NORMAL NUMBERS AND UNIFORM DISTRIBUTION (WEEKS 1-3) OPEN PROBLEMS IN NUMBER THEORY SPRING 2018, TEL AVIV UNIVERSITY

ZEÉV RUDNICK

Contents

0.1. Normal numbers.

Definition. *A real number* $\alpha \in (0,1)$ *is* simply normal *(to base* 10*), if in the decimal expansion*

$$\alpha = 0.a_1a_2\dots,$$

each digit occurs with the same frequency (namely $1/10$*): For any digit* $t \in \{0,1,\dots,,9\}$,

$$\lim_{N\to\infty} \frac{1}{N} \# \{n \le N : a_n = t\} = \frac{1}{10}$$

We say that α is *normal* to base 10 if for every $k \geq 1$, every string $t_1 \dots t_k$ of k digits $t_j \in \{0,1,\dots,9\}$ appears with the same frequency, namely $1/10^k$:

$$\lim_{N\to\infty} \frac{1}{N} \# \{n \le N : a_{n+1} = t_1, a_{n+2} = t_2, \dots, a_{n+k} = t_k\} = \frac{1}{10^k}$$

Date: March 25, 2018.

We can naturally change base 10 to any other base $b \geq 2$, with the same definitions.

Exercise 1. *Show that a rational number is not normal (to any base).*

The natural questions are: Is there a normal number?

0.2. Un-natural examples.

- Champernowne's number (1933, [1]): Concatenate all *natural numbers* into a decimal expansion
$$0.1234567891011121314\dots$$
- Copeland Erdős number (1946 [2], conjectured by Champernowne): Concatenate all *primes* into a decimal expansion.
$$0.23571113172329\dots$$
- Davenport and Erdős (1952 [3], conjectured by Copeland and Erdős): Let $f(x)$ be any polynomial in x, all of whose values for $x = 1, 2, \dots$ are positive integers. Then the decimal $0.f(1)f(2)f(3)\dots$, where $f(n)$ is written in the scale of 10, is normal (in base 10).

Open Problem 1. *Find a single example of a "naturally occurring" number which is normal (to some base). For instance, is the golden ration $\varphi = (1+\sqrt{5})/2$ normal?*

It is conjectured that any real algebraic number is normal to all bases.

0.3. Normality and uniform distribution.

Let $\mathcal{X} = \{x_n\} \subset \mathbb{R}/\mathbb{Z} \simeq [0,1)$ be a sequence of numbers on the unit circle. We say that $\mathcal{X}$ is *uniformly distributed* (mod 1) if for every subinterval $I \subset [0,1)$, the proportion of elements of $\mathcal{X}$ contained in I equals the length of I:

$$\lim_{N\to\infty} \frac{1}{N} \# \{n \leq N : x_n \in I\} = |I|.$$

Likewise, if we take a sequence x_n of real numbers, we use the fractional parts $\{x \mod 1\}$.

Note that a uniformly distributed sequence $\mathcal{X} \subset [0,1)$ is necessarily *dense*. The converse is not true: A standard example is the sequence of fractional parts $\{\log n : n = 1, \dots\}$

Exercise 2. *Show that the sequence of fractional parts* $\{\{\log n\} : n = 1, 2, \dots\}$ *is* dense *in* $[0,1)$.

As we shall later see, if $\alpha \in \mathbb{R}\backslash\mathbb{Q}$ is irrational, then the sequence $\{\alpha n : n = 1, 2, \dots\}$ is uniformly distributed mod 1.

The relation to our previous discussion of normal numbers lies in the following observation:

Proposition 0.1. *α is normal to base 10 (resp., base b) if and only if the sequence $\{\alpha 10^n : n = 1, 2, \dots\}$ is uniformly distributed modulo 1 (resp. αb^n).*

Proof. It suffices to consider intervals $I = [a, b)$ with endpoints being finite decimals, i.e. of the form $a = 0.a_1 \dots .a_r$, in fact when we only change the last digit (exercise: why?). For simplicity, take $I = [0.123, 0, 124)$. Now note that if $\alpha = 0.a_1 a_2 \dots$, then the fractional part of $10^n\alpha = 0.a_{n+1}a_{n+2}a_{n+3}\dots$, so that

$$\{10^n\alpha\} \in I = [0.123, 0, 124) \qquad \Leftrightarrow \qquad a_{n+1} = 1,\ a_{n+2} = 2,\ a_{n+3} = 3.$$

Thus the number of $n \le N$ for which the fractional parts $\{\alpha 10^n\} \in I$ is exactly equal to the number of occurrences of the string "123" in the first $N + 3$ digits of α. Normality of α means that this number is asymptotically $N/10^3$. Noting that the length of our interval I is $1/10^3$, we see that we get the number of $n \le N$ such that $\{10^n\alpha\} \in I$ is asymptotically $N|I|$, which is what is required in the definition of uniform distribution. □

This observation shifts the focus from normality to the general context of uniform distribution of sequences. So far we have not proved that any sequence is uniformly distributed. Before doing so, we develop Weyl's breakthrough method for establishing this.

0.4. **Weyl's criterion (1916).**

Theorem 0.2. *Let $\mathcal{X} = \{x_n : n = 1, 2, \dots\} \subset \mathbb{R}$. Then $\mathcal{X}$ is uniformly distributed modulo 1 if and only if for all integers $k \neq 0$,*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} e^{2\pi i k x_n} = 0.$$

In what follows, we shall abbreviate

$$e(z) := e^{2\pi i z}$$

Example: We shall show that for any irrational α, the fractional parts of αn are u.d.: By Weyl's criterion, it suffices to show cancellation in the "Weyl sums" $\sum_{n=1}^{N} e^{2\pi i k \alpha n}$. But for this sequence, these are just geometric progressions, so as long as $k\alpha \notin \mathbb{Z}$ (which is guaranteed by irrationality of α if $k \neq 0$), so that

$$\sum_{n=1}^{N} e^{2\pi i k\alpha n} = \frac{e\left((N+1)k\alpha\right) - e(k\alpha)}{1 - e(k\alpha)}.$$

Hence

$$\left|\frac{1}{N}\sum_{n=1}^{N} e^{2\pi i k\alpha n}\right| \leq \frac{1}{N}\frac{2}{|1-e(k\alpha)|} \to 0, \quad \text{as} \quad N \to \infty,$$

so that Weyl's criterion is satisfied. □

Example: The sequence of fractional parts of $\log n$ is not uniformly distributed mod 1 (earlier we saw that it is *dense* mod 1). To see this, we need to see that Weyl's criterion does not hold. We will show that

$$\frac{1}{N}\sum_{n\leq N} e(\log n) \not\to 0$$

Indeed, we use summation by parts to evaluate the Weyl sum. Recall that for a differentiable function $f(t)$, and any sequence $\{a_n\}$, we denote by

$$A(t) := \sum_{n\leq t} a_n$$

the partial sums of the sequence, then the weighted sum $\sum_n a_n f(n)$ can be written as

$$\sum_{1\leq n\leq x} a_n f(n) = A(x)f(x) - \int_1^x A(t)f'(t)dt$$

and more generally, if $z < x$ then

$$\sum_{z<n\leq x} a_n f(n) = A(x)f(x) - A(z)f(z) - \int_z^x A(t)f'(t)dt$$

Exercise 3. *Using summation by parts, show that*

$$\sum_{n\leq x} \log n = x\log x - x + O(\log x)$$

$$\sum_{n=1}^{N} \frac{1}{n} = \log N + C - O(\frac{1}{N})$$

for some constant C.

We apply this with $f(t) = e^{2\pi i \log t} = t^{2\pi i}$, and $a_n = 1$, so that $A(t) = \lfloor t \rfloor$ to obtain

$$\begin{aligned} \sum_{1 \le n \le N} e(\log n) &= \lfloor N \rfloor N^{2\pi i} - \int_1^N \lfloor t \rfloor 2\pi i t^{2\pi i - 1} dt \\ &= N^{1+2\pi i} - 2\pi i \int_1^N t^{2\pi i} dt + 2\pi i \int_1^N t^{2\pi i - 1}\{t\} dt \\ &= N^{1+2\pi i} - 2\pi i \frac{N^{1+2\pi i}}{1+2\pi i} + O\left(\int_1^N t^{-1} dt \right) \\ &= \frac{N^{1+2\pi i}}{1+2\pi i} + O\left(\log N\right), \end{aligned}$$

which is clearly not $o(N)$.

0.5. **Proof of Weyl's criterion.** The argument is all about approximating various functions by step functions and by trigonometric polynomials. For a periodic function f, we ask whether the following holds

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

Lemma 0.3. *Let $\mathcal{X} \subset \mathbb{R}/\mathbb{Z}$. The following are equivalent:*

(1) *The sequence $\mathcal{X}$ is uniformly distributed.*
(2) (*) *holds for all continuous f.*
(3) (*) *holds for all Riemann integrable f.*

Proof. Clearly (3) implies (1). For the converse, note that (1) (uniform distribution) implies that (*) holds for all step functions, that is linear combinations of the indicator functions of intervals. But for any Riemann integrable function, by definition, given any $\varepsilon > 0$, there are step functions $s_- \le f \le s_+$ with $\int_0^1 (s_+ - s_-) < \varepsilon$. Choose $N(\varepsilon) > 0$ so that for all $N \ge N(\varepsilon)$,

$$\left| \frac{1}{N} \sum_{n=1}^{N} s_+(x_n) - \int_0^1 s_+(x) dx \right| < \varepsilon \tag{0.1}$$

and then

$$\frac{1}{N}\sum_{n=1}^{N} f(x_n) - \int_0^1 f(x)dx = \frac{1}{N}\sum_{n=1}^{N} \left(f(x_n) - s_+(x_n)\right) + \frac{1}{N}\sum_{n=1}^{N} s_+(x_n) - \int_0^1 s_+(x)dx + \int_0^1 s_+(x)dx - \int_0^1 f(x)dx$$

Now the first expression is non-positive, since $f \leq s_+$, so that the LHS is bounded above by the sum of the last two expressions. By (0.1), the second expression lies in $(-\varepsilon, \varepsilon)$, and since $\int_0^1 (s_+ - s_-) < \varepsilon$, the third expression is in $[0, \varepsilon)$. Hence

$$\frac{1}{N}\sum_{n=1}^{N} f(x_n) - \int_0^1 f(x)dx < 2\varepsilon.$$

Arguing with s_+ replaced by s_- will give

$$\frac{1}{N}\sum_{n=1}^{N} f(x_n) - \int_0^1 f(x)dx > -2\varepsilon.$$

and hence

$$\left|\frac{1}{N}\sum_{n=1}^{N} f(x_n) - \int_0^1 f(x)dx\right| < 2\varepsilon.$$

for all $N \geq N(\varepsilon)$. Hence (3) holds.

Since continuous functions are Riemann integrable, we have (3) $\Rightarrow$ (2).

For the implication (2) $\Rightarrow$ (1), argue similarly, approximating the indicator function of an interval above and below by continuous functions. □

Proof of Weyl's criterion: Since the exponential functions $e_k(x) = e(ks)$ are continuous, by the above Lemma uniform distribution implies that (*) holds for them, that is one direction follows. We need to show that assuming that (*) for $f(x) = e(kx)$, for all $k \neq 0$ ($k = 0$ is obvious), implies uniform distribution, and by the Lemma, it suffices to show (*) holds for continuous functions.

Note that (*) for all $e(kx)$ for all integer k implies (*) holds for all trigonometric polynomials, by linearity. By the Weierstrass approximation theorem, given a continuous function f, for any $\varepsilon > 0$ there is a trigonometric polynomial $T(x)$ so that $||f - T||_\infty < \varepsilon$. One then argues as in the Lemma that

$$\begin{aligned}\left|\frac{1}{N}\sum_{n=1}^{N} f(x_n) - \int_0^1 f(x)dx\right| &\leq \left|\frac{1}{N}\sum_{n=1}^{N}\Big(f(x_n) - T(x_n)\Big)\right| \\ &+ \left|\frac{1}{N}\sum_{n=1}^{N} T(x_n) - \int_0^1 T(x)dx\right| \\ &+ \int_0^1 \Big|T(x) - f(x)\Big| dx\end{aligned}$$

The first and third expressions are at most ε, since $||f - T||_\infty < \varepsilon$, and the second expression is at most ε for all $N \geq N(\varepsilon)$. Thus we have uniform distribution. □

0.6. **Polynomial sequences.** Weyl's criterion allows one to get a first step up on a number of problems. As an example, we present one of Weyl's original breakthroughs, namely that the sequence αn^2 is uniformly distributed mod 1 for α irrational. However, unlike the linear case αn, this does not come for free, and needed some significant extra ideas. We start with Dirichlet's theorem on rational approximations.

Lemma 0.4. *Let $x \in \mathbb{R}$ be a real number. Then for any integer $Q \geq 1$, there are integers $a \in \mathbb{Z}$, $q \geq 1$, with $q \leq Q$ so that*

$$\left|x - \frac{a}{q}\right| < \frac{1}{qQ}$$

In particular for the fractional part $\{qx\}$ we get $0 \leq \{qx\} < 1/Q$.

If x is irrational, then we must have $q \to \infty$ as $Q \to \infty$.

Proof. We consider the $Q + 1$ numbers $\{nx\} \in [0, 1)$, $0 \leq n \leq Q$. Dividing the unit interval $[0, 1)$ into Q subintervals of length $1/Q$, we use Dirichlet's box principle to deduce that at least one of these subintervals contains two points of the sequence, that is there are $0 \leq m \neq n \leq Q$ so that

$$0 \leq \{nx\} - \{mx\} < \frac{1}{Q}$$

Writing $\{mx\} = mx - M$, $\{nx\} = nx - N$ with $M, N \in \mathbb{Z}$ we obtain

$$0 \leq nx - N - (mx - M) = (n - m)x - (N - M) < \frac{1}{Q}$$

Taking $q = |n - m| \in [1, Q]$ and $a = \pm(N - M)$ we obtain

$$|qx - a| < \frac{1}{Q}$$

as claimed.

Now if $x \notin \mathbb{Q}$ is irrational, then $\{qx\} \neq 0$ and hence we cannot have $0 \le \{qx\} < 1/Q$ for infinitely many Q's. Hence $q \to \infty$ as $Q \to \infty$. □

Theorem 0.5. *For irrational α, the sequence $\{\alpha n^2 : n = 1, 2 \dots\}$ is uniformly distributed modulo 1.*

By Weyl's criterion, it suffices to show that for any nonzero integer k, the "Weyl sums"

$$S(N) := \sum_{n=1}^{N} e(k\alpha n^2) = o_{k,\alpha}(N)$$

(the implied constants are allowed to depend on α and k).

We square out the sum

$$|S(N)|^2 = N + 2\Re \sum_{1 \le m < n \le N} e(k\alpha(n^2 - m^2))$$

Writing $n = m + h$, with $1 \le m + h \le N$, so that

$$n^2 - m^2 = h(2m + h) = h^2 + 2hm,$$

we obtain

$$\Big| \sum_{1 \le m < n \le N} e(k\alpha(n^2 - m^2)) \Big| = \Big| \sum_{h=1}^{N-1} e(k\alpha h^2) \sum_{m=1}^{N-h} e(\alpha \cdot 2k \cdot h \cdot m) \Big|$$
$$\le \sum_{h=1}^{N-1} \Big| \sum_{m=1}^{N-h} e(\gamma \cdot h \cdot m) \Big|$$

where we have set $\gamma := 2k\alpha$, which is irrational if and only if α is irrational.

Now we sum the geometric progression, which is the inner sum:

$$\Big| \sum_{m=1}^{N-h} e(\gamma \cdot h \cdot m) \Big| = \begin{cases} N - h, & h \cdot \gamma \in \mathbb{Z} \\ \Big| \frac{e(h\gamma) - e(h\gamma(N-h+1))}{1 - e(h\gamma)} \Big| \le \frac{2}{2|\sin(\pi h\gamma)|}, & \text{else} \end{cases}$$
$$\ll \min\Big(N, \frac{1}{||h\gamma||}\Big)$$

where $||x|| := \mathrm{dist}(x, \mathbb{Z})$. Thus we obtain

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

Hence it suffices to show that

Proposition 0.6. *For $\gamma \notin \mathbb{Q}$,*

$$\sum_{h=1}^{N} \min\Big(N, \frac{1}{||h\gamma||}\Big) = o(N^2)$$

Proof. We use Dirichlet's lemma to obtain coprime a, q, with $1 \le q \le N$ so that

$$|\gamma - \frac{a}{q}| < \frac{1}{qN} \quad \text{or} \quad \gamma = \frac{a}{q} + \frac{\theta}{qN}, \quad |\theta| < 1.$$

Divide the range of summation $[1, N]$ into consecutive intervals of length q, plus perhaps an extra leftover interval. So if $(M-1)q < N \le Mq$ then writing $h = qk + j$, $0 \le k < M$, $j = 0, \dots, q-1$, we have

$$||\gamma h|| = ||\frac{ah}{q} + \frac{\theta h}{qN}|| = ||\frac{aj}{q} + ak + \frac{\theta h}{qN}|| = ||\frac{aj}{q} + \frac{\tilde{\theta}}{q}||$$

where $|\tilde{\theta}| < 1$. Thus

$$\begin{aligned} \sum_{h=1}^{N} \min\Big(N, \frac{1}{||h\gamma||}\Big) &\le M \max_{|\tilde{\theta}|<1} \sum_{j=0}^{q-1} \min\Big(N, \frac{1}{||\frac{aj}{q} + \frac{\tilde{\theta}}{q}||}\Big) \\ &\ll \frac{N}{q} \max_{|\tilde{\theta}|<1} \sum_{i=0}^{q-1} \min\Big(N, \frac{1}{||\frac{i}{q} + \frac{\tilde{\theta}}{q}||}\Big) \end{aligned}$$

where we have changed variables $aj \bmod q \to i \bmod q$, as we may since a is coprime to q, so that as we vary over all residues $j \bmod q$, the set $aj \bmod q$ varies over all residues $i \bmod q$ (recall $||\frac{aj}{q} + z||$ only depends on $aj \bmod q$).

For at most one value of $i \bmod q$, we have

$$||\frac{i}{q} + \frac{\tilde{\theta}}{q}|| < \frac{1}{2q}$$

and for that value we replace the corresponding term in the sum by N. For the remaining i's, we have

$$||\frac{i}{q} + \frac{\tilde{\theta}}{q}|| \ge \frac{i}{2q}$$

Hence we find

$$\max_{|\tilde{\theta}|<1} \sum_{i=0}^{q-1} \min\Big(N, \frac{1}{||\frac{i}{q} + \frac{\tilde{\theta}}{q}||}\Big) \ll N + \sum_{i=1}^{q} \frac{1}{q/i} \ll N + q\log q$$

Therefore

$$\sum_{h=1}^{N} \min\Big(N, \frac{1}{||h\gamma||}\Big) \ll \frac{N}{q}\Big(N + q\log q) \ll \frac{N^2}{q} + N\log N$$

Recall that since γ is irrational, we have $q \to \infty$ as $N \to \infty$, and hence the above is $o(N^2)$. □

An elaboration of the above argument gives

Theorem 0.7. *Let $P(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$ be a polynomial of degree $d \geq 2$, with at least one of the ceofficients $a_d, \dots, a_1$ irrational (the constant term a_0 does not matter). Then the sequence $\{P(n) : n = 1, 2, \dots\}$ is uniformly distributed mod 1.*

0.7. **Metric Theory.**

Theorem 0.8. *Let $\{a(n)\}$ be a sequence of* distinct *integers: $a(n) \neq a(m)$ if $n \neq m$. Then for* almost all *$\alpha \in \mathbb{R}$, the sequence $\{\alpha a(n)\}$ is uniformly distributed mod 1.*

Note that the proof does not provide a single example of such an α.

As an example, we may take $a(n) = 10^n$, and find that almost all α are normal to base 10. Likewise, given any integer $b \geq 2$, almost all α are normal to base b. Intersection this union of subsets having full measure shows that in fact almost all α are normal to any case b.

Proof. By Weyl's criterion, it suffices to show that for almost all α, and any integer $k \neq 0$, the normalized Weyl sums

$$S_k^*(\alpha; N) := \frac{1}{N}\sum_{n=1}^{N} e(k\alpha a(n))$$

tend to zero. In fact it suffices to show that given $k \neq 0$, this holds for almost all α (apriori depending on k). Replacing $a(n)$ by $ka(n)$, it suffices to take $k = 1$, and we write $S^*(\alpha; N) = S_1^*(\alpha; N)$. We may also restrict to $\alpha \in [0, 1)$ by periodicity.

From now on we take $N = M^2$, and first show that for almost all α, $S^*(\alpha; M^2) \to 0$. Now one way to show this is to show that for almost all α, the series

$$\sum_{M=1}^{\infty} |S^*(\alpha; M^2)|^2 < \infty$$

converges, since this forces the individual terms of the series to tend to zero.

Next, note that by what we learnt in measure theory about the Lebesgue integral, it suffices to show that

$$\int_0^1 \left(\sum_{M=1}^{\infty} |S^*(\alpha; M^2)|^2 \right) d\alpha < \infty$$

since for a function to be integrable, a necessary condition is that it is finite almost everywhere.

By Fatou's Lemma,

$$\int_0^1 \left(\sum_{M=1}^{\infty} |S^*(\alpha; M^2)|^2 \right) d\alpha \leq \sum_{M=1}^{\infty} \int_0^1 |S^*(\alpha; M^2)|^2 d\alpha$$

so it suffices to show that the sum of the integrals converges. But squaring out the Weyl sum gives

$$\begin{aligned} \int_0^1 |S^*(\alpha; M^2)|^2 d\alpha &= \frac{1}{M^4} \sum_{m=1}^{M^2} \sum_{n=1}^{M^2} \int_0^1 e\left(\alpha(a(m) - a(n))\right) d\alpha \\ &= \frac{1}{M^4} \sum_{m=1}^{M^2} \sum_{n=1}^{M^2} \delta\left(a(m), a(n)\right) \end{aligned}$$

since the $a(n)$'s are integers. Now (and only now!) we use the assumption that $a(n)$ are distinct, to deduce that only the diagonal terms survive, giving

$$\int_0^1 |S^*(\alpha; M^2)|^2 d\alpha = \frac{1}{M^4} \sum_{m=1}^{M^2} 1 = \frac{1}{M^2}$$

and so we deduce that

$$\int_0^1 \left(\sum_{M=1}^{\infty} |S^*(\alpha; M^2)|^2 \right) d\alpha < \infty$$

so that for almost all α,

$$S^*(\alpha, M^2) \to 0.$$

Finally, we move from M^2 to general N: Given N, we can find M so that $M^2 \leq N < (M+1)^2$, and then we claim that

$$S^*(\alpha, N) = S^*(\alpha, M^2) + O(\frac{1}{\sqrt{N}})$$

and hence will deduce that for almost all α, $S(\alpha, N) \to 0$.

Indeed (assuming $N \neq M^2$),

$$S^*(\alpha,N)-S^*(\alpha,M^2) = \frac{1}{N}\sum_{n=M^2+1}^{N} e(\alpha a(n)) - \left(\frac{1}{M^2}-\frac{1}{N}\right)\sum_{n=1}^{M^2} e(\alpha a(n))$$

so that

$$\begin{aligned}\left|S^*(\alpha,N)-S^*(\alpha,M^2)\right| &\le \frac{1}{N}(N-M^2)+\left(\frac{1}{M^2}-\frac{1}{N}\right)M^2 \\ &\qquad \text{on trivially bounding} \quad |e(x)|\le 1 \\ &\le 2\frac{N-M^2}{N} \ll \frac{1}{\sqrt{N}}\end{aligned}$$

as claimed. □

0.8. **Quantitative aspects of uniform distribution: Discrepancy.** If a sequence $\mathcal{X}$ is uniformly distributed mod 1, it is in particular dense in the unit interval. This means that every subinterval of *fixed* length contains at least one point of the sequence, in fact the proportion of points falling into it is roughly the length of the interval. The next question is: What about *shrinking* intervals? That is, we ask that every interval of length at least $1/m(N)$ contains at least one element from the first N elements of the sequence $\{\{x_n\} : n \le N\}$, where $m(N) \to 0$ as $N \to \infty$.

Definition. *The discrepancy of the sequence* $\mathcal{X}$ *is*

$$D(N) = \sup_{I\subseteq[0,1)} \left|\frac{1}{N}\#\{n \le N : x_n \in I\} - |I|\right|$$

Clearly if $D(N) \to 0$ then $\mathcal{X}$ is uniformly distributed; the converse also holds.

Exercise 4. *Show that* $1/N \le D(N) \le 1$.

Recall that Weyl's criterion is that $\mathcal{X}$ is uniformly distributed if and only if all the normalized Weyl sums

$$S^*(k,N) := \frac{1}{N}\sum_{n\le N} e(kx_n)$$

tend to zero ($k \neq 0$). What is important is that we can use Weyl sums to estimate the discrepancy $D(N)$.

Theorem 0.9 (Erdős-Turan)**.** *For any* $K \ge 1$ *and* $N \ge 1$,

$$D(N) \le \frac{1}{K+1} + 3\sum_{k=1}^{K}\frac{1}{k}|S^*(k,N)|.$$

0.8.1. *Example: The linear case* $x_n = \alpha n \bmod 1$. We want to use the Erdős-Turan inequality. We use the bound for the geometric series (for irrational α)

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

and so by the Erdős-Turan inequality,

$$D(N) \ll \frac{1}{K} + \sum_{k=1}^{K}\frac{1}{k}|S^*(k,N)| \ll \frac{1}{K} + \frac{1}{N}\sum_{k=1}^{K}\frac{1}{k||k\alpha||}$$

so we need to estimate the sum $\sum_{k=1}^{K}\frac{1}{k||k\alpha||}$. Here the Diophantine type of α plays a special role. We say that α is *of bounded type*, or *badly approximable* if there is some constant $c = c(\alpha) > 0$ so that

$$||q\alpha|| > \frac{c}{q}.$$

This is a measure zero condition, and is equivalent to the continued fraction expansion of α to have bounded partial quotients: $\alpha = [a_0; a_1, a_2, \dots]$, with $1 \le a_k \le M$. The main example are quadratic irrationalities:

Lemma 0.10. *Let* $\alpha = \sqrt{D}$, $D \neq \square > 1$ *an integer which is not a perfect square. Then for any integers* p, $q \ge 1$

$$|\frac{p}{q} - \sqrt{D}| > \frac{c}{q^2}, \qquad c = 1/(3\sqrt{D})$$

Proof. We may assume that $|p/q - \sqrt{D}| < 1/10$, otherwise there is nothing to prove. Let $f(x) = x^2 - D$ (which is the minimal polynomial of $\sqrt{D}$). Then

$$|\frac{p}{q} - \sqrt{D}| = \frac{|f(\frac{p}{q})|}{\frac{p}{q} + \sqrt{D}} > \frac{|f(p/q)|}{3\sqrt{D}}$$

since $0 < p/q + \sqrt{D} = 2\sqrt{D} + (p/q - \sqrt{D}) < 2\sqrt{D} + 1/10 < 3\sqrt{D}$. Moreover,

$$|f(p/q)| = \frac{|p^2 - Dq^2|}{q^2} \ge \frac{1}{q^2}$$

because $p^2 - Dq^2$ is an integer, which is not zero because $\sqrt{D}$ is irrational if $D \neq \square$, hence is at least 1 in absolute value. Altogether we obtain

$$|\frac{p}{q} - \sqrt{D}| > \frac{1}{3\sqrt{D}}\frac{1}{q^2}$$

as claimed. $\square$

Note: The argument extends to give Liouville's theorem, that for a real algebraic number of degree d, we have $|p/q - \alpha| > c/q^d$ with $c = c(\alpha)$ effectively computable. Roth's theorem improves that to $|p/q - \alpha| > c/q^{2+\varepsilon}$, for all $\varepsilon > 0$, with $c = c(\alpha, \varepsilon) > 0$ some constant (not effective).

Open Problem 2. *A real algebraic number of degree $d \geq 3$ is not of bounded type, equivalently the partial quotients in the continued fraction expansion are not bounded.*

Proposition 0.11. *Suppose that α is irrational of bounded type. Then*

$$D(\{\alpha n\}, N) \ll \frac{(\log N)^2}{N}.$$

Note: This can be improved to $O(\log N/N)$.

Corollary 0.12. *If α is of bounded type, then every interval of length $\gg_\alpha (\log N)^2/N$ contains an element of the form αn, $n \leq N$.*

Lemma 0.13. *Suppose that α is irrational of bounded type. Then*

$$A(t) := \sum_{k \leq t} \frac{1}{||k\alpha||} \ll t \log t.$$

and

$$G(K) := \sum_{k=1}^{K} \frac{1}{k||k\alpha||} \ll (\log K)^2$$

Proof. The key is that if α is of bounded type, then the points $||k\alpha|| \in (0, \frac{1}{2}]$ are *well spaced* in the sense that

$$\Big| ||m\alpha|| - ||n\alpha|| \Big| \gg \frac{1}{j}, \qquad 1 \leq m \neq n \leq j$$

Indeed, $m\alpha = m\alpha - M$ for $M - m\alpha$ for some integer M; hence for a suitable $L \in \mathbb{Z}$,

$$||m\alpha|| - ||n\alpha|| = \pm(m \pm n)\alpha - L$$

so that if $1 \leq m \neq n \leq j$ then

$$\Big| ||m\alpha|| - ||n\alpha|| \Big| \geq || \ |m \pm n|\alpha \ || \geq \frac{1}{(m+n)} \geq \frac{1}{2j}$$

as claimed.

Hence, an interval of length $< 1/(2K)$ will contain at most one element of the form $||k\alpha||$, $1 \leq k \leq K$.

We use this to bound the sum $A(t)$ by dividing the range of summation into intervals of length $\delta = 1/(2t)$

$$A(t) = \sum_{j=1}^{1/\delta} \sum_{\substack{k \le t \\ ||k\alpha|| \in (j\delta, (j+1)\delta]}} \frac{1}{||k\alpha||}$$

each interval contains at most one summand, and the summand is bounded above by $1/j\delta$, so that

$$A(t) \le \sum_{j=1}^{1/\delta} \frac{1}{j\delta} \ll \frac{1}{\delta} \log \frac{1}{\delta} \ll t \log t.$$

To bound $G(K)$, we use the bound on $A(t)$ and get rid of the factor $1/k$ by using summation by parts:

Exercise 5. *Suppose that α is irrational of bounded type, and set $||x|| = \mathrm{dist}(x, \mathbb{Z})$. Let*

$$A(t) := \sum_{k \le t} \frac{1}{||k\alpha||}, \qquad G(K) := \sum_{k=1}^{K} \frac{1}{k||k\alpha||}$$

We saw that $A(t) \ll t \log t$. Show that

$$G(K) \ll (\log K)^2.$$

□

We can now bound the discrepancy:

$$D(N) \ll \frac{1}{K} + \sum_{k=1}^{K} \frac{1}{k} |S^*(k, N)| \ll \frac{1}{K} + \frac{1}{N} \sum_{k=1}^{K} \frac{1}{k||k\alpha||} \ll \frac{1}{K} + \frac{(\log K)^2}{N}$$

Taking $K = N$ gives $D(N) \ll (\log N)^2/N$.

References

[1] Champernowne, D. G. The Construction of Decimals Normal in the Scale of Ten. J. London Math. Soc. 8, 1933.

[2] Copeland, Arthur H.; Erdős, Paul. Note on normal numbers. Bull. Amer. Math. Soc. 52, (1946). 857–860.

[3] Davenport, H.; Erdős, P. Note on normal decimals. Canadian J. Math. 4, (1952). 58–63.