Uniform Distribution of Sequences

Based on work by Hermann Weyl using ideas from Diophantine approximation.

Weyl's Criterion

Def.: Let x_n, $n = 1, 2, \ldots$ be an (infinite) sequence $\in \mathbb{R}$.
$\#(E; N)$ = number of $\{x_i\}$, $i = 1, \ldots, N$, $\in E \subset [0,1]$, subintervals.
$\{x_i\}$ is uniformly distributed modulo 1 if:

$$\text{from. put} \quad \lim_{N\to\infty} \frac{\#([a,b); N)}{N} = b - a \quad \forall\, a, b \in \mathbb{R},\ 0 \le a < b \le 1.$$

Theorem: x_n is u.d.m.1 $\iff$

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

$\forall\, f$, real, continuous defined on $[0,1]$.

Theorem: x_n is udm1 $\iff \forall\, h \neq 0 \in \mathbb{Z}$

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

This is an exponential sum, $hx_n \to [0, 2\pi)$, and if x_n "random" understood $\to \sqrt{N}$. This is true $\forall\, h \neq 0$!

Example: θ irr., Weyl sqn. $n\theta$ is udm1.

Def: $\#(E;N,d) = \#\, x_{d+1} \cdots x_{d+N} \in E$, x_n is well-distributed modulo 1 if

$$\lim_{N\to\infty} \frac{\#([a,b);N,d)}{N} = b-a, \text{ uniformly in } d$$

Note well-distributed modulo 1 $\Rightarrow$ udm 1, can generalize more

Theorem: x_n is udm 1 $\Leftrightarrow$

$$\lim_{N\to\infty} N^{-1} \sum_{n=d+1}^{d+N} f([x_n]) = \int_0^1 f\,dx \quad \text{unif. in } d$$

$\forall f$, real, continuous on $[0,1]$.

Theorem: x_n is udm 1 $\Leftrightarrow \forall\, h \neq 0 \in \mathbb{Z}$

$$\lim_{N\to\infty} N^{-1} \sum_{n=d+1}^{d+N} e^{2\pi i h x_n} = 0 \quad \text{unif in } d.$$

Note: $n\theta$, Weyl, is udm 1, but others are scarce!

Def: $\bar{x}_n \in \mathbb{R}^k$, $\#(E;N) = \#$ w/ fractional parts $\in E \subset \mathbb{R}^k$ a subinterval of $[0,1]^k$. $\bar{x}_n$ is udm 1 if

$$\lim_{N\to\infty} \frac{1}{N} \#([a,b);E,N) = \prod_{i=1}^{k} (b_i - a_i)$$

$\forall\, [\bar{a},b) \in [0,1]^k$.

Theorem: $\bar{x}_n$ is udm 1 $\Leftrightarrow \lim_{N\to\infty} N^{-1} \sum_{n=1}^{N} f([\bar{x}_n]) = \int_{[0,1]^k} f(x)\,dx$

$\forall f$, real, cont. in $[0,1]^k$.

Theorem: $\bar{x}_n$ is udm1 in $\mathbb{R}^k \Leftrightarrow \forall\, \bar{h} \in \mathbb{Z}^k \neq 0$

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} e^{2\pi i \langle \bar{h}, \bar{x}_n \rangle} = 0$$

Example: Weyl in $\mathbb{R}^k$, let $1, \theta_1, \dots, \theta_k$ be linearly indep. over $\mathbb{Q}$, then $\bar{x}_n = (n\theta_1, n\theta_2, \dots, n\theta_k)$ is udm1 over $\mathbb{R}^k$

Def: $x_n \in [0,1)$ is k-distributed if $\bar{x}_n = (x_n, \dots, x_{n+k-1})$ is udm1 in $\mathbb{R}^k$

Def: $x_n \in [0,1)$ is ∞-distributed if it is k-distributed for $k = 1, 2, 3, \dots$

Theorem: $x_n = \theta^n$ is ∞-dist. for almost all $\theta > 1$.

Note: Knuth asks "Does ∞-distr. = random?"

Def: $a_n \in \mathbb{Z}$, for $N \geq 1$, $m \geq 2$, $j \in \mathbb{Z}$: $\#(j, m, N) =$ # of $a_1, \dots, a_N$ satisfying $a_n \equiv j \pmod m$. A sequence is unif. distr. modulo m if

$$\lim_{N\to\infty} N^{-1} \#(j, m, N) = m^{-1} \quad \forall j = 0, \dots, m-1$$

Example: $a_n = n \pmod m$ is udm $k \Leftrightarrow k \geq 1$, $k \nmid m$.

Theorem: a_n is udm $m \Leftrightarrow \forall\, h \neq 0 \in \mathbb{Z}$

$$\lim_{N\to\infty} N^{-1} \sum_{n=1}^{N} e^{2\pi i h \left(\frac{a_n}{m}\right)} = 0$$

Theorem: $\bar{a}_n = (a_{n1}, a_{n2}, \dots, a_{nk}) \in \mathbb{Z}^k$, $\#(\bar{j}, m, N) = \#\{\bar{a}_n ; 1, \dots, N \Rightarrow a_{ni} \equiv j_i \pmod m\}$, $i = 1, \dots, k$. This is udmm if $\lim_{N\to\infty} N^{-1} \#(\bar{j}, m, N) = m^{-k}$

$\forall\, \bar{j} \in \mathbb{Z}^k$ $j_1, \dots, j_k \in 0, 1, \dots, m-1$, and a lot

Theorem: $\bar{a}_n$ is udmm $\Leftrightarrow \forall\, \bar{h} \not\equiv 0 \pmod m \in \mathbb{Z}^k$

$$\lim_{N\to\infty} N^{-1} \sum_{n=1}^{N} e^{2\pi i \langle \bar{h}, \bar{a}_n \rangle / m} = 0$$

Def: $a_n \in \mathbb{Z}$ are k-distr. modulo m if $\bar{a}_n = (a_n, a_{n+1}, \dots, a_{n+k-1})$ is udmm.

Polynomial Case:

Def: Let $\alpha \in GF(q)$, $q = p^r$. Let $w_1, \dots, w_r$ be a fixed basis for $GF(q)$ over $GF(p)$, $\alpha = \sum_{i=1}^{r} a_i w_i$ a_i's $\in GF(p)$, then the character of α is $e(\alpha/q) \triangleq e^{2\pi i a_1/p}$

Def: Let $\alpha(z) = c_w z^w + c_{w-1} z^{w-1} \in GF\{q, z\}$, $q = p^r$. Let $w_1, w_2 \dots, w_r$ be a fixed basis for $GF(q)$ over $GF(p)$. Let $c_{-1} = \sum_{i=1}^{r} a_i w_i$, a_i's $\in GF(p)$, the character of $\alpha(z)$

$$e(\alpha(z)) \triangleq e(c_{-1}/q) = e^{2\pi i a_1/p}$$

Def: $X_n(z) \in GF\{q, z\}$, $\alpha(z) \in GF\{q, z\}$, $\#(\alpha, r, N) = \#$ of $X_n(z)$, $n = 1, \dots, N \Rightarrow \deg(X_n(z) - \alpha(z)) \le -r$. Then $X_n(z)$ is uniformly distr. modulo 1 in $GF\{q, z\}$ if

$$\lim_{N\to\infty} N^{-1} \#(\alpha, r, N) = q^{-r} \quad \forall\, r \ge 1, \forall\, \alpha \in GF\{q, z\} \text{ w/ } \nu(\alpha) \ge -r$$

Theorem (Weyl Criterion): $a_n(z)$ is $\mathrm{udm}\ 1 \in GF[q,z] \Leftrightarrow$
$\forall\ h(z) \neq 0 \in GF[q,z]$:

$$\lim_{N\to\infty} N^{-1} \sum_{n=1}^{N} e(h(z)a_n(z)) = 0$$

Def: Let $f_n(z) \in GF[q,z]$, $M(z) \in GF[q,z]$ w/ $\deg = v$. For any $b(z)$ w/ $\deg < v$, $\forall\ 1 \leq N \in \mathbb{Z}$, $\#(b(z), M(z), N) =$ # of $f_1(z), \ldots, f_N(z) \ni f_n(z) \equiv b(z) \pmod{M(z)}$, then $f_i(z)$ is uniformly distributed modulo $M(z)$ if $\forall$ $b(z) \in GF[q,z]$ w/ $\deg < v$

$$\lim_{N\to\infty} N^{-1} \#(b(z), M(z), N) = q^{-v}$$

If $f_n(z)$ is $\mathrm{udm}\ M(z)$ then it is also $\mathrm{udm}\ m(z)\ \forall\ m(z) \setminus M(z)$

Theorem: $f_n(z) \in GF[q,z]$ is $\mathrm{udm} M(z) \Leftrightarrow \forall h \neq 0 \in GF[q,z]$ reduced $M(z)$

$$\lim_{N\to\infty} N^{-1} \sum_{n=1}^{N} e\left(\frac{h(n) f_n(z)}{M(z)}\right) = 0 \qquad (*)$$

Let $a(z) = a_{v-1} z^{v-1} \ldots + a_0$, $b(z) = b_{v-1} z^{v-1} \ldots + b_0$

$\langle a(z), b(z) \rangle = \sum_{i=0}^{v} a_i b_i \in GF(q)$ then $(*)$ is

Theorem: $f_n(z) \in GF[q,z]$ is $\mathrm{udm}\ M(z) \Leftrightarrow \forall h \neq 0$ reduced $M(z)$ with $\deg(h) < \deg(M)$,

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} e(\langle \bar{f}_n(z), h(z) \rangle / q) = 0$$

where $\bar{f}_n(z) = f_n(z) \pmod{M(z)}$, $\deg(f_n) < \deg(M)$

for $q = 2$ this is the XOR lemma in CS

Irregularities of Distribution:

Def: (Discrepancy the measure of irregularity)
$P = \{\bar{x}_n, n = 0, \dots, N-1\} \in [0,1]^k$, $\bar{y} \in [0,1]^k$, $E(\bar{y})$ is the rectangle w/ $\bar{0}$ & $\bar{y}$; $\#(E(\bar{y}); N) = \#$ of x_n's $\in$ rectangle

$$T_N^{(k)} = \left(\int_{[0,1]^k} \left(\frac{\#(E(\bar{y}); N)}{N} - \prod_{i=1}^{k} y_i \right)^2 d\bar{y} \right)^{1/2} : L^2$$

$$D_N^{(k)} = \sup_{\bar{y} \in [0,1]^k} \left| \frac{\#(E(\bar{y}); N)}{N} - \prod_{i=1}^{k} y_i \right| : L^\infty$$

$T_N^{(k)} \le D_N^{(k)}$ (why?)

Remark: $\lim_{N \to \infty} D_N^{(k)} = 0 \iff x_n$ is ud in $[0,1]^k$

1D: $(T_N^{(1)})^2 = (12N^2)^{-1} + N^{-1} \sum_{n=0}^{N-1} \left(x_n - \frac{2n+1}{2N} \right)^2$

$$D_N^{(1)} = (2N)^{-1} + \max_{0 \le n \le N-1} \left| x_n - \frac{2n+1}{2N} \right|$$

In both cases $x_n = 2n+1/2N$ minimize

$$T_N^{(1)} \ge \frac{1}{2\sqrt{3}N}, \quad D_N^{(1)} \ge \frac{1}{2N}$$

kD:

$$(T_N^{(k)})^2 = N^{-2} \sum_{n=0}^{N-1} \sum_{m=0}^{N-1} \prod_{i=1}^{k} \left(1 - \max(x_n^{(i)}, x_m^{(i)})\right)$$

$$- 2^{1-k} \cdot (N^{-1}) \sum_{n=0}^{N-1} \prod_{i=1}^{k} \left(1 - (x_n^{(i)})^2\right) + 3^{-k}$$

this formula can be used for computation

Theorem: $E\left((T_N^{(d)})^2\right) = N^{-1}\left(2^{-d} - 3^{-d}\right)$ via averaging over all sets of N pts $\in [0,1]^d$

Theorem: (Roth) $\forall d \geq 1$, $\exists\, c_1(d) > 0 \ni \forall N > 1$, any set of N pts $\in [0,1]^d$:

$$T_N^{(d)} \geq c_1(d) \frac{(\log N)^{(d-1)/2}}{N}$$

this is a sharp bound! As good as you can hope.

Theorem: $\forall K \geq 1$, $c_2(d)$ $\exists\, \forall N$ a set of N pts. $\in [0,1]^d \ni$

$$T_N^{(d)} \leq c_2(d) \frac{(\log N)^{d-1/2}}{N}$$

Theorem: (based on $\mathbb{Z}^2$) $\forall d \geq 1$, $\exists\, c_1(d) > 0 \ni \forall N \geq 1$, $\forall$ sets of N pts. $\in [0,1]^d$ $D_N^{(d)} > c_1(d) \frac{(\log N)^{d-1/2}}{N}$

For $d = 2$ Wolfgang Schmidt got it to be sharp

Theorem: $\exists\, c > 0 \ni \forall N > 1$, $\forall$ set of N pts $\in [0,1]^2$ we have

$$D_N^{(2)} > c \frac{\log N}{N}$$

"Great Open Problem": $\forall d \geq 1$ $\exists\, c_3(d) > 0 \ni \forall N > 1$, $\forall$ sets of N pts. $\in [0,1]^d$ we have

$$D_N^{(d)} > c_3(d) \frac{(\log N)^{d-1}}{N}$$ conjecture

Theorem: For N pts. $\mathcal{U}[0,1]^d$, i.i.d.:

$$\overline{\lim_{N \to \infty}} \frac{\sqrt{2N}\, D_N^{(d)}}{\sqrt{\log\log N}} = 1 \text{ with probability } 1$$

Law of the iterated logarithm

Def: $x_i \in [0,1]^k$ is a low-discrepancy sequence $\Rightarrow \forall N > 1$

$$D_N^{(k)} \le c(k) \frac{(\log N)^k}{N} \quad \text{(first } N \text{ points)}$$

↑ depends only on k

Theorem. $x_n \in [0,1]^{k-1}$ be a lds in $k-1$-D, $\forall N > 1$

$x_n = \left(\overset{k-1}{x_n}, \frac{n}{N} \right)$ $n = 0, 1, \ldots, N-1$ satisfies

$$D_N^{(k)} \le c(k) \frac{(\log N)^{k-1}}{N}$$

Halton Sequence

Def: for $n \ge 0$, $b \ge 2$ $\phi_b(n) = \frac{a_0}{b} + \frac{a_1}{b^2} + \cdots + \frac{a_m}{b^{m+1}}$, where $n = a_0 + a_1 b + \cdots + a_m b^m$, a_i reduced mod b, $m = \lceil \log_b n \rceil$

Def: $\phi_2(n)$, $n = 0, 1, \ldots$ is the van der Corput sequence

Def: The k-D Halton sequence $x_n = (\phi_{b_1}(n), \ldots, \phi_{b_k}(n))$ where $b_1, \ldots, b_k$ are pairwise coprime

Theorem: $\forall N > 1$, first N Halton pts. obey

$$D_N^{(k)} \le c(b_1, \ldots, b_k) \frac{(\log N)^k}{N} + O\left((\log N)^{k-1} \right)$$

$$c(b_1, \ldots, b_k) = \prod_{i=1}^{k} b_i (\log b_i)^{-1}$$

Def: The Hammersly point set w/ N pts is

$$x_n = \left(\phi_{b_1}(n), \ldots, \phi_{b_{k-1}}(n), \frac{n}{N} \right)$$

Now consider the scrambled or "Generalized" Halton sequence: For $n \geq 0$ define

$$\phi_b(n,\pi) \triangleq \frac{\pi_0(a_0)}{b} + \frac{\pi_1(a_1)}{b^2} + \cdots + \frac{\pi_m(a_m)}{b^{m+1}}, \text{ with}$$

$n = a_0 + a_1 b + \cdots + a_m b^m$, $m = \lceil \log_b n \rceil$ $\pi = (\pi_0, \ldots)$ is a set of permutations on $\{0,1,\ldots,b-1\}$.

<u>Generalized Halton</u>: $x_n = (\phi_{b_1}(n,\pi^{(1)}), \ldots, \phi_{b_k}(n,\pi^{(k)}))$

with $b_1, \ldots, b_k$ pairwise coprime

Halton: $\pi = I_b$ Warnock: $\pi_a^{(a)} = a+a \pmod{b}$

<u>Def</u>: $S_{max}(N) = \max_{h \in C_k(M) \setminus 0} \left| N^{-1} \sum_{n=0}^{N-1} e^{2\pi i \langle h, x_n \rangle / M} \right|$

$C_k(M) = \{(i_1,\ldots,i_k) \in \mathbb{Z}^k \mid -M/2 \leq i_m \leq M/2\}$

<u>Theorem</u>: $\forall M,N > 1$, $P = \{\{x_n/M\}, x_n \in \mathbb{Z}^k\}$:

$$1 - \left(1 - \frac{1}{M}\right)^k \leq D_N^{(k)} \leq 1 - \left(1 - \frac{1}{M}\right)^k + c(k) S_{max}(N) (\log N)^k \quad (*)$$

where $c(k) > 0$ depends only on k.

$(*)$ is called the discretization error.