)} |F(r)F(re^{i\theta})|^2] \ll e^{4M} \mathbb{E}[\mathbf{1}_{\tilde{\mathcal{L}}} \exp(2A_0(M) + 2A_\theta(M)) \prod_{M+1 \leq m \leq \log K_r} \exp(2Z_0(m) + 2Z_\theta(m))].$$

We now state a proposition (to be proved in the next section) which amounts to two applications of the ballot problem, and granting this proposition, we will be able to finish the proof of Proposition 10.2.

Proposition 11.1. *Keep notations as above. Given a real number B , let $\mathcal{E}$ denote the following event: for all $M+1 \leq m \leq \log K_r$ one has*

$$(11.7) \quad \sum_{e^M \leq k < e^m} \left(\operatorname{Re} \frac{X(k)}{\sqrt{k}} r^k - \frac{r^{2k}}{k}\right), \quad \sum_{e^M \leq k < e^m} \left(\operatorname{Re} \frac{X(k)}{\sqrt{k}} r^k e^{ik\theta} - \frac{r^{2k}}{k}\right) \leq B.$$

Then

$$\mathbb{E}[\mathbf{1}_{\mathcal{E}} \prod_{M+1 \leq m \leq \log K_r} \exp(2Z_0(m) + 2Z_\theta(m))] \ll \frac{K_r^2}{e^{2M}} \left(\frac{1 + \max(0, B)}{\sqrt{1 + \log(K_r/e^M)}}\right)^2.$$

Assuming this proposition, we now resume the proof of Proposition 10.2, starting from (11.6). Applying Proposition 11.1 with $B = A - \min(A_0(M), A_\theta(M), 0)$ we obtain

$$\begin{aligned} & \mathbb{E}[\mathbf{1}_{\mathcal{L}(0) \cap \mathcal{L}(\theta)} |F(r)F(re^{i\theta})|^2] \\ & \ll \frac{K_r^2 e^{2M}}{1 + \log(K_r/e^M)} \mathbb{E}[\mathbf{1}_{\tilde{\mathcal{L}}} \exp(2A_0(M) + 2A_\theta(M)) (A + \max(-A_0(M), -A_\theta(M), 0))^2]. \end{aligned}$$

Here we have abused notation a little, and the event $\tilde{\mathcal{L}}$ refers now only to the constraint (11.4) on the variables $X(k)$ with $k < e^M$. Notice also that we have used Proposition 11.1 treating

$X(k)$ for $k < e^M$ as fixed. By rotational symmetry, we may assume that $A_0(M) \leq A_\theta(M)$; the other case contributes an identical amount. Then bounding $A_\theta(M)$ by $A - 5 \log M$, we conclude that

$$(11.8) \quad \mathbb{E}[\mathbf{1}_{\mathcal{L}(0) \cap \mathcal{L}(\theta)} |F(r)F(re^{i\theta})|^2] \ll \frac{K_r^2 e^{2M}}{1 + \log(K_r/e^M)} \frac{e^{2A}}{M^{10}} \mathbb{E}[\mathbf{1}_{A_0(M) \leq A - 5 \log M} \exp(2A_0(M)) (A + \max(-A_0(M), 0))^2].$$

Now $\operatorname{Re} \sum_{k < e^M} X(k)r^k/\sqrt{k}$ is a real Gaussian with mean 0 and variance $\frac{1}{2} \sum_{k < e^M} r^{2k}/k$. Therefore, using also that $\sum_{k < e^M} r^{2k}/k = M + O(1)$,

$$\begin{aligned} & \mathbb{E}[\mathbf{1}_{A_0(M) \leq A - 5 \log M} \exp(2A_0(M)) (A + \max(-A_0(M), 0))^2] \\ &= \frac{1}{\sqrt{\pi \sum_{k < e^M} r^{2k}/k}} \int_{-\infty}^{A - 5 \log M} e^{2x} (A + \max(-x, 0))^2 \exp\left(-\frac{(x + \sum_{k < e^M} r^{2k}/k)^2}{\sum_{k < e^M} r^{2k}/k}\right) dx \\ &\ll (A^2 + M)e^{-M}. \end{aligned}$$

Inserting this in (11.8), we conclude that

$$\mathbb{E}[\mathbf{1}_{\mathcal{L}(0) \cap \mathcal{L}(\theta)} |F(r)F(re^{i\theta})|^2] \ll \frac{K_r^2 e^M}{1 + \log(K_r/e^M)} \frac{e^{2A}}{M^{10}} (A^2 + M) \ll \frac{K_r^2 e^M}{1 + \log(K_r/e^M)} \frac{A^2 e^{2A}}{M^9}.$$

Upon recalling the definition of M in (11.1), and noting that $M(1 + \log(K_r/e^M)) \geq \frac{1}{2} \log K_r$, this completes the proof of Proposition 10.2. $\square$

12. PROOF OF PROPOSITION 11.1

The proof of the lower bound for Theorem 2.1 has been reduced to Proposition 11.1. Here we are focussing on the range $e^M \leq K \leq K_r$ where there is substantial oscillation in the terms $e^{ik\theta}$, and we shall see that the variables $Z_0(m)$ and $Z_\theta(m)$ for $M+1 \leq m \leq \log K_r$ are largely uncorrelated (or more precisely, very weakly correlated). By exploiting properties of bivariate Gaussian vectors, these weakly correlated Gaussians may be replaced with *independent* Gaussians. Thus, the expectation in Proposition 11.1 will essentially split into two independent Gaussian random walks where an analysis similar to Section 7 will ultimately carry over.

We first dispense with the case when $\log(K_r/e^M) \leq 10$. Note that

$$\begin{aligned} & \mathbb{E}\left[\mathbf{1}_{\mathcal{E}} \prod_{M+1 \leq m \leq \log K_r} \exp(2Z_0(m) + 2Z_\theta(m))\right] \\ & \leq \frac{1}{2} \left(\mathbb{E}\left[\prod_{M+1 \leq m \leq \log K_r} \exp(4Z_0(m))\right] + \mathbb{E}\left[\prod_{M+1 \leq m \leq \log K_r} \exp(4Z_\theta(m))\right] \right) \\ & = \mathbb{E}\left[\prod_{M+1 \leq m \leq \log K_r} \exp(4Z_0(m))\right] = \mathbb{E}\left[\exp\left(4 \operatorname{Re} \sum_{e^M \leq k < K_r} \frac{X(k)r^k}{\sqrt{k}}\right)\right], \end{aligned}$$

by rotational symmetry. Now $\sum_{e^M \leq k < K_r} \operatorname{Re}(X(k)r^k/\sqrt{k})$ is distributed like a Gaussian random variable with mean 0 and variance $\frac{1}{2} \sum_{e^M \leq k < K_r} r^{2k}/k$, and this variance is bounded by our assumption that $\log(K_r/e^M) \leq 10$. It follows that in this case, our desired quantity is bounded by an absolute constant, and the proposition follows at once.

Therefore we may assume that $K_r > e^{M+10}$ below. Upon recalling the definition of M (see (11.1)) we may thus assume that $\theta \in (-\pi, \pi]$ satisfies $10^3/|\theta| \leq K_r/e$ and that

$$e^M |\theta| \geq 10^3.$$

With this easy case out of the way, we now embark on the proof proper.

For $M+1 \leq m \leq \log K_r$ note that the variables $Z_0(m)$ and $Z_\theta(m)$ depend only on $X(k)$ for $e^{m-1} \leq k < e^m$, and so these variables $Z_0(m)$ and $Z_\theta(m)$ are independent for different values of m . We therefore begin by discussing, for a given $M+1 \leq m \leq \log K_r$, the probability that $Z_0(m)$ and $Z_\theta(m)$ satisfy some event, and then by combining those results for different m we will obtain Proposition 11.1.

We recall that a pair of real random variables (Y_1, Y_2) is said to have a bivariate normal distribution if every linear combination $a_1 Y_1 + a_2 Y_2$ with $a_1, a_2 \in \mathbb{R}$ is a univariate normal random variable. The bivariate normal distribution is determined by the means $\mu_1 = \mathbb{E}[Y_1]$ and $\mu_2 = \mathbb{E}[Y_2]$ together with the 2×2 (symmetric) covariance matrix $\mathbb{E}[Y_i Y_j]$ for $1 \leq i, j \leq 2$. Denote by $\sigma_i^2 = \mathbb{E}[Y_i^2]$ for $i = 1, 2$, and by $\rho \sigma_1 \sigma_2$ the covariance $\mathbb{E}[Y_1 Y_2]$ so that $|\rho| \leq 1$. For a bivariate normal vector (Y_1, Y_2) with these parameters, the probability density at $(x_1, x_2) \in \mathbb{R}^2$ is given by

$$(12.1) \quad \frac{1}{2\pi\sigma_1\sigma_2\sqrt{1-\rho^2}} \exp\left(-\frac{1}{2(1-\rho^2)}\left(\left(\frac{x_1-\mu_1}{\sigma_1}\right)^2 - 2\rho\left(\frac{x_1-\mu_1}{\sigma_1}\right)\left(\frac{x_2-\mu_2}{\sigma_2}\right) + \left(\frac{x_2-\mu_2}{\sigma_2}\right)^2\right)\right).$$

Here we ignore the degenerate case when $|\rho| = 1$.

If (Y_1, Y_2) is a bivariate normal vector, then in general Y_1 and Y_2 need not be independent, and indeed the case when they are independent corresponds to requiring the covariance $\mathbb{E}[Y_1 Y_2]$ to be 0 (equivalently $\rho = 0$ above). We next observe that even in the general case, we can upper bound the probability density in (12.1) by replacing (Y_1, Y_2) by a suitable pair of independent normal variables. This is especially useful when the covariance parameter ρ is small, which will be the case for us.

Suppose (Y_1, Y_2) is a bivariate normal vector, with probability density as in (2.1). Since

$$\left|2\rho\left(\frac{x_1-\mu_1}{\sigma_1}\right)\left(\frac{x_2-\mu_2}{\sigma_2}\right)\right| \leq |\rho|\left(\left(\frac{x_1-\mu_1}{\sigma_1}\right)^2 + \left(\frac{x_2-\mu_2}{\sigma_2}\right)^2\right),$$

we see that the probability density in (12.1) is bounded above by

$$(12.2) \quad \frac{\sqrt{1+|\rho|}}{\sqrt{1-|\rho|}} \frac{1}{2\pi\sigma_1\sigma_2(1+|\rho|)} \exp\left(-\frac{1}{2(1+|\rho|)}\left(\left(\frac{x_1-\mu_1}{\sigma_1}\right)^2 + \left(\frac{x_2-\mu_2}{\sigma_2}\right)^2\right)\right).$$

Apart from the factor $\sqrt{(1+|\rho|)/(1-|\rho|)}$, the quantity above is the probability density of a pair of independent normal variables $(\tilde{Y}_1, \tilde{Y}_2)$ with means μ_1, μ_2 , and variances $\sigma_1^2(1+|\rho|), \sigma_2^2(1+|\rho|)$. Thus given any event $\mathcal{B}$ (thought of as a Borel measurable subset of $\mathbb{R}^2$) we have

$$(12.3) \quad \mathbb{P}[(Y_1, Y_2) \in \mathcal{B}] \leq \frac{\sqrt{1+|\rho|}}{\sqrt{1-|\rho|}} \mathbb{P}[(\tilde{Y}_1, \tilde{Y}_2) \in \mathcal{B}].$$

With this preliminary discussion in place, we are now ready to handle Proposition 11.1. Since $\text{Re}(X(k))$ and $\text{Im}(X(k))$ are independent normal variables, it follows that

$$(\text{Re}(X(k)), \text{Re}(X(k)e^{ik\theta})) = (\text{Re}(X(k)), \cos(k\theta)\text{Re}(X(k)) - \sin(k\theta)\text{Im}(X(k)))$$

is a bivariate normal vector. Being a linear combination of independent such vectors we see that $(Z_0(m), Z_\theta(m))$ is also a bivariate normal vector. Note that both $Z_0(m)$ and $Z_\theta(m)$

have mean 0, variance

$$(12.4) \quad \mathbb{E}[|Z_0(m)|^2] = \mathbb{E}[|Z_\theta(m)|^2] = \sigma_m^2 = \sum_{e^{m-1} \leq k < e^m} \frac{r^{2k}}{2k}$$

and covariance

$$(12.5) \quad \mathbb{E}[Z_0(m)Z_\theta(m)] = \rho_m(\theta)\sigma_m^2 = \sum_{e^{m-1} \leq k < e^m} \frac{r^{2k}}{2k} \cos(k\theta).$$

In the range $M+1 \leq m \leq \log K_r$,

$$(12.6) \quad \frac{1}{4} \leq \sum_{e^{m-1} \leq k \leq e^m} \frac{1}{4k} \leq \sigma_m^2 \leq \sum_{e^{m-1} \leq k < e^m} \frac{1}{2k} \leq \frac{1}{2} + \frac{1}{2e^{m-1}}.$$

because $\frac{1}{2} \leq r^{2k} \leq 1$ for $k \leq K_r$. Further the covariance satisfies

$$(12.7) \quad |\rho_m(\theta)\sigma_m^2| = \left| \sum_{e^{m-1} \leq k < e^m} r^{2k} \frac{\cos(k\theta)}{2k} \right| \leq \left| \int_0^r \sum_{e^{m-1} \leq k < e^m} t^{2k-1} e^{ik\theta} dt \right| \leq \frac{\pi}{|\theta|e^{m-1}},$$

since by summing the geometric series, and using $|1 - t^2 e^{i\theta}| \geq |\sin(\theta/2)| \geq |\theta|/\pi$ (for all $0 \leq t \leq 1$ and $\theta \in (-\pi, \pi]$), we may see that

$$\left| \sum_{e^{m-1} \leq k < e^m} t^{2k-1} e^{ik\theta} \right| \leq \frac{2t^{2\lceil e^{m-1} \rceil - 1}}{|1 - te^{i\theta}|} \leq \frac{\pi}{|\theta|} 2t^{2\lceil e^{m-1} \rceil - 1}.$$

Thus in this range $|\rho_m| \leq 4\pi/(|\theta|e^{m-1})$ is small, being always $\leq 4\pi/10^3 < 1/10$.

Now define independent normal random variables $\tilde{Z}_0(m)$ and $\tilde{Z}_\theta(m)$ distributed identically with mean 0 and variance $\sigma_m^2(1 + |\rho_m(\theta)|)$. As noted in (12.2) and (12.3) we obtain that for any event $\mathcal{B}$ (thought of as a Borel measurable subset of $\mathbb{R}^2$) we have

$$\mathbb{E}[\mathbf{1}_{\mathcal{B}} \exp(2(Z_0(m) + Z_\theta(m)))] \leq \frac{\sqrt{1 + |\rho_m(\theta)|}}{\sqrt{1 - |\rho_m(\theta)|}} \mathbb{E}[\mathbf{1}_{\mathcal{B}} \exp(2(\tilde{Z}_0(m) + \tilde{Z}_\theta(m)))].$$

Applying this to all $M+1 \leq m \leq \log K_r$ (and recalling that $Z_0(m)$ and $Z_\theta(m)$ are independent for different values of m) we conclude that

$$(12.8) \quad \begin{aligned} \mathbb{E}[\mathbf{1}_{\mathcal{E}} \prod_{M+1 \leq m \leq \log K_r} \exp(2(Z_0(m) + Z_\theta(m)))] &\leq \prod_{M+1 \leq m \leq \log K_r} \frac{\sqrt{1 + |\rho_m(\theta)|}}{\sqrt{1 - |\rho_m(\theta)|}} \\ &\times \mathbb{E}[\mathbf{1}_{\mathcal{E}} \prod_{M+1 \leq m \leq \log K_r} \exp(2(\tilde{Z}_0(m) + \tilde{Z}_\theta(m)))] \\ &\ll \mathbb{E}[\mathbf{1}_{\mathcal{E}} \prod_{M+1 \leq m \leq \log K_r} \exp(2(\tilde{Z}_0(m) + \tilde{Z}_\theta(m)))]. \end{aligned}$$

Here we estimated $\prod_{M+1 \leq m \leq \log K_r} \sqrt{(1 + |\rho_m(\theta)|)/(1 - |\rho_m(\theta)|)}$ as $\ll 1$ using (12.6), (12.7), and our assumption that $e^M |\theta| \geq 10^3$. Let us also clarify that the event $\mathcal{E}$ denotes (on the left side of (12.8)) the inequalities given in (11.7), and on the right side of (12.8) these inequalities amount to, for all $M+1 \leq m \leq \log K_r$

$$(12.9) \quad \sum_{M+1 \leq \ell \leq m} \tilde{Z}_0(\ell), \quad \sum_{M+1 \leq \ell \leq m} \tilde{Z}_\theta(\ell) \leq B + \sum_{e^M \leq k < e^m} \frac{r^{2k}}{k} = B + \sum_{M \leq \ell \leq m} 2\sigma_\ell^2.$$

Since $\tilde{Z}_0(m)$ and $\tilde{Z}_\theta(m)$ are independent, the right side of (12.8) equals

$$\left(\mathbb{E} \left[\mathbf{1}_{\mathcal{E}} \prod_{M+1 \leq m \leq \log K_r} \exp(2\tilde{Z}_0(m)) \right] \right)^2,$$

where now by $\mathcal{E}$ we understand the constraints in (12.9) holding just for $\tilde{Z}_0(m)$. If we put $Y_m = \tilde{Z}_0(m) - 2\sigma_m^2(1 + |\rho_m(\theta)|)$ then (completing the square as in Section 7) we obtain

$$\begin{aligned} \mathbb{E} \left[\mathbf{1}_{\mathcal{E}} \prod_{M+1 \leq m \leq \log K_r} \exp(2\tilde{Z}_0(m)) \right] &= \exp \left(\sum_{M+1 \leq m \leq \log K_r} 2\sigma_m^2(1 + |\rho_m(\theta)|) \right) \\ &\times \int \cdots \int_{\mathcal{E}'} \exp \left(- \sum_{M+1 \leq m \leq \log K_r} \frac{Y_m^2}{2\sigma_m^2(1 + |\rho_m(\theta)|)} \right) \prod_{M+1 \leq m \leq \log K_r} \frac{dY_m}{\sqrt{2\pi\sigma_m^2(1 + |\rho_m(\theta)|)}}, \end{aligned}$$

where $\mathcal{E}'$ now denotes the constraint

$$\sum_{M+1 \leq \ell \leq m} Y_m \leq B + \sum_{M+1 \leq \ell \leq m} (2\sigma_\ell^2 - 2\sigma_\ell^2(1 + |\rho_\ell(\theta)|)) = B - \sum_{M+1 \leq \ell \leq m} 2\sigma_\ell^2|\rho_\ell(\theta)|.$$

We conclude that

$$\begin{aligned} \mathbb{E} \left[\mathbf{1}_{\mathcal{E}} \prod_{M+1 \leq m \leq \log K_r} \exp(2\tilde{Z}_0(m)) \right] &\leq \exp \left(\sum_{M+1 \leq m \leq \log K_r} 2\sigma_m^2(1 + |\rho_m(\theta)|) \right) \\ &\times \mathbb{P} \left[\sum_{M+1 \leq \ell \leq m} Y_m \leq B \text{ for all } M+1 \leq m \leq \log K_r \right] \\ &\ll \exp \left(\sum_{M+1 \leq m \leq \log K_r} 2\sigma_m^2(1 + |\rho_m(\theta)|) \right) \frac{1 + \max(0, B)}{\sqrt{1 + \log(K_r/e^M)}}, \end{aligned}$$

upon appealing to Lemma 2.3. Finally recalling (12.4) and (12.7) we have

$$\sum_{M+1 \leq m \leq \log K_r} 2\sigma_m^2(1 + |\rho_m(\theta)|) = \sum_{e^M \leq k < K_r} \frac{r^{2k}}{k} + O(1) = \log K_r - M + O(1).$$

This establishes Proposition 11.1, and hence the lower bound in Theorem 2.1. $\square$

REFERENCES

- [1] L. Addario-Berry and B. A. Reed. Ballot theorems, old and new. In *Horizons of combinatorics*, volume 17 of *Bolyai Soc. Math. Stud.*, pages 9–35. Springer, Berlin, 2008.
- [2] Louis-Pierre Arguin, David Belius, Paul Bourgade, Maksym Radziwiłł, and Kannan Soundararajan. Maximum of the Riemann zeta function on a short interval of the critical line. *Comm. Pure Appl. Math.*, 72(3):500–535, 2019.
- [3] Louis-Pierre Arguin, David Belius, and Adam J. Harper. Maxima of a randomized Riemann zeta function, and branching random walks. *Ann. Appl. Probab.*, 27(1):178–215, 2017.
- [4] Louis-Pierre Arguin, Paul Bourgade, and Maksym Radziwiłł. The Fyodorov-Hiary-Keating conjecture. I. *arXiv preprint arXiv:2007.00988*, 2020.
- [5] Louis-Pierre Arguin, Frédéric Ouimet, and Maksym Radziwiłł. Moments of the Riemann zeta function on short intervals of the critical line. *arXiv preprint arXiv:1901.04061*, 2019.
- [6] Emma C. Bailey and Jonathan P. Keating. Maxima of log-correlated fields: some recent developments. *arXiv preprint arXiv:2106.15141*, 2021.
- [7] Nathanaël Berestycki. An elementary approach to Gaussian multiplicative chaos. *Electron. Commun. Probab.*, 22:Paper No. 27, 12, 2017.
- [8] Jörg Brüdern, Kaisa Matomäki, Robert Vaughan, and Trevor Wooley. Analytic number theory. *Oberwolfach Reports*, 16(4):3141–3205, Nov 2020.

- [9] Sourav Chatterjee and Kannan Soundararajan. Random multiplicative functions in short intervals. *Int. Math. Res. Not. IMRN*, (3):479–492, 2012.
- [10] Reda Chhaibi and Joseph Najnudel. On the circle $GMC^\gamma = \varprojlim C\beta E_n$ for $\gamma = \sqrt{\frac{2}{\beta}}$, ($\gamma \leq 1$). *arXiv preprint arXiv:1904.00578*, 2019.
- [11] Bertrand Duplantier, Rémi Rhodes, Scott Sheffield, and Vincent Vargas. Renormalization of critical Gaussian multiplicative chaos and KPZ relation. *Comm. Math. Phys.*, 330(1):283–330, 2014.
- [12] Sean Eberhard, Kevin Ford, and Ben Green. Permutations fixing a k -set. *Int. Math. Res. Not. IMRN*, (21):6713–6731, 2016.
- [13] Kevin Ford. The distribution of integers with a divisor in a given interval. *Ann. of Math. (2)*, 168(2):367–433, 2008.
- [14] Yan V. Fyodorov, Ghaith A. Hiary, and Jonathan P. Keating. Freezing transition, characteristic polynomials of random matrices, and the Riemann zeta function. *Physical review letters*, 108(17):170601, 2012.
- [15] Yan V. Fyodorov and Jonathan P. Keating. Freezing transitions and extreme values: random matrix theory, and disordered landscapes. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 372(2007):20120503, 2014.
- [16] Maxim Gerspach. Low Pseudomoments of the Riemann Zeta Function and Its Powers. *International Mathematics Research Notices*, 07 2020. rnaa159.
- [17] Andrew Granville, Adam J. Harper, and Kannan Soundararajan. Mean values of multiplicative functions over function fields. *Res. Number Theory*, 1:Art. 25, 18, 2015.
- [18] Gábor Halász. On random multiplicative functions. In *Hubert Delange colloquium (Orsay, 1982)*, volume 83 of *Publ. Math. Orsay*, pages 74–96. Univ. Paris XI, Orsay, 1983.
- [19] Adam J. Harper. Bounds on the suprema of Gaussian processes, and omega results for the sum of a random multiplicative function. *Ann. Appl. Probab.*, 23(2):584–616, 2013.
- [20] Adam J. Harper. On the limit distributions of some sums of a random multiplicative function. *J. Reine Angew. Math.*, 678:95–124, 2013.
- [21] Adam J. Harper. Moments of random multiplicative functions, II: High moments. *Algebra Number Theory*, 13(10):2277–2321, 2019.
- [22] Adam J. Harper. On the partition function of the Riemann zeta function, and the Fyodorov–Hiary–Keating conjecture. *arXiv preprint arXiv:1906.05783*, 2019.
- [23] Adam J. Harper. Almost sure large fluctuations of random multiplicative functions. *arXiv preprint arXiv:2012.15809*, 2020.
- [24] Adam J. Harper. Moments of random multiplicative functions, I: Low moments, better than squareroot cancellation, and critical multiplicative chaos. *Forum Math. Pi*, 8:e1, 95, 2020.
- [25] Adam J. Harper, Ashkan Nikeghbali, and Maksym Radziwiłł. A note on Helson’s conjecture on moments of random multiplicative functions. In *Analytic number theory*, pages 145–169. Springer, Cham, 2015.
- [26] Henry Helson. Hankel forms. *Studia Math.*, 198(1):79–84, 2010.
- [27] Bob Hough. Summation of a random multiplicative function on numbers having few prime factors. *Math. Proc. Cambridge Philos. Soc.*, 150(2):193–214, 2011.
- [28] Christopher P. Hughes, Jonathan P. Keating, and Neil O’Connell. On the characteristic polynomial of a random unitary matrix. *Comm. Math. Phys.*, 220(2):429–451, 2001.
- [29] Yuk-Kam Lau, Gérald Tenenbaum, and Jie Wu. On mean values of random multiplicative functions. *Proc. Amer. Math. Soc.*, 141(2):409–420, 2013.
- [30] Joseph Najnudel. On the extreme values of the Riemann zeta function on random intervals of the critical line. *Probab. Theory Related Fields*, 172(1-2):387–452, 2018.
- [31] Joseph Najnudel, Elliot Paquette, and Nick Simm. Secular coefficients and the holomorphic multiplicative chaos. *arXiv preprint arXiv:2011.01823*, 2020.
- [32] Marc Renault. Four proofs of the ballot theorem. *Math. Mag.*, 80(5):345–352, 2007.
- [33] Rémi Rhodes and Vincent Vargas. Gaussian multiplicative chaos and applications: a review. *Probab. Surv.*, 11:315–392, 2014.

DEPARTMENT OF MATHEMATICS, STANFORD UNIVERSITY, 450 SERRA MALL, BUILDING 380, STANFORD, CA, USA, 94305

Email address: `ksound@stanford.edu`

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF TORONTO, 40 ST. GEORGE STREET, ROOM 6290, TORONTO, ON, CANADA, M5S 2E4

Email address: `zaman@math.toronto.edu`