乱数と力学系の生成点

秋山茂樹

18 Dec 2019
RCMSサロン

Kolmogorov の乱数

二進有限語 x のコルモゴロフ複雑度は万能チューリング機械 u に対して

$$K_u(x) = \min_{u(p)=x} \ell(p)$$

で定義される。 p はプログラム。 $\ell(p)$ は p の長さ。 $u(p)$ は p の出力を表す。とくに

$$K_u(x) \geq |x|$$

が成立するとき x は圧縮不能という。

Martin-Löf の乱数

二進片側無限語 w に対してある自然数 c が存在して、任意の w の prefix x について

$$K_u(x) > |x| - c$$

が成り立つとき Martin-Löf の意味で圧縮不能という。

このような無限語を Algorithmically Random という。

Mauduit-Sarkozy の乱数

$E_N = (e_1, e_2, \ldots, e_N)$ を ± 1 からなる長さ N のベクトルとする。

$$W(E_N) = \max_{a,b,t} \left| \sum_{j=1}^{t} e_{a+bj} \right|$$

を Well distribution measure という。 ここで a, b, t は $1 \leq a+b, a+tb \leq N$ なる整数を動く。また

$$C_k(E_N) = \max_{0 \leq d_1 < \cdots < d_k} \left| \sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \cdots e_{n+d_k} \right|$$

を Correlation measure という。 但し $d_k + M \leq N$ とする。

ランダムな列では

$$\sqrt{N} \ll W(E_n) \ll \sqrt{N \log N}$$

$$\sqrt{N} \ll C_k(E_n) \ll \sqrt{kN \log N}$$

が期待される。これを満たすならば Mauduit-Sarkozy の意味で乱数という。

p を素数としたとき

$$E_{p-1} = \left\{ \left(\frac{i}{p}\right) \;\middle|\; i = 1, \ldots, p-1 \right\}$$

はMauduit-Sarkozy の意味で乱数となる。[3, 2]

ここで

$$\left(\frac{i}{p}\right) = \begin{cases} 1 & x^2 \equiv i \pmod{p} \text{が可解} \\ -1 & x^2 \equiv i \pmod{p} \text{が解なし} \end{cases}$$

$\left(\frac{i}{p}\right)$ は数論で Legendre 記号と呼ばれている。

力学系と乱数

$T : [0, 1] \to [0, 1]$ をルベグ測度に対してエルゴード的な写像とする。このとき x が生成点とは、すべての連続関数 f に対して

$$\lim_{N\to\infty} \frac{1}{N} \sum_{i=1}^{N} f(T^{i-1}(x)) = \int_0^1 f(x)dx$$

が成り立つこととする。 $T(x) = 2x - \lfloor 2x \rfloor$ だと、x が生成点とは、x の二進展開で正規数であることを意味する。

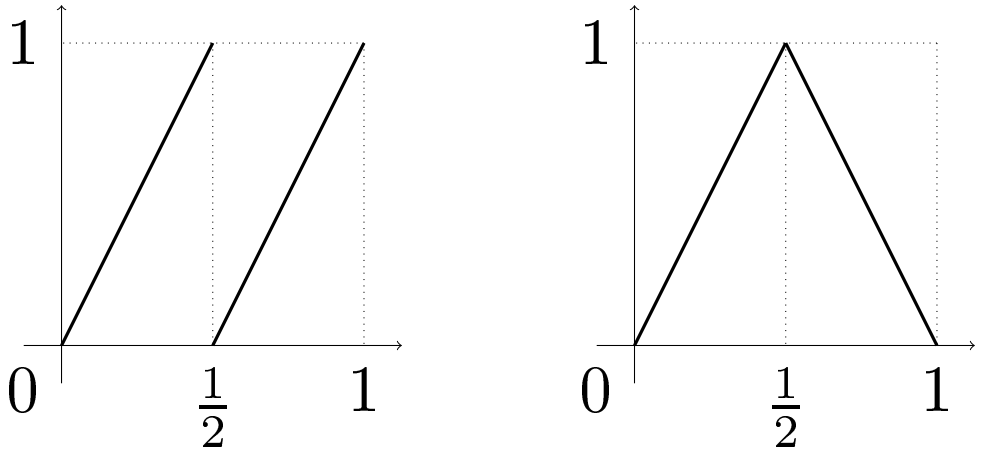

Figure 1: Generic Point Equivalent

この二つの写像は生成点の集合が同一である。(c.f. [1])

Hot Spot Lemma

ある定数 $C \geq 1$ があって任意の $[0,1]$ の部分区間 $[a,b]$ に対して

$$\lim_{N\to\infty} \frac{1}{N} \sum_{i=1}^{N} \chi_{[a,b]}(T^{i-1}(x)) \leq C(b-a)$$

が成り立てば x は生成点となる。名前の由来は命題の対偶をとると理解できる。

References

[1] Shigeki Akiyama, Hajime Kaneko, and Dong Han Kim, *Generic point equivalence and Pisot numbers*, Ergodic Theory and Dynamical systems (Online 11 July 2019).

[2] Julien Cassaigne, Christian Mauduit, and András Sárközy, *On finite pseudorandom binary sequences. VII. The measures of pseudorandomness*, Acta Arith. **103** (2002), no. 2, 97–118.

[3] Christian Mauduit and András Sárközy, *On finite pseudorandom binary sequences. I. Measure of*

pseudorandomness, the Legendre symbol, Acta Arith. **82** (1997), no. 4, 365–377.