Equidistribution and Weyl's criterion

by Brad Hannigan-Daley

We introduce the idea of a sequence of numbers being *equidistributed* (mod 1), and we state and prove a theorem of Hermann Weyl which characterizes such sequences. We also discuss a few interesting results that follow from Weyl's theorem.

Weyl's equidistribution criterion

Definition. *Let $u_1, u_2, \ldots$ be a bounded sequence of real numbers. We say that this sequence is* ***equidistributed*** *or* ***uniformly distributed*** (mod 1) *if, for every subinterval (α, β) of $[0,1]$, we have*

$$\lim_{N\to\infty} \frac{1}{N} |\{\{u_1\}, \ldots, \{u_N\}\} \cap (\alpha, \beta)| = \beta - \alpha.$$

(For each $x \in \mathbb{R}, \{x\}$ denotes its fractional part $x - \lfloor x \rfloor$.)

That is to say, the proportion of the $\{u_j\}$ that lie in any given subinterval is proportional to the length of that subinterval, and thus this sequence of fractional parts is "evenly distributed" in $[0,1]$[1] Observe that for such a sequence, it immediately follows that $\{u_1\}, \{u_2\}, \ldots$ is dense in $[0,1]$: for any subinterval $(\alpha, \beta) \subseteq [0,1]$, since $\lim_{N\to\infty} \frac{1}{N} |\{\{u_1\}, \ldots, \{u_N\}\} \cap (\alpha, \beta)| = \beta - \alpha > 0$ there exists some least integer N such that $\frac{1}{N} |\{\{u_1\}, \ldots, \{u_N\}\} \cap (\alpha, \beta)| \neq 0$, whence $\{u_N\} \in (\alpha, \beta)$. We note also that we may replace instances of (α, β) by any of $[\alpha, \beta)$ in this definition since the difference between $\frac{1}{N} |\{\{u_1\}, \ldots, \{u_N\}\} \cap (\alpha, \beta)|$ and $\frac{1}{N} |\{\{u_1\}, \ldots, \{u_N\}\} \cap [\alpha, \beta)|$ is at most $\frac{1}{N}$, which vanishes in the limit. A similar remark holds for replacing such instances by $(\alpha, \beta]$ or $[\alpha, \beta]$.
Weyl's criterion provides a characterization of the sequences that are equidistributed (mod 1) which, among other things, implies that questions about equidistribution can be reduced to finding bounds on certain exponential sums.

Theorem (Weyl's criterion). *Let $u_1, u_2, \ldots$ be a sequence of real numbers. The following are equivalent:*

(1) $u_1, u_2, \ldots$ *is equidistributed* (mod 1)

(2) *For each nonzero integer k, we have*

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

(3) *For each Riemann-integrable $f : [0,1] \to \mathbb{C}$, we have*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f(\{u_n\}) = \int_0^1 f(x)dx$$

Before proceeding to the proof of this result, we offer some heuristic justification for it. Suppose we are given a sequence $u_1, \ldots$, and the fractional parts $\{u_1\}, \ldots$ are placed on the interval [0,1], which is then

[1]The notion of equidistributivity of a sequence is more generally defined in certain classes of locally compact groups, using the Haar measure, and results such as analogues to Weyl's criterion can be proved in this more general setting. The original results can be recovered by considering the compact group $\mathbb{T} = \mathbb{R}/\mathbb{Z}$. See, for example, [3].

wrapped around the unit circle k times for some nonzero integer k. We would expect that, if the sequence is equidistributed (mod 1), the corresponding points on the circle should be also be evenly distributed. The condition (2) states that equidistribution (mod 1) is equivalent to the first N of these points having a centroid which approaches the centre of the circle as N becomes large, regardless of the choice of k, which we would expect of a sequence of points that is evenly distributed on the circle. The third condition can be interpreted as saying that, given a sequence of numbers in [0,1), it is equidistributed in [0,1] if and only if the average value of each integrable function on [0,1] can be obtained by averaging over only the points of that sequence, which is a plausible consequence of equidistribution.

Proof. (1) ⇒ (3) Let $f : [0,1] \to \mathbb{C}$ be an integrable function. Assume without loss of generality that f is real-valued, since otherwise we can just consider the real and imaginary parts separately. Let $I = [\alpha, \beta) \subseteq [0,1]$. Noting that

$$\frac{1}{N}|\{\{u_1\}, \ldots, \{u_N\}\} \cap [\alpha, \beta)| = \frac{1}{N}\sum_{n=1}^{N} 1_{[\alpha,\beta)}(\{u_n\})$$

and that $\int_0^1 1_I = \beta - \alpha$, we conclude from (1) that (3) holds in the case that f is the characteristic function of an open subinterval I, and the same reasoning shows that this also holds if I is a closed or half-open subinterval.

Now, if λ_1, λ_2 are real numbers and f_1, f_2 are functions for which (3) holds, we have

$$\begin{aligned}\frac{1}{N}\sum_{n=1}^{N}(\lambda_1 f_1 + \lambda_2 f_2)(\{u_n\}) &= \lambda_1 \frac{1}{N}\sum_{n=1}^{N} f_1(\{u_n\}) + \lambda_2 \frac{1}{N}\sum_{n=1}^{N} f_2(\{u_n\}) \\ &\overset{N\to\infty}{\longrightarrow} \lambda_1 \int_0^1 f_1 + \lambda_2 \int_0^1 f_2 \\ &= \int_0^1 (\lambda_1 f_1 + \lambda_2 f_2)\end{aligned}$$

and we conclude that (3) holds for all $\mathbb{R}-$linear combinations of characteristic functions of subintervals, hence for all step functions on $[0,1]$. Now, let $f : [0,1] \to \mathbb{R}$ be an arbitrary integrable function, and let $\varepsilon > 0$. Then there exist step functions $f_1, f_2 : [0,1] \to \mathbb{R}$ such that $f_1 \leq f \leq f_2$ pointwise and $\int_0^1 (f_2 - f_1) < \frac{\varepsilon}{2}$. As $f_2 \geq f$, we have

$$\int_0^1 (f - f_1) \leq \int_0^1 (f_2 - f) + \int_0^1 (f - f_1) = \int_0^1 (f_2 - f_1) < \frac{\varepsilon}{2},$$

hence

$$\int_0^1 f - \frac{\varepsilon}{2} < \int_0^1 f_1 = \lim_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} f_1(\{u_n\}).$$

It follows that, for large enough N, $\frac{1}{N}\sum_{n=1}^{N} f_1(\{u_n\}) > \int_0^1 f - \varepsilon$ and thus $\frac{1}{N}\sum_{n=1}^{N} f(\{u_n\}) > \int_0^1 f - \varepsilon$ for large N. We similarly obtain $\frac{1}{N}\sum_{n=1}^{N} f(\{u_n\}) < \int_0^1 f + \varepsilon$ for large N, hence $\left|\frac{1}{N}\sum_{n=1}^{N} f(\{u_n\}) - \int_0^1 f\right| < \varepsilon$ for sufficiently large N, proving the equality in (3).

(3) ⇒ (1)

As above, taking $f = 1_{[\alpha,\beta)}$ for each $[\alpha, \beta) \subseteq [0,1]$ shows that (1) holds.

(3) ⇒ (2)

Fix $k \in \mathbb{Z}\backslash\{0\}$, and let $f(x) = e(kx)$. Since $f(x+1) = f(x)$ for all x, it follows that $f(\{x\}) = f(x)$ and so the left-hand side of the equation in (3) is equal to the left-hand side in (2). But the right-hand side in (3) is

$$\int_0^1 e(kx)dx = \int_0^1 \cos(2\pi kx) + i\sin(2\pi kx)dx = 0,$$

for $k \neq 0$, and hence (2) follows.

(2) $\Rightarrow$ (3)

As before, we need only concern ourselves with real-valued integrable functions. We proceed by showing that (3) holds for all continuous functions on $[0,1]$, then that it holds for all step functions on $[0,1]$. This is sufficient to prove (3), as shown in the proof that (1) $\Rightarrow$ (3). Clearly (3) holds for the constant function 1, since in this case

$$\lim_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} f(\{u_n\}) = \lim_{N\to\infty} \frac{1}{N} N = 1 = \int_0^1 1.$$

As in the proof that (1) $\Rightarrow$ (3), we also see that (2) implies immediately that (3) holds for the real and imaginary parts of functions f of the form $f(x) = e(kx)$ with k a nonzero integer, hence for all functions $\cos(2\pi kx)$ and $\sin(2\pi kx)$. It follows that (3) holds for all $\mathbb{R}$-linear combinations of such functions and the constant function 1. Hence it holds for all trigonometric polynomials of the form

$$q(x) = a_0 + (a_1 \cos 2\pi x + b_1 \sin 2\pi x) + \cdots + (a_r \cos 2\pi rx + b_r \sin 2\pi rx)$$

for $a_j, b_j \in \mathbb{R}$. Let f be a continuous real-valued function on $[0,1]$ and fix $\varepsilon > 0$. By the Stone-Weierstrass theorem, there exists a trigonometric polynomial q such that $|f - q| < \frac{\varepsilon}{2}$. Taking $f_1 = q - \frac{\varepsilon}{2}$ and $f_1 = q + \frac{\varepsilon}{2}$, we have $f_1 \leq f \leq f_2$ and $\int_0^1 (f_2 - f_1) = \varepsilon$. As before, we conclude that (3) holds for this choice of f. Now, if g is any step function on $[0,1]$, we can find continuous functions g_1, g_2 on $[0,1]$ with $g_1 \leq g \leq g_2$ and $\int_0^1 (g_2 - g_1) < \varepsilon$. We again conclude that (3) holds for g, as desired. □

Applications

One of the most well-known corollaries to Weyl's criterion is the following result.

Corollary. *Let θ be an irrational number. Then the sequence $(n\theta)_{n=1}^{\infty}$ is equidistributed* (mod 1).

Proof. We show that this sequence satisfies the condition (2). Let k be a nonzero integer. Since θ is irrational, $k\theta$ is not an integer and so $1 - e^{2\pi ik\theta}$ is nonzero. Then for each N, we have

$$\begin{aligned} \left| \frac{1}{N}\sum_{n=1}^{N} e(kn\theta) \right| &= \frac{1}{N}\frac{|e(k\theta) - e(k(N+1)\theta)|}{|1 - e(k\theta)|} \\ &\leq \frac{1}{N}\frac{2}{|1 - e(k\theta)|} \end{aligned}$$

and this tends to zero as $N \to \infty$, as desired. □

Weyl generalized the above corollary to the following:

Theorem. *Let $p(n)$ be a polynomial with real coefficients such that some coefficient, other than the constant term, is irrational. Then $(p(n))_{n=1}^{\infty}$ is equidistributed* (mod 1).

To prove this result, Weyl introduced a general procedure for finding upper bounds on exponential sums of the form $S(t) = \sum_{n \leq N} e(tf(n))$ for certain integer-valued functions f. This technique has come to be known as *Weyl differencing.* [2]

Given $\alpha \in \mathbb{R}$, we will give a bound on the sum $\sum_{n=0}^{N} e(n^2\alpha)$ which will, using the second part of Weyl's criterion, show that the sequence $(n^2\alpha)_{n=1}^{\infty}$ is equidistributed (mod 1) in the case that α is irrational. We first require two lemmata. For $x \in \mathbb{R}$, we denote by $\|x\|$ the distance $\min(\{x\}, 1 - \{x\})$ from x to the nearest integer.

Lemma 1. *Let $a < b$ be nonnegative integers, and θ an irrational number. Then*

$$\left| \sum_{n=a}^{b} e(n\theta) \right| \ll \min(b - a, \frac{1}{\|\theta\|}).$$

Proof. This is straightforward computation. The fact that $\sum_{n=a}^{b} e(n\theta) \leq b - a + 1 \ll b - a$ is immediate from the triangle inequality. Now,

$$\begin{aligned} \left| \sum_{n=a}^{b} e(n\theta) \right| &= \frac{|e(a\theta) - e((b+1)\theta)|}{|1 - e(\theta)|} \\ &\leq \frac{2}{|1 - e(\theta)|} \\ &= \frac{2}{|e(\frac{\theta}{2}) - e(\frac{-\theta}{2})|} \\ &= \frac{1}{|\sin(\pi\theta)|}. \end{aligned}$$

It is easy to see (from their graphs, for example) that $|\sin(\pi x)| \geq 2\|x\|$ for all x, and the result follows. □

Lemma 2. *Let α be an irrational number, and suppose that $|\alpha - \frac{a}{q}| \leq \frac{1}{q^2}$ with $(a, q) = 1$ and $q \geq 2$. Then for $N \geq 1$, we have*

$$\left| \sum_{n=0}^{N} e(n^2\alpha) \right| \ll \frac{N}{\sqrt{q}} + \sqrt{(q + N)\log q}.$$

From this second lemma we can show that if α is irrational, then $(n^2\alpha)_{n=1}^{\infty}$ is equidistributed (mod 1): given such α and q, we have

$$\left| \frac{1}{N} \sum_{n=1}^{N} e(n^2\alpha) \right| \ll \frac{1}{\sqrt{q}} + \sqrt{\frac{q \log q}{N^2} + \frac{\log q}{N}} \overset{N \to \infty}{\longrightarrow} \frac{1}{\sqrt{q}}$$

and since by Dirichlet's theorem we can take q to be arbitrarily large, we conclude that the sequence $(n^2\alpha)_{n=1}^{\infty}$ satisfies condition (2) of Weyl's criterion. As for the lemma itself:

Proof. Let S denote the sum in question. Then

$$|S|^2 = \sum_{n_1=0}^{N} \sum_{n_2=0}^{N} e(\alpha(n_1^2 - n_2^2)).$$

[2] Furstenberg later proved the result using ergodic-theoretic techniques.

We re-index this sum by setting $h = n_1 - n_2$ so that $-N \le h \le N$ and, for each such h, we have $\max(0, -h) \le n_2 = n_1 - h \le \min(N, N-h)$. The sum can then be written as

$$|S|^2 = \sum_{h=-N}^{N} \sum_{n_2=\max(-h,0)}^{\min(N,N-h)} e(\alpha(2hn_2 + h^2)) = \sum_{h=-N}^{N} e(\alpha h^2) \sum_{n_2=\max(-h,0)}^{\min(N,N-h)} e(\alpha(2hn_2)).$$

(The limits of n_2 in this second sum are $0 \le n_2 \le N$ when $h \le 0$ and $-h \le n_2 \le N - h$ when $h > 0$.) Observe that we have reduced the quadratic polynomial $n_1^2 - n_2^2$ to a polynomial $2hn_2 + h^2$ which is linear in n_2, and this sum is easier to work with. This is an example of Weyl differencing. Now, using the triangle inequality and Lemma 1, we deduce that

$$|S|^2 \ll \sum_{h=-N}^{N} \min(N, \frac{1}{\|2h\alpha\|}).$$

Divide $[-N, N]$ into intervals of length at most $\frac{q}{2}$, each of the form $M \le h < M + \frac{q}{2}$. We claim that the sum of $\min(N, \frac{1}{\|2h\alpha\|})$ over each such interval is $\ll N + q \log q$:
We first assume that $M = 0$. Write $S' = \sum_{0 \le h < q/2} \min(N, \frac{1}{\|2h\alpha\|})$, and write $\alpha = \frac{a}{q} + \theta$ with $|\theta| \le \frac{1}{q^2}$. Since $0 \le 2h < q$, the residues of $2h$ (mod q) are distinct, and hence so are the residues of $2ha$ (mod q) since $(a, q) = 1$. Thus $2ha$ is congruent to each of 0,1,-1 (mod q) at most once, and the total contribution to S' in these cases is therefore at most $3N$. For other values of h, observe that

$$\|2h\alpha\| = \left\| \frac{2ha}{q} + 2h\theta \right\| \ge \left\| \frac{2ha}{q} \right\| - \frac{2h}{q^2} > \left\| \frac{2ha}{q} \right\| - \frac{1}{q} > 0.$$

We thus have

$$S' \le 3N + \sum_{\substack{0 \le h < q/2 \\ 2ah \not\equiv 0,1,-1 (mod q)}} \min\left(N, \frac{1}{\left\|\frac{2ha}{q}\right\| - \frac{1}{q}}\right).$$

In the right-hand side of the above inequality, $\left\|\frac{2ha}{q}\right\|$ takes on each of the values $\frac{2}{q}, \ldots, \frac{\lfloor q/2 \rfloor}{q}$ at most twice. Then

$$S' \le 3N + 2 \sum_{j=2}^{\lfloor q/2 \rfloor} \frac{1}{\frac{j}{q} - \frac{1}{q}} = 3N + 2q \sum_{j=1}^{\lfloor q/2 \rfloor - 1} \frac{1}{j} \ll N + q \log q$$

as desired. The case where $M \le h < M + \frac{q}{2}$ for other values of M is similar.
Now, there are clearly $\ll \frac{N}{q} + 1$ of these intervals. It follows that

$$|S|^2 \ll (N + q \log q)(\frac{N}{q} + 1) = \frac{N^2}{q} + N + (q + N) \log q \ll \frac{N^2}{q} + (q + N) \log q.$$

The result follows since $\sqrt{\frac{N^2}{q} + (q + N) \log q} \le \frac{N}{\sqrt{q}} + \sqrt{(q + N) \log q}$. $\square$

We have shown that, for irrational α, $\left(n^2\alpha\right)_{n=1}^{\infty}$ is equidistributed (mod 1). It follows that this sequence is dense in $[0, 1]$, and so for any $\varepsilon > 0$ we can find n with $\|n^2\alpha\| < \varepsilon$. In fact, we can use these results to give a lower bound for an n that satisfies this inequality.

Lemma 3. *Given $M \ge 1$ and $\frac{a}{q}$ with $(a, q) = 1$, there exists $m \le M$ with* $\left\|\frac{am^2}{q}\right\| \ll \frac{\sqrt{q}(\log q)^{\frac{3}{2}}}{M}$.

Proof. If $M > q$ then we can simply take $m = q$, since then $\left\|\frac{am^2}{q}\right\| = 0$. Then assume $M \le q$. We want to minimize $\left\|\frac{am^2}{q}\right\|$, and hence we want to find solutions in m to $am^2 \equiv b \pmod q$ with $|b|$ small. Given b and m, observe that the expression

$$\frac{1}{q}\sum_{r(\text{mod} q)} e\left(\frac{(am^2-b)r}{q}\right)$$

is equal to 1 if $am^2 \equiv b(\text{mod } q)$, and 0 otherwise. Then for a given upper bound L on $|b|$,

$$\varphi(L) := \frac{1}{q}\sum_{|b|\le L}\sum_{r(\text{mod } q)}\sum_{m\le M} e\left(\frac{(am^2-b)r}{q}\right)$$

counts the number of solutions to $am^2 \equiv b(\text{mod } q)$ with $|b| \le L$ and $m \le M$. Our objective is thus to find a lower bound for L subject to the constraint that $\varphi(L) > 0$. The contribution to $\varphi(L)$ from $r = 0$ is clearly $\frac{(2L+1)M}{q}$. For $r \neq 0$, the contribution to $\varphi(L)$ is

$$\begin{aligned}\frac{1}{q}\sum_{|b|\le L}\sum_{m\le M} e\left(\frac{(am^2-b)r}{q}\right) &= \frac{1}{q}\sum_{|b|\le L} e\left(\frac{-br}{q}\right)\sum_{m\le M} e\left(\frac{am^2r}{q}\right)\\ &\ll \frac{1}{q}\sum_{|b|\le L} e\left(\frac{-br}{q}\right)\left(\frac{M}{\sqrt{q}}+\sqrt{(q+M)\log q}\right)\end{aligned}$$

by Lemma 2. From Lemma 1, we have $\sum_{|b|\le L} e\left(\frac{-br}{q}\right) \ll \min\left(L, \frac{1}{\left\|\frac{r}{q}\right\|}\right)$, and since $M \le q$ we have $\frac{M}{\sqrt{q}} + \sqrt{(q+M)\log q} \ll \sqrt{q} + \sqrt{2q\log q} \ll \sqrt{q\log q}$. Summing over all r, we thus have

$$\begin{aligned}\varphi(L) - \frac{(2L+1)M}{q} &\ll \frac{1}{q}\sqrt{q\log q}\sum_{r=1}^{q-1}\min\left(L, \frac{1}{\left\|\frac{r}{q}\right\|}\right)\\ &\ll \frac{1}{q}\sqrt{q\log q}(q\log q) = \sqrt{q}(\log q)^{\frac{3}{2}}\end{aligned}$$

i.e. $\varphi(L) = \frac{(2L+1)M}{q} + O(\sqrt{q}(\log q)^{\frac{3}{2}})$. Hence if $L \gg \frac{q\sqrt{q}(\log q)^{\frac{3}{2}}}{M}$ we are guaranteed solutions, as required. □

Corollary. *Let α be a real number. For every $M \ge 1$ there exists $m \le M$ with $\|m^2\alpha\| \ll \frac{\log M}{M^{\frac{1}{3}}}$.*

Proof. Let $Q \ge 1$ be a parameter. By Dirichlet's theorem, we can find $\frac{a}{q}$ with $q \le Q, (a, q) = 1$, and $\left|\alpha - \frac{a}{q}\right| \le \frac{1}{qQ}$. If $q \le M$, then take $m = q$ so that $|m^2\alpha - qa| \le \frac{q}{Q} \le MQ$ and hence $\|m^2\alpha\| \le \frac{M}{Q}$. Now suppose $q > M$. By Lemma 3, there exists $m \le M$ with $\left\|m^2\frac{a}{q}\right\| \ll \frac{\sqrt{q}(\log q)^{\frac{3}{2}}}{M}$. Since $|m^2\alpha - m^2\frac{a}{q}| \le \frac{m^2}{qQ}$, we have $|\|m^2\alpha\| - \|m^2\frac{a}{q}\|| \le \frac{m^2}{qQ}$ and so

$$\|m^2\alpha\| \le \left\|m^2\frac{a}{q}\right\| + \frac{m^2}{qQ} \ll \frac{\sqrt{q}(\log q)^{\frac{3}{2}}}{M} + \frac{M^2}{qQ} \ll \frac{\sqrt{Q}(\log Q)^{\frac{3}{2}}}{M} + \frac{M}{Q}.$$

Thus, in either case, we can achieve the bound $\|m^2\alpha\| \ll \frac{\sqrt{Q}(\log Q)^{\frac{3}{2}}}{M} + \frac{M}{Q}$. Take $Q = \frac{M^{\frac{4}{3}}}{\log M}$, so that

$$\begin{aligned} \|m^2\alpha\| &\ll \frac{1}{M^{\frac{1}{3}}\sqrt{\log M}}\left(\log \frac{M^{\frac{4}{3}}}{\log M}\right) + \frac{\log M}{M^{\frac{1}{3}}} \\ &= \frac{1}{M^{\frac{1}{3}}}\left(\frac{\frac{4}{3}\log M - \log\log M}{\sqrt{\log M}} + \log M\right) \\ &\ll \frac{\log M}{M^{\frac{1}{3}}} \end{aligned}$$

as required. □

This corollary shall be used later as part of a density increment argument to prove Gowers's Theorem for the case $k = 4$:

Theorem (Gowers's Theorem). *There exists a positive constant c_k such that any subset A in $[1, N]$ with $|A| \gg \frac{N}{(\log\log N)^{c_k}}$ contains a non-trivial $k-$term artihmetic progression.*

References

[1] K. Chandrasekharan, *Introduction to Analytic Number Theory*. Springer-Verlag, 1968.

[2] K. Soundararajan, *Additive Combinatorics: Winter 2007*. Stanford University, 2007.

[3] S. Hartman, Remarks on equidistribution in non-compact groups. *Compositio Mathematica* (tome 16, p. 66-71), 1964.