МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра системного анализа и автоматического управления

Отчет по заданию 3. Вариант 29

Студента 3 курса 321 группы направления 09.03.01 ИВТ
Факультета компьютерных наук и информационных технологий
Чесакова Максима Евгеньевича

Задача №1 Транзитивна ли заданная функция $h : \mathbb{Z}_2 \to \mathbb{Z}_2$? Решить задачу аналитически, затем проверить с помощью программной реализации транзитивность по модулю 256.

$h(x) = (x \oplus 1) \oplus$
$(2(x \wedge (1 + 2x) \wedge (3 + 4x) \wedge (7 + 8x) \wedge (15 + 16x) \wedge (31 + 32x) \wedge (63 + 64x))) \oplus$
$(4(x^2 + \mathbf{29}))$

Аналитическое решение. $h(x)$ не является многочленом над $\mathbb{Z}_2$, следовательно, критерий транзиивности многочленов не работает.

Функция h есть композиция арифметических и логических операций: сложения, умножения, XOR и AND, следовательно, функция h 1-Липшицева, поскольку композиция 1-Липшицевых функций — 1-Липшицева. Значит, нашу функцию h можно записать в виде ряда

$$h(x) = \sum_{i=0}^{\infty} \psi_i(x_0, ..., x_i)2^i,$$

где $\psi_i : \{0, 1\}^{i+1} \to \{0, 1\}$.

Представим нашу функцию h в виде поразрядной суммы трех функций

$$h(x) = F_0(x) \oplus 2F_1(x) \oplus 4F_2(x),$$

где $F_0(x) = x \oplus 1$,
$F_1(x) = x \wedge (1 + 2x) \wedge (3 + 4x) \wedge (7 + 8x) \wedge (15 + 16x) \wedge (31 + 32x) \wedge (63 + 64x)$,
$F_2(x) = x^2 + \mathbf{29}$.

Координатные функции для $F_0(x)$:

$$\delta_0(F_0(x)) = \delta_0(x) \oplus 1 = x_0 \oplus 1,$$

$$\delta_1(F_0(x)) = \delta_1(x) = x_1,$$

$$\delta_2(F_0(x)) = \delta_2(x) = x_2,$$

$$\dots$$

$$\delta_i(F_0(x)) = \begin{cases} x_0 \oplus 1, & \text{если } i = 0 \\ x_i, & \text{если } i > 0. \end{cases}$$

Координатные функции для $2F_1(x)$:

$$\delta_0(2F_1(x)) = 0, \qquad \delta_i(2F_1(x)) = \delta_{i-1}(F_1(x)), \quad \text{при } i = 1, 2, \dots$$

$$\delta_0(F_0 \oplus (2F_1(x))) = \delta_0(x) \oplus 1,$$

$$\delta_i(F_0 \oplus (2F_1(x))) = \delta_i(x) \oplus \delta_{i-1}(F_1(x)), \quad \text{для } i = 1, 2, \dots$$

Координатные функции для $F_1(x)$:

$$\begin{aligned} &\delta_0(F_1(x)) = \delta_0(x); \\ &\delta_1(F_1(x)) = \delta_1(x) \cdot \delta_0(x); \\ &\delta_2(F_1(x)) = \delta_2(x) \cdot \delta_1(x) \cdot \delta_0(x); \\ &\delta_3(F_1(x)) = \delta_3(x) \cdot \delta_2(x) \cdot \delta_1(x) \cdot \delta_0(x); \\ &\qquad\qquad \dots \\ &\delta_6(F_1(x)) = \delta_6(x) \cdot \dots \cdot \delta_1(x) \cdot \delta_0(x). \end{aligned}$$

В общем виде:

$$\delta_i(F_1(x)) = \delta_i(x) \cdot \dots \cdot \delta_{\max\{0,\, i-6\}}(x).$$

Координатные функции для $4F_2(x)$:

$$\delta_0(4F_2(x)) = 0, \qquad \delta_1(4F_2(x)) = 0, \qquad \delta_i(4F_2(x)) = \delta_{i-2}(F_2(x)), \quad \text{при } i = 2, 3, \dots$$

Координатные функции для h:

$$\delta_0(h(x)) = \delta_0(x) \oplus 1 = 1 \oplus x_0;$$

$$\delta_1(h(x)) = \delta_1(x) \oplus \delta_0(x) = x_1 \oplus x_0;$$

$$\delta_i(h(x)) = \delta_i(x) \oplus [\delta_{i-1}(x) \cdot \ldots \cdot \delta_{\max\{0,\, i-7\}}(x)] \oplus \delta_{i-2}(F_2(x)), i = 2, 3, \ldots$$

Заметим, что $\delta_{i-2}(F_2(x))$ не зависит от $\delta_{i-1}(x)$.

В итоге имеем:

$$h(x) = \sum_{i=0}^{\infty} \psi_i(x_0, ..., x_i) 2^i, \tag{1}$$

Здесь

$$\psi_0(x_0) = 1 \oplus \delta_0(x) = 1 \oplus x_0,$$

$$\psi_1(x_0, x_1) = \delta_1(x) \oplus \delta_0(x) = x_1 \oplus x_0,$$

$$\psi_i(x_0, \ldots, x_i) = \delta_i(f(x)) = x_i \oplus \Phi_i(x_0, \ldots, x_{i-1}),$$

где $\Phi_i(x_0, \ldots, x_{i-1})$ есть АНФ степени i и $\Phi_0(x_0) = 1$.

Представление функций из $\mathbb{Z}_2$ в $\mathbb{Z}_2$ с помощью координатных функций позволяет определить, принадлежит ли функция классу сохраняющих меру или эргодических функций. При этом используется установленный фольклорный критерий для 2-адических 1-липшицевых функций.

Теорема 1 (фольклор). Функция f, определенная равенством (1), сохраняет меру тогда и только тогда, когда для каждого $i = 0, 1, 2, \ldots$ АНФ i-й координатной функции есть

$$\psi_i(x_0, \ldots, x_i) = x_i \oplus \phi_i(x_0, \ldots, x_{i-1}),$$

где ϕ_i есть АНФ от булевой функции от булевых переменных $x_0, \ldots, x_{i-1}$ и ϕ_0 есть константа из $\{0, 1\}$.

Функция f эргодична тогда и только тогда, когда, дополнительно, $\phi_0 = 1$, и каждая булева функция ϕ_i имеет нечетный вес, т.е. принимает значение 1 в точности в нечетном числе точек из $\{0, 1\}^i$ для $i = 1, 2, \ldots$. Последнее условие выполнено тогда и только тогда, когда степень АНФ ϕ_i для $i \geq 1$ в точности равна 1, т.е. тогда и только тогда, когда АНФ ϕ_i содержит моном $x_0 \cdots x_{i-1}$.

Теорема 2 (основная эргодическая). Пусть функция $f : \mathbb{Z}_p^n \to \mathbb{Z}_p^m$, $m \leq n$, есть 1-липшицева функция. Если $m = n$, функция f сохраняет меру μ_p (является эргодической) тогда и только тогда, когда f биективна по модулю p^k (транзитивна по модулю p^k) при всех $k = 1, 2, 3, \ldots$ (при достаточно больших значениях k). При $m \leq n$ функция f сохраняет меру μ_p тогда и только тогда, когда f сбалансирована по модулю p^k при всех $k = 1, 2, 3, \ldots$ (при достаточно больших значениях k).

Из построения по теореме 1 следует, что исследуемая 1-Липшицева функция $h(x)$

эргодична, из чего по теореме 2 следует её транзитивность в целом и по модулю 256 в частности.

Ответ: Да. функция транзитивна.

Программная реализация на Python. Полный код программы приведён в файле.

Программа вычисляет вычеты по модулю 256 и проверет, составляют ли они одноцикловую перестановку. Результат работы программы представлен на рисунке.

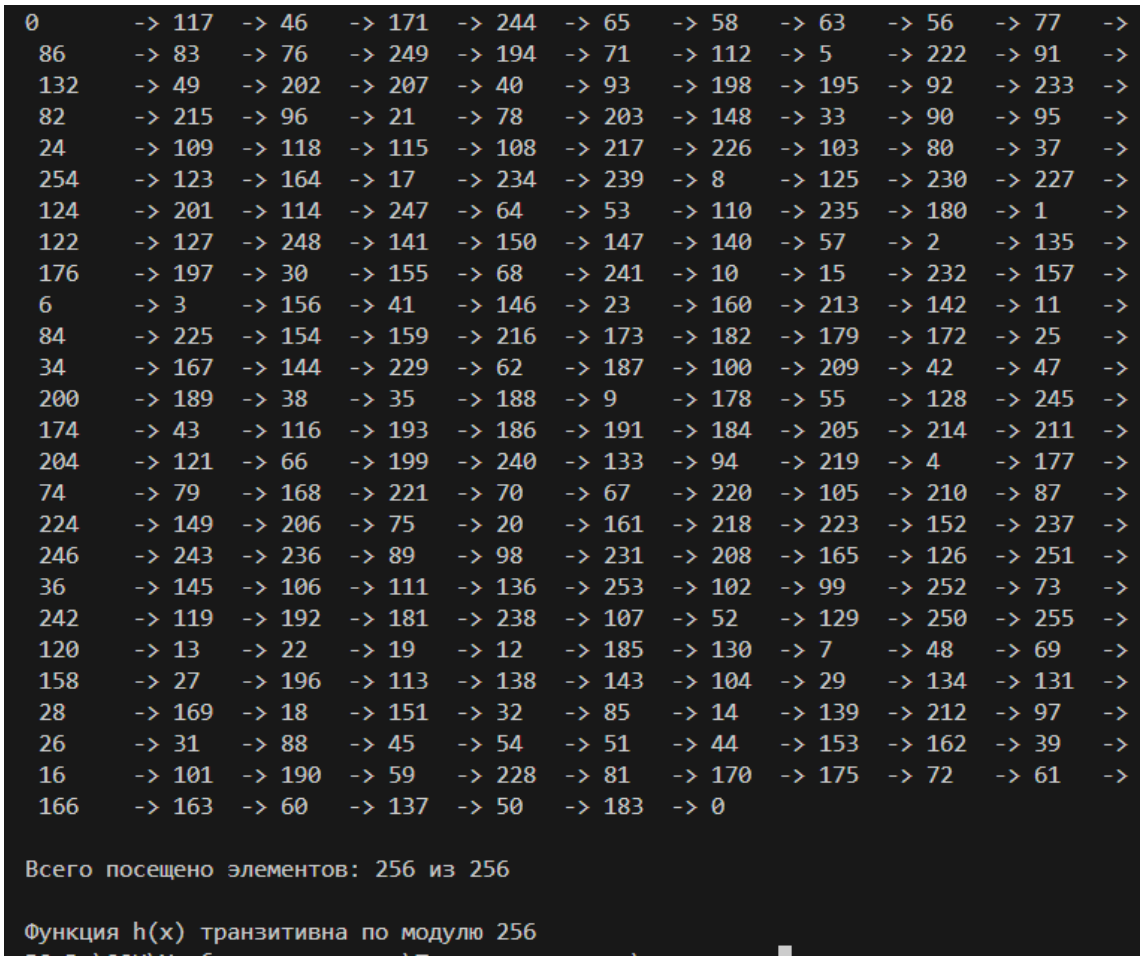

Рисунок 1 – Проверка $h(x)$

1