

ON PROBABILITY MEASURES ARISING FROM LATTICE POINTS ON CIRCLES

PÄR KURLBERG AND IGOR WIGMAN

ABSTRACT. A circle, centered at the origin and with radius chosen so that it has non-empty intersection with the integer lattice \mathbb{Z}^2 , gives rise to a probability measure on the unit circle in a natural way. Such measures, and their weak limits, are said to be *attainable* from lattice points on circles.

We investigate the set of attainable measures and show that it contains all extreme points, in the sense of convex geometry, of the set of all probability measures that are invariant under some natural symmetries. Further, the set of attainable measures is closed under convolution, yet there exist symmetric probability measures that are *not* attainable. To show this, we study the geometry of projections onto a finite number of Fourier coefficients and find that the set of attainable measures has many singularities with a “fractal” structure. This complicated structure in some sense arises from prime powers — singularities do not occur for circles of radius \sqrt{n} if n is *square free*.

1. INTRODUCTION

Let S be the set of nonzero integers expressible as a sum of two integer squares. For $n \in S$, let

$$\Lambda_n := \{\vec{\lambda} = a + bi \in \mathbb{Z}[i] : a^2 + b^2 = n\}$$

denote the intersection of the lattice $\mathbb{Z}[i] \subset \mathbb{C}$ with a circle centered at the origin and of radius \sqrt{n} . For $n \in S$, let $r_2(n) := |\Lambda_n|$ denote the cardinality of Λ_n ; for $n \notin S$ it is convenient to define $r_2(n) = 0$. We define a probability measure μ_n on the unit circle

$$\mathcal{S}^1 := \{z \in \mathbb{C} : |z| = 1\}$$

by letting

$$\mu_n := \frac{1}{r_2(n)} \sum_{\vec{\lambda} \in \Lambda_n} \delta_{\vec{\lambda}/\sqrt{n}},$$

where δ_z denotes the Dirac delta function with support at z . The measures μ_n are clearly invariant under multiplication by i and under

Date: April 26, 2018.

complex conjugation. We say that a measure on \mathcal{S}^1 is *symmetric* if it is invariant under these symmetries.

Definition 1.1. *A probability measure ν is said to be **attainable from lattice points on circles**, or simply just **attainable**, if ν is a weak limit point of the set $\{\mu_n\}_{n \in S}$.*

We note that any attainable measure is automatically symmetric. Now, if two integers $m, n \in S$ are co-prime,

$$(1) \quad \mu_{mn} = \mu_m \star \mu_n,$$

where \star denotes convolution of measures on \mathcal{S}^1 . Thus measures μ_n for n a prime power are of particular interest. It turns out that the closure of the set of measures given by μ_{p^e} for p ranging over all primes $p \equiv 1 \pmod{4}$ and exponents e ranging over integers $e \geq 1$ contains μ_{2^k} , as well as $\mu_{q^{2k}}$ for any prime $q \equiv 3 \pmod{4}$, and any exponent $k \geq 0$. (Note that $q^l \in S$ forces l to be even.)

Motivated by the above, we say that a measure μ is *prime power attainable* of μ is a weak limit point of the set $\{\mu_{p^e}\}_{p \equiv 1 \pmod{4}, e \geq 1}$. Similarly, we say that a measure μ is *prime attainable* if μ is a weak limit point of the set $\{\mu_p\}_{p \equiv 1 \pmod{4}}$.

Proposition 1.2. *The set of attainable measures is closed under convolution. Further, it is the closure (in the weak topology) of the collection of all convolutions of finitely many prime power attainable measures, i.e., it is topologically generated by the prime power attainable measures.*

Hence the set of attainable measures is the smallest closed (in the weak topology) set containing all the prime power attainable measures and closed w.r.t. convolution of probability measures. The set of all symmetric probability measures is clearly a convex set, hence equals the convex hull of its extreme points. Quite interestingly, the set of prime attainable measures is exactly the set of extreme points. Now, since the set of attainable measures contains the extreme points, and is closed under convolution one might wonder if *all* symmetric probability measures are attainable? By studying Fourier coefficients of attainable measures we shall show that **not all symmetric measures are attainable**.

Given a measure μ on \mathcal{S}^1 and $k \in \mathbb{Z}$, define the k -th Fourier coefficient of μ by

$$\hat{\mu}(k) := \int_{\mathcal{S}^1} z^{-k} d\mu(z).$$

If μ is symmetric it is straightforward to see that $\hat{\mu}(k) = 0$ unless $4|k$. Since μ is a probability measure, $\hat{\mu}(0) = 1$, hence the first two informative Fourier coefficients are $\hat{\mu}(4)$ and $\hat{\mu}(8)$; note that $\hat{\mu}(-k) = \hat{\mu}(k)$ for all k since μ is both real and even (i.e. it is invariant under complex conjugation).

Theorem 1.3. *If μ is attainable and $|\hat{\mu}(4)| > 1/3$ then*

$$(2) \quad 2\hat{\mu}(4)^2 - 1 \leq \hat{\mu}(8) \leq \mathcal{M}(\hat{\mu}(4)),$$

where

$$(3) \quad \mathcal{M}(x) = \max(x^4, (2|x| - 1)^2)$$

denotes the “max curve”. Conversely, given x, y such that $|x| \leq 1$ and

$$2x^2 - 1 \leq y \leq \mathcal{M}(x),$$

there exists an attainable measure μ such that $(\hat{\mu}(4), \hat{\mu}(8)) = (x, y)$.

For comparison, we note that the Fourier coefficients of the full set of symmetric probability measures has the following quite simple description (see section 3.2 below):

$$\{(\hat{\mu}(4), \hat{\mu}(8)) : \mu \text{ is symmetric}\} = \{(x, y) : |x| \leq 1, 2x^2 - 1 \leq y \leq 1\}.$$

As Figure 1 illustrates, the discrepancy between all symmetric measures and the attainable ones is fairly large. In particular, note that the curves $y = x^4$, $y = 2x^2 - 1$, and $(2|x| - 1)^2$ all have the same tangent at the two points $(\pm 1, 1)$, consequently the set of attainable measures has cusps near $(\pm 1, 1)$. However, there are attainable measures corresponding to points above the red curve for $|x| \leq 1/3$.

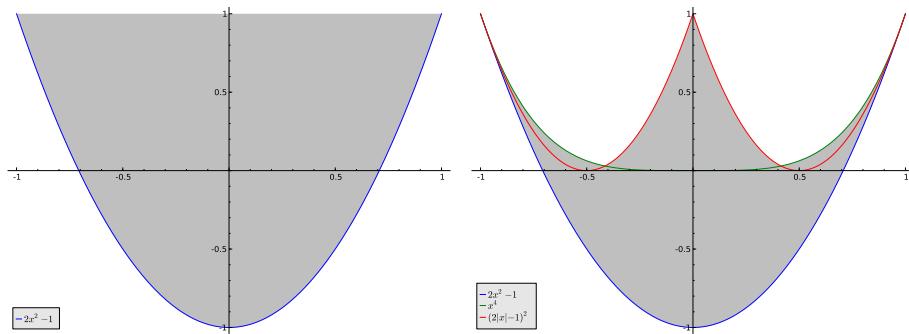


FIGURE 1. Left: $\{(\hat{\mu}(4), \hat{\mu}(8)) : \mu \text{ is symmetric}\}$. Right: the region defined by the inequalities $2x^2 - 1 \leq y \leq \max(x^4, (2|x| - 1)^2)$.

To give an indication of the rate at which the admissible region is “filled out”, as well as illuminate what happens in the region $|\hat{\mu}(4)| \leq 1/3$, we next present the results of some numerical experiments in Figures 2 and 3.

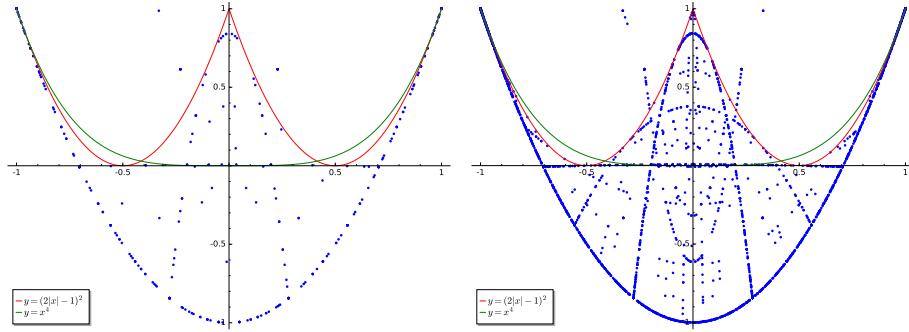


FIGURE 2. Left: $(\hat{\mu}_n(4), \hat{\mu}_n(8))$ for $n \in S, n \leq 1000$.
Right: $(\hat{\mu}_n(4), \hat{\mu}_n(8))$ for $n \in S, n \leq 10000$.

Note that points lying clearly above the red curve, but below the green one, are quite rare. However, “spikes” in the region $|\hat{\mu}(n)| \leq 1/3$ are clearly present.

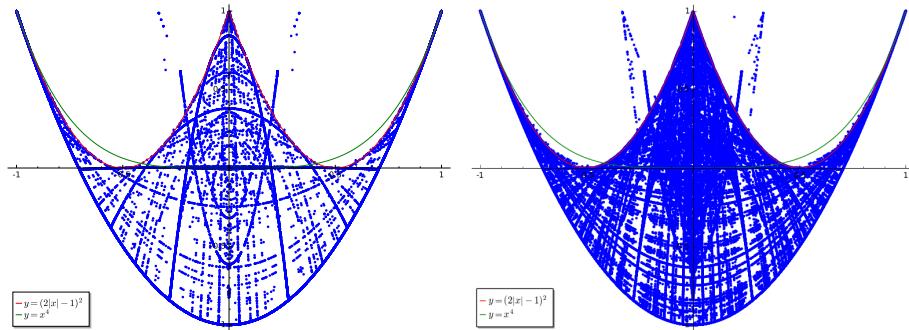


FIGURE 3. Left: $(\hat{\mu}_n(4), \hat{\mu}_n(8))$ for $n \in S, n \leq 100000$.
Right: $(\hat{\mu}_n(4), \hat{\mu}_n(8))$ for $n \in S, n \leq 1000000$.

1.1. Square free attainable measures. As we shall see, the spikes in the region $|\hat{\mu}(4)| \leq 1/3$ are limits of measures μ_n where n is divisible by p^e for $e \geq 2$, but for measures arising from square free $n \in S$, the structure is much simpler.

We say that a measure μ is *square free attainable* if μ is a limit point of the set $\{\mu_n : n \in S \text{ and } n \text{ is square free}\}$. The set of square free attainable measures is also closed under convolution, and it is easy to

see that it is generated by the set $\{\mu_p\}_{p \equiv 1 \pmod{4}}$, whose closure is the set of prime attainable measures.

Theorem 1.4. *If μ is square free attainable then*

$$(4) \quad 2\hat{\mu}(4)^2 - 1 \leq \hat{\mu}(8) \leq \mathcal{M}(\hat{\mu}(4)).$$

Conversely, if $2x^2 - 1 \leq y \leq \mathcal{M}(x)$ there exists a square free attainable measure μ such that $(\hat{\mu}(4), \hat{\mu}(8)) = (x, y)$.

The proof of Theorem 1.4 is very similar to the proof of Proposition 1.2, cf. Remark 4.2.

1.2. Prime power attainable measures. As mentioned before, the spikes in the region $|\hat{\mu}(4)| \leq 1/3$ are due to measures μ_n for which n is divisible by a prime power p^e , for e large. Recall that a measure μ is prime power attainable if μ is a weak limit point of the set $\{\mu_{p^e}\}_{p \equiv 1 \pmod{4}, e \geq 1}$. If μ is a prime power attainable measure, then the point $(\hat{\mu}(4), \hat{\mu}(8))$ can indeed lie *above* the curve $\max(x^4, (2|x| - 1)^2)$ in the region $|\hat{\mu}(4)| \leq 1/3$, though this phenomenon only occurs for even exponents (see Figure 4). In fact, we will show that for every $k \in \mathbb{Z}^+$

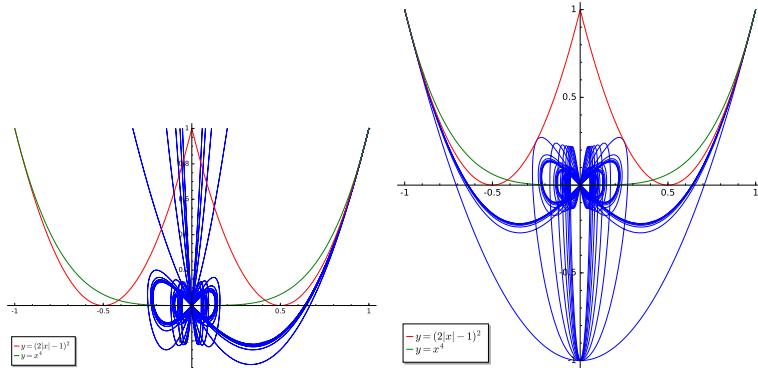


FIGURE 4. Prime power attainable measures attainable by p^M , $p \equiv 1(4)$ primes, $M \leq 19$. Left picture: even M . Right picture: odd M .

there exists prime power attainable μ such that

$$(\hat{\mu}(4), \hat{\mu}(8)) = \left(\frac{1}{2k+1}, 1 \right).$$

1.3. Fractal structure for $|\hat{\mu}(4)| \leq \frac{1}{3}$. Let

$$(5) \quad \mathcal{A}_2 := \{(\hat{\mu}(4), \hat{\mu}(8)) : \mu \text{ is attainable}\}$$

denote the projection of the set of attainable measures onto the first two non-trivial Fourier coefficients. The intersection of \mathcal{A}_2 with the

vertical strip $\{(x, y) : |x| \leq 1/3\}$ turns out to have a rather complicated fractal structure with infinitely many spikes — see Figure 5. Since \mathcal{A}_2 is closed under multiplication and $(-1, 1) \in \mathcal{A}_2$ it implies that it is invariant w.r.t.

$$(6) \quad (x, y) \mapsto (-x, y),$$

and hence we may assume $x \geq 0$.

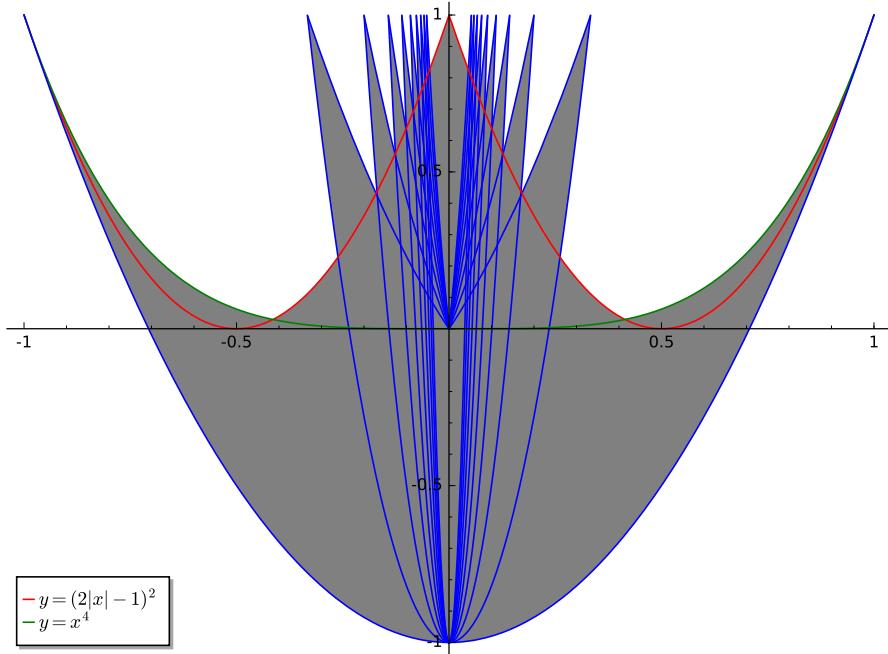


FIGURE 5. Points $(\hat{\mu}(4), \hat{\mu}(8))$ for some attainable measures μ giving rise to spikes in the region $|\hat{\mu}(4)| \leq 1/3$.

To be able to give a complete description of \mathcal{A}_2 we need a definition.

Definition 1.5. Let $x_0 \in [0, 1]$ and $a < x_0$.

- (1) We say that a pair of continuous functions

$$f_1, f_2 : (a, x_0] \rightarrow [0, 1],$$

defines a **cornered domain between a and x_0** if for all $x \in (a, x_0]$ one has $f_1(x) \leq f_2(x)$, and $f_1(x) = f_2(x)$ if and only if $x = x_0$, whence $f_1(x_0) = f_2(x_0) = 1$.

- (2) For a pair of functions f_1, f_2 as above the corresponding **cornered domain between a and x_0** is

$$\mathcal{D}_{a,x_0}(f_1, f_2) = \{(x, y) \in \mathbb{R}^2 : x \in (a, x_0], f_1(x) \leq y \leq f_2(x)\}.$$

The function f_1 and f_2 will be referred to as the “lower and upper” bounds for $\mathcal{D}_{a,x_0}(f_1, f_2)$ respectively.

Theorem 1.6. *The intersection of the set \mathcal{A}_2 with the line $y = 1$ equals*

$$\left\{ \left(\frac{\pm 1}{2k+1}, 1 \right) : k \geq 1 \right\} \cup \{(0, 1)\} \cup \{(\pm 1, 1)\}.$$

Further, for $k \geq 1$, let $x_k = \frac{1}{2k+1}$ be the x -coordinate of a point of the intersection described above. Then, for every $k \geq 1$ there exists a pair of continuous piecewise analytic functions $f_{1;k}, f_{2;k}$ defining a cornered domain between 0 and x_k , so that \mathcal{A}_2 admits the following global description:

$$(7) \quad \mathcal{A}_2 \cap \left\{ 0 < x \leq \frac{1}{3} \right\} = \left(\bigcup_{k=1}^{\infty} \mathcal{D}_{0,x_k}(f_{1;k}, f_{2;k}) \right) \cup \bigcup \left\{ (x, y) : 0 < x \leq \frac{1}{3}, 2x^2 - 1 \leq y \leq (2x - 1)^2 \right\}.$$

Theorem 1.6 is a rigorous explanation of the thin strips or “spikes” connecting all the reciprocals of odd numbers on $y = 1$, and the curve $y = (2|x| - 1)^2$, as in Figure 5. We remark that the functions $f_{1;k}$ and $f_{2;k}$ can with some effort be computed explicitly. The lower bound $f_{1;k}$ is given as the (component-wise) product of $(x_k, 1)$ by the parabola $y = 2x^2 - 1$ mapping $(1, 1) \mapsto (x_k, 1)$; we re-parameterize the resulting curve $(x \cdot x_k, 2x^2 - 1)$ so that it corresponds to the function

$$(8) \quad f_{1;k}(x) = \frac{2}{x_k^2} x^2 - 1,$$

whose slope at x_k is $f'_{1;k}(x_k) = 4(2k + 1)$.

The upper bound $f_{2;k}(x)$ is of a somewhat more complicated nature, see Definition 6.3; it is analytic around the corner with the slope $f'_{2;k}(x_k) = \frac{4}{3}(2k + 1)$ (see the proof of Theorem 1.6 in section 6), and it is *plausible* that it is (everywhere) analytic. It then follows that the set \mathcal{A}_2 has a discontinuity, or a jump, at $x = x_k$ (this is a by-product of the fact that the slopes of both $f_{1;k}$ and $f_{2;k}$ at x_k are *positive*.)

1.4. Discussion. Our interest in attainable measures originates in the study [5] of zero sets (“nodal lines”) of random Laplace eigenfunctions on the standard torus $\mathbb{T} := \mathbb{R}^2/\mathbb{Z}^2$. More precisely, for each $n \in S$ there is an associated Laplace eigenvalue given by $4\pi^2 n$, with eigenspace dimension equal to $r_2(n)$. On each such eigenspace there is a natural notion of a “random eigenfunction”, and the variance (appropriately

normalized) of the nodal line lengths of these random eigenfunctions equals $(1 + \widehat{\mu_n}(4)^2)/512 + o(1)$ as $r_2(n) \rightarrow \infty$. It was thus of particular interest to show that the accumulation points of $\widehat{\mu_n}(4)^2$, as $n \in S$ tends to infinity in such a way that also the eigenspace dimension $r_2(n) \rightarrow \infty$, is maximal — namely the full interval $[0, 1]$. This is indeed the case (cf. [5, Section 1.4]), but a very natural question is: which measures are attainable?

In order to obtain asymptotics for the above variance it is essential to assume that the eigenspace dimension grows, and one might wonder if “fewer” measures are attainable under this additional assumption. However, as the following shows, this is not the case (the proof can be found in section 4.4.)

Proposition 1.7. *A measure $\mu \in \mathcal{P}$ is attainable (i.e. $\mu \in \mathcal{A}$), if and only if there exists a sequence $\{n_j\}$ such that $\mu_{n_j} \Rightarrow \mu$ with the additional property that $r_2(n_j) \rightarrow \infty$.*

1.5. Outline. For the convenience of the reader we briefly outline the contents of the paper. In Section 2 we give some explicit examples of attainable, and non-attainable measures, and describe our motivation for studying the set of attainable measures. In Section 3 we give a brief background on Fourier coefficients of probability measures, and in Section 4 we recall some needed facts from number theory along with proving the more basic results above. Section 5 contains the proof of Theorem 1.3 (a complete classification of attainable measures in the region $|\hat{\mu}(4)| > 1/3$), and Section 6 contains the proof of Theorem 1.6 (the complete classification of attainable measures in the region $|\hat{\mu}(4)| \leq 1/3$), postponing some required results of technical nature to the appendix. Finally, in Section 7, we classify the set of square-free attainable measures.

1.6. Acknowledgements. We would like to thank Zeév Rudnick and Mikhail Sodin for raising the problem considered in this manuscript, and the many fruitful discussions concerning various subjects related to the presented research. We thank Fedor Nazarov and Peter Sarnak for many stimulating and fruitful discussions leading to some improvements of our results. Finally, it is a pleasure to thank the anonymous referee for reading our manuscript very carefully and giving a large number of comments that helped us to greatly improve the exposition.

P.K. was partially supported by grants from the Göran Gustafsson Foundation for Research in Natural Sciences and Medicine, and the Swedish Research Council (621-2011-5498). The research leading to these results has received funding from the European Research

Council under the European Union's Seventh Framework Programme (FP7/2007-2013), ERC grant agreement n° 335141 (I.W.), and an EP-SRC Grant EP/J004529/1 under the First Grant Scheme (I.W.).

2. EXAMPLES OF ATTAINABLE AND UNATTAINABLE MEASURES

2.1. Some conventions.

$$\tilde{\delta}_0 := \frac{1}{4} \sum_{k=0}^3 \delta_{i^k}$$

be the atomic probability measure supported at the 4 symmetric points $\pm 1, \pm i$ (“Cilleruelo measure”). Given an angle $\theta \in [0, \pi/4]$, let

$$(9) \quad \tilde{\delta}_\theta := \tilde{\delta}_0 \star (\delta_{e^{i\theta}} + \delta_{e^{-i\theta}})/2 = \frac{1}{8} \sum_{k=0}^3 (\delta_{e^{i(\pi k/2+\theta)}} + \delta_{e^{i(\pi k/2-\theta)}});$$

recall that \star denotes convolution on S^1 . For $\theta = 0, \pi/4$ the measure $\tilde{\delta}_\theta$ is supported at 4 points whereas for all other values of θ the support consists of 8 points. Given an integer $m \geq 1$ and $\theta \in [0, \pi/4]$, let

$$\tilde{\delta}_{\theta,m} := \tilde{\delta}_0 \star \left(\frac{1}{m+1} \sum_{j=0}^m \delta_{e^{i\theta(m-2j)}} \right).$$

We note that $\tilde{\delta}_\theta = \tilde{\delta}_{\theta,1}$, and that a measure μ , a priori invariant under complex conjugation, is symmetric if and only if μ is invariant under convolution with $\tilde{\delta}_0$; in this case convolving with $\tilde{\delta}_0$ is a convenient way to ensure that a measure is symmetric.

2.2. Some examples of attainable and unattainable measures.

Given $\theta \in [0, \pi/4]$ let τ_θ denote the symmetric probability measure with uniform distribution on the four arcs given by

$$\{z : |z| = 1, \arg(z) \in \cup_{k=0}^4 [k\pi/2 - \theta, k\pi/2 + \theta]\}.$$

Using some well known number theory given below (cf. section 4) it is straightforward to show that τ_θ is attainable for all $\theta \in [0, \pi/4]$. In particular, $d\mu_{\text{Haar}} = d\tau_{\pi/4}$, the Haar measure on S^1 normalized to be a probability measure, is attainable. In fact, it is well known (see e.g. [2]) that there exists a density one subsequence $\{n_j\} \subseteq S$, for which the corresponding lattice points Λ_{n_j} become equidistributed on the circle; this gives another construction of $d\mu_{\text{Haar}}$ as an attainable measure.

It is also possible to construct other singular measures. In Section 4 we will outline a construction of attainable measures, uniformly supported on Cantor sets. Moreover, if q is a prime congruent to 3 modulo 4 it is well known that the solutions to $a^2 + b^2 = q^2$ are given by

$(a, b) = (0, \pm q)$, or $(\pm q, 0)$, thus $\tilde{\delta}_0$ is attainable. A subtler fact, due to Cilleruelo, is that there exists sequences $\{n_j\}_{j \geq 1}$ for which Λ_{n_j} has very singular angular distribution even though the number of points $r_2(n_j)$ tends to infinity. Namely, it is possible to force all angles to be arbitrarily close to integer multiples of $\pi/2$, hence $\frac{1}{4} \sum_{k=0}^3 \delta_{ik}$ is an accumulation point of $d\mu_{n_j}$ as $n_j \rightarrow \infty$ in such a way that $r_2(n_j) \rightarrow \infty$.

We may also construct some explicit *unattainable* probability measures on \mathcal{S}^1 satisfying all the symmetries; in fact the following corollary of Theorem 1.6 constructs explicit unattainable measures, remarkably supported on 8 points only — the minimum possible for symmetric unattainable measures.

Corollary 2.1 (Corollary from Theorem 1.6). *The probability measure*

$$\eta_a := a\tilde{\delta}_0 + (1-a)\tilde{\delta}_{\pi/4}$$

is attainable, if and only if $a = 0, \frac{1}{2}, 1$ or a is of the form

$$a = \frac{1}{2} \pm \frac{1}{2(2k+1)}$$

for some $k \geq 1$.

3. FOURIER ANALYSIS OF PROBABILITY MEASURES

3.1. Some notation and de-symmetrization of probability measures. It is convenient to work with two models: either with the unit circle embedded in \mathbb{C} , or

$$\mathbb{T}^1 := \mathbb{R}/2\pi\mathbb{Z}.$$

Rather than working with $\{\mu_n\}$ and its weak partial limits, for notational convenience we work with their de-symmetrized variants, i.e.

$$(10) \quad d\nu_n(\theta) = d\mu_n\left(\frac{\theta}{4}\right),$$

$\theta \in \mathbb{T}^1$. The measures ν_n are invariant under complex conjugation (recall that $\mathcal{S}^1 \subseteq \mathbb{C}$); equivalently, for $\theta \in \mathbb{T}^1$,

$$d\nu_n(-\theta) = d\nu_n(\theta).$$

Notation 3.1. Let \mathcal{P} be the set of all probability measures μ on \mathcal{S}^1 satisfying for $\theta \in \mathbb{T}^1$

$$(11) \quad d\mu(-\theta) = d\mu(\theta).$$

Further, let $\mathcal{A} \subseteq \mathcal{P}$ be the set of all weak partial limits of $\{\nu_n\}$ i.e. all probability measures $\mu \in \mathcal{P}$ such that there exists a sequence $\{n_j\}$ with

$$\nu_{n_j} \Rightarrow \mu.$$

The set \mathcal{A} defined above is the de-symmetrization of the collection of attainable measures via (10); by abuse of notation we will refer to the elements of \mathcal{A} as attainable measures. One may restate Proposition 1.2 as stating that \mathcal{A} is closed w.r.t. convolutions; thus \mathcal{A} is an abelian monoid with identity $\delta_0 \in \mathcal{A}$. The effect of the de-symmetrization (10) is that for all $m \in \mathbb{Z}$

$$\widehat{\nu}_n(m) = \widehat{\mu_n}(4m);$$

since by the $\pi/2$ -rotation invariance of μ_n , $\widehat{\mu}(k) = 0$ unless k is divisible by 4, this transformation preserves all the information.

3.2. Measure classification on the Fourier side. We would like to study the image of \mathcal{A} under Fourier transform, or, rather, its projections into finite dimensional spaces. Since $\mathcal{A} \subseteq \mathcal{P}$ we first study the Fourier image of the latter; a proper inclusion of the image of \mathcal{A} inside the image of \mathcal{P} would automatically imply the existence of unattainable measures $\mu \in \mathcal{P} \setminus \mathcal{A}$.

For $\theta \in (0, \pi)$ let v_θ be the probability measure

$$(12) \quad v_\theta = \frac{1}{2} (\delta_\theta + \delta_{-\theta}),$$

and for the limiting values $\theta = 0, \pi$ we denote $v_0 = \delta_0$ and $v_\pi = \delta_\pi$. As for $\theta \in [0, \pi]$, δ_θ are the de-symmetrizations of $\tilde{\delta}_{\theta/4}$ in (9), attainable by Proposition 1.2 (see also Lemma 4.1 below), and it then follows that $v_\theta \in \mathcal{A}$. Clearly (see e.g. [6], Chapter 1) the set \mathcal{P} is the convex hull of

$$\{v_\theta : \theta \in [0, \pi]\}.$$

Let $\mathcal{P}_k \subseteq \mathbb{R}^k$ be the image of \mathcal{P} under the projection $\mathcal{F}_k : \mathcal{P} \rightarrow \mathbb{R}^k$ given by

$$\mathcal{F}_k(\mu) := (\widehat{\mu}(1), \dots, \widehat{\mu}(k)),$$

i.e. $\mathcal{P}_k = \mathcal{F}_k(\mathcal{P})$ are the first k Fourier coefficients of the measure μ as μ varies in \mathcal{P} . Recalling the invariance (11) for $\mu \in \mathcal{P}$ we may write

$$\mathcal{F}_k \mu = (\widehat{\mu}(1), \dots, \widehat{\mu}(k)) = \int_0^{2\pi} \gamma_k(\theta) d\mu(\theta),$$

where γ_k is the curve

$$\gamma_k(\theta) = (\cos(\theta), \cos(2\theta), \dots, \cos(k\theta))$$

for $\theta \in [0, 2\pi]$. Thus $\mathcal{P}_k = \mathcal{F}_k(\mathcal{P})$ could be regarded as a convex combination of points lying on γ_k (corresponding to v_θ); it would be then reasonable to expect \mathcal{P}_k to be equal to the convex hull of γ_k .

This intuition was made rigorous in a more general scenario by F. Riesz [8] in a classical theorem on the generalized moments problem (cf. [6], Chapter 1, Theorem 3.5 on p. 16). The sets \mathcal{P}_k are the convex hulls of the curves γ_k in \mathbb{R}^k indeed. Interestingly, since $\cos(m\theta)$ is a polynomial in $\cos(\theta)$, the curve γ_k is algebraic. As a concrete example, for $k = 2$ the image \mathcal{P}_2 of \mathcal{P} under

$$\mathcal{F}_2 : \mu \mapsto (\widehat{\mu}(1), \widehat{\mu}(2))$$

is the convex hull of the parabola $y = 2x^2 - 1$, $x \in [-1, 1]$, i.e. the set

$$(13) \quad \mathcal{P}_2 = \{(x, y) : x \in [-1, 1], 2x^2 - 1 \leq y \leq 1\},$$

as shown in Figure 1, to the left.

Analogously to the above, define

$$\mathcal{A}_k = \mathcal{F}_k(\mathcal{A}) \subseteq \mathcal{P}_k,$$

(cf. (5), and bear in mind the de-symmetrization (10)). Since, by the definition, \mathcal{A} is closed in \mathcal{P} (i.e. the weak limit set of \mathcal{A} satisfies $\mathcal{A}' \subseteq \mathcal{A}$), it follows that for every $k \geq 2$, \mathcal{A}_k is closed in \mathcal{P}_k in the usual sense. The shell $y = 2x^2 - 1$ of the convex hull \mathcal{P}_2 is (uniquely) attained by the family $\{v_\theta : \theta \in [0, \pi]\}$ of measures as in (12) with the Fourier coefficients

$$(14) \quad (\widehat{v}_\theta(1), \widehat{v}_\theta(2)) = (\cos(\theta), \cos(2\theta)).$$

Finally, it is worth mentioning that the set \mathcal{A} is *not convex*, as \mathcal{A}_2 contains the parabola

$$\{(x, 2x^2 - 1) : x \in [-1, 1]\} \subseteq \mathcal{A}_2,$$

whose points correspond to the measures (12), though not its convex hull. (In other words, had \mathcal{A} been convex, that would force all symmetric measures to be attainable.)

4. PROOFS OF THE BASIC RESULTS

4.1. Number theoretic background. We start by giving a brief summary on the structure of Λ_n (equivalently, μ_n or their de-symmetrized by (10) versions ν_n) given the prime decomposition of n . These results follow from the (unique) prime factorization of Gaussian integers, see e.g. [1]. First, for every “split” prime

$$p \equiv 1 \pmod{4},$$

there exists an angle $\theta_p \in [0, \pi]$, such that the measure ν_p arising from p is given by

$$\nu_p = v_{\theta_p} = (\delta_{\theta_p} + \delta_{-\theta_p})/2.$$

More generally, if a split prime p occurs to a power p^e , we find that the resulting measure is given by

$$\nu_{p^e} = \nu_{\theta_p, e},$$

where

$$(15) \quad \nu_{\theta; M} = \frac{1}{M+1} \sum_{k=0}^M \delta_{(M-2k)\theta},$$

and hence, in particular,

$$r_2(p^e) = 4(e+1)$$

(recall the de-symmetrization (10)). Both the $\{\nu_n\}$ and $\frac{1}{4}r_2(n)$ are multiplicative in the sense that for n_1, n_2 co-prime numbers $(n_1, n_2) = 1$,

$$(16) \quad \nu_{n_1 \cdot n_2} = \nu_{n_1} \star \nu_{n_2},$$

and

$$r_2(n_1)r_2(n_2) = 4r_2(n_1n_2).$$

In particular, $r_2(n) = 0$ unless n is of the form

$$n = 2^a p_1^{e_1} \cdot \dots \cdot p_k^{e_k} q_1^{2r_1} \cdot \dots \cdot q_l^{2r_l},$$

for $p_i \equiv 1 \pmod{4}$, $q_j \equiv 3 \pmod{4}$ primes (in particular, all the exponents of primes $\equiv 3 \pmod{4}$ are even); in this case

$$\nu_n = \star_{i=1}^k \nu_{p_i^{e_i}},$$

and

$$r_2(n) = 4 \prod_{i=1}^k (e_i + 1).$$

By Hecke's celebrated result [3, 4] the angles θ_p are equidistributed in $[0, \pi/4]$: for every $0 \leq \alpha < \beta \leq \pi$,

$$\#\{p \leq X, p \equiv 1(4) : \theta_p \in [\alpha, \beta]\} \sim \frac{(\beta - \alpha)}{\pi/4} \cdot \frac{X}{2 \log X}$$

In particular, the following lemma is an immediate consequence.

Lemma 4.1. *For every $\theta \in [0, \pi]$ and $\epsilon > 0$ there exist a split prime p with*

$$|\theta_p - \theta| < \epsilon.$$

4.2. Proof of Proposition 1.2.

Proof. We will prove the equivalent de-symmetrized version of the statement, i.e. that if $\gamma_1, \gamma_2 \in \mathcal{A}$ then

$$\gamma_1 \star \gamma_2 \in \mathcal{A}.$$

Let $\{m_k\}, \{n_k\} \subseteq S$ be two sequences so that $\nu_{m_k} \Rightarrow \gamma_1, \nu_{n_k} \Rightarrow \gamma_2$. We would like to invoke the multiplicativity (16) of $\{\nu_n\}$; we cannot apply it directly, as n_k and m_k may fail to be co-prime. To this end rather than using ν_{m_k} we are going to substitute¹ it with $\nu_{m'_k}$ chosen to approximate ν_{m_k} , so that m'_k is co-prime to n_k , via Lemma 4.1. In the remaining part of the proof we shall argue that

$$(17) \quad \nu_{m'_k \cdot n_k} = \nu_{m'_k} \star \nu_{n_k} \Rightarrow \gamma_1 \star \gamma_2,$$

provided we care to choose m'_k so that $\nu_{m'_k}$ approximates ν_{m_k} sufficiently well.

To this end it is more convenient to work with the space of Fourier coefficients; the weak convergence of probability measures corresponds to point-wise convergence of the Fourier coefficients. By Lemma 4.1 we may replace m_k with m'_k co-prime to n_k that satisfies for every $j \leq k$

$$|\widehat{\nu_{m_k}}(j) - \widehat{\nu_{m'_k}}(j)| < \frac{1}{k}.$$

It then readily follows that $\nu_{m'_k} \Rightarrow \gamma_1$, and hence we establish (17), which in turn implies that $\gamma_1 \star \gamma_2 \in \mathcal{A}$, finally yielding the closedness of \mathcal{A} w.r.t. convolutions.

As for the second assertion, if $\mu \in \mathcal{A}$, then μ is a weak limit of a sequence ν_{n_j} for some $\{n_j\} \subseteq S$. Factoring $n_j = p_{j;1}^{e_{j;1}} \cdots p_{j;r}^{e_{j;r}}$ we have

$$\nu_{n_j} = \nu_{p_{j;1}}^{e_{j;1}} \star \cdots \star \nu_{p_{j;r}}^{e_{j;r}}$$

and thus μ indeed lies in the closure of finite convolutions of prime power attainable measures of the form ν_p .

□

Remark 4.2. *The proof of Theorem 1.4 is similar — replacing prime power attainable measures with prime attainable measures in the above argument yields the corresponding result for square-free attainable measures.*

¹One may think about this procedure as a number theoretical analogue of choosing an independent identically distributed copy of a given random variable.

4.3. Cantor sets are attainable. By Proposition 1.2, \mathcal{A} is closed under convolution, it contains [5] uniform measures supported on symmetric intervals $[-\theta, \theta]$, as well as symmetric sums $(\delta_\theta + \delta_{-\theta})/2$ for all $\theta > 0$. Thus, by using an “additive” construction of Cantor sets, we easily see that uniform measures supported on Cantor sets are attainable.

Namely, given $\theta > 0$, let $C_{n,\theta}$ be the n -th level Cantor set obtained by starting with the interval $[-\theta, \theta]$ and deleting the middle third part of the interval: $C_{0,\theta}$ consists of one closed interval $[-\theta, \theta]$, and $C_{n+1,\theta} \subset C_{n,\theta}$ is the union of the 2^{n+1} intervals obtained by removing the middle third in each of the 2^n intervals that $C_{n,\theta}$ consists of. Now,

$$(18) \quad C_{n+1,\theta} = (C_{n,\theta/3} - 2\theta/3) \sqcup (C_{n,\theta/3} + 2\theta/3),$$

where \sqcup denotes disjoint union, and $C_{n+1,\theta/3} + \alpha$ denotes the translation of the set $C_{n+1,\theta/3}$ by α .

Since $C_{0,\theta}$ is a symmetric interval, the measure corresponding to its characteristic function is attainable, as mentioned above. Further, since convolving $(\delta_\theta + \delta_{-\theta})/2$ with a uniform measure having support on some set D yields a measure with support on $(D + \theta) \cup (D - \theta)$, uniform measures supported on $C_{n,\theta}$ are attainable by induction, via (18). Letting $n \rightarrow \infty$ we find that measures with uniform support on Cantor sets are attainable.

4.4. Proof of Proposition 1.7.

Proof. We are going to make use of a (de-symmetrized) Cilleruelo sequence n_j , i.e. $\nu_{n_j} \Rightarrow \delta_0$ and $r_2(n_j) \rightarrow \infty$. Let $\mu \in \mathcal{A}$ be an attainable measure and assume that $\nu_{m_j} \Rightarrow \mu$. Using the same idea as in the course of proof of Proposition 1.2 above we may assume with no loss of generality that $(n_j, m_j) = 1$ are co-prime (recall that $\{n_j\}$ is a Cilleruelo sequence of our choice). Then

$$\nu_{m_j \cdot n_j} = \nu_{m_j} \star \nu_{n_j} \Rightarrow \mu \star \delta_0 = \mu,$$

and

$$r_2(m_j \cdot n_j)/4 = r_2(m_j) \cdot r_2(n_j) \rightarrow \infty,$$

so that the sequence $\{n_j \cdot m_j\}$ is as required. □

5. PROOF OF THEOREM 1.3: MEASURE CLASSIFICATION FOR $x > \frac{1}{3}$

5.1. Some conventions related to Fourier Analysis. We adapt the following conventions. The k -th Fourier coefficient of a measure

$\mu \in \mathcal{P}$ is given by

$$\widehat{\mu}(k) = \int_{\mathbb{T}^1} \cos(k\theta) d\mu(\theta);$$

clearly $|\widehat{\mu}(k)| \leq 1$. The convolution of two probability measures $\mu, \mu' \in \mathcal{P}$ is the probability measure $\mu \star \mu'$ defined as

$$d(\mu \star \mu')(\theta) = \int_{\mathbb{T}^1} d\mu(\theta') d\mu'(\theta - \theta').$$

With the above conventions we have

$$\widehat{\mu \star \mu'}(k) = \widehat{\mu}(k) \cdot \widehat{\mu'}(k).$$

It is easy to compute the Fourier coefficients of $v_{\theta;M}$ as in (15) to be

$$\widehat{v}_{\theta;M}(k) = \frac{1}{M+1} \sum_{j=0}^M \cos((M-2j)k\theta) = G_{M+1}(k\theta),$$

where

$$(19) \quad G_A(\theta) := \frac{\sin(A\theta)}{A \sin \theta};$$

for $M = 1$, $G_2(\theta) = \cos(\theta)$ is consistent with (14).

By the definition of \mathcal{A} and $\mathcal{A}_k = \mathcal{F}_k(\mathcal{A})$ and in light of Lemma 4.1, we can describe \mathcal{A}_k geometrically as the smallest multiplicative set, closed in \mathcal{P}_k , containing all the curves²

$$\{\gamma_{k;A}(\theta) := (G_A(\theta), \dots, G_A(k\theta)) : \theta \in [0, \pi]\}_{A \geq 2},$$

i.e. \mathcal{A}_k is the closed multiplicative subset of \mathcal{P}_k generated by the above curves. Similarly, the set corresponding to the square-free attainable measures \mathcal{A}_k^0 is the smallest closed multiplicative set containing the single curve

$$\gamma_{k;2}(\theta) = (\cos(\theta), \dots, \cos(k\theta)),$$

$$\theta \in [0, \pi].$$

From this point on we will fix $k = 2$ and suppress the k -dependence in the various notation, e.g. γ_A will stand for $\gamma_{2;A}$. The curves

$$(20) \quad \gamma_A(\theta) := (G_A(\theta), G_A(2\theta))$$

for $2 \leq A \leq 20$ are displayed in Figure 4, separately for odd and even $M = A - 1$.

²Since G_A is even we have $\gamma_{k;2}(-\theta) = \gamma_{k;2}(\theta)$, and hence it is enough to consider $\theta \in [0, \pi]$ (rather than $\theta \in [0, 2\pi]$.)

5.2. Proof of Theorem 1.3. The two statements of Theorem 1.3 are claimed in Propositions 5.1 and 5.2, and proved in sections 5.3 and 5.6 respectively. Note that Proposition 5.2 yields attainable measures with the relevant Fourier coefficients regardless whether $x > \frac{1}{3}$ or $x \leq \frac{1}{3}$.

Proposition 5.1. *Points (x, y) with $x > \frac{1}{3}$ corresponding to attainable measures lie under the max curve, i.e. if $(x, y) \in \mathcal{A}_2$ then*

$$(21) \quad y \leq \mathcal{M}(x),$$

where $\mathcal{M}(x)$ is given by (3).

Proposition 5.2. *Given x, y such that $|x| \leq 1$ and*

$$2x^2 - 1 \leq y \leq \mathcal{M}(x),$$

there exists an attainable measure μ such that $(\hat{\mu}(4), \hat{\mu}(8)) = (x, y)$.

5.3. Proof of Proposition 5.1: attainable measures lie under the max curve for $x > 1/3$. In what follows, by componentwise product we will mean

$$(22) \quad (x_1, y_1) \cdot (x_2, y_2) = (x_1 \cdot x_2, y_1 \cdot y_2).$$

Definition 5.3 (Totally positive and mixed sign points.). *Let $\mathcal{A}_2^+ \subseteq \mathcal{A}_2$ be the set of **totally positive** attainable points admitting a representation as finite componentwise products*

$$(23) \quad (x, y) = \prod_{i=1}^K (x_i, y_i)$$

*of points $(x_i, y_i) = \gamma_{2;A_i}(\theta_i)$ for some $A_i \geq 2$, $\theta_i \in [0, \pi]$, so that for all $i \leq K$ we have $y_i > 0$. Similarly, $\mathcal{A}_2^- \subseteq \mathcal{A}_2$ is the set of **mixed sign** attainable points admitting representation (23) with at least one $y_i < 0$.*

Note that a point in \mathcal{A}_2 may be both totally positive and of mixed sign, i.e. \mathcal{A}_2^+ may intersect \mathcal{A}_2^- . Furthermore, a priori it may be in neither of these. However, by the definition of \mathcal{A}_2 , it is the closure of the union of the sets defined:

$$(24) \quad \overline{\mathcal{A}_2^+ \cup \mathcal{A}_2^-} = \mathcal{A}_2.$$

Therefore to prove the inequality (21) on \mathcal{A}_2 it is sufficient to prove the same for points in \mathcal{A}_2^+ and \mathcal{A}_2^- separately. These are established in Lemma 5.4 and Proposition 5.5, proved in sections 5.4 and 5.5 respectively.

Lemma 5.4. *If $(x, y) \in \mathcal{A}_2^-$ is a mixed sign attainable point then*

$$y \leq (2|x| - 1)^2.$$

Proposition 5.5. *Let $(x, y) = \gamma_A(\theta)$ for some $A \geq 2$ and $\theta \in [0, \pi]$ such that $x > \frac{1}{3}$. Then $y \leq x^4$.*

We are now in a position to prove Proposition 5.1.

Proof of Proposition 5.1 assuming Lemma 5.4 and Proposition 5.5. If the point $(x, y) \in \mathcal{A}_2^-$ is of mixed sign, Lemma 5.4 applies and hence $y \leq (2|x| - 1)^2$. Otherwise, if the point is totally positive,

$$(x, y) = \left(\prod_i x_i, \prod_i y_i \right)$$

where (x_i, y_i) are prime power attainable, and $y_i \geq 0$ for all i .

Now, $|x_i| \leq 1$ for all i since x_i is a Fourier coefficient of a probability measure, so if $|x| > 1/3$ we must have $|x_i| > 1/3$ for all i . By Proposition 5.5, $y_i \leq x_i^4$ for all i , and thus $y \leq x^4$. Thus it follows that the statement (21) of Proposition 5.1 holds on $\mathcal{A}_2^+ \cup \mathcal{A}_2^-$ and thus on its closure, \mathcal{A}_2 (cf. (24)).

□

5.4. Proof of Lemma 5.4: the mixed sign points \mathcal{A}_2^- lie under the max curve. To pursue the proof of Lemma 5.4 we will need some further notation.

Notation 5.6. *Let $B_1 \subseteq [-1, 1] \times [-1, 1]$ be the set*

$$B_1 = \{(x, y) : x \in [-1/2, 1/2], 0 \leq y \leq (2|x| - 1)^2\},$$

and $B \subseteq [-1, 1] \times [-1, 1]$ be the domain

$$B_2 = \{(x, y) : x \in [-1/\sqrt{2}, 1/\sqrt{2}], 2x^2 - 1 \leq y \leq 0\}$$

Recall the Definition 5.3 of totally positive attainable points \mathcal{A}_2^+ , and componentwise product of points (22). It is obvious that the points of either B_1 and B_2 are all lying under the max curve, i.e. if

$$(x, y) \in B_1 \cup B_2,$$

then

$$y \leq \mathcal{M}(x).$$

Therefore the following lemma implies Lemma 5.4.

Lemma 5.7. *If $(x, y) \in \mathcal{A}_2^-$ is a mixed sign attainable point then*

$$(x, y) \in B_1 \cup B_2.$$

To prove Lemma 5.7 we establish the following two auxiliary lemmas whose proof is postponed until immediately after the proof of Lemma 5.7.

Lemma 5.8. *If $(x, y) = (\hat{\mu}(1), \hat{\mu}(2))$ for μ some probability measure on \mathcal{S}^1 and $y \leq 0$, then $(x, y) \in B_2$.*

Lemma 5.9. *If $p_1, p_2 \in B_2$, then $p_1 \cdot p_2 \in B_1$.*

Proof of Lemma 5.7 assuming the auxiliary lemmas. Let

$$(x, y) \in \mathcal{A}_2^-$$

be given. First, if $(x, y) \in \mathcal{A}_2^-$ with $y \leq 0$, then $(x, y) \in B_2$ by Lemma 5.8; hence we may assume $y > 0$. Let (x_i, y_i) be as in (23), which according to the Definition 5.3 have mixed signs. Since $y \geq 0$ we can in fact find $i \neq j$ for which $y_i, y_j < 0$, and without loss of generality we may assume that $(i, j) = (1, 2)$. Letting

$$(\tilde{x}, \tilde{y}) = \left(\prod_{k \neq 1, 2} x_k, \prod_{k \neq 1, 2} y_k \right)$$

we find that

$$(x, y) = (x_1, y_1) \cdot (x_2, y_2) \cdot (\tilde{x}, \tilde{y}),$$

where $\tilde{y} \in [0, 1]$ and $\tilde{x} \in [-1, 1]$.

We further note that both (x_1, y_1) and (x_2, y_2) lie in B_2 . Thus by Lemma 5.9,

$$(x_1, y_1) \cdot (x_2, y_2) \in B_1.$$

Since $|\tilde{x}|, \tilde{y} \leq 1$, the result follows on noting that B_1 is mapped into itself by any map of the form

$$(x, y) \rightarrow (\alpha x, \beta y),$$

provided that

$$0 \leq |\alpha|, \beta \leq 1.$$

□

5.4.1. Proofs of the auxiliary lemmas 5.8 and 5.9.

Proof of Lemma 5.8. The assumptions are equivalent to $(x, y) \in \mathcal{P}_2$ with $y \leq 0$. The statement follows immediately upon using the explicit description (13) of \mathcal{P}_2 :

$$\mathcal{P}_2 \cap \{y \leq 0\} = B_2.$$

□

Proof of Lemma 5.9. The case of either point having zero y -coordinate is trivial, so we may assume that both p_1, p_2 have negative y -coordinates, and it suffices to prove the statement for points p_1, p_2 having minimal y -coordinates, i.e.,

$$p_1 = (a, 2a^2 - 1), \quad p_2 = (b, 2b^2 - 1),$$

and we may further assume $ab \neq 0$ as otherwise the statement is trivial.

By symmetry it suffices to consider the case $a, b \in (0, 1/\sqrt{2})$. Thus, if we fix $c \in (0, 1/2)$ it suffices to determine the maximum of

$$(2a^2 - 1)(2b^2 - 1)$$

subject to the constraint $ab = c$. Taking logs we find that the constraint is given by

$$\log a + \log b = \log c$$

and we wish to maximize

$$\log(1 - 2a^2) + \log(1 - 2b^2).$$

Using Lagrange multipliers we find that all internal maxima satisfies

$$(1/a, 1/b) = \lambda \left(\frac{4a}{1 - 2a^2}, \frac{4b}{1 - 2b^2} \right)$$

for some $\lambda \in \mathbb{R}$. If $c = ab \neq 0$ we find that

$$(1, 1) = \lambda \left(\frac{4a^2}{1 - 2a^2}, \frac{4b^2}{1 - 2b^2} \right)$$

and thus $\frac{4a^2}{1-2a^2} = \frac{4b^2}{1-2b^2}$ which implies that $a^2 = b^2$, and hence, recalling that we assumed $a, b \geq 0$, it yields $a = b$. In particular, any internal maximum gives a point $(a^2, (2a^2 - 1)^2) = (c, (2|c| - 1)^2)$, which lies on the boundary of B_1 . As mentioned earlier, for points on the boundary, the inequality holds trivially. \square

5.5. Proof of Proposition 5.5: totally positive points \mathcal{A}_2^+ corresponding to prime powers.

Lemma 5.10. *The function $\frac{\sin t}{t}$ is decreasing and is ≥ 0 on $[0, \pi]$.*

Proof. Taking derivatives, this amounts to the fact that $\tan t > t$ on $(0, \pi/2)$. \square

Lemma 5.11. *If $A \geq 4$ and $|G_A(t)| \geq 1/3$ for $t \in [0, \pi/2]$, then $t \leq \frac{\pi}{A}$. For $A = 3$, we have the further possibility that $t = 3\pi/(2A) = \pi/2$.*

Proof. The inequality $\sin t \geq 2t/\pi$, valid for $t \in [0, \pi/2]$, and strict except at the end points, gives that

$$|G_A(t)| = \left| \frac{\sin(At)}{A \sin t} \right| \leq \frac{1}{A \sin t} \leq \frac{1}{A \cdot \frac{2}{\pi} t}$$

and hence $|G_A(t)| < 1/3$ for $t > 3\pi/(2A)$, for any $A > 0$. It thus suffices to consider $t \in [0, 3\pi/(2A)]$.

Consider first the case $A = 3$. We begin by showing that $G_3(t)$ is decreasing on $[0, \pi/2]$. Taking derivatives, this amounts to the fact that

$$3 \tan t \neq \tan 3t$$

on $(0, \pi/2)$ (note that the derivative is negative for $t = \pi/6$). Now, since $G_3(\pi/3) = 0$ and $G_3(\pi/2) = -1/3$ and G_3 is decreasing, we find that the only possibility for $|G_3(t)| = 1/3$ and $t \in [\pi/3, \pi/2]$ is $t = \pi/2$. Thus, any other solution must lie in $[0, \pi/3] = [0, \pi/A]$.

For $A \geq 4$, note that

$$(25) \quad \left| \frac{\sin At}{A \sin t} \right| = \left| \frac{\sin(At)/(At)}{\sin(t)/t} \right| < \left| \frac{\sin(At)/(At)}{\sin(At/3)/(At/3)} \right|$$

(for $t \leq 3\pi/(2A)$ we have $At/3 \leq \pi/2$, hence

$$|\sin(At/3)/(At/3)| \leq |\sin(t)/t|,$$

since $(\sin x)/x$ is decreasing on the interval $[0, \pi]$ by Lemma 5.10.)

Taking $s = At/3$, the RHS of (25) becomes

$$\frac{(\sin 3s)/3s}{(\sin s)/s} = \frac{\sin 3s}{3 \sin s}$$

and $t \leq 3\pi/(2A)$ implies that $s \leq \pi/2$. For this range of s , by the first part of the lemma, we find that $\left| \frac{\sin 3s}{3 \sin s} \right| \geq 1/3$ implies that either $s = \pi/2$ or $s \leq \pi/3$, which in turn implies that $t = 3\pi/(2A)$ or $t \leq \pi/A$. Noting that the first possibility is ruled out by the strict inequality in (25), the proof is concluded. \square

We proceed to characterize points lying on curves $\{(x, y) = \gamma_A(t)\}_{A \geq 2}$, for which $x > 1/3$ and $y \geq 0$, showing that any such point satisfies $y \leq x^4$. We begin with the following key Lemma.

Lemma 5.12. *For $t \in (0, \pi/2]$, define*

$$(26) \quad h(t) := \frac{t^3 \cos t}{\sin^3 t}$$

and extend h to $[0, \pi/2]$ by continuity. Then $h(t)$ is decreasing on $[0, \pi/2]$.

Proof. We have

$$h'(t) = \frac{t^2 \sin^2(t) (\sin(t) \cos(t) - t \sin^2(t) - 3t \cos^2(t))}{\sin^6 t},$$

and it is enough to show that

$$(27) \quad \sin(t) \cos(t) - t \sin^2(t) - 3t \cos^2(t) < 0$$

for $t \in (0, \pi/2)$. Since for $t = 0$ the expression on the left hand side of (27) vanishes it is sufficient to show that its derivative is strictly negative on $(0, \frac{\pi}{2})$. We find that

$$\begin{aligned} (\sin(t)\cos(t) - t\sin^2(t) - 3t\cos^2(t))' &= \\ &= 4\sin(t)(t\cos(t) - \sin(t)) = 4\sin(t)\cos(t)(t - \tan t) < 0 \end{aligned}$$

since $\tan(t) > t$ on $(0, \frac{\pi}{2})$.

□

Proof of Proposition 5.5. If $A = 2$, the points lying on the curve γ_2 are of the form

$$(x, y) = \gamma_2(t) = (t, 2t^2 - 1),$$

and it is straightforward to check that $2t^2 - 1 \leq t^4$. For $A \geq 3$, since we assume that $x > 1/3$ and

$$(x, y) = (G_A(t), G_A(2t)),$$

Lemma 5.11 implies that $t \leq \pi/A$. In fact, $t \leq \pi/(2A)$, as we assume that $y \geq 0$. Hence it is sufficient to show that

$$\frac{\sin 2At}{A \sin 2t} \leq \left(\frac{\sin At}{A \sin t} \right)^4$$

holds for $t \in [0, \pi/(2A)]$.

This in turn is equivalent (note that all individual trigonometric terms are non-negative since $t \in [0, \pi/(2A)]$) to

$$A^3 \cos At \sin^3 t \leq \sin^3 At \cos t$$

which is equivalent to

$$\frac{(At)^3 \cos At}{\sin^3 At} \leq \frac{t^3 \cos t}{\sin^3 t}.$$

Setting

$$s = At \in [0, \pi/2],$$

we find that this is equivalent to

$$\frac{s^3 \cos s}{\sin^3 s} \leq \frac{(s/A)^3 \cos s/A}{\sin^3 s/A},$$

or, equivalently on recalling (26), that

$$h(s) \leq h(s/A).$$

which, as $A > 1$, follows from Lemma 5.12.

□

5.6. Proof of Proposition 5.2: all points under the max curve are attainable.

Lemma 5.13. *The curve $\{(x, x^4) : x \in [0, 1]\}$ is square-free attainable, i.e. all the points on this curve correspond to at least one attainable measure.*

Proof of Proposition 5.2 assuming Lemma 5.13. By the definition of the max curve (3) it is sufficient to prove that if (x_0, y_0) is lying under one of the curves $y = x^4$ and $y = (2|x| - 1)^2$ then $(x_0, y_0) \in \mathcal{A}_2$ is attainable; with no loss of generality we may assume that $x_0 \geq 0$. Now we know that the parabola $\{(t, 2t^2 - 1) : t \in [0, 1]\}$ is attainable, and from Lemma 5.13 so is the curve $\{(x, x^4) : x \in [0, 1]\}$.

It then follows by multiplicativity of \mathcal{A}_2 that all the points of the form

$$(x_0, y_0) = (x, x^4) \cdot (t, 2t^2 - 1)$$

are attainable (recalling the notation (22) for componentwise multiplication). On the other hand it is clear that the union of the family of the parabolas

$$\{(xt, x^4(2t^2 - 1)) : t \in [0, 1]\},$$

as x ranges over $[0, 1]$, is exactly the set

$$\{(x, y) : x \in [0, 1], 2x^2 - 1 \leq y \leq x^4\}.$$

Concerning points under the other curve $y = (2x - 1)^2$ we may employ the multiplicativity of \mathcal{A}_2 again to yield that the curve

$$\{(x^2, (2x^2 - 1)^2)\}_{x \in [0, 1]}$$

is attainable; this curve in turn can be re-parameterized as $\{(t, (2t - 1)^2) : t \in [0, 1]\}$. A similar argument to the above shows that function

$$(x, t) \mapsto (x, (2x - 1)^2) \cdot (t, 2t^2 - 1)$$

maps $[0, 1]^2$ onto the domain

$$\{(x, y) : x \in [0, 1], 2x^2 - 1 \leq y \leq (2x - 1)^2\},$$

i.e. as the parameter x varies along $[0, 1]$ the parabolas

$$\{(xt, (2x - 1)^2 \cdot (2t^2 - 1))\}$$

tessellate the domain under the curve $y = (2x - 1)^2$, $x \in [0, 1]$. Hence all the points under the latter curve are attainable, as claimed. \square

Proof of Lemma 5.13. We start with the case $x \geq 0$. We know that the curve $\{(x, 2x^2 - 1)\}_{x \in [-1, 1]}$ is attainable as a re-parametrization of $(\cos \theta, \cos 2\theta)$ (i.e. all the points on that curve correspond to attainable measures), hence for $n \geq 1$ the curve $\{(x^n, (2x^2 - 1)^n)\}$ is attainable by the multiplicativity (cf. Proposition 1.2). Fix $\alpha > 0$, and take $x = x_n = e^{-\alpha/n}$. Thus

$$(e^{-\alpha}, (2e^{-2\alpha/n} - 1)^n)$$

is attainable for every $\alpha > 0$ and $n \geq 1$.

Upon using Taylor series, we find that, as $n \rightarrow \infty$,

$$\begin{aligned} (2e^{-2\alpha/n} - 1)^n &= \left(2 \left(1 - \frac{2\alpha}{n} + O\left(\frac{1}{n^2}\right) \right) - 1 \right)^n = \\ &\quad \left(1 - \frac{4\alpha}{n} + O\left(\frac{1}{n^2}\right) \right)^n = e^{-4\alpha} + o(1). \end{aligned}$$

Since this holds for any fixed $\alpha > 0$, bearing in mind that \mathcal{A} is closed in \mathcal{P} (and hence the set $\mathcal{A}_2 \subseteq [-1, 1]^2$ is closed in the usual sense), we indeed find that the curve (x, x^4) lies in the attainable set for every $x \in (0, 1)$. It is easy to see that also $(0, 0)$ and $(1, 1)$ are attainable. By reflecting the curve (x, x^4) (for $x \geq 0$) in the x -axis (using that $(-1, 1)$ is attainable and multiplying) we find that (x, x^4) is attainable for $x \in [-1, 1]$. \square

6. PROOF OF THEOREM 1.6: FRACTAL STRUCTURE FOR $x < \frac{1}{3}$

It is obvious that the second assertion of Theorem 1.6 implies the first part, so we only need to prove the second one. However, since the proof of the second assertion is fairly complicated we give a brief outline of how the first assertion can be deduced, and then indicate how to augment the argument to give the second assertion.

We are to understand the closure of all the points (x, y) of the form

$$(28) \quad (x, y) = \prod_{i=1}^K (G_{A_i}(t_i), G_{A_i}(2t_i))$$

with $A_i \geq 2$ arbitrary integers. Using that $G_A(\pi/2 + t)$ is either even or odd (depending on the parity of A) and that $G_A(2(\pi/2 + t))$ is even, together with signs of x -coordinates being irrelevant (since (x, y) is attainable if and only if $(-x, y)$ is attainable) we may assume that $t_i \in [0, \frac{\pi}{2}]$ for all i . A curve $(x_0, y_0) = (G_{A_0}(t_0), G_{A_0}(2t_0))$ turns out to intersect the line $y = 1$ with $|x| \leq \frac{1}{3}$ only for A_0 odd, and further forces $t_0 = \frac{\pi}{2}$, and $x = \pm \frac{1}{A_0}$. Hence the point (x, y) as in (28) satisfies $y = 1$

only for A_i odd and $t_i = \frac{\pi}{2}$ for all $i \leq K$, whence $(x, y) = (\pm \frac{1}{A}, 1)$ with $A = \prod_{i=1}^K A_i$.

To prove the second assertion we investigate a (fairly large) neighborhood of the point $(\frac{1}{A}, 1)$; given an odd A we consider all finite products (28) with $A = \prod_{i=1}^K A_i$ and $t_i \approx \frac{\pi}{2}$ (and $A_i \geq 3$.) We will prove that all products (x, y) of this form will stay between two curves defined below; after taking logarithms this will amount to the fortunate log-convexity of the curves $(G_{A_0}(t), G_{A_0}(2t))$, $A_0 \geq 3$ odd, in the suitable range (see Lemma 6.8 below). We argue that this property is invariant with respect to multiplying by curves $(G_{A_1}(t), G_{A_1}(2t))$ for $A_1 \geq 2$ even, and also for odd $A_1 \geq 3$ for t near $\pi/2$.

6.1. Proof of the second assertion of Theorem 1.6. To prove the main result of the present section we will need the following results. (The proofs of Propositions 6.1 and 6.2 are postponed to Appendix A and B, respectively.)

Proposition 6.1. *Let $\{A_i\}_i$ be a finite collection of integers $A_i \geq 2$, and consider a point (x, y) of the form*

$$(29) \quad (x, y) = \left(\prod_i G_{A_i}(t_i), \prod_i G_{A_i}(2t_i) \right),$$

where all $t_i \in [0, \pi/2]$. Assume that one of the following is satisfied:

- There exists i such that $A_i \geq 3$ is odd and $t_i \in [\pi/(2A_i), \pi/2 - \pi/(2A_i)]$.
- There exists i such that A_i is even and $t_i \geq \pi/(2A_i)$.

Then necessarily

$$y \leq (2|x| - 1)^2.$$

Proposition 6.2. *Let $A \geq 3$ be an odd number, and*

$$A = \prod_{i=1}^K A_i$$

an arbitrary (fixed) factorization of A into (not necessarily co-prime) integers $A_i \geq 3$. For $x \leq \frac{1}{A}$ define

$$(30) \quad g_{\{A_i\}}(x) = \sup_{(t_i)_i \in \mathcal{X}_{\{A_i\}}(x)} \prod_{i=1}^K G_{A_i}(2t_i),$$

the supremum taken w.r.t. all $(t_i)_{i \leq K}$ lying in
(31)

$$\mathcal{X}_{\{A_i\}}(x) := \left\{ (t_i)_i : \forall i \leq K, t_i \in \left[\frac{\pi}{2} - \frac{\pi}{2A_i}, \pi/2 \right], \left| \prod_{i=1}^K G_{A_i}(t_i) \right| = x \right\}.$$

Then for every $0 < x < \frac{1}{A}$ there exists an index $i_0 = i_0(x) \leq K$ and $t \in [\frac{\pi}{2} - \frac{\pi}{2A_{i_0}}, \pi/2]$ such that³

$$(x, g_{\{A_i\}}(x)) = \left(\frac{A_{i_0}}{A} |G_{A_{i_0}}(t)|, G_{A_{i_0}}(2t) \right),$$

and moreover the map $x \mapsto i_0(x)$ is piecewise constant. In particular, the function $g_{\{A_i\}}(x)$ is continuous, analytic in some (left) neighbourhood of $x = \frac{1}{A}$, and piecewise analytic on $(0, \frac{1}{A}]$.

We may finally define the function $f_{2;k}$ introduced in Theorem 1.6.

Definition 6.3. Given $k \geq 1$, $0 < x \leq \frac{1}{2k+1}$, define

$$f_{2;k}(x) = \max_{\substack{K \\ \prod_{i=1}^K A_i = 2k+1}} g_{\{A_i\}}(x),$$

the maximum taken w.r.t. all non-trivial factorizations of $2k+1$, i.e., all sets of (odd) integers $\{A_i\}_{i=1}^K \subseteq \mathbb{Z}_{\geq 3}$, whose product is $2k+1$.

Remark 6.4. (1) For $A \geq 3$ odd, $t \in [\frac{\pi}{2} - \frac{\pi}{2A}, \pi/2]$ we have

$$(32) \quad |G_A(t)| \leq \frac{1}{A}.$$

(2) By the definition of $g_{\{A_i\}}$ and $f_{2;k}$, if (x, y) is of the form

$$(x, y) = \prod_{i=1}^K (|G_{A_i}(t_i)|, G_{A_i}(2t_i))$$

with all $A_i \geq 3$ odd, $x > 0$, and if in addition for all i we have

$$t_i \in \left[\frac{\pi}{2} - \frac{\pi}{2A_i}, \pi/2 \right]$$

(whence $x \leq \frac{1}{2k+1}$ via (32)), then necessarily

$$(33) \quad y \leq g_{\{A_i\}_{i \leq K}}(x) \leq f_{2;k}(x),$$

³The reason for $\frac{A_{i_0}}{A} |G_{A_{i_0}}(t)|$ appearing is that the supremum is attained by having $t_i = \frac{\pi}{2}$ for $i \neq i_0$ and hence $\prod_{i \neq i_0} G_{A_i}(0) = \prod_{i \neq i_0} 1/A_i = A_{i_0}/A$.

where k is defined as in

$$\prod_{i=1}^K A_i = 2k + 1.$$

(3) Proposition 6.2 implies that for $k \geq 1$ and $x < \frac{1}{2k+1}$,

$$f_{2;k}(x) = \max_{1 < A | 2k+1} \max_{t \in [\frac{\pi}{2} - \frac{\pi}{2A}, \pi/2] : |\frac{A}{2k+1} G_A(t)| = x} G_A(2t),$$

a maximum w.r.t. all (odd) divisors $A > 1$ of $2k+1$; the latter yields an algorithm for computing $f_{2;k}(x)$, reducing the original problem into maximizing a finite set of numbers.

The following 3 results will be proven in Appendix B.

Lemma 6.5. Let $A \geq 3$ be an odd integer, and η_A be the parametric curve in \mathbb{R}^2 defined by

$$(34) \quad \eta_A(t) = (\eta_{A;1}(t), \eta_{A;2}(t)) = (\log(A \cdot |G_A(t)|), \log(G_A(2t))),$$

for $t \in (\frac{\pi}{2} - \frac{\pi}{2A}, \frac{\pi}{2}]$. Then we may re-parameterize η as $(z, h_A(z))$ for some analytic function $h : (-\infty, 0) \rightarrow \mathbb{R}_{\leq 0}$ with $h(0) = 0$, and moreover $0 < h'(z) \leq \frac{4}{3}$ everywhere in the above range.

Corollary 6.6. Let $\{A_i\}_{i=1}^K \subseteq \mathbb{Z}_{\geq 3}$ be a set of odd integers, $A = \prod_{i=1}^K A_i$, and (x, y) of the form

$$(x, y) = \prod_{i=1}^K (G_{A_i}(t_i), G_{A_i}(2t_i)),$$

such that for all $i \leq K$ we have $t_i \in [\frac{\pi}{2} - \frac{\pi}{2A_i}, \frac{\pi}{2}]$. Then necessarily

$$y \geq (Ax)^{4/3}.$$

Lemma 6.7. For every $x_1, x_2 \in [0, 1]$ the following inequality holds:

$$(35) \quad (2x_1^2 - 1) \cdot (2x_2^2 - 1) \geq (2(x_1 x_2)^2 - 1).$$

We are finally in a position to prove Theorem 1.6 (with the first assertion following from the second.)

Proof of the second assertion of Theorem 1.6 assuming the results above. We first prove that any point $(x, y) \in \mathcal{A}_2$ with $0 < x \leq \frac{1}{3}$ either satisfies $y \leq (2x - 1)^2$ or $(x, y) \in \mathcal{D}_{0,x_k}(f_{1;k}, f_{2;k})$ for some $k \geq 1$, i.e. establish

the inclusion \subseteq of (7). Since \mathcal{A}_2 is the closure (in \mathbb{R}^2) of the set of finite products

$$(36) \quad (x, y) = \prod_{i=1}^K (G_{A_i}(t_i), G_{A_i}(2t_i)),$$

with some $A_i \geq 2$, $t_i \in [0, \pi]$, and the set on the r.h.s. of (7) is closed in $\{x > 0\}$, it is sufficient to prove it for the finite products (36).

Thus let (x, y) be given by a finite product (36); by the invariance of \mathcal{A}_2 w.r.t. $x \mapsto -x$ we may assume that all t_i , $i \leq K$ satisfy $t_i \in [0, \pi/2]$. If there exists either an odd A_i such that $t_i \in [\frac{\pi}{2A_i}, \frac{\pi}{2} - \frac{\pi}{2A_i}]$, or an even A_i such that $t_i \in [\frac{\pi}{2A_i}, \frac{\pi}{2}]$, then one of the sufficient conditions of Proposition 6.1 is satisfied, implying that $y \leq (2x - 1)^2$, so that our present statement holds.

We may then assume that for all odd A_i we have either $t_i \in [0, \frac{\pi}{2A_i}]$ or $t_i \in [\frac{\pi}{2} - \frac{\pi}{2A_i}, \frac{\pi}{2}]$, and for all even A_i we have $t_i \in [0, \frac{\pi}{2A_i}]$. Up to reordering the indexes, we may assume that $K = K_1 + K_2$ with $K_1 > 0$, and where all the A_i with $i \leq K_1$ are odd and $t_i \in [\frac{\pi}{2} - \frac{\pi}{2A_i}, \frac{\pi}{2}]$, and for all $K_1 + 1 \leq i \leq K_2$ we have

$$(37) \quad t_i \in \left[0, \frac{\pi}{2A_i}\right],$$

whether the corresponding A_i is odd or even. Let

$$(38) \quad A = \prod_{i=1}^{K_1} A_i = 2k + 1.$$

be the product of the first K_1 odd A_i . We claim that, with k as defined in (38), necessarily

$$(39) \quad f_{1;k}(x) \leq y \leq f_{2;k}(x).$$

Define

$$(x_0, y_0) = \prod_{i=1}^{K_1} (G_{A_i}(t_i), G_{A_i}(2t_i))$$

and

$$(40) \quad (x_1, y_1) = \prod_{i=K_1+1}^{K_1+K_2} (G_{A_i}(t_i), G_{A_i}(2t_i)),$$

so that

$$(41) \quad (x, y) = (x_0, y_0) \cdot (x_1, y_1).$$

Since by the above, (x_0, y_0) satisfies the assumptions of (33), we have $y_0 \leq g_{\{A_i\}_{i \leq K_1}}(x_0)$, and by Proposition 6.2 there exists $i_0 \leq K_1$ and $t_0 \in \left(\frac{\pi}{2} - \frac{\pi}{2A_{i_0}}, \frac{\pi}{2}\right]$, so that

$$(42) \quad x_0 = \frac{A_{i_0}}{A} |G_{A_{i_0}}(t_0)|$$

and $g_{\{A_i\}_{i \leq K_1}}(x_0) = G_{A_{i_0}}(2t_0)$; we then have

$$(43) \quad y_0 \leq G_{A_{i_0}}(2t_0).$$

For the sake of brevity of notation we assume with no loss of generality that $i_0 = 1$, and consider the curve η_{A_1} in $\mathbb{R}_{>0}^2$ as in Lemma 6.5; by the virtue of the latter lemma we may re-parameterize η_{A_1} as $(z, h_{A_1}(z))$ in the range $z \in (-\infty, 0]$, and $0 < h'_{A_1}(x) \leq \frac{4}{3}$ everywhere. Hence, on noting that all the logarithms involved are *negative*, the mean value theorem gives that

$$(44) \quad \begin{aligned} h_{A_1}(\log(Ax_0x_1)) &= h_{A_1}(\log(Ax_0) + \log(x_1)) \\ &\geq h_{A_1}(\log(Ax_0)) + \frac{4}{3} \log(x_1). \end{aligned}$$

Note that by (42) and the definition of h_{A_1} as a re-parametrization of (34), we have

$$h_{A_1}(\log(Ax_0)) = h_{A_1}(\log(A_1|G_{A_1}(t_0)|)) = \log G_{A_1}(2t_0)$$

(recall that we assumed that $i_0 = 1$).

Substituting the latter into (44) implies that there exist a number $\theta_1 \in \left(\frac{\pi}{2} - \frac{\pi}{2A_1}, \frac{\pi}{2}\right]$ satisfying $A_1|G_{A_1}(\theta_1)| = Ax_0x_1$ (note that $x_0 \in (0, 1/A]$) and

$$\log(G_{A_1}(2\theta_1)) \geq \log G_{A_1}(2t_0) + \frac{4}{3} \log(x_1).$$

Equivalently,

$$(45) \quad |G_{A_1}(\theta_1)| = \frac{A}{A_1} x_0 x_1$$

and

$$(46) \quad G_{A_1}(2\theta_1) \geq G_{A_1}(2t_0) \cdot x_1^{4/3} \geq y_0 \cdot x_1^{4/3},$$

by (43).

Note that for the choice $t_1 = \theta_1$ and $t_i = \frac{\pi}{2}$ for $2 \leq i \leq K_1$, we have

$$(47) \quad \left| \prod_{i=1}^{K_1} G_{A_i}(t_i) \right| = \frac{A}{A_1} x_0 x_1 \cdot \prod_{i=2}^{K_1} \frac{1}{A_i} = x_0 x_1,$$

by (45) and (38). Now, bearing in mind (41), as $g_{\{A_i\}_{i \leq K_1}}(x)$ is defined to be the supremum of all the expressions (30) with $\{t_i\}_{i \leq K_1}$ satisfying (47), and recalling Definition 6.3 of $f_{2;k}(x)$, (46) implies that

$$(48) \quad f_{2;k}(x) \geq g_{\{A_i\}_{i \leq K_1}}(x) \geq y_0 \cdot x_1^{4/3}.$$

On the other hand, (37) implies that for every $K_1 + 1 \leq i \leq K_1 + K_2$ we have $G_{A_i}(t_i) > \frac{1}{3}$ (for A fixed, $G_A(t)$ is decreasing for $t \in [0, \pi/A]$ and it is enough to show that $G_A(\pi/(2A)) = (A \sin(\pi/(2A)))^{-1} > 1/3$; this in turn follows from $\sin(x)/x$ being decreasing on $[0, \pi]$.) Hence Proposition 5.5 is applicable for each of the terms on the r.h.s. of (40), and therefore their product (x_1, y_1) satisfies

$$(49) \quad y_1 \leq x_1^4.$$

The inequality (49) together with (48) and the fact that $x^{4/3} > x^4$ for $x < 1$ yield that

$$f_{2;k}(x) \geq y_0 \cdot x_1^{4/3} \geq y_0 \cdot x_1^4 \geq y_0 \cdot y_1 = y,$$

as in (41), which is the second inequality of (39).

To prove the first inequality of (39) we use Corollary 6.6 to yield $y_0 \geq (Ax_0)^{4/3}$ with A as in (38). These combined imply

$$\begin{aligned} y &= y_0 \cdot y_1 \geq (Ax_0)^{4/3} \cdot (2x_1^2 - 1) \geq (Ax_0)^4 \cdot (2x_1^2 - 1) \\ &\geq (2(Ax_0)^2 - 1) \cdot (2x_1^2 - 1) \end{aligned}$$

where we used the obvious inequality $x^4 \geq 2x^2 - 1$, valid on $[-1, 1]$. Finally, an application of the inequality (35) of Lemma 6.7 yields

$$y \geq 2(Ax_0 x_1)^2 - 1 = 2A^2 \cdot x^2 - 1 = f_{1;k}(x),$$

by the definition (8) of $f_{1;k}$, and recalling that $x_k = \frac{1}{2k+1}$.

Conversely, we need to prove that any point (x, y) satisfying

$$f_{1;k}(x) \leq y \leq f_{2;k}(x)$$

necessarily lies in \mathcal{A}_2 . To this end fix a number $k \geq 1$ and consider all the points (x, y) of the form

$$(50) \quad (x, y) = (s, f_{2;k}(s)) \cdot (t, 2t^2 - 1)$$

with $s \in (0, \frac{1}{2k+1}]$, $t \in (0, 1]$ (recalling the notation (22) for componentwise multiplication). Note that by the multiplicativity of \mathcal{A}_2 (Proposition 1.2) all the points of the form (50) are attainable, i.e., $(x, y) \in \mathcal{A}_2$. Since $f_{2;k}(\frac{1}{2k+1}) = 1$, for $s = \frac{1}{2k+1}$ fixed, t varying in $(0, 1]$, (x, y) attains all the curve $(x, y) = (x, f_{1;k}(x))$; for $t = 1$ fixed, s varying in $(0, \frac{1}{2k+1})$, (x, y) attains the curve $(x, y) = (x, f_{2;k}(x))$.

We claim that for every (x, y) with $f_{1;k}(x) \leq y \leq f_{2;k}(x)$ there exists s, t in the range as above, satisfying (50). To show the latter statement, given such a point (x, y) consider $s \in [x, \frac{1}{2k+1}]$ and $t = \frac{x}{s}$. We are then to solve the equation

$$y = f_{2;k}(s) \cdot \left(\frac{2x^2}{s^2} - 1 \right)$$

for the given $y, s \in [x, \frac{1}{2k+1}]$; as the r.h.s. of the latter equation attains the values $f_{1;k}(x)$ and $f_{2;k}(x)$ for $s = \frac{1}{2k+1}$ and $s = x$ respectively, we are guaranteed a solution by the intermediate value theorem. Geometrically, the above argument shows that as s varies, the family of parabolas

$$t \mapsto (s, f_{2;k}(s)) \cdot (t, 2t^2 - 1)$$

tesselates the domain $\mathcal{D}_{0,x_k}(f_{1;k}, f_{2;k})$ (cf. the proof of Proposition 5.2 in section 5.6).

□

6.2. Proof of Proposition 6.2 by convexity. The convexity of the component-wise logarithm of a curve implies that finite products of points lying on that curve would stay below it. We aim at eventually proving that all the curves $\gamma_A = (G_A(t), G_A(2t)), A \geq 3$ odd, $t \in [\frac{\pi}{2} - \frac{\pi}{2A}, \frac{\pi}{2}]$, satisfy the above property (see Lemma 6.8 below). We exploit their convexity in Lemma 6.9, which, after taking logarithm, is equivalent to the statement of Proposition 6.2 (see the proof of Proposition 6.2 below); the latter follow from finite products of points on a curve, with the property above, staying below that curve.

Lemma 6.8. *Let η_A be the curve*

$$\eta_A(t) = (\log(A \cdot |G_A(t)|), \log(G_A(2t))),$$

$t \in (\frac{\pi}{2} - \frac{\pi}{2A}, \frac{\pi}{2}]$ with $A \geq 3$ odd. Then in the above domain of t both components of $\eta_A = (\eta_{A;1}, \eta_{A;2})$ are strictly increasing, and moreover η_A may be re-parametrized as $(z, h_A(z))$ with $h_A : (-\infty, 0] \rightarrow \mathbb{R}$ convex analytic, increasing, and $h(0) = 0$.

The somewhat technical proof of Lemma 6.8 is postponed to Appendix B.

Lemma 6.9. *Let $\{h_i : (-\infty, 0] \rightarrow \mathbb{R}\}_{i \leq K}$ be a finite collection of continuous convex functions such that for all $i \leq K$ we have $h_i(0) = 0$.*

Define $h : (-\infty, 0] \rightarrow \mathbb{R}$ by

$$(51) \quad h(z) = \sup_{z_i \leq 0: \sum_{i=1}^K z_i = z} \left\{ \sum_{i=1}^K h_{A_i}(z_i) \right\}.$$

Then for every $z \in (-\infty, 0]$ there exists an index $i_0 = i_0(z)$ so that $h(z) = h_{i_0}(z)$.

Before giving a proof for Lemma 6.9 we may finally prove Proposition 6.2.

Proof of Proposition 6.2 assuming lemmas 6.8 and 6.9. Let $A = 2k + 1 \geq 3$ be odd, and (38) be an arbitrary factorization of A into integers $A_i \geq 3$. Consider the curves $\{\eta_{A_i}(t) : t \in [\frac{\pi}{2} - \frac{\pi}{2A_i}, \frac{\pi}{2}]\}_{i \leq K}$ as defined in (34). By Lemma 6.8 all of the η_{A_i} can be re-parametrized as $(z_i, h_{A_i}(z_i))$ on $(-\infty, 0]$, with h_{A_i} convex analytic, and $h(0) = 0$.

Hence, by Lemma 6.9 for every $z \in (0, \frac{1}{A}]$ there exists $i_0 = i_0(x)$, so that

$$h(z) := \sup_{z_i \leq 0: \sum_{i=1}^K z_i = z} \left\{ \sum_{i=1}^K h_{A_i}(z_i) \right\} = h_{A_{i_0}}(z),$$

Note that, after taking logarithms, maximizing $\prod_{i=1}^K G_A(2t_i)$ under the constraint $(t_i)_{i \leq K} \in \mathcal{X}_{\{A_i\}}(x)$ with $\mathcal{X}_{\{A_i\}}(x)$ as in (31), $0 < x \leq \frac{1}{A}$ is equivalent to maximizing

$$\sum_{i=1}^K \log G_A(2t_i) = \sum_{i=1}^K h_{A_i}(z_i)$$

under the constraint $\sum_{i=1}^K z_i = z$, where $z = \log Ax \in (-\infty, 0]$. More formally, recalling the definition (34) of η_{A_i} and $(z_i, h_{A_i}(z_i))$ being a re-parametrization of η_{A_i} , the function $h(z)$ defined as in (51), on noting that $z = \log Ax$, satisfies

$$(52) \quad h(\log(Ax)) = \log \sup_{(t_i)_{i \leq K} \in \mathcal{Y}_{\{A_i\}}(x)} \left\{ \prod_{i=1}^K G_{A_i}(2t_i) \right\},$$

where

$$\mathcal{Y}_{\{A_i\}}(x) = \left\{ (t_i)_{i \leq K} : \forall i. t_i \in \left[\frac{\pi}{2} - \frac{\pi}{2A_i}, \frac{\pi}{2} \right], \sum_{i=1}^K \log(A_i |G_{A_i}(t_i)|) = \log(Ax) \right\}.$$

Since $\sum_{i=1}^K \log(A_i |G_{A_i}(t_i)|) = \log(Ax)$ is equivalent to $\sum_{i=1}^K \log(|G_{A_i}(t_i)|) = \log(x)$ via (38), we have $\mathcal{Y}_{\{A_i\}}(x) = \mathcal{X}_{\{A_i\}}(x)$ (as in (31)), and hence (52) is

$$h(\log(Ax)) = \log(g_{\{A_i\}}(x)).$$

The latter equality together with Lemma 6.9 then imply that we have

$$h_{i_0}(\log(Ax)) = \log(g_{\{A_i\}_{i \leq K}}(x))$$

for some $i_0 \leq K$; since h_{i_0} is a re-parametrization of $\eta_{A_{i_0}}$, this is equivalent to

$$(\log(A_{i_0}|G_{A_{i_0}}(t_{i_0})|), \log(G_{A_{i_0}}(2t_{i_0}))) = (\log(Ax), \log g_{\{A_i\}_{i \leq K}}(x))$$

for some $t_{i_0} \in [\frac{\pi}{2} - \frac{\pi}{2A_{i_0}}, \frac{\pi}{2}]$, i.e.

$$\left(\frac{A_{i_0}}{A} |G_{A_{i_0}}(t_{i_0})|, G_{A_{i_0}}(2t_{i_0}) \right) = (x, g_{\{A_i\}_{i \leq K}}(x)),$$

which is the first statement of the present proposition, at least for $x > 0$. For $x = 0$ it is sufficient to notice that for all $i \leq K$,

$$(G_{A_i}(t), G_{A_i}(2t))|_{t=\frac{\pi}{2}-\frac{\pi}{2A_i}} = (0, 0),$$

so that in particular $g_{\{A_i\}_{i \leq K}}(x) = 0$, whatever $\{A_i\}_{i \leq K}$ are.

To see that the map $x \mapsto i_0(x)$ is in fact piecewise constant on $[0, \frac{1}{A}]$ (with finitely many pieces), we note that it is readily shown that on $(0, \frac{1}{A}]$, $g_{\{A_i\}_{i \leq K}}$ is a maximum of finitely many analytic curves (namely, $(\frac{A_i}{A} |G_{A_i}(t)|, G_{A_i}(2t))$), and vanishes at 0, which happens to lie on all of them. Since such a collection of analytic curves may only intersect in finitely many points for $x \in [0, \frac{1}{A}]$, it follows that $i_0(x)$ is uniquely determined as the maximum of these outside of finitely many points (that include $(0, 0)$), and i_0 is constant between any two such consecutive points.

□

Proof of Lemma 6.9. It is easy to check that with the assumptions of the present lemma, the function $H : (-\infty, 0]^K \rightarrow \mathbb{R}$ defined by

$$H(t_1, \dots, t_K) = \sum_{i=1}^K h_i(t_i)$$

is a convex function. Now fix $t < 0$ and consider the set

$$\Omega(t) := \left\{ (t_i)_{i \leq K} : \sum_{i=1}^K t_i = t, \quad t_i \leq 0 \text{ for } 1 \leq i \leq K \right\} \subseteq (-\infty, 0]^K;$$

$\Omega(t)$ is a compact convex domain, and it is evident that

$$h(t) = \max_{(t_i) \in \Omega(t)} H(t_1, \dots, t_k).$$

Now, a convex function cannot attain a maximum in the interior of a convex domain (all the local extrema of a convex function are necessarily minima). Hence there exists an index $i_1 \leq K$ so that

$$h(t) = \sum_{i=1}^K h_i(t_i)$$

for some $(t_i) \in \Omega(t)$ with $t_{i_1} = 0$, i.e. one of the elements of (t_i) must vanish. By induction, we find that all but one element of (t_i) vanish, say $t_i = 0$ for $i \neq i_0$, whence $t_{i_0} = t$, and $h(t) = h_{i_0}(t)$, as $h_i(0) = 0$ for $i \neq i_0$ by the assumptions of the present lemma. \square

7. PROOF OF THEOREM 1.4: SQUARE-FREE ATTAINABLE MEASURES

Proof. Recall that we de-symmetrized all the probability measures by an analogue of (10). First we show that (4) holds for any square-free attainable measure; as the first inequality in (4) holds for every probability measure (13) it only remains to show that every point $(x, y) = (\hat{\mu}(1), \hat{\mu}(2))$ corresponding to a square-free attainable μ satisfies (21).

By the definition of square-free attainable measures, if μ is square-free attainable then (x, y) is lying in the closure of the set of finite products

$$(53) \quad \begin{aligned} (\tilde{x}, \tilde{y}) &= \left\{ \prod_{i=1}^K (\cos(\theta_i), \cos(2\theta_i)) : \theta_i \in [0, \pi] \right\} \\ &= \left\{ \prod_{i=1}^K (x_i, y_i) : x_i \in [-1, 1] \right\}, \end{aligned}$$

where for all $i \leq K$, $y_i = 2x_i^2 - 1$. Now if $\tilde{y} > 0$ and $y_{i_0} < 0$ for some $i_0 \leq K$, then $(\tilde{x}, \tilde{y}) \in \mathcal{A}_2^-$ is a mixed sign attainable point, and (upon recalling Notation 5.6) Lemma 5.7 implies that $(\tilde{x}, \tilde{y}) \in B_1$, i.e., $|\tilde{x}| \leq 1/2$ and $\tilde{y} \leq (2|\tilde{x}| - 1)^2$.

If $\tilde{y} > 0$ and $y_i \geq 0$ for all i , then $y_i = 2x_i^2 - 1 \leq x_i^4$ for all i as it is easy to check the latter inequality explicitly, consequently $\tilde{y} \leq \tilde{x}^4$. Since (21) holds on the collection of all products (53), it also holds on its closure, namely for square-free attainable measures. This concludes the proof of the necessity of the inequality (4).

It then remains to show the sufficiency, i.e. any point (x, y) satisfying (4) corresponds to a square-free attainable measure. We claim that the attainable measures constructed by Proposition 5.2 are in fact square-free attainable. To this end recall that the collection of all square-free attainable measures is closed under convolutions, so that the products of points corresponding to square-free attainable measures correspond to square-free attainable measures. It is then crucial to notice that the measures corresponding to points lying on the curves

$$\{(x, x^4) : x \in [0, 1]\}$$

(constructed by Lemma 5.13), and

$$\{(x, (2x - 1)^2) : x \in [0, 1]\}$$

(a re-parameterized product of the parabola $y = 2x^2 - 1$ by itself) exploited in the course of the proof of Proposition 5.2 are both square-free attainable. Hence the tessellation argument used in the proof of Proposition 5.2 works in this case too.

□

APPENDIX A. PROOF OF PROPOSITION 6.1: BELOW THE “MIXED SIGNS” CURVE $y = (2x - 1)^2$

By the assumptions of Proposition 6.1 there exists i such that $t_i \in [\pi/(2A_i), \pi/2 - \pi/(2A_i)]$ (for A_i odd), or $t_i \in [\pi/(2A_i), \pi/2]$ (for A_i even.) The following lemma exploits this property to yield more information about (at least) one point in the product.

Lemma A.1. *Let $A \geq 3$ and $(x, y) = (G_A(t), G_A(2t))$. If A is odd and $t \in [\frac{\pi}{2A}, \frac{\pi}{2} - \frac{\pi}{2A}]$, or A is even and $t \in [\frac{\pi}{2A}, \frac{\pi}{2}]$, then either $y \leq 0$, or $y \leq (2|x| - 1)^2$ and $|x| < \frac{1}{3}$.*

If $A = 2$ and $t \in [\frac{\pi}{4}, \frac{\pi}{2}]$, then $y = G_2(2t) \leq 0$.

Proof of Proposition 6.1 assuming Lemma A.1. Assume with no loss of generality that the postulated index is $i = 1$, i.e.

$$(x_1, y_1) = (G_{A_1}(t_1), G_{A_1}(2t_1))$$

with either $A_1 \geq 3$ being odd and $t \in [\frac{\pi}{2A_1}, \frac{\pi}{2} - \frac{\pi}{2A_1}]$, or $A_1 \geq 2$ being even and $t \in [\frac{\pi}{2A_1}, \frac{\pi}{2}]$. Suppose first that $y_1 \leq 0$. In this case the point (x, y) is “mixed sign attainable” (cf. Definition 5.3), so that Lemma 5.4 implies that $y \leq (2|x| - 1)^2$.

Otherwise we assume that $y_1 > 0$ and $y > 0$. Then Lemma A.1 implies that $A \geq 3$, and $|x_1| < \frac{1}{3}$, whence

$$0 < y \leq y_1 \leq (2|x_1| - 1)^2 \leq (2|x| - 1)^2,$$

since $|x| \leq |x_1|$ and the function $x \mapsto (2x - 1)^2$ is decreasing on $[0, \frac{1}{2}]$. \square

Proof of Lemma A.1. First, upon recalling that for $A = 2$ we have $G_2(t) = \cos(t)$, the second statement of Lemma A.1 is obvious. We are left with proving the first statement. For $A = 3$ if $t \in [\frac{\pi}{6}, \frac{\pi}{3}]$, then

$$y = \frac{\sin(6t)}{3\sin(2t)} \leq 0$$

again. We may thus assume that $A \geq 4$.

Next, we would like to consolidate the even and the odd A cases, by showing that if A is even and $t \in [\frac{\pi}{2} - \frac{\pi}{2A}, \frac{\pi}{2}]$, then the statement of the present lemma holds. To do this we note that in this range $2At \in [(A-1)\pi, A\pi]$, so that

$$G_A(2t) = \frac{\sin(2At)}{A\sin(2t)} \leq 0$$

once more.

Hence we may assume that $t \in [\frac{\pi}{2A}, \frac{\pi}{2} - \frac{\pi}{2A}]$, whether A is even or odd. We would like to further cut out the short intervals $[\frac{\pi}{2A}, \frac{\pi}{A}]$ and $[\frac{\pi}{2} - \frac{\pi}{A}, \frac{\pi}{2} - \frac{\pi}{2A}]$, i.e. establish the validity of the present lemma in these intervals. If $t \in [\frac{\pi}{2A}, \frac{\pi}{A}]$ whether A is even or odd, then $2At \in [\pi, 2\pi]$, so that $y = G_A(2t) \leq 0$ in this regime too.

If $t \in [\frac{\pi}{2} - \frac{\pi}{A}, \frac{\pi}{2} - \frac{\pi}{2A}]$, then $2At \in [(A-2)\pi, (A-1)\pi]$, so that if A is odd then $y = G_A(2t) = \frac{\sin(2At)}{A\sin(2t)} \leq 0$. In the remaining case A even, for the same range $t \in [\frac{\pi}{2} - \frac{\pi}{A}, \frac{\pi}{2} - \frac{\pi}{2A}]$, we write $A = 2B$ for $B \in \mathbb{Z}$, and note that

$$\begin{aligned} (x, y) &= (G_A(t), G_A(2t)) = \left(\frac{\sin(Bt)\cos(Bt)}{B\sin(t)}, \frac{\sin(2Bt)\cos(2Bt)}{B\sin(2t)} \right) \\ &= (G_B(t), G_B(2t)) \cdot (G_2(t), G_2(2t)). \end{aligned}$$

Hence if in turn B is even, then $G_B(2t) = \frac{\sin(2Bt)}{B\sin(2t)} \leq 0$, since $2Bt \in [(B-1)\pi, (B-1)\pi + \frac{\pi}{2}]$. Hence (x, y) is mixed sign attainable, and therefore by Lemma 5.4, $y \leq (2|x| - 1)^2$, and, in addition, $|x| \leq \frac{1}{3}$ by Lemma 5.11.

Otherwise, if B is odd, we may assume that $A \geq 6$ is even (in the same range $t \in [\frac{\pi}{2} - \frac{\pi}{A}, \frac{\pi}{2} - \frac{\pi}{2A}]$); in this case we claim that $|x| = |G_A(t)| \leq \frac{1}{5}$ and $y = |G_A(2t)| \leq \frac{1}{3}$. As $\frac{1}{3} \leq (2/5-1)^2$, and $x \mapsto (2x-1)^2$ is decreasing on $[0, \frac{1}{2}]$ this is sufficient to yield $y \leq (2|x| - 1)^2$. To show this, we first note that $G_A(2t) = \pm G_A(2(\pi/2 - t))$; hence Lemma 5.11 implies that $y \leq \frac{1}{3}$ indeed. Concerning the value of $|x|$, we have for t

in the range as above (bearing in mind that $A \geq 6$):

$$\begin{aligned} |G_A(t)| &\leq \frac{1}{A \sin(t)} \leq \frac{1}{A \sin(\pi/2 - \pi/A)} = \frac{1}{A \cos(\pi/A)} \\ &\leq \frac{1}{6 \cos(\pi/6)} = 0.19\dots < \frac{1}{5}, \end{aligned}$$

since $A \mapsto A \cdot \cos(\pi/A)$ is strictly increasing for $A \geq 6$.

Finally, we take care of the case $A \geq 4$, whether A is even or odd, and the remaining range

$$(54) \quad t \in \left[\frac{\pi}{A}, \frac{\pi}{2} - \frac{\pi}{A} \right],$$

and $(x, y) = (G_A(t), G_A(2t))$. Noting that $\sin(t) \geq \frac{2}{\pi}t$ everywhere on $[0, \frac{\pi}{2}]$, we find that for $t \in [\frac{2\pi}{A}, \frac{\pi}{2}]$,

$$|G_A(t)| \leq \frac{1}{A \sin(t)} \leq \frac{\pi}{2} \frac{1}{A \cdot 2\pi/A} = \frac{1}{4}.$$

Hence (under the assumption (54) on t), if $t > \frac{2\pi}{A}$, $|x| = |G_A(t)| \leq \frac{1}{4}$, and (using the natural symmetry $G_A(t) = \pm G_A(\pi - t)$), $y \leq |y| = |G_A(2t)| \leq \frac{1}{4}$.

If both $|x| \leq \frac{1}{4}$ and $y \leq \frac{1}{4}$, then $y \leq (2|x| - 1)^2$, as $x \mapsto (2x - 1)^2$ is decreasing on $[0, \frac{1}{2}]$. Hence we are left with taking care of the range $t \in [\frac{\pi}{A}, \frac{2\pi}{A}]$, where we still have $y \leq \frac{1}{4}$, and we may assume $x > \frac{1}{4}$. Moreover, if $t \in [\frac{3\pi}{2A}, \frac{2\pi}{A}]$, $2At \in [3\pi, 4\pi]$, so that $y = G_A(2t) \leq 0$, hence it is enough to prove the statement for $t \in [\frac{\pi}{A}, \frac{3\pi}{2A}]$.

Now, recall that by Lemma 5.10 the function $t \mapsto \frac{\sin t}{t}$ is decreasing on $[0, \pi]$, so that, bearing in mind that $A \geq 4$,

$$\frac{\sin t}{t} \geq \frac{\sin(At/4)}{At/4},$$

and thus

$$\begin{aligned} (55) \quad |x| &= |G_A(t)| = \frac{|\sin(At)|/(At)}{|\sin(t)|/t} \leq \frac{|\sin(At)|/(At)}{\sin(At/4)/(At/4)} \\ &= \frac{|\sin(At)|}{4 \sin(At/4)} = |G_4(s)| =: |x'|, \end{aligned}$$

where we rescale by letting $s = \frac{At}{4} \in [\frac{\pi}{4}, \frac{3\pi}{8}]$. Arguing along the same lines we obtain

$$(56) \quad |y| = |G_A(2t)| \leq |G_4(2s)| =: |y'|$$

(note that $2At/4 = At/2 < \pi$, so that Lemma 5.10 is valid in this range).

Since

$$G_4(s) = \frac{\sin(4s)}{4\sin(s)} = \cos(s)\cos(2s) = G_2(s) \cdot G_2(2s),$$

we have that

$$(x', y') = (G_4(s), G_4(2s)) = (G_2(s), G_2(2s)) \cdot (G_2(2s), G_2(4s)),$$

is a product of two attainable points, and moreover, since $s \in [\frac{\pi}{4}, \frac{3\pi}{8}]$, $G_2(2s) = \cos(2s) \leq 0$ (and also $G_2(4s) \leq 0$). That means that (x', y') is “mixed sign attainable” (cf. Definition 5.3), and hence Lemma 5.4 implies that $y' \leq (2|x'| - 1)^2$. Finally, bearing in mind (55) and (56), as well as $x \mapsto (2x - 1)^2$ decreasing on $[0, \frac{1}{2}]$, we have

$$y \leq |y'| \leq (2x' - 1)^2 \leq (2x - 1)^2.$$

□

APPENDIX B. PROOF OF AUXILIARY TECHNICAL LEMMAS

Proof of Lemma 6.8. First, by using some simple trigonometric identities (in particular, that $\sin(\pi/2 - t) = \cos(t)$), we may re-parametrize $\eta_A(t)$ as

$$\begin{aligned} \eta_A(t) &= (x(t), y(t)) = \left(\log \left(A \frac{\cos(At)}{A \cos(t)} \right), \log \left(\frac{\cos(At)}{\cos(t)} \cdot \frac{\sin(At)}{A \sin(t)} \right) \right) \\ &= \left(\log \cos(At) - \log(\cos(t)), \right. \\ &\quad \left. \log(\cos(At)) - \log(\cos(t)) + \log(\sin(At)) - \log(A \sin(t)) \right), \end{aligned}$$

for $t \in [0, \frac{\pi}{2A}]$. By taking the derivatives, it is easy to see that both $x(t)$ and $y(t)$ are strictly decreasing, thus, by the inverse function theorem, the curve $(x(t), y(t))$ can be re-parametrized as $(x, h_A(x))$ with $h_A : (-\infty, 0] \rightarrow \mathbb{R}$ real analytic and strictly increasing. Hence to prove that η_A is convex (or equivalently, that h_A is convex), it is sufficient to show that the slope

$$\frac{dy}{dx} = \frac{y'(t)}{x'(t)} = 1 + \frac{(\log(\sin(At)) - \log(A \sin t))'}{(\log(\cos(At)) - \log(\cos t))'}$$

is decreasing on $(0, \frac{\pi}{2A})$, which in turn is equivalent to the function

$$t \mapsto \frac{(\log(\sin(At)) - \log(\sin t))'}{(\log(\cos(At)) - \log(\cos t))'}$$

being decreasing on the same domain. We rescale by setting $s = At$ and let $\alpha := \frac{1}{A} \in (0, \frac{1}{3}]$, $g(s) := -\log(\sin(s))$, $f(s) := -\log(\cos(s))$; we are then to prove that

$$s \mapsto \frac{(g(s) - g(\alpha s))'}{(f(s) - f(\alpha s))'}$$

is decreasing on $(0, \frac{\pi}{2})$.

Recall the product expansion formulas

$$\sin(x) = x \prod_{k=1}^{\infty} \left(1 - \frac{x^2}{k^2 \pi^2}\right), \quad \cos(x) = \prod_{k=1}^{\infty} \left(1 - \frac{4x^2}{(2k-1)^2 \pi^2}\right)$$

of the sine and cosine respectively, and the Taylor series expansion $-\log(1-x) = \sum_{k=1}^{\infty} \frac{x^k}{k}$. Under the above notation we have

$$f(s) = \sum_{i=1}^{\infty} a_i s^{2i}, \quad h(s) := g(s) + \log(s) = \sum_{j=1}^{\infty} b_j s^{2j},$$

with

$$a_i = \frac{2^{2i} \zeta^*(2i)}{i \pi^{2i}} > 0; \quad b_j = \frac{\zeta(2j)}{j \pi^{2j}} > 0,$$

where ζ is the usual Riemann Zeta function, and $\zeta^*(r) := \sum_{k=1}^{\infty} \frac{1}{(2k-1)^r}$, for $r > 1$.

We then have

$$F(s) := f(s) - f(\alpha s) = \sum_{i=1}^{\infty} a_i (1 - \alpha^{2i}) s^{2i},$$

and

$$\begin{aligned} G(s) &:= g(s) + \log(s) - (g(\alpha s) + \log(\alpha s)) = g(s) - g(\alpha s) - \log(\alpha) \\ &= \sum_{j=1}^{\infty} b_j (1 - \alpha^{2j}) s^{2j} - \log(\alpha). \end{aligned}$$

Further, since $(g(s) - g(\alpha s))' = G'(s)$ and $(f(s) - f(\alpha s))' = F'(s)$ it is enough to prove that

$$G''(s)F'(s) - G'(s)F''(s) < 0$$

on $s \in (0, \frac{\pi}{2})$; note that $G'' \cdot F' - G' \cdot F''$ is defined and analytic on the interval $(0, \frac{\pi}{2})$. Now, we have

$$\begin{aligned} G''(s)F'(s) &= \sum_{j=1}^{\infty} b_j \cdot 2j(2j-1)(1-\alpha^{2j})s^{2j-2} \cdot \sum_{i=1}^{\infty} a_i \cdot 2i(1-\alpha^{2i})s^{2i-1} \\ &= 4(1-\alpha^2)^2 a_1 b_1 s + \sum_{k=1}^{\infty} c_k s^{2k+1}, \end{aligned}$$

and

$$\begin{aligned} G'(s)F''(s) &= \sum_{j=1}^{\infty} b_j \cdot 2j(1-\alpha^{2j})s^{2j-1} \cdot \sum_{i=1}^{\infty} a_i \cdot 2i(2i-1)(1-\alpha^{2i})s^{2i-2} \\ &= 4(1-\alpha^2)^2 a_1 b_1 s + \sum_{k=1}^{\infty} d_k s^{2k+1}, \end{aligned}$$

and similarly

$$h''(s)f'(s) = \frac{1}{3}s + \sum_{k=1}^{\infty} \gamma_k s^{2k+1}$$

and

$$h'(s)f''(s) = \frac{1}{3}s + \sum_{k=1}^{\infty} \delta_k s^{2k+1},$$

where for $k \geq 1$ we have $0 < c_k < \gamma_k$, and (since $a_i, b_j \geq 0$ together with $\alpha \leq 1/3$)

$$d_k \geq (1-\alpha^2)^2 \delta_k > \frac{3}{4} \delta_k > 0$$

(say).

Hence

$$(57) \quad G''(s)F'(s) - 4(1-\alpha^2)^2 a_1 b_1 s < \left(h''(s)f'(s) - \frac{1}{3}s \right)$$

and

$$(58) \quad G'(s)F''(s) - 4(1-\alpha^2)^2 a_1 b_1 s > \frac{3}{4} \left(h'(s)f''(s) - \frac{1}{3}s \right).$$

In a moment we are going to show that the inequality

$$(59) \quad K(s) := \frac{h'(s)f''(s) - \frac{s}{3}}{h''(s)f'(s) - \frac{s}{3}} \geq 2$$

holds for $s \in (0, \frac{\pi}{2})$. Assuming (59), use (57) and (58) to finally obtain (note that $\gamma_k > 0$ for all k and hence $h''(s)f'(s) - s/3 > 0$ for $s \in$

$(0, \pi/2)$) that

$$\begin{aligned} G''(s)F'(s) - G'(s)F''(s) &< \left(h''(s)f'(s) - \frac{1}{3}s \right) - \frac{3}{4} \left(h'(s)f''(s) - \frac{1}{3}s \right) \\ &< -\frac{1}{2} \left(h''(s)f'(s) - \frac{1}{3}s \right) < 0. \end{aligned}$$

Now we turn to showing (59). We may compute explicitly $K(s)$ to be

$$K(s) = \frac{-s(\cos(s)^2 \cdot \sin(s) \cdot s^2 + 3 \cdot \cos(s) \cdot s - 3 \cdot \sin(s))}{\cos(s) \cdot (-\cos(s) \cdot \sin(s) \cdot s^3 + 3 \cdot \cos(s)^2 + 3 \cdot s^2 - 3)},$$

with both numerator and denominator non-negative; hence (59) is equivalent to

$$\begin{aligned} q(s) := & -s(\cos(s)^2 \cdot \sin(s) \cdot s^2 + 3 \cdot \cos(s) \cdot s - 3 \cdot \sin(s)) \\ & - 2\cos(s)(-\cos(s) \cdot \sin(s) \cdot s^3 + 3 \cdot \cos(s)^2 + 3 \cdot s^2 - 3) \geq 0, \end{aligned}$$

and we may simplify

$$(60) \quad q(s) = s^3 \cos(s)^2 \sin(s) - 9s^2 \cos(s) + 3s \sin(s) + 6 \cos(s) \sin(s)^2$$

That $q(s) \geq 0$ on $[0, \frac{\pi}{2}]$ is the content of Lemma B.1. \square

Lemma B.1. *The function $q(s)$, defined by (60), satisfies $q(s) \geq 0$ on $s \in [0, \frac{\pi}{2}]$.*

Proof. The result of the lemma is evident from plotting $q(s)$ numerically, but a formal argument can be given along the following lines. We have

$$\begin{aligned} q(s) &= \frac{s^3}{2} \cos(s) \sin(2s) - 9s^2 \cos(s) + 3s \sin(s) + 3 \sin(2s) \sin(s) \\ &= \frac{s^3}{4} (\sin(3s) + \sin(s)) - 9s^2 \cos(s) + 3s \sin(s) \\ &\quad + \frac{3}{2} (\cos(s) - \cos(3s)) \end{aligned}$$

thus we may Taylor expand q around $s = 0$ (we caution the reader that d_k is not the same as in the proof of the previous Lemma):

$$(61) \quad q(s) = \sum_{k=4}^{\infty} d_k s^{2k},$$

where

$$(62) \quad d_k = (-1)^k \left(\frac{9}{(2k-2)!} + \frac{3^{2k-3} + 1}{4 \cdot (2k-3)!} \right) \\ + (-1)^{k+1} \left(\frac{3^{2k+1} - 3}{2 \cdot (2k)!} + \frac{3}{(2k-1)!} \right)$$

in particular $d_4 = \frac{29}{105}$, $d_5 = -\frac{797}{9450}$. The general formula (62) clearly implies that as $k \rightarrow \infty$, $d_k \sim (-1)^k \frac{3^{2k-3}}{4(2k-3)!}$, and moreover, a crude estimate (using that $|3^{2k+1} - 3|/(2 \cdot 2k(2k-1)(2k-2)) < 3^{2k-3} \cdot 3^4/(16(k-1)^3)$ and $|9/(2k-2) - 3|/((2k-1)(2k-2)) < 9/(2k-2)$) shows that for $k \geq 4$,

$$d_k = (-1)^k \frac{3^{2k-3}}{4(2k-3)!} \left(1 + \theta \left(\frac{1}{3^{2k-7}(2k-2)} + \frac{1}{3^{2k-3}} + \frac{21}{(k-1)^3} \right) \right),$$

where⁴ $|\theta| \leq 1$. For $k \geq 6$ we then have

$$(63) \quad d_k = (-1)^k \frac{3^{2k-3}}{4(2k-3)!} \left(1 + \frac{1}{5}\theta \right);$$

it is evident that the signs of d_k are alternating.

Now separate the summands of (61) corresponding to $k \leq 5$ from the rest; the remaining summands are united into pairs, i.e. write

$$(64) \quad q(s) = s^8 q_0(s) + \sum_{r=3}^{\infty} (d_{2r}s^{4r} + d_{2r+1}s^{4r+2}),$$

where

$$q_0(s) = d_4 + d_5 s^2 = \frac{29}{105} - \frac{797}{9450} s^2 \geq 0$$

on $[0, \frac{\pi}{2}]$, using the explicit Taylor coefficients mentioned above.

For the remaining terms, note that by the above, for $r \geq 3$ we have $d_{2r} > 0$ and $d_{2r+1} < 0$, and upon employing (63) with $k = 2r$ and $k = 2r+1$, we obtain

$$\begin{aligned} |d_{2r+1}| &< \frac{6}{5} \frac{3^{4r-1}}{4(4r-1)!} < \frac{6}{5} \cdot 9 \cdot \frac{1}{(4r-2)^2} \frac{3^{4r-3}}{4(4r-3)!} \\ &\leq \frac{6}{5} \cdot 9 \cdot \frac{1}{(4r-2)^2} \cdot \frac{5}{4} |d_{2r}| < 0.2 |d_{2r}|. \end{aligned}$$

Hence each of the summands in (64), for $s \in [0, \frac{\pi}{2}]$, satisfies:

$$d_{2r}s^{4r} + d_{2r+1}s^{4r+2} > d_{2r}s^{4r} - 0.2d_{2r}s^{4r+2} \geq 0$$

⁴In writing this way we follow Vinogradov: the exact value of θ might change, but the inequality $|\theta| \leq 1$ always holds.

as $0.2 \left(\frac{\pi}{2}\right)^2 < 1$. Finally $q(s) \geq 0$, since all the summands in (64) are nonnegative.

□

Proof of Lemma 6.5. By Lemma 6.8 (note that the proof of Lemma 6.8 does not use Lemma 6.5) we may re-parametrize η_A as $(x, h_A(x))$ on $x \in (-\infty, 0]$. Since both components $\eta_{A;1}$ and $\eta_{A;2}$ are strictly increasing, it follows that $h'_A(x) > 0$ everywhere, and $h'_A(x) \leq \frac{4}{3}$ follows from the convexity of h_A , and the explicit computation $h'_A(0) = \frac{4}{3}$.

□

Proof of Corollary 6.6. By the multiplicativity, it is sufficient to prove the statement for a single A_i , i.e. that if

$$(x, y) = (G_A(t), G_A(2t))$$

with A odd and $t \in [\frac{\pi}{2} - \frac{\pi}{2A}, \frac{\pi}{2}]$, then

$$y \geq (Ax)^{4/3}.$$

As we may assume with no loss of generality that $x > 0$ (note that $y > 0$ by the assumption of t_i being near $\pi/2$) the latter is equivalent to

$$(65) \quad \log y \geq \frac{4}{3} \log(Ax).$$

Note that, with η_A defined as in Lemma 6.5, $\eta_A(t) = (z, h_A(z)) = (\log(Ax), \log(y))$, with h_A analytic convex, $h_A(0) = 0$, and a straightforward computation shows that $h'_A(0) = \frac{4}{3}$. By the convexity of η_A then the curve lies above its tangent line at the origin, i.e. (65) follows.

□

Proof of Lemma 6.7. The claimed inequality follows from the identity

$$(2x_1^2 - 1)(2x_2^2 - 1) - (2(x_1 x_2)^2 - 1) = 2(x_1^2 - 1)(x_2^2 - 1).$$

□

REFERENCES

- [1] Cilleruelo, Javier. The distribution of the lattice points on circles. *J. Number Theory* 43 (1993), no. 2, 198–202.
- [2] Fainsilber, L.; Kurlberg, P. ; Wennberg, B. Lattice points on circles and discrete velocity models for the Boltzmann equation, *SIAM J. Math. Anal.* 37 no. 6 (2006), 1903–1922.
- [3] Hecke, E. Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen. *Math. Z.*, 1(4):357–376, 1918.
- [4] Hecke, E. Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen. *Math. Z.*, 6(1-2):11–51, 1920.

- [5] Krishnapur, K., Kurlberg, P., Wigman, I. Nodal length fluctuations for arithmetic random waves. *Ann. of Math.* (2) 177 (2013), no. 2, 699–737.
- [6] Kreĭn, M. G.; Nudel'man, A. A. The Markov moment problem and extremal problems. Ideas and problems of P. L. Čebyšev and A. A. Markov and their further development. Translated from the Russian by D. Louvish. *Translations of Mathematical Monographs*, Vol. 50. American Mathematical Society, Providence, R.I., 1977. v+417 pp. ISBN: 0-8218-4500-4.
- [7] Landau, E. Über die Einteilung der positiven Zahlen nach vier Klassen nach der Mindestzahl der zu ihrer addition Zusammensetzung erforderlichen Quadrate. *Arch. Math. und Phys.* III, 1908
- [8] Riesz, F. Sur certains systèmes singuliers d'équations intégrales. (French) *Ann. Sci. cole Norm. Sup.* (3) 28 (1911), 33-62

URL: www.math.kth.se/~kurlberg

DEPARTMENT OF MATHEMATICS, KTH ROYAL INSTITUTE OF TECHNOLOGY,
SE-100 44 STOCKHOLM, SWEDEN

E-mail address: kurlberg@math.kth.se

DEPARTMENT OF MATHEMATICS, KING'S COLLEGE LONDON, UK

E-mail address: igor.wigman@kcl.ac.uk