УДК 512.625.5

# ЭРГОДИЧЕСКИЕ ДИНАМИЧЕСКИЕ СИСТЕМЫ В ДЕКАРТОВОЙ СТЕПЕНИ КОЛЬЦА ЦЕЛЫХ 2-АДИЧЕСКИХ ЧИСЕЛ

В. В. Сопин

*Московский государственный университет им. М. В. Ломоносова, г. Москва, Россия*

Доказывается, что для любого 1-липшицева эргодического отображения $F : \mathbb{Z}_2^k \mapsto \mathbb{Z}_2^k$, где $k > 1$ и $k \in \mathbb{N}$, существуют 1-липшицево эргодическое отображение $G : \mathbb{Z}_2 \mapsto \mathbb{Z}_2$ и два биективных отображения $H_k$, $T_{k,P}$, что $G = H_k \circ T_{k,P} \circ F \circ H_k^{-1}$ и $F = H_k^{-1} \circ T_{k,P^{-1}} \circ G \circ H_k$.

**Ключевые слова:** *эргодическая теория, 1-липшицевы сохраняющие меру преобразования, декартово произведение, T-функции.*

DOI 10.17223/20710410/27/3

# ERGODIC DYNAMICAL SYSTEMS OVER THE CARTESIAN POWER OF THE RING OF 2-ADIC INTEGERS

V. V. Sopin

*Lomonosov Moscow State University, Moscow, Russia*

**E-mail:** VvS@myself.com

It is proved that, for any 1-lipschitz ergodic map $F : \mathbb{Z}_2^k \mapsto \mathbb{Z}_2^k$, where $k > 1$ and $k \in \mathbb{N}$, there are 1-lipschitz ergodic map $G : \mathbb{Z}_2 \mapsto \mathbb{Z}_2$ and two bijections $H_k$, $T_{k,P}$ such that $G = H_k \circ T_{k,P} \circ F \circ H_k^{-1}$ and $F = H_k^{-1} \circ T_{k,P^{-1}} \circ G \circ H_k$.

**Keywords:** *ergodic, 1-lipschitz measure-preserving p-adic functions, p-adic analysis, cartesian product, T-functions.*

## Введение

T-функция — это такое преобразование двоичных слов в двоичные слова, что каждый $i$-й бит выходного слова не зависит от бит с номерами $i + 1$, $i + 2$, ... входных слов. Все логические и большинство арифметических операций по модулю $2^n$, $n \in \mathbb{N}$, а также их композиции являются T-функциями.

Транзитивные T-функции (последнее означает, что последовательность $n$-битных слов $w, f(w), f(f(w)), \ldots$ имеет максимально длинный период, т. е. период длины $2^n$) являются криптографическими примитивами, так как на их основе можно строить псевдослучайные генераторы с многими важными криптографическими свойствами: высокой линейной сложностью, равномерным распределением подслов и другими, а главное — с хорошим быстродействием, так как T-функции легко программируются.

А. Климов и А. Шамир привлекли внимание мирового криптографического сообщества к T-функциям в своей работе [1], хотя и сами T-функции, и важность их для криптографии были известны значительно ранее (см., например, [2 – 5], где получены критерии транзитивности T-функций). Отметим также, что, как указано в [2, 6], исторически первый критерий транзитивности T-функций (булевых отображений треугольного вида) был известен ещё с 1970-х годов.

Задача описания транзитивных T-функций одной переменной была решена во многом благодаря $p$-адическому анализу, так как T-функция — это 1-липшицево отображение в 2-адической метрике, а её транзитивность эквивалентна эргодичности [6, 7].

Более формально: рассмотрим $\mathbb{Z}_2^k$, $k \in \mathbb{N}$, — декартову степень кольца целых 2-адических чисел с мерой Хаара $\mu$, нормализованной так, что $\mu(\mathbb{Z}_2^k) = 1$. Везде далее будем рассматривать эргодичность только в классе сохраняющих нормированную меру Хаара отображений.

Отображение $f : \mathbb{Z}_2^k \mapsto \mathbb{Z}_2^k$ называется сохраняющим меру, если $\mu(f^{-1}(S)) = \mu(S)$ для любого измеримого множества $S \subseteq \mathbb{Z}_2^k$.

Сохраняющее меру отображение $g : \mathbb{Z}_2^k \mapsto \mathbb{Z}_2^k$ называется эргодическим, если для любого измеримого множества $S$ из $g^{-1}(S) = S$ следует, что $\mu(S) = 0$ или $\mu(S) = 1$.

В главе 4.6.2 работы [6] описывается способ построения эргодического 1-липшицева отображения на $\mathbb{Z}_2^k$, $k \in \mathbb{N}$, из эргодического 1-липшицева отображения на $\mathbb{Z}_2$. Такой способ часто используется в вычислительной технике, но, очевидно, описывает не весь класс эргодических 1-липшицевых отображений на $\mathbb{Z}_2^k$ (пояснения можно найти в п. 3 данной работы) ввиду их более сложной структуры.

В работе доказано, что любое эргодическое 1-липшицево отображение $F$ на $\mathbb{Z}_2^k$, $k \in \mathbb{N}$, может быть представлено определённым образом через $k$ сохраняющих меру 1-липшицевых отображений на $\mathbb{Z}_2$ и $k$ отображений на $\mathbb{F}_2^k$ (векторном пространстве размерности $k$ над полем из двух элементов), возможно, с помощью некоторого дополнительного преобразования, определяющегося через перестановку степени $2^k$. Данный результат представлен в п. 2.

Кроме того, для отображения $F$ существует 1-липшицево эргодическое отображение $G$ на $\mathbb{Z}_2$, что $F$ может быть получено из $G$ двумя преобразованиями, одному из которых также можно поставить в соответствие некоторую перестановку степени $2^k$, а второе отвечает за представление вектора длины $k$ из целых 2-адических чисел через целое 2-адическое число. Важно, что верно обратное утверждение для $F$ и $G$ при использовании обратных преобразований к описанным двум. Последний результат содержится в п. 3.

Краткое напоминание о 2-адических числах дано в п. 1.

## 1. 2-адические числа

Для произвольного ненулевого целого числа $a$ определим $\operatorname{ord}_2 a$ равным кратности вхождения 2 в разложение $a$ на простые сомножители. Для произвольного рационального числа $x = a/b$ положим $\operatorname{ord}_2 x = \operatorname{ord}_2 a - \operatorname{ord}_2 b$.

Определим на $\mathbb{Q}$ норму $\|\cdot\|_2$:

$$\|x\|_2 = \begin{cases} 2^{-\operatorname{ord}_2 x}, \text{ если } x \neq 0, \\ 0, \text{ если } x = 0. \end{cases}$$

Определим расстояние между двумя числами $a$ и $b$

$$d(a, b) = \|a - b\|_2$$

и тем самым зададим на кольце рациональных чисел метрику. Пополнение метрического пространства $(\mathbb{Q}, d)$ будем называть полем 2-адических чисел и обозначать $\mathbb{Q}_2$.

Множество $\mathbb{Z}_2 = \{x \in \mathbb{Q} : \|x\|_2 \leqslant 1\}$ называется множеством целых 2-адических чисел. Элементы кольца $\mathbb{Z}_2$ называются целыми 2-адическими числами.

Каждому целому 2-адическому числу $x$ можно сопоставить бесконечную последовательность $x_1, x_2, \ldots$ вычетов $x_n$ по модулю $2^n$, $0 \leqslant x_n < 2^n$, удовлетворяющих условию $x_{n+1} \equiv x_n \pmod{2^n}$, и это сопоставление взаимно-однозначное. Сложение и умножение целых 2-адических чисел определяется как почленное сложение и умножение таких последовательностей.

Кроме того, каждому целому 2-адическому числу $x$ можно поставить во взаимно-однозначное соответствие ряд

$$\sum_{j=0}^{\infty} \alpha_j 2^j \quad \left( x_n = \sum_{j=0}^{n-1} \alpha_j 2^j \right), \text{ где } \alpha_i \in \{0,1\},\ i \in \mathbb{N}.$$

Будем рассматривать на декартовой степени $\mathbb{Z}_2^k$, $k > 1$, следующую метрику:

$$\|(\sigma_1, \ldots, \sigma_k) - (\delta_1, \ldots, \delta_k)\|_2 = \max\{\|\sigma_i - \delta_i\|_2 : i = 1, \ldots, k\}$$

для любых $\sigma = (\sigma_1, \ldots, \sigma_k), \delta = (\delta_1, \ldots, \delta_k) \in \mathbb{Z}_2^k$.

Определим отображение mod $2^n$, $n \in \mathbb{N}$, для любого $x = (x^1, \ldots, x^k) \in \mathbb{Z}_2^k$, $k \in \mathbb{N}$:

$$(x^1, \ldots, x^k) \bmod 2^n = (x_n^1, \ldots, x_n^k) = \left( \sum_{i=0}^{2^{n-1}} \alpha_i^1 2^i, \ldots, \sum_{i=0}^{2^{n-1}} \alpha_i^k 2^i \right).$$

## 2. Описание через $k$ отображений от одной переменной

**Определение 1** [6, 7]. 1-липшицевость $F : \mathbb{Z}_2^k \mapsto \mathbb{Z}_2^k$, $k \in \mathbb{N}$, означает, что

$$\forall x, y \in \mathbb{Z}_2^k \ (\|F(x) - F(y)\|_2 \leqslant \|x - y\|_2),$$

то есть $F(x) \equiv F(x \bmod 2^n) \bmod 2^n$.

**Определение 2.** Графом 1-липшицева сохраняющего меру отображения $F : \mathbb{Z}_2^k \mapsto \mathbb{Z}_2^k$, $k \in \mathbb{N}$, по модулю $2^n$ назовём ориентированный граф, вершинами которого являются векторы $(i_1, \ldots, i_k)$, где $i_j \in \{0, \ldots, 2^n - 1\}$, $j = 1, \ldots, k$. Из вершины $y$ идёт дуга в вершину $z$, если $F(y) \equiv z \bmod 2^n$.

**Определение 3.** 1-липшицево сохраняющее меру отображение $F : \mathbb{Z}_2^k \mapsto \mathbb{Z}_2^k$, где $k \in \mathbb{N}$, называется транзитивным по модулю $2^n$, если граф $F$ по модулю $2^n$ представляет собой цикл.

Из работ [6, 7] известно, что 1-липшицево сохраняющее меру отображение $F$ на $\mathbb{Z}_2^k$, $k \in \mathbb{N}$, является эргодическим тогда и только тогда, когда оно транзитивно по всем модулям $2^n$, $n \in \mathbb{N}$.

Для 1-липшицевых отображений из транзитивности по всем модулям $2^n$, $n \in \mathbb{N}$, следует сохранение меры. Кроме того, для сохранения меры 1-липшицевому отображению необходимо и достаточно быть биективным по всем модулям натуральной степени двойки [6, 7].

В работе [6] описывается способ построения 1-липшицева эргодического отображения на $\mathbb{Z}_2^k$, $k > 1$, из 1-липшицева эргодического отображения на $\mathbb{Z}_2$. Однако такой способ описывает не всевозможные такие отображения на $\mathbb{Z}_2^k$ хотя бы из тех соображений, что транзитивность по модулю два 1-липшицева сохраняющего меру отображения $f : \mathbb{Z}_2 \mapsto \mathbb{Z}_2$ предполагает

$$f(0) \bmod 2 = 1 \text{ и } f(1) \bmod 2 = 0,$$

то есть «чётные значения» переводятся отображением $f$ в «нечётные» и наоборот. Предлагаемый в [6] способ разбиения на $k$ координат сохранит данное свойство отображения $f$ в какой-то координате (возможно, в другом разряде, а не нулевом), что, вообще говоря, не предполагает общий случай.

Определим класс отображений $\mathfrak{F}_k$, $k > 1$, как множество всех эргодических 1-липшицевых отображений $F : \mathbb{Z}_2^k \mapsto \mathbb{Z}_2^k$, которые по модулю 2 любой вектор из $\mathbb{F}_2^k$ с $1 \leqslant j \leqslant k$ нулевых координат НЕ переводят в вектор, у которого все эти $j$ координат также нулевые, и выполняется сравнение $F((1,\ldots,1)) \equiv (0,\ldots,0) \pmod 2$.

Класс отображений $\mathfrak{F}_k$ не является пустым для любого $k > 1$, так как содержит по крайней мере те 1-липшицевы эргодические отображения, граф которых по модулю 2 представляет собой следующий цикл: $0, 1, 2, \ldots, 2^k - 1$, где значения разрядов, начиная от нулевого и заканчивая $(k-1)$-м, в двоичном представлении данных чисел рассматриваются как значения соответствующих координат двоичных векторов размерности $k$.

Принадлежность таких отображений классу $\mathfrak{F}_k$ становится очевидной, если увидеть, что последовательность $0, 1, 2, \ldots, 2^k - 1$ генерируется отображением $x + 1$, и прибавление единицы как раз и означает, что какой-то нулевой разряд станет ненулевым.

Формальное доказательство существования таких отображений будет следовать из теоремы 2 или теоремы 3. В дальнейшем мы увидим, что на самом деле графы 1-липшицевых эргодических отображений по модулю 2 имеют всевозможные циклы.

**Теорема 1.** Для любых $F \in \mathfrak{F}_k$ и $\sigma = (\sigma_1, \ldots, \sigma_k) \in \mathbb{Z}_2^k$ выполняется

$$F(\sigma) = \sum_{i=1}^{k} f_i(\sigma_i) p_i(\sigma \bmod 2),\ \ f_i : \mathbb{Z}_2 \mapsto \mathbb{Z}_2,\ \ p_i : \mathbb{F}_2^k \mapsto \mathbb{F}_2^k,$$

где $f_i$ — 1-липшицевы сохраняющие меру отображения, у которых граф по модулю 2 есть цикл длины 2, а значения $p_i(\sigma \bmod 2)$, $i = 1, \ldots, k$, такие, что $i$-я координата равна единице, причём определитель матрицы, составленной из $p_i(\sigma \bmod 2)$, не равен нулю.

***Доказательство.*** Покажем, как можно построить $p_i$; при этом необходимо помнить, что $f_i(0) \bmod 2 = 1$ и $f_i(1) \bmod 2 = 0$, $i = 1, \ldots, k$, ввиду условия транзитивности по модулю 2.

Пусть вектор $\sigma \bmod 2$ имеет $1 \leqslant j \leqslant k$ каких-то нулевых координат, а отображение $F \bmod 2$ переводит его в другой вектор $\delta = (\delta_1, \ldots, \delta_k)$, у которого не все эти $j$ координат нулевые (такие условия гарантирует принадлежность отображения классу $\mathfrak{F}_k$). Тогда $p_i$ построим следующим образом:

— в случае $\sigma \bmod 2 = (1, \ldots, 1)$ каждому $p_i$ ставим в соответствие вектор с одной единичной координатой на $i$-м месте;
— иначе
  1) всем $p_i(\sigma \bmod 2)$, кроме одного произвольного $p_l(\sigma \bmod 2)$: $\delta_l = 1$, $\sigma_l = 0$ (такой существует по условию), поставим в соответствие вектор с одной единичной координатой на $i$-м месте;
  2) $p_l(\sigma \bmod 2)$ поставим в соответствие вектор, у которого единичная координата стоит на $l$-м месте и на всех тех местах, где $\delta_m$ и $\sigma_m \bmod 2$ одновременно равны нулю или единице, $m = 1, \ldots, k$, $m \neq l$.

Очевидно, что построенные $p_i(\sigma \bmod 2)$ удовлетворяют заявленным условиям.

Тем самым доказано равенство

$$F(\sigma) \bmod 2 = \sum_{i=1}^{k} f_i(\sigma_i) p_i(\sigma \bmod 2) \bmod 2$$

для любых 1-липшицевых сохраняющих меру $f_i$, у которых граф по модулю 2 представляет собой цикл длины 2 ($f_i(0) \bmod 2 = 1$ и $f_i(1) \bmod 2 = 0$, $i = 1, \ldots, k$).

Например, рассмотрим цикл $(0,0); (1,0); (0,1); (1,1)$, тогда

$$\begin{gathered} p_1(0,0) = (1,1);\ p_2(0,0) = (0,1); \\ p_1(1,0) = (1,0);\ p_2(1,0) = (0,1); \\ p_1(0,1) = (1,1);\ p_2(0,1) = (0,1); \\ p_1(1,1) = (1,0);\ p_2(1,1) = (0,1). \end{gathered}$$

Цикл $(0,0); (1,0); (1,1); (0,1)$ представить с линейно независимыми $p_1$ и $p_2$ в $\mathbb{F}_2^2$ уже нельзя.

Далее будем строить $f_i$ индукционно по разрядам 2-адических чисел. Опишем переход $n \mapsto n+1$. Рассмотрим два таких произвольных вектора $\sigma = (\sigma_1, \ldots, \sigma_k)$ и $\delta = (\delta_1, \ldots, \delta_k)$, что $F(\sigma) \equiv \delta \pmod{2^{n+1}}$, причём по предположению

$$F(\sigma \bmod 2^n) \equiv \sum_{i=1}^{k} f_i(\sigma_i \bmod 2^n) p_i(\sigma \bmod 2) \equiv \delta \bmod 2^n.$$

Далее

$$\begin{gathered} F(\sigma) - (F(\sigma \bmod 2^n) \bmod 2^n) \equiv \sum_{i=1}^{k} [f_i(\sigma_i) - (f_i(\sigma_i \bmod 2^n) \bmod 2^n)] p_i(\sigma \bmod 2) \equiv \\ \equiv \delta - (\delta \bmod 2^n) \bmod 2^{n+1}. \end{gathered}$$

Матрица из $p_i(\sigma \bmod 2)$ имеет ненулевой определитель, значит, $p_i(\sigma \bmod 2)$ являются базисом в $\mathbb{F}_2^k$. Тогда по вектору $\triangle^n(\delta)$, координаты которого равны соответствующим $n$-м разрядам координат $\delta$, можно найти единственный вектор $(e_1, \ldots, e_k)$, $e_j \in \{0,1\}$, что

$$(e_1 p_1(\sigma \bmod 2) \oplus \ldots \oplus e_k p_k(\sigma \bmod 2)) = \triangle^n(\delta).$$

Определим

$$f_i(\sigma_i) \bmod 2^{n+1} = f_i(\sigma_i \bmod 2^n) \bmod 2^n + e_i 2^n, \quad i = 1, \ldots, k,$$

и перейдём к пределу по $n$, который существует ввиду определения 2-адических чисел через вычеты (см. п. 1).

Для полученных $f_i$ выполняется равенство

$$F(\sigma) = \sum_{i=1}^{k} f_i(\sigma_i) p_i(\sigma \bmod 2)$$

для любого $\sigma = (\sigma_1, \ldots, \sigma_k)$ из $\mathbb{Z}_2^k$, так как оно выполняется по любому модулю, равному натуральной степени двойки.

Действительно, если предположить противное, то существует $\xi \in \mathbb{Z}_2^k$, для которого

$$F(\xi) \neq \sum_{i=1}^{k} f_i(\xi_i) p_i(\xi \bmod 2),$$

значит, существует какая-то координата и разряд в этой координате, в котором значения $F(\xi)$ и $\sum\limits_{i=1}^{k} f_i(\xi_i)p_i(\xi \bmod 2)$ отличаются, что приводит к противоречию с их равенством по всем модулям натуральной степени двойки.

По построению полученные $f_i$, $i = 1, \ldots, k$, 1-липшицевы. Действительно, возьмём произвольные $x, y \in \mathbb{Z}_2$, тогда для $\mathbf{x} = (0, \ldots, 0, x, 0, \ldots, 0)$, $\mathbf{y} = (0, \ldots, 0, y, 0, \ldots, 0) \in \in \mathbb{Z}_2^k$ выполняется

$$\|f_j(x)p_j(\mathbf{x}) - f_j(y)p_j(\mathbf{y}) + \sum_{i=1, i\neq j}^{k} f_i(0)(p_i(\mathbf{x}) - p_i(\mathbf{y}))\|_2 =$$
$$= \|F((0, \ldots, 0, x, 0, \ldots, 0)) - F((0, \ldots, 0, y, 0, \ldots, 0))\|_2 \leqslant \|x - y\|_2.$$

Если $x \equiv y \bmod 2$, то $p_i(\mathbf{x}) = p_i(\mathbf{y})$, $i = 1, \ldots, k$ (см. определение $p_i$), иначе справедливо $\|x-y\|_2 = 1$; 1 является максимальным возможным значением (см. п. 1), и неравенство превращается в тривиальное.

Отображение $f_i$ сохраняет меру (ввиду 1-липшицевости для этого необходима и достаточна биективность по всем модулям $2^n$, $n \in \mathbb{N}$ [6]), так как, предполагая противное, мы не получим транзитивность $F$ по какому-то модулю ввиду того, что если

$$f_i(\sigma_i \bmod 2^n) \equiv f_i(\sigma_i \bmod 2^n + 2^n) \bmod 2^{n+1},$$

то мы не получим всевозможные значения $F$ по модулю $2^{n+1}$.

Более того, если при данных $p_i$, $i = 1, \ldots, k$, $i$-я координата отображения $F$ выражается только через $f_i$, то отображение $f_i$ является эргодическим, так как иначе оно не транзитивно по какому-то модулю $2^m$. Следовательно, мы также не получим все значения $i$-й координаты отображения $F$ по этому модулю ввиду того, что тогда граф $f_i$ по модулю $2^m$ имеет не один цикл и $i$-я координата $F \bmod 2^m$ принимает только значения вершин какого-то цикла графа $f_i$ по модулю $2^m$, в котором не представлены всевозможные значения. ■

Все 1-липшицевы эргодические отображения сопряжены друг с другом [8]. Более подробно об этом можно найти в работах В. Сущанского и его соавторов [9, 10]. Но для описания всего класса 1-липшицевых эргодических отображений из какого-то одного требуется счётное число соответствующих преобразований, вид которых может быть очень сложным [10].

Возьмём произвольное сохраняющее меру 1-липшицево отображение $F : \mathbb{Z}_2^k \mapsto \mathbb{Z}_2^k$, где $k > 1$, и представим всё множество $\mathbb{Z}_2^k$ в виде разбиения на подмножества мощности $2^k$ следующего вида:

$$\mathcal{F}_k(x_0) = \{x_0, F(x_0), \ldots, F^{2^k-1}(x_0)\}, \quad x_0 \in \mathbb{Z}_2^k \;\; x_0 \equiv (0, \ldots, 0) \bmod 2.$$

Подмножества $\mathcal{F}_k(x_0)$ при различных $x_0$ не пересекаются ввиду сохранения меры отображением $F$, так как сохранение меры означает биекцию отображения [6]. А за счёт 1-липшицевости $F$ выполняется

$$F^{2^k}(x_0) = x, \text{ где } x \equiv (0, \ldots, 0) \bmod 2.$$

Преобразование $T_{k,P}$, которому можно поставить в соответствие перестановку $P$ степени $2^k$, определяется для любого $x \in \mathbb{Z}_2^k$, где $x$ принадлежит некоторому $\mathcal{F}_k(x_0)$, причём $F^j(x_0) = x$, $j = 0, \ldots, 2^k - 1$, следующим образом:

$$T_{k,P} \circ F(x) = F^{P(j+1)}(x_0).$$

**Теорема 2.** Для любого эргодического 1-липшицева отображения $F \notin \mathfrak{F}_k$ существуют такие перестановка $P$ степени $2^k$ и отображение $G \in \mathfrak{F}_k$, что

$$G = T_{k,P} \circ F \text{ и } F = T_{k,P^{-1}} \circ G.$$

***Доказательство.*** Выберем перестановку $P$ вершин на графе $F$ по модулю 2 (данный граф представляет собой цикл ввиду эргодичности $F$ [6, 7]) так, чтобы её цикл принадлежал множеству циклов, полученных рассмотрением графов всех отображений класса $\mathfrak{F}_k$ по модулю 2. Такая перестановка существует, но не единственна.

Рассмотрим отображение $G = T_{k,P} \circ F : \mathbb{Z}_2^k \mapsto \mathbb{Z}_2^k$; оно сохраняет меру, так как произвольная перестановка не влияет на свойство сохранения меры; 1-липшицевость отображения $G$ следует из 1-липшицевости $F$. Напомним, что 1-липшицевость означает $F(x) \equiv F(x \bmod 2^n) \bmod 2^n$ для любых $x \in \mathbb{Z}_2^k$, $n \in \mathbb{N}$.

Так как эргодичность в случае 1-липшицева сохраняющего меру отображения эквивалента транзитивности по любому модулю натуральной степени двойки [6, 7], а произвольная перестановка элементов на графе 1-липшицева сохраняющего меру отображения не влияет на транзитивность этого отображения (цикл останется циклом), то $G$ является эргодическим отображением. Значит, $G \in \mathfrak{F}_k$.

Равенство $F = T_{k,P^{-1}} \circ G$ следует из определения отображения $T_{k,P}$. ■

### 3. Описание через одно отображение от одной переменной

Определим отображение $H_k : \mathbb{Z}_2^k \mapsto \mathbb{Z}_2$ для любого натурального $k > 1$ следующим образом:

$$H_k\left(\sum_{i=0}^{\infty} \alpha_i^0 2^i, \sum_{i=0}^{\infty} \alpha_i^1 2^i, \ldots, \sum_{i=0}^{\infty} \alpha_i^{k-1} 2^i\right) = \sum_{i=0}^{\infty} \sum_{j=0}^{k-1} \alpha_i^j 2^{ik+j}, \text{ где } \alpha_i^j \in \{0, 1\}.$$

Так как элементы $\mathbb{Z}/2^n\mathbb{Z}$ — кольца вычетов по модулю $2^n$, $n \in \mathbb{N}$, — можно рассматривать как элементы $\mathbb{Z}_2$, то для любого 1-липшицева сохраняющего меру отображения $F : \mathbb{Z}_2^k \mapsto \mathbb{Z}_2^k$ определим также следующие отображения из $(\mathbb{Z}/2^n\mathbb{Z})^k$ в $\mathbb{Z}/2^{kn}\mathbb{Z}$:

$$H_{k,n} = H_k(x_1 \bmod 2^n, \ldots, x_k \bmod 2^n) \text{ и } T_{k,n,P} \circ F(x) = H_{k,n} \circ T_{k,P} \circ F(x).$$

Отметим, что $T_{k,n,P}$ и $H_{k,n}$, $T_{k,P}$ и $H_k$, очевидно, имеют обратные при любых натуральных $k$, $n$ и любой перестановки степени $2^k$, так как они являются биективными отображениями.

Для любого 1-липшицева сохраняющего меру отображения $G : \mathbb{Z}_2 \mapsto \mathbb{Z}_2$ рассмотрим разбиение $\mathbb{Z}_2$ на непересекающиеся подмножества мощности $2^k$ следующего вида:

$$\mathcal{G}_k(y_0) = \{y_0, G(y_0), \ldots, G^{2^k-1}(y_0)\},$$

где $y_0 \in \mathbb{Z}_2$, $y_0 \equiv 0 \bmod 2$, $k$ — некоторое натуральное. Тот факт, что это именно разбиение, следует из свойств отображения $G$ и доказывается теми же рассуждениями, что и для $\mathcal{F}_k$. Таким образом, можно определить отображения $T_{k,P}$ и $T_{k,n,P}$ в случае $G : \mathbb{Z}_2 \mapsto \mathbb{Z}_2$.

**Теорема 3.** Для любого 1-липшицева сохраняющего меру транзитивного по модулю 2 отображения $F : \mathbb{Z}_2^k \mapsto \mathbb{Z}_2^k$, $k > 1$, существуют такие 1-липшицево сохраняющее меру транзитивное по модулю $2^k$ отображение $G : \mathbb{Z}_2 \mapsto \mathbb{Z}_2$ и перестановка $P$ степени $2^k$, что справедливо

$$G = H_k \circ T_{k,P} \circ F \circ H_k^{-1} \quad \text{и} \quad F = H_k^{-1} \circ T_{k,P^{-1}} \circ G \circ H_k,$$

причём $F$ — эргодическое отображение тогда и только тогда, когда $G$ эргодическое.

***Доказательство.*** Возьмём произвольное 1-липшицево сохраняющее меру транзитивное по модулю $2^k$ отображение на $\mathbb{Z}_2$ и вычислим его цикл $C$ по модулю $2^k$.

Выберем такую перестановку $P$ элементов цикла отображения $H_{k,1} \circ F \circ H_{k,1}^{-1}$, чтобы получившийся цикл был равен $C$.

Для любого натурального $n$ рассмотрим $G_n = T_{k,n,P} \circ F \circ H_{k,n}^{-1}$. Очевидно, $G_n$ можно описать через некоторый граф.

При переходе $n \mapsto n+1$, $n > 1$, каждый цикл графа 1-липшицева сохраняющего меру отображения на $\mathbb{Z}_2^k$ или увеличивает в $2^k$ раз число своих элементов, или превращается в 2, 4, ..., либо $2^k$ цикла с одинаковым числом элементов (см. определение 1-липшицевости в п. 2). Каждый цикл графа 1-липшицевых сохраняющих меру отображений на $\mathbb{Z}_2$ при переходе $n \mapsto n+1$, $n > 1$, или увеличивает число своих элементов в 2 раза, или превращается в два цикла с одинаковым числом элементов. Таким образом, существует 1-липшицево сохраняющее меру отображение на $\mathbb{Z}_2$, что его граф по модулю $2^{k(n+1)}$ имеет такое же количество циклов соответствующей длины, что и граф $G_{n+1}$.

Благодаря преобразованию $T_{k,P}$, которое мы применяем к $F$, можно утверждать, что граф отображения $G_n$ может быть построен с помощью некоторого 1-липшицева сохраняющего меру отображения $\hat{G}_n$ от одной переменной ввиду $F(x) \equiv \equiv F(x \bmod 2^n) \bmod 2^n$, а значит, $G_{n+1}(y) \equiv G_n(y \bmod 2^{kn}) \bmod 2^{kn}$ (см. определение $H_k$), так как можно описать таким образом граф $G_1$ (см. начало доказательства) и соответственно — для всех последующих $G_n$ ввиду того, что при переходе $kn \mapsto k(n+1)$, $n > 1$, старшие $k$ разрядов у вершин графов по модулю $2^{kn+k}$ всех 1-липшицевых сохраняющих меру отображений от одной переменной принимают всевозможные значения, поэтому можем выбрать подходящее.

Отображение $G$ определяется как предел по $n$ отображений $\hat{G}_n \bmod 2^n$. Предел существует ввиду определения 2-адических чисел через вычеты (см. п. 1).

Свойства 1-липшицевости и сохранения меры $G$ следуют из 1-липшицевости и сохранения меры отображений $\hat{G}_n$, так как 1-липшицевость очевидна (по построению, см. определение 1-липшицевости), для сохранения меры необходима и достаточна биективность по любому модулю натуральной степени двойки в случае 1-липшицевости отображения [6], и биективность по большему модулю означает биективность по меньшему ввиду 1-липшицевости.

Рассмотрим $F_n = T_{k,n,P}^{-1} \circ G \circ H_{k,n}$ и теми же рассуждениями получим некоторое сохраняющее меру 1-липшицево отображение $\tilde{F} : \mathbb{Z}_2^k \mapsto \mathbb{Z}_2^k$. Переходя к пределу, построим последовательность векторов с координатами, представляющими собой вычеты по модулю $2^n$, а каждая координата ввиду определения 2-адических чисел из п. 1 через вычеты сходится к 2-адическому числу. Значит, предел существует.

Предположим, что $F \neq \tilde{F}$, тогда существует $x \in \mathbb{Z}_2^k$, что $F(x) \neq \tilde{F}(x)$. Отсюда у векторов $F(x)$, $\tilde{F}(x)$ должна существовать координата, в которой они отличаются. Значит, существует разряд $m \in \mathbb{N}$ в этой координате, по которому $F(x)$, $\tilde{F}(x)$ отличаются, что, в свою очередь, приводит к противоречию с равенством $F \bmod 2^n$ и $F_n$ для любого натурального $n$, так как

$$F_n = T_{k,n,P}^{-1} \circ G \circ H_{k,n}, \quad G \bmod p^{kn} = T_{k,n,P} \circ F \circ H_{k,n}^{-1}.$$

Теми же рассуждениями доказывается, что $F = H_k^{-1} \circ T_{k,P^{-1}} \circ G \circ H_k$ и соответственно $G = H_k \circ T_{k,P} \circ F \circ H_k^{-1}$. Очевидно, что $T_{k,P}^{-1} = T_{k,P^{-1}}$.

Рассмотрим вопрос эргодичности.

Необходимость следует из того, что если $F$ транзитивно по каждому модулю натуральной степени двойки (граф представляет собой один единственный цикл), то транзитивным по этим модулям будет и $G$ по построению (на самом деле по построению следует для $2^{kn}$ при любом натуральном $n$, но транзитивность по большему модулю означает транзитивность по всем меньшим ввиду 1-липшицевости), а это и означает эргодичность для 1-липшицевых сохраняющих меру отображений [6].

Действительно, воспользуемся равенством $F \bmod 2^n = T_{k,n,P}^{-1} \circ G \circ H_{k,n}$. Так как произвольная перестановка элементов на графе по некоторому модулю не влияет на свойство транзитивности по этому модулю, то $T_{k,n,P} \circ F \circ H_{k,n}^{-1}$ определяет некоторый цикл. Следовательно, $G \bmod 2^{kn}$ определит тот же цикл.

Достаточность следует из того, что все рассуждения можно повторить в обратную сторону, воспользовавшись равенством $G \bmod 2^{kn} = T_{k,n,P} \circ F \circ H_{k,n}^{-1}$. ■

## ЛИТЕРАТУРА


1. *Klimov A. and Shamir A.* Cryptographic applications of T-functions, Selected areas in cryptography // LNCS. 2004. No. 3006. P. 248–261.
2. *Anashin V. S.* Uniformly distributed sequences of $p$-adic integers // Math. Notes. 1994. V. 55. No. 1–2. P. 109–133.
3. *Anashin V. S.* Uniformly distributed sequences over $p$-adic integers // Proc. Intern. Conf. “Number Theoretic and Algebraic Methods in Computer Science”, Moscow, Juny–July 1993. World Scientific, 1995. P. 1–18.
4. *Anashin V. S.* Uniformly distributed sequences in computer algebra or how to construct program generators of random numbers // J. Math. Sci. 1998. V. 89. No. 4. P. 1355–1390.
5. *Anashin V. S.* Uniformly distributed sequences of $p$-adic integers // Discr. Math. Appl. 2002. V. 12. No. 6. P. 527–590.
6. *Anashin V. S. and Khrennikov A. U.* Applied Algebraic Dynamics. Berlin: de Gruyter Expositions in Mathematics, 2009. 558 p.
7. *Anashin V. S., Khrennikov A. U., and Yurova E.* T-functions revisited: new criteria for bijectivity/transitivity // Designs, Codes, and Cryptography. 2014. V. 71. No. 3. P. 383–407.
8. *Durand F. and Paccaut F.* Minimal polynomial dynamics on the set of 3-adic integers // Designs, Codes, and Cryptography. 2009. V. 41. No. 2. P. 302–314.
9. *Slupik A. and Sushchansky V.* Minimal generating sets and Cayley graphs of Sylow $p$-subgroups of finite symmetric groups // Algebra Discr. Math. 2009. No. 4. P. 167–184.
10. *Lavrenyuk Y. and Sushchansky V.* Automorphisms of homogeneous symmetric groups and hierarchomorphisms of rooted trees // Algebra Discr. Math. 2003. No. 4. P. 33–49.


## REFERENCES


1. *Klimov A. and Shamir A.* Cryptographic applications of T-functions, Selected areas in cryptography. LNCS, 2004, no. 3006, pp. 248–261.
2. *Anashin V. S.* Uniformly distributed sequences of $p$-adic integers. Math. Notes, 1994, vol. 55, no. 1–2, pp. 109–133.
3. *Anashin V. S.* Uniformly distributed sequences over $p$-adic integers. Proc. Intern. Conf. “Number Theoretic and Algebraic Methods in Computer Science”, Moscow, Juny–July 1993. World Scientific, 1995, pp. 1–18.
4. *Anashin V. S.* Uniformly distributed sequences in computer algebra or how to construct program generators of random numbers. J. Math. Sci., 1998, vol. 89, no. 4, pp. 1355–1390.
5. *Anashin V. S.* Uniformly distributed sequences of $p$-adic integers. Discr. Math. Appl., 2002, vol. 12, no. 6, pp. 527–590.

6. *Anashin V. S. and Khrennikov A. U.* Applied Algebraic Dynamics. Berlin, de Gruyter Expositions in Mathematics, 2009. 558 p.
7. *Anashin V. S., Khrennikov A. U., and Yurova E.* T-functions revisited: new criteria for bijectivity/transitivity. Designs, Codes, and Cryptography, 2014, vol. 71, no. 3, pp. 383–407.
8. *Durand F. and Paccaut F.* Minimal polynomial dynamics on the set of 3-adic integers. Designs, Codes, and Cryptography, 2009, vol. 41, no. 2, pp. 302–314.
9. *Slupik A. and Sushchansky V.* Minimal generating sets and Cayley graphs of Sylow $p$-subgroups of finite symmetric groups. Algebra Discr. Math., 2009, no. 4, pp. 167–184.
10. *Lavrenyuk Y. and Sushchansky V.* Automorphisms of homogeneous symmetric groups and hierarchomorphisms of rooted trees. Algebra Discr. Math., 2003, no. 4, pp. 33–49.