超立方体への均等分布の証明

f を集合 S から S への一対一上への写像（全単射）とする。
ここで

f を n 個合成した写像　$f \circ f \circ f \circ \cdots \circ f$　を　f^n
f^{-1} を n 個合成した写像　$f^{-1} \circ f^{-1} \circ f^{-1} \circ \cdots \circ f^{-1}$　を　f^{-n}
恒等写像を　f^0

と表す。
s_0 が与えられているとして，n を整数として

$$s_n = f^n(s_0)$$

と定める。
このとき，　$s_m = s_n$　が成り立つならば

任意の整数 k に対して，　$f^k(s_m) = f^k(s_n)$　すなわち　$s_{m+k} = s_{n+k}$　が成り立つ。

定理 1

q を素数として，$f(s_0) \neq s_0$　かつ　$f^q(s_0) = s_0$　すなわち　$s_1 \neq s_0$　かつ　$s_q = s_0$　が成り立つとする。

このとき
(1)　$s_k = s_0$，　$0 < k < q$　となる k はない。
(2)　$s_k = s_0$ が成り立てば，k は q の倍数
(3) すべての $m, n \in Z$，　$0 \leqq m < n < q$ について，　$s_m \neq s_n$

証明
(1)　$s_k = s_0$，　$1 < k < q$　を満たす k があると仮定し，その k のうちで最小な自然数を k_0 とする。
q を k_0 で割った商を a，余りを r とすると

$$q = k_0 a + r \quad (0 \leqq r < k_0)$$

これを　$s_q = s_0$　に代入して

$$s_{k_0 a + r} = s_0$$

ここで，$s_{k_0} = s_0$ より

$$s_{k_0 a + r} = s_{k_0 (a-1) + r} = \cdots = s_r$$

であるから

$$s_r = s_0$$

$0 \leqq r < k_0$ であり，k_0 は $s_k = s_0$ となる最小の自然数 k であったから

$$r = 0$$

したがって

$$q = k_0 a$$

となるが，q は素数であるから

$k_0 = 1$　または　$k_0 = q$

ここで　$1 < k_0 < q$　であるから矛盾

(2) k を q で割った商を a，余りを r とすると

$k = qa + r$　(0≦r<q)

よって

$s_{qa+r} = s_k = s_0$

ここで，$s_q = s_0$ より

$s_{qa+r} = s_{q(a-1)+r} = \cdots = s_r$

であるから

$s_r = s_0$

0≦r<q であるから，(1)より r=0

したがって，k は q の倍数である。

(3)　$0 \leqq m < n < q$　かつ　$s_m = s_n$

となる m，n が存在すると仮定する。このとき

$0 < n - m < q$　かつ　$s_{n-m} = s_0$

となるから(1)に反する。

証明終り

定理 2

自然数 n と素数 q は互いに素であるとして，$g = f^n$ とする。このとき

$f(s_0) \neq s_0$　かつ　$f^q(s_0) = s_0$　ならば　$g(s_0) \neq s_0$　かつ　$g^q(s_0) = s_0$

証明

$g(s_0) = s_0$ を仮定すると，$f^n(s_0) = s_0$ となるから，定理 1（2）により n は q の倍数となる。

これは，n と q は互いに素であることに反する。よって，$g(s_0) \neq s_0$

また

$g^q(s_0) = f^{nq}(s_0) = (f^q \circ f^q \circ \cdots \circ f^q)(s_0) = s_0$

証明終り

p を素数，$q = 2^{p-1} - 1$ をメルセンヌ素数とし，直積集合 $S = \{0,1\}^p$ 考える。

$s = (a_0, a_1, a_2, \cdots, a_{p-1}) \in S$

とし，GL(2)上の線形漸化式

$a_{n+p} + \cdots + a_{n+k} + \cdots + a_n = 0$　(n は整数)

により

$$s' = (a_1, a_2, a_3, \cdots, a_p) \in S$$

を定め，S から S への写像 f を

$$s' = f(s)$$

により定める。このとき s' から s がただ一通りに定まるため，f は全単射となる。
いま，s_0 が与えられているとして，n を整数として

$$s_n = f^n(s_0)$$

と定める。

いま，$s_1 \neq s_0$　かつ　$s_q = s_0$ が成り立つとする。

このとき，任意の整数 n について $s_n \neq (0,0,0,\cdots,0,\cdots,0)$ であり，定理 1（3）により，$s_0, s_1, s_2, \cdots, s_{q-1}$ はすべて異なる。
さらに，p を 32 で割った商を k，余りを r とする。32k と q は互いに素であるから，$g = f^{32k}$ とすると，定理 2 により

$$g(s_0) \neq s_0 \quad \text{かつ} \quad g^q(s_0) = s_0$$

ここで，$t_0 = s_0$ とし，n を整数として

$$t_n = g^n(t_0)$$

により，S の要素の列を定める。このとき

$$t_0 = (a_0, a_1, a_2, \cdots, a_{32k-1}, \cdots, a_{p-1})$$

$$t_1 = (a_{32k}, a_{32k+1}, a_{32k+2}, \cdots, a_{64k-1}, \cdots, a_{p+32k-1})$$

$$t_2 = (a_{64k}, a_{64k+1}, a_{64k+2}, \cdots, a_{96k-1}, \cdots, a_{p+64k-1})$$

……

となる。

このとき，$t_0, t_1, t_2, \cdots, t_{q-1}$ は，どれも $(0,0,0,\cdots,0,\cdots,0)$ ではなく，しかも，定理 1（3）によりすべて異なる。

ここで，S の要素の数は q+1 個であるから，$t_0, t_1, t_2, \cdots, t_{q-1}$ に $(0,0,0,\cdots,0,\cdots,0)$ を付け加えたものは，S のすべての要素をちょうど 1 回ずつとる。したがって，次のことが成り立つ。

$t_0, t_1, t_2, \cdots, t_{q-1}$ の初めから 32k ビットを取り出して

$$u_0 = (a_0, a_1, a_2, \cdots, a_{32k-1})$$
$$u_1 = (a_{32k}, a_{32k+1}, a_{32k+2}, \cdots, a_{64k-1})$$
$$u_2 = (a_{64k}, a_{64k+1}, a_{64k+2}, \cdots, a_{96k-1})$$
……

とする。$u_0, u_1, u_2, \cdots, u_{q-1}$ を 32 ビットずつに区切って，1 辺が 32 ビットの k 次元超立方体に 32 ビット×k 個を q 通り並べると，原点を除いて均等分布する。

さらに，直積集合 $\{0,1\}^{32k}$ から $\{0,1\}^{32k}$ への全単射を h とするとき，

$$u'_n = h(u_n) \quad (n = 0,1,2,\cdots,q-1)$$

と変換しても，1 点を除いて均等分布する。

特に，u_n を 32 ビットずつに区切って $\{0,1\}^{32}$ から $\{0,1\}^{32}$ への全単射によって，$\{0,1\}^{32k}$ から $\{0,1\}^{32k}$ へ変換しても全単射となるから，このように Tempering を行っても，1 点を除いて均等分布する。