Notes on Equidistribution

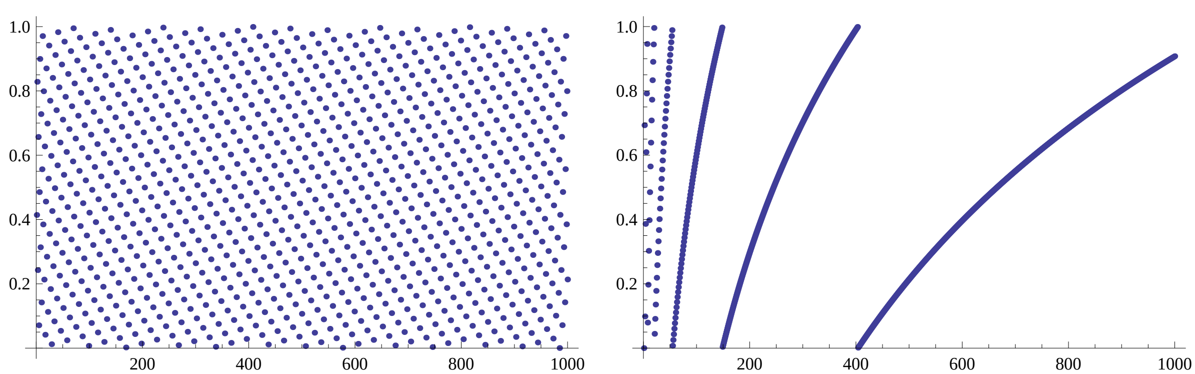
Jacques Verstraëte
Department of Mathematics
University of California, San Diego
La Jolla, CA, 92093.
E-mail: jacques@ucsd.edu.

1 Introduction

For a real number a we write $\{a\}$ for the fractional part of a. A sequence $(a_n)_{n\in\mathbb{N}}$ is *equidistributed* if for every $a, b \in [0,1]$ with $a < b$,

$$\lim_{N\to\infty} \frac{|\{n \leq N : \{a_n\} \in (a,b)\}|}{N} = b - a.$$

For convenience, we refer to the nth term as representative of the whole sequence. For instance, the sequence $n\sqrt{2}$ appears to be equidistributed as the plot of the fractional parts up to one thousand suggests, whereas $\log n$ does not:



Plot of $\{\sqrt{2}n\}$ and $\{\log n\}$ for $n \leq 1000$.

We shall see shortly that the evidence supports the truth for these two examples. Weyl's (1909) celebrated equidistribution theorem states that integer multiples of an irrational number are equidistributed. The key to proving Weyl's Theorem is the equivalence of equidistribution with vanishing upper bounds on *exponential sums* – sums of the form

$$\sum_{n=1}^{N} \exp(2\pi i f(n))$$

where $f : \mathbb{N} \to \mathbb{C}$. It is traditional to write $e(x)$ instead of $\exp(2\pi i x)$. The following is a part of *Weyl's criterion* for equidistribution:

Theorem 1 *A sequence a_n is equidistributed if and only if for each $k \in \mathbb{N}$,*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} e(ka_n) = 0.$$

This is to say that if we wrap the sequence a_n around the unit circle in the complex plane k times, then the centroid of the points obtained converges to the origin. The proof of this theorem is fairly straightforward, and hinges on approximating integrable functions by step functions and trigonometric polynomials – specifically the Stone-Weierstrass theorem. We defer the proof of the theorem until later, since it is part of more general theory.

2 Weyl's Equidistribution Theorem

For an irrational α, we want to show that the sequence αn is equidistributed. This is an instant consequence of Weyl's criterion and the following lemma. Throughout this material, $\|\alpha\|$ is the distance from the real number α to the nearest integer.

Lemma 1 *Let $\alpha, \beta \in \mathbb{R}$. Then for $N \in \mathbb{N}$,*

$$\left|\sum_{n=1}^{N} e(\alpha n + \beta)\right| \leq \min\{N, (2\|\alpha\|)^{-1}\}$$

Proof. The constant β does not affect the inequality. If $\alpha = 0$, then the sum is N. If $\alpha \neq 0$, then the sum is $e(\alpha)(1 - e(\alpha n))/(1 - e(\alpha))$ since it is a geometric series. As

$$\sin z = \frac{1}{2i}(e^{iz} - e^{-iz}),$$

this is at most $|\sin \pi\alpha|^{-1}$. Since $|\sin \pi\alpha| \geq 2\|\alpha\|$, the inequality follows. ∎

Theorem 2 *Let α be irrational. Then αn is equidistributed.*

Proof. By Weyl's criterion, we have to show for every $k \in \mathbb{N}$ that

$$\lim_{N\to\infty} \frac{1}{N}\Big|\sum_{n=1}^{N} e(k\alpha n)\Big| = 0.$$

Now $k\alpha$ is irrational, so by the last lemma if N is large enough then the sum is at most $1/2\|k\alpha\|$. Relative to N, this is a constant, and therefore

$$\frac{1}{N}\Big|\sum_{n=1}^{N} e(k\alpha n)\Big| \ll \frac{1}{N}$$

which clearly converges to zero. ∎

In the proof of Weyl's Theorem above, a key fact is that $\|k\alpha\|$ is non-zero when α is irrational. In the next sections, we will be exploring equidistribution of polynomial sequences i.e. sequences $\{\alpha\phi(n)\}$ where ϕ is a monic polynomial and α is irrational. In this case, a key to bounding the appropriate exponential sum is the quality of approximation of α by a rational with small denominator.

3 Rational approximation

How well can we approximate an irrational number α by a rational number? Of course the answer is arbitrarily well since the rationals are dense in the reals. More importantly, given $N \in \mathbb{N}$, how well can one approximate α by a rational with denominator at most N? A good answer is given by the so-called *Dirichlet box principle*, which is in fact an application of the pigeonhole principle.

Theorem 3 *Let $\alpha \in \mathbb{R}$ and $N \in \mathbb{N}$. Then there exist $p, q \in \mathbb{N}$ such that $q \leq N$ and*

$$\Big|\alpha - \frac{p}{q}\Big| \leq \frac{1}{q(N+1)}.$$

Proof. Notice that for distinct $0 \leq n \leq N$, we have $\{n\alpha\} \in [0,1]$ so there are two integers $m, n \leq N$ such that $\{m\alpha\}$ and $\{n\alpha\}$ lie in an interval of width $1/(N+1)$. It is left then as an exercise as to what q should be. ∎

The reader may then verify the following consequence of Dirichlet's Theorem as an exercise:

Corollary 1 *Let $\alpha \in \mathbb{R}$. Then there are infinitely many pairs (p, q) of coprime integers such that $|\alpha - p/q| \leq 1/q^2$.*

3.1 Liouville's Theorem

It is not hard to check that this corollary is best possible by considering algebraics of degree two over $\mathbb{Q}$. More generally, one has Liouville's Theorem (1844):

Theorem 4 *Let $\alpha \in \mathbb{R}$ be algebraic of degree n over $\mathbb{Q}$. Then there is a constant $c > 0$ such that for any $p, q \in \mathbb{N}$,*

$$\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^n}.$$

Proof. Let f be an irreducible polynomial of degree n with integer coefficients such that $f(\alpha) = 0$ – for instance consider a minimal polynomial for α over $\mathbb{Q}$ and use Gauss' Lemma. For any $p, q \in \mathbb{N}$, we have $|q^n f(p/q)| \geq 1$. By the mean value theorem, there is $x \in [\alpha, p/q]$ such that

$$\frac{f(p/q) - f(\alpha)}{p/q - \alpha} = f'(x).$$

Taking absolute values we obtain

$$|f'(x)||\alpha - p/q| \geq \frac{1}{q^n}$$

which completes the proof upon taking $c = 1/|f'(x)|$. ∎

The above result shows that transcendental numbers exist – any real α for which Theorem 4 fails in the sense that for every n there exists p, q such that $|\alpha - p/q| \leq 1/q^n$ is called a *Liouville number* and must be transcendental. The Thue-Siegel-Roth Theorem, proved first by Thue (1909) shows further that if α is algebraic over $\mathbb{Q}$, then for every $\varepsilon > 0$ the inequality

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\varepsilon}}$$

has only finitely many solutions (p, q), and so the c/q^n term in Liouville's Theorem can be replaced by $q^{2+o(1)}$ as $q \to \infty$. Lang conjectures the upper bound $1/(q^2 \log q)^{1+o(1)}$ as $q \to \infty$.

4 Bounds on exponential sums

A first step to proving bounds on exponential sums is the following lemma:

Lemma 2 *Let $M, r, N \in \mathbb{N}$ and let $\alpha_1, \alpha_2, \ldots, \alpha_M$ be real numbers with $\|\alpha_i - \alpha_j\| \geq r^{-1}$ whenever $i \neq j$. Then*

$$\sum_{i=0}^{M} \min\left\{\frac{1}{\|\alpha_i\|}, N\right\} \leq 2N + 2r(\log N + 2).$$

Proof. Without loss of generality, $\alpha_i \in [-1/2, 1/2]$ and the contribution to the sum from the non-negative α_i is at least one half of the total. We may assume $0 \le \alpha_0 < \alpha_1 < \cdots < \alpha_n$. Then

$$\sum_{i=0}^{n} \min\Big\{\frac{1}{\|\alpha_i\|}, N\Big\} \quad \le \quad N + \Big\lfloor \frac{r}{N} \Big\rfloor N + \sum_{i > \lfloor r/N \rfloor} \frac{r}{i}.$$

If $N > r$, then the last term is at most $r(\log n + 1)$. However since $n/r \le \alpha_n \le 1/2$, we have $2n \le r < N$ and so the bound is $r(\log N + 1)$ in this case. If $N \le r$, then estimating the last term with logarithms shows that it is at most $r \log(2nN/r) + r \le r(\log N + 1)$. It follows that the whole sum is at most $2N + 2r(\log N + 2)$. ∎

Lemma 3 *Let $N, M \in \mathbb{N}$, and let $\alpha \in \mathbb{R}$ be chosen so that there exists $p, q \in \mathbb{N}$ with $(p, q) = 1$ and $|\alpha - p/q| \le 1/q^2$. Then*

$$\sum_{n=1}^{M} \min\Big\{\frac{1}{\|\alpha n + \beta\|}, N\Big\} \le \Big(\frac{2M}{q} + 1\Big)(2N + 4q(\log N + 2)).$$

Proof. For $i, j \in \mathbb{N}$, it is straightforward to see that

$$\|i\alpha - j\alpha\| \ge \|(i-j)p/q\| - \frac{|i-j|}{q^2}.$$

When $0 < |i - j| \le q/2$, $\|(i-j)p/q\| \ge 1/q$ since p and q are relatively prime, whereas $|i-j|/q^2 \le 1/2q$. It follows that $\|i\alpha - j\alpha\| \ge 1/2q$ for $0 < |i-j| \le q/2$. Split the range of summation, namely $[M]$, into $m \le M/(q/2+1) + 1$ intervals $I_1, I_2, \ldots, I_m$ of length at most $q/2 + 1$. On each of these intervals, we apply the last lemma with $r = 2q$, so that for each $j \in [m]$,

$$\sum_{n \in I_j} \min\Big\{\frac{1}{\|\alpha n + \beta\|}, N\Big\} \le 2N + 4q(\log N + 2).$$

It follows that the entire sum is at most

$$2mN + 4qm(\log 2q + 2) < \Big(\frac{2M}{q} + 1\Big)(2N + 4q(\log N + 2)).$$

This completes the proof. ∎

5 Weyl differencing

The above lemmas allow us to find bounds on exponential sums using a method known as *Weyl differencing*. This method is encapsulated by the following lemma.

Lemma 4 *Let $N \in \mathbb{N}$ and $M \in [N]$, and let $f : [N] \to \mathbb{C}$. Then*

$$\Big|\sum_{n=1}^{N} e(f(n))\Big|^2 \le \frac{N}{M}\sum_{m=0}^{M-1}\Big|\sum_{n=1}^{N-m} e(f(n+m)-f(n))\Big|.$$

Proof. We have the identity

$$\sum_{n=1}^{N} e(f(n)) = \frac{1}{M}\sum_{m=1}^{M}\sum_{n=1-m}^{N-m} e(f(n+m)).$$

Applying Cauchy-Schwarz to this identity, we get

$$\Big|\sum_{n=1}^{N} e(f(n))\Big|^2 \le \frac{1}{M}\sum_{m=1}^{M}\Big|\sum_{n=1-m}^{N-m} e(f(n+m))\Big|^2.$$

Applying the differencing method to the inner sum, the whole expression is bounded above by

$$\frac{1}{M}\sum_{k=1}^{M}\sum_{\ell=1}^{M}\Big|\sum_{n\in I_{k,\ell}} e(f(n+k)-f(n+\ell))\Big|$$

where $I_{k,\ell}$ consists of all n such that $1 \le n+k \le N$ and $1 \le n+\ell \le N$. This is the key point of the lemma: the inner sum depends only on $|k-\ell|$, which takes on at most M values. Letting $m = |k-\ell|$, each value of m occurs at most N times and so we get the bound

$$\frac{N}{M}\sum_{m=0}^{M-1}\Big|\sum_{n=1}^{N-m} e(f(n+m)-f(n))\Big|.$$

This is the required bound. ∎

Weyl use the method of differencing to show that $\alpha\phi(n)$ is equidistributed whenever ϕ is a monic non-constant polynomial. We apply this result explicitly in the quadratic case as follows:

Theorem 5 *Let $q, N \in \mathbb{N}$ and let ϕ be a monic quadratic polynomial. Suppose $\alpha \in \mathbb{R}$ and for some relatively prime $p, q \in \mathbb{N}$, $|\alpha - p/q| \le 1/q^2$. Then*

$$\Big|\sum_{n=1}^{N} e(\alpha\phi(n))\Big| \le \Big(\frac{4N}{q}+1\Big)^{1/2}(2N+4q(\log N+2))^{1/2}.$$

Proof. Consider the preceding lemma with $f(x) = \alpha\phi(x)$ and $M = N$. It is necessary to estimate

$$\sum_{m=0}^{N-1}\Big|\sum_{n=1}^{N-m} e(f(n+m) - f(n))\Big|.$$

The inner sum is

$$\Big|\sum_{n=1}^{N-m} e(2\alpha mn)\Big| \leq \min\Big\{\frac{1}{2\|2\alpha m\|}, N-m\Big\}$$

according to Lemma 1. Doubling the range of m, this is at most

$$\sum_{m=0}^{2N-2} \min\Big\{\frac{1}{\|\alpha m\|}, N\Big\}.$$

By Lemma 3 with $M = 2N-2$, this sum is at most

$$\Big(\frac{4N}{q} + 1\Big)(2N + 4q(\log N + 2)).$$

Applying Lemma 4,

$$\Big|\sum_{n=1}^{N} e(\alpha\phi(n))\Big|^2 \leq \Big(\frac{4N}{q} + 1\Big)(2N + 4q(\log N + 2)).$$

This completes the proof. ∎

An equidistribution theorem for $\alpha\phi(n)$ when ϕ is monic and quadratic follows quickly from Theorem 5:

Corollary 2 *Let ϕ be a monic quadratic polynomial and α irrational. Then $\alpha\phi(n)$ is equidistributed.*

Proof. Fix $k \in \mathbb{N}$. Infinitely many choices of q are available so that there exists p, q relatively prime with $|k\alpha - p/q| \leq 1/q^2$. By Weyl's criterion, we require

$$\frac{1}{N}\Big|\sum_{n=1}^{N} e(k\alpha\phi(n))\Big| \to 0$$

as $N \to \infty$. The upper bound for the left side given by Theorem 5 is

$$\Big(\frac{4}{q} + \frac{1}{N}\Big)^{1/2}\Big(2 + \frac{4q(\log N + 2)}{N}\Big)^{1/2}.$$

For each fixed q, taking the limit as $N \to \infty$ the above expression converges to $\sqrt{8/q}$. Since q can be taken to be arbitrarily large, the limit must be zero. ∎

This corollary effectively shows that if α is irrational and ϕ is quadratic, then for infinitely many N we have

$$\Big|\sum_{n=1}^{N} e(\alpha\phi(n))\Big| \ll \sqrt{N \log N}.$$

The reader may wish to find α for which the above sum is as close to linear in N as desired for infinitely many N.

Before we move on to the case that ϕ is a polynomial of higher degree, we consider Gauss sums. Remarkably, it is possible to give a simple explicit formula in the case $\phi(x) = x^2$, as shown by Gauss (1811). Let χ denote the *quadratic character* in $\mathbb{Z}_N$, so $\chi(x) = 1$ if x is a non-zero quadratic residue, $\chi(x) = -1$ if x is a non-residue, and $\chi(0) = 0$. This is a special example of a *character* of a group, and much here be generalized to work with characters of general abelian groups. Gauss proved the following result, which can be proved fairly simply by squaring each side (recall here $\omega = e^{2\pi i/N}$):

Lemma 5 *Let N be prime. Then*

$$\Big|\sum_{x\in\mathbb{Z}_N} \chi(x)\omega^x\Big| = \sqrt{N}.$$

It is actually a tricky task to determine the sign of the sum itself. It can be shown (as Gauss did after determining the sum up to sign) that the sum is $\sqrt{N}$ if $N = 1 \bmod 4$ and $i\sqrt{N}$ if $N = 3 \bmod 4$. The reader may then wish to check the value of $\sum_{n=1}^{N} e(n^2)$.

6 Equidistribution of polynomials

Weyl generalized his equidistribution theorem to show that for a polynomial ϕ, $\phi(n)$ is equidistributed if and only if ϕ has at least one non-constant irrational coefficient. This result actually follows quickly from the differencing method of Lemma 4, and generalizes as follows:

Theorem 6 *Let a_n be a sequence such that $a_{n+m} - a_n$ is equidistributed for all $m \in \mathbb{N}$. Then a_n is itself equidistributed.*

Proof. Lemma 4 gives, for any fixed $M \in [N]$,

$$\lim_{N\to\infty} \frac{1}{N^2}\Big|\sum_{n=1}^{N} e(a_n)\Big|^2 \leq \frac{1}{M}\sum_{m=0}^{M-1} \lim_{N\to\infty} \frac{1}{N}\Big|\sum_{n=1}^{N-m} e(a_{n+m} - a_n)\Big|.$$

The inner term for $m=0$ is N. Since $a_{n+m}-a_n$ is equidistributed for all $m \in \mathbb{N}$,

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N-m} e(a_{n+m}-a_n) = 0$$

for each $m \in \mathbb{N}$. So the inner sum converges to 1 for $m=0$ and to zero otherwise. It follows that

$$\lim_{N\to\infty} \frac{1}{N^2} \Big|\sum_{n=1}^{N} e(a_n)\Big|^2 \le \frac{1}{M}$$

and since M was arbitrary, the limit is zero. By Weyl's criterion, this means a_n is equidistributed. ∎

Corollary 3 *If ϕ is a monic polynomial and α is irrational, then $\alpha\phi(n)$ is equidistributed.*

Proof. This is Weyl's Theorem if ϕ is linear. Suppose ϕ has degree $k \ge 2$ and proceed by induction on k. Let $\beta = \alpha k m$, which is an irrational number, and $a_n = \alpha\phi(n)$. Then

$$a_{n+m} - a_n = \beta n^{k-1} + \cdots := \beta\tilde{\phi}(n)$$

where $\tilde{\phi}$ is a monic polynomial of degree $k-1$. By induction, $\beta\tilde{\phi}(n)$ is equidistributed and therefore $a_{n+m}-a_n$ is equidistributed for every fixed $m \in \mathbb{N}$. The last lemma finishes the proof. ∎

7 Weyl's Inequality

We turn now to bounds on exponential sums with polynomial exponent. The main result of this section, which gives such a bound depending on the quality of rational approximation of the leading coefficient of the polynomial exponent, is Weyl's inequality. We need the following preliminary lemma.

Lemma 6 *Let $k,n \in \mathbb{N}$. For every $\varepsilon > 0$, the number $d(n)$ of ways of writing n has an ordered product of k positive integers satisfies $d(n) \ll n^{\varepsilon}$.*

Proof. Let $n = \prod_{i=1}^{r} p_i^{a_i}$ where $p_1, p_2, \ldots, p_r$ are the primes in $[n]$ and a_i is a non-negative integer. Then the number $\tau(n)$ of divisors of n satisfies

$$\tau(n) = \prod_{i=1}^{r} (a_i + 1).$$

Fixing $t \in [r]$,

$$\begin{aligned}\tau(n) &\leq \prod_{i=1}^{t}(a_i+1) \cdot \prod_{i=t+1}^{r} 2^{a_i} \\ &\leq \prod_{i=1}^{t}(\log_2 n+1) \cdot \prod_{i=t+1}^{r} p_i^{a_i/\log_2 p_i} \\ &\leq (1+\log_2 n)^t n^{1/\log_2 t} \leq \exp\Big(2t \log\log n + \frac{2\log n}{\log p_t}\Big).\end{aligned}$$

Choose $t = \lfloor \log n/(\log\log n)^2 \rfloor$. Then the above expression is at most $n^{4/\log\log n}$. Now the number of ways of writing n as an ordered product of k positive integers is at most $\tau(n)^k \ll n^{\varepsilon}$. ∎

The reader may check that one make take $\varepsilon = 4/\log\log n$, and this is roughly best possible up to the constant four in the exponent, which can be improved to $\log 2$ as $n \to \infty$. We are now in a position to prove Weyl's Inequality, which we state in the following form:

Theorem 7 *Let ϕ denote a monic linear polynomial of degree $k \geq 2$ and let $\alpha \in \mathbb{R}$ satisfy $|\alpha - p/q| \leq 1/q^2$ where $(p,q) = 1$. Then for every $\varepsilon > 0$,*

$$\Big|\sum_{n=1}^{N} e(\alpha\phi(n))\Big| \ll N^{1+\varepsilon}\Big(\frac{1}{q} + \frac{q\log N}{N^k} + \frac{1}{N}\Big)^{2^{1-k}}.$$

Proof. For $j \in [k-1]$ let

$$f_j := f_j(m_1, m_2, \ldots, m_{j+1}) = \alpha\frac{k!}{(k-j)!}m_{j+1}^{k-j}m_1 \ldots m_j.$$

We shall prove that for $j \in [k]$,

$$\Big|\sum_{n=1}^{N} e(\alpha\phi(n))\Big|^{2^j} \leq N^{2^j-j-1}\sum_{i=1}^{j}\sum_{m_i=0}^{M_i}\Big|\sum_{m_{j+1}=1}^{M_{j+1}} e(f_j)\Big|$$

where $M_1 = N-1$ and $M_i = N - \sum_{j<i} m_j$ for $i \geq 2$. For $j = 1$, this is precisely Lemma 4. Proceeding inductively, assume we have the above inequality up to a certain value

$j-1$, then

$$\begin{aligned}
\Big|\sum_{n=1}^{N} e(\alpha\phi(n))\Big|^{2^j} &\leq N^{2^j-2j}\left(\sum_{i=1}^{j-1}\sum_{m_i=0}^{M_i}\Big|\sum_{m_j=1}^{M_j} e(f_{j-1})\Big|\right)^2 \\
&\leq N^{2^j-2j}\cdot N^{j-1}\left(\sum_{i=1}^{j-1}\sum_{m_i=0}^{M_i}\Big|\sum_{m_j=1}^{M_j} e(f_{j-1})\Big|\right)^2 \\
&\leq N^{2^j-j-1}\sum_{i=1}^{j-1}\sum_{m_i=0}^{M_i}\Big|\sum_{m_j=1}^{M_j} e(f_{j-1})\Big|^2 \\
&\leq N^{2^j-j-1}\sum_{i=1}^{j}\sum_{m_i=0}^{M_i}\Big|\sum_{m_{j+1}=1}^{M_{j+1}} e(f_j)\Big|
\end{aligned}$$

as required. Now we use the case $j=k-1$, namely

$$\Big|\sum_{n=1}^{N} e(\alpha\phi(n))\Big|^{2^{k-1}} \leq N^{2^{k-1}-k}\sum_{i=1}^{k-1}\sum_{m_i=0}^{M_i}\Big|\sum_{m_k=1}^{M_k} e(f_{k-1})\Big|.$$

We consider first the contribution to the sum from all terms where some m_i is zero. Since $f_{k-1}=0$ in that case, the contribution is trivially less than N^{k-1}. Now consider the contribution from all terms where no m_i is zero. Crucially, f_{k-1} is linear in all variables and therefore Lemma 1 applies:

$$\Big|\sum_{m_k=1}^{M_k} e(f_{k-1})\Big| \leq \min\Big\{\frac{1}{2\|\alpha k! m_1 m_2 \dots m_k\|}, N\}.$$

We change the summation variables to $m := k! m_1 m_2 \dots m_{k-1}$. With $M = k! N^{k-1}$, by Lemma 6, there are at most $M^{\varepsilon} < k!^{\varepsilon} N^{2^{k-1}\varepsilon}$ solutions to $m = k! m_1 m_2 \dots m_{k-1}$ for $m \in [M]$. Therefore the sums are at most

$$L\sum_{m=1}^{M}\min\Big\{\frac{1}{\|\alpha m\|}, N\Big\}.$$

By Lemma 3, this is at most

$$k!^{\varepsilon} N^{2^{k-1}\varepsilon}\Big(\frac{2M}{q}+1\Big)(2N+4q(\log N+2)).$$

Finally, cleaning up all the upper bounds together gives, for any $\varepsilon > 0$,

$$\begin{aligned}\Big|\sum_{n=1}^{N} e(\alpha\phi(n))\Big|^{2^{k-1}} &\leq N^{2^{k-1}-k} k!^{\varepsilon} N^{2^{k-1}\varepsilon}\Big(\frac{2M}{q}+1\Big)(2N+4q(\log N+2)) \\ &\ll k!^{\varepsilon} N^{2^{k-1}(1+\varepsilon)}\Big(\frac{2M}{qN^k}+\frac{1}{N^k}\Big)(2N+4q(\log N+2)) \\ &\ll k!^{\varepsilon+1} N^{2^{k-1}(1+\varepsilon)}\Big(\frac{1}{q}+\frac{q\log N}{N^k}+\frac{1}{N}\Big).\end{aligned}$$

Taking 2^{k-1}th roots completes the proof. ∎

The reader should verify that Weyl's Inequality does not show that the exponential sum is $o(N)$, so equidistribution of $\alpha\phi(n)$ does not follow immediately. It is possible to obtain equidistribution from Weyl's Inequality by carefully partition the range of summation of the exponential sum according to an infinite sequence $q_1, q_2, \dots$ of integers such that $|\alpha - p_i/q_i^2| \leq 1/q_i^2$ where $(p_i, q_i) = 1$ for all i, and the details are left to the reader. We also remark that there is a weakness in the proof where we replace the summation variable $m_1 m_2 \dots m_k$ by m and use the estimate on the number of divisors uniformly for all terms in the sum. This is responsible for the N^{ε} in Weyl's Inequality, and one may take $\varepsilon \ll 1/\log\log N$. In reality, this can be improved to $(\log N)^c$ for a constant c depending on k, since for every $\eta > 0$, for almost every integer n, $\tau(n) = (\log n)^{\log 2+\eta}$.

8 Application to rational approximation

We show how to use Weyl's Inequality to say something more about rational approximation. Another view of Dirichlet's Theorem is to state that for every $N \in \mathbb{N}$ and $\alpha \in \mathbb{R}$, there exists $q \leq N$ such that $\|\alpha q\| \leq 1/N$. Putting forth the same question for $\|\alpha\phi(q)\|$ where ϕ is a monic polynomial with integer coefficients, we shall use Weyl's Inequality to prove the following theorem:

Theorem 8 *Let $\alpha \in \mathbb{R}$ and $k, N \in \mathbb{N}$ where $k \geq 2$ and let $0 < \delta < 2^{-k-1}$. Then there exists $q \leq N$ such that*

$$\|\alpha q^k\| \ll N^{-\delta}.$$

The following lemma shows that if a set A of elements of $\mathbb{Z}_N$ is disjoint from a large interval, then there is a non-zero r such that $|\hat{A}(r)|$ is large. The idea is that if Theorem 8 were false, and α is close to P/Q, then $A = \{P, 2^k P, \dots, N^k P\}$ is disjoint from $(-2QN^{-\delta}, 2QN^{-\delta}]$, and so $|\hat{A}(r)|$ is large for some non-zero r, but this would contradict Theorem 7, Weyl's Inequality.

Lemma 7 *Let Q be a prime and $A \subset \mathbb{Z}_Q$, and suppose $A \cap (-2M, 2M] = \emptyset$. Then there exists $r : 0 < r < (Q/M)^2$ such that*

$$|\hat{A}(r)| \geq \frac{M|A|}{2Q}.$$

Proof. Put $I = (-M, M]$ and note

$$\sum_{x \in \mathbb{Z}_Q} (I * I)(x) A(x) = 0.$$

It follows that

$$\sum_{r \in \mathbb{Z}_Q} |\hat{I}(r)|^2 \hat{A}(r) = 0.$$

Taking out the term for $r = 0$ and using the triangle inequality, we obtain

$$\sum_{r \neq 0} |\hat{I}(r)|^2 |\hat{A}(r)| \geq 4M^2 |A|.$$

However by Lemma 1,

$$|\hat{I}(r)| = \left| \sum_{x \in I} \omega^{-rx} \right| \leq \min\{\frac{1}{\|\frac{r}{Q}\|}, |I|\}.$$

If $-Q/2 < r < Q/2$, then this is $\min\{Q/r, 2M\}$. Consequently if $L = (Q/M)$,

$$\begin{aligned} \sum_{r \neq 0} |\hat{I}(r)|^2 |\hat{A}(r)| &\leq \max_{0 < |r| \leq L} |\hat{A}(r)| \sum_r |\hat{I}(r)|^2 + |A| \sum_{|r| > L} \left(\frac{Q}{r}\right)^2 \\ &\leq |I| Q \max_{0 < r \leq L} |\hat{A}(r)| + \frac{3|A|Q^2}{L^2}. \end{aligned}$$

Therefore there exists r for which $|\hat{A}(r)| \geq M|A|/2Q$. ∎

Proof of Theorem 8. Approximate α arbitrarily closely by a rational P/Q with Q prime. Without loss of generality, $\alpha = P/Q$. If the theorem were false, then $A = \{P, 2^k P, \ldots, N^k P\}$ and $(-2M, 2M]$ are disjoint when $M = \lfloor QN^{-\delta} \rfloor$. Applying the last lemma, we find r such that $0 < r \leq (Q/M)^2 \leq 2N^{2\delta}$, and such that

$$|\hat{A}(r)| \gg N^{1-\delta}.$$

Let $R = N^{k-1/4}$. Via Dirichlet's Theorem, choose $q \leq R$ with $\|\alpha q r/N\| < 1/R$ using Dirichlet's Theorem. If $R \geq q > \frac{1}{2} N^{1/4}$, then Weyl's Inequality shows that for any $\varepsilon > 0$ we have

$$|\hat{A}(r)| \ll N^{1+\varepsilon-2^{-k-1}}.$$

This is a contradiction since $\delta < 2^{-k-1}$. Therefore $q \leq \frac{1}{2}N^{1/4}$, which shows

$$\|\alpha(qr)^k\| \ll N^{(k-1)(2\delta+1/4)} \cdot \frac{N}{R} \ll N^{1-3k/4+(k-1)(2\delta)} \ll N^{-\delta}$$

by the choice of δ. Also by the choice of δ,

$$qr \leq N^{1/4+2\delta} < N,$$

and this completes the proof. ∎