Инструментарий для работы с псевдослучайными последовательностями

Генерация псевдослучайных последовательностей на основе моделей хаотической динамики и анализ их свойств.

Динамический хаос

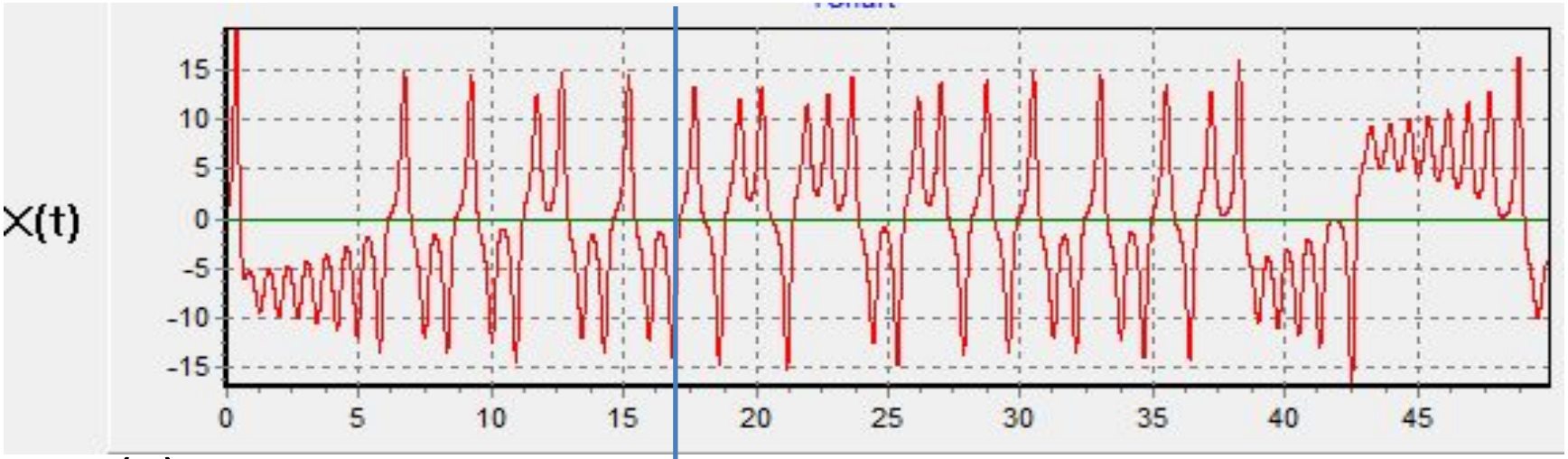
Существуют динамические системы

$$\begin{cases} x' = f_x(t, x, y, z) \\ y' = f_y(t, x, y, z) \\ z' = f_z(t, x, y, z) \end{cases}$$

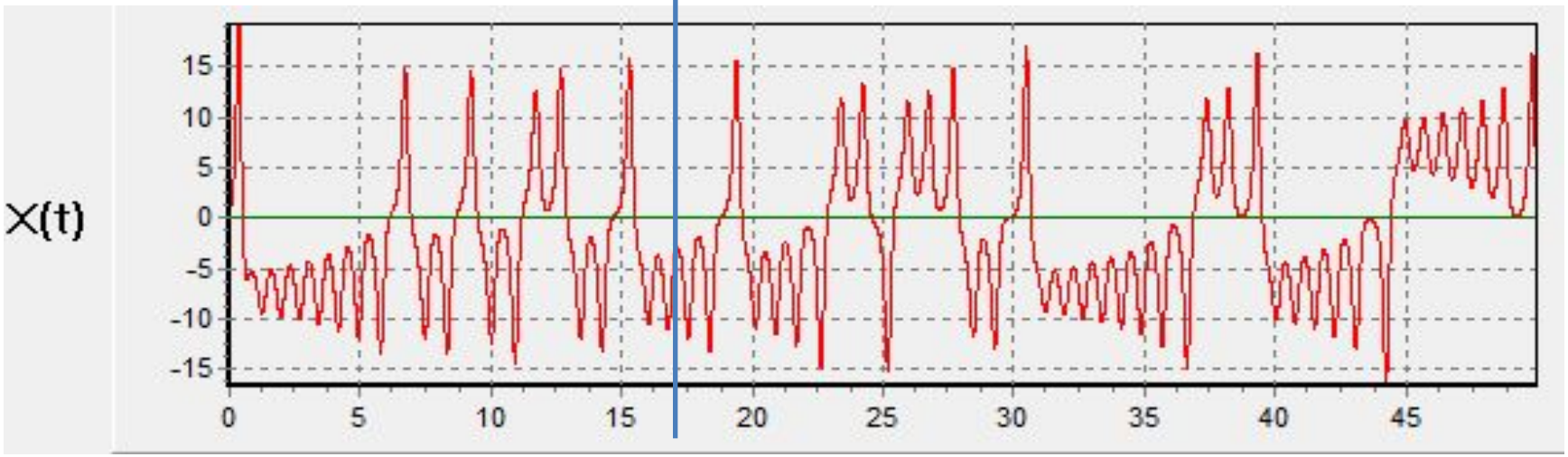
решение которых обладает хаотическими свойствами.

Динамический хаос

- X(0)=1



- X(0)=1,001



Постановка задачи

Разработать набор программных средств для

1) решения системы ОДУ,
2) генерации на основе получаемых решений бинарных последовательностей,
3) анализа статистических свойств полученных последовательностей .

Работа с динамической моделью

Для решения системы ОДУ используется метод Рунге-Кутты 4-ого порядка точности.

$$\begin{cases} x_{i+1} = x_i + \frac{h}{6}(k1_x + 2k2_x + 2k3_x + k4_x) \\ y_{i+1} = y_i + \frac{h}{6}(k1_y + 2k2_y + 2k3_y + k4_y) \\ z_{i+1} = z_i + \frac{h}{6}(k1_z + 2k2_z + 2k3_z + k4_z) \end{cases}$$

Расшифровка коэффициентов

$$k1_j = f_j(t_j, x_i, y_i, z_i)$$

$$k2_j = f_j\left(x_i + k1_j\frac{h}{2}, y_i + k1_j\frac{h}{2}, z_i + k1_j\frac{h}{2}\right)$$

$$k3_j = f_j(x_i + k2_j\frac{h}{2}, y_i + k2_j\frac{h}{2}, z_i + k2_j\frac{h}{2})$$

$$k4_j = f_j(x_i + k3_j h, y_i + k3_j h, z_i + k3_j h)$$

Формирование бинарной последовательности

- Полученное решение разбивается на отрезки определенной длины.
- На каждом отрезке подсчитывается количество пиков функции-решения.
- Если на отрезке количество пиков четно, то в бинарную последовательность добавляется значение 0, если нечетно – 1.

Формирование бинарной последовательности

Рассматривается несколько вариантов определения пиков

- 1) $\begin{cases} abs(X_{i-1}) < abs(X_i) \\ abs(X_{i+1}) < abs(X_i) \end{cases}$
- 2) $\begin{cases} X_{i-1} < X_i \\ X_{i+1} < X_i \end{cases}$
- 3) $\begin{cases} X_i < X_{i-1} \\ X_i < X_{i+1} \end{cases}$

Анализ «случайности» построенной последовательности

- Для определения статистических свойств полученной бинарной последовательности применяются следующие тесты.

1)Частотный тест

$$V_1 = \frac{(n_0 - n_1)^2}{n_0 + n_1}$$

Анализ «случайности» построенной последовательности

- Для определения статистических свойств полученной бинарной последовательности применяются следующие тесты.

1)Частотный тест

$$V_1 = \frac{(n_0 - n_1)^2}{n_0 + n_1}$$

Анализ «случайности» построенной последовательности

- Для определения статистических свойств полученной бинарной последовательности применяются следующие тесты.

1)Частотный тест

$$V_1 = \frac{(n_0 - n_1)^2}{n_0 + n_1}$$

Анализ «случайности» построенной последовательности

- Для определения статистических свойств полученной бинарной последовательности применяются следующие тесты.

1)Частотный тест

$$V_1 = \frac{(n_0 - n_1)^2}{n_0 + n_1}$$

Анализ «случайности» построенной последовательности

- Для определения статистических свойств полученной бинарной последовательности применяются следующие тесты.

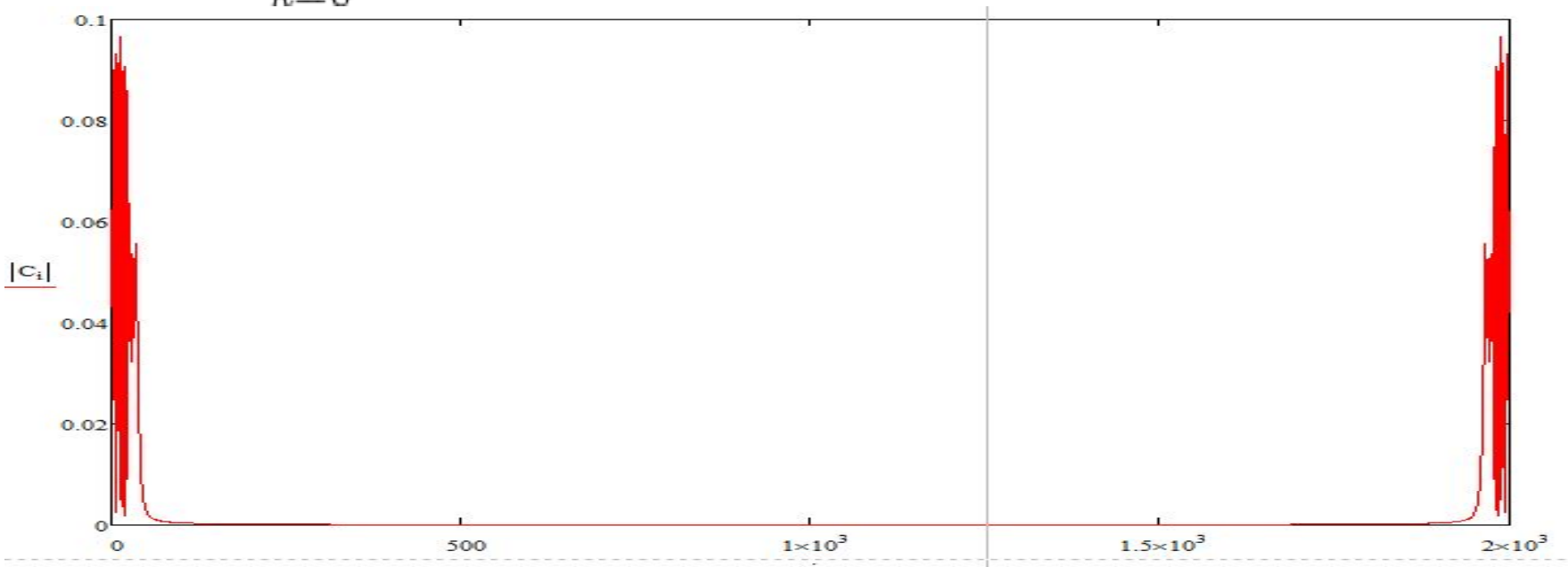
1)Частотный тест

$$V_1 = \frac{(n_0 - n_1)^2}{n_0 + n_1}$$

Анализ «случайности» построенной последовательности

- 5) Проверка спектра Фурье.

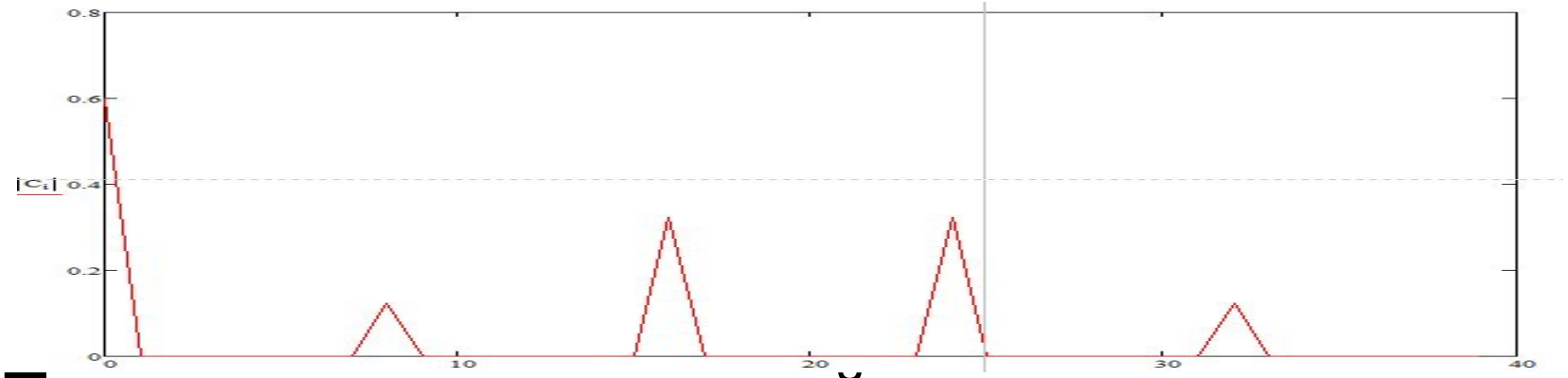
$$x_n = \frac{1}{N} \sum_{k=0}^{N-1} X_k e^{\frac{2\pi i}{N} kn} \qquad n = 0, \ldots, N-1.$$



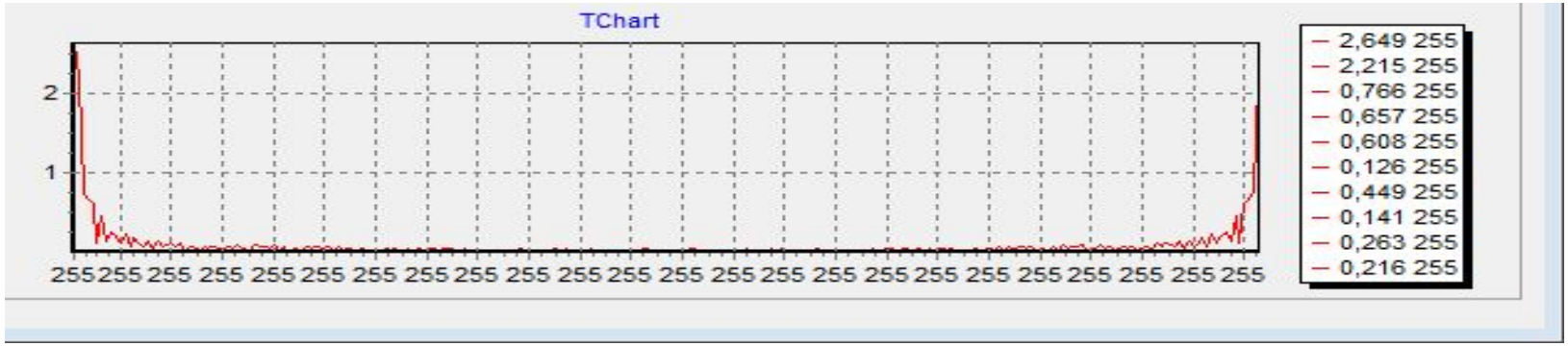
Коэффициенты исходной последовательности

Анализ «случайности» построенной последовательности

Если исходная последовательность неслучайна



Если исходная - случайна



Пример

Для определения статистических свойств полученной бинарной последовательности применяются следующие тесты.

1)Частотный тест

$$V_1 = \frac{(n_0 - n_1)^2}{n_0 + n_1}$$

Численный эксперимент

Начальные условия примем такие:

X(0)=1; Y(0)=1; Z(0)=1;

h=0,01; (шаг Рунге-Кутты)

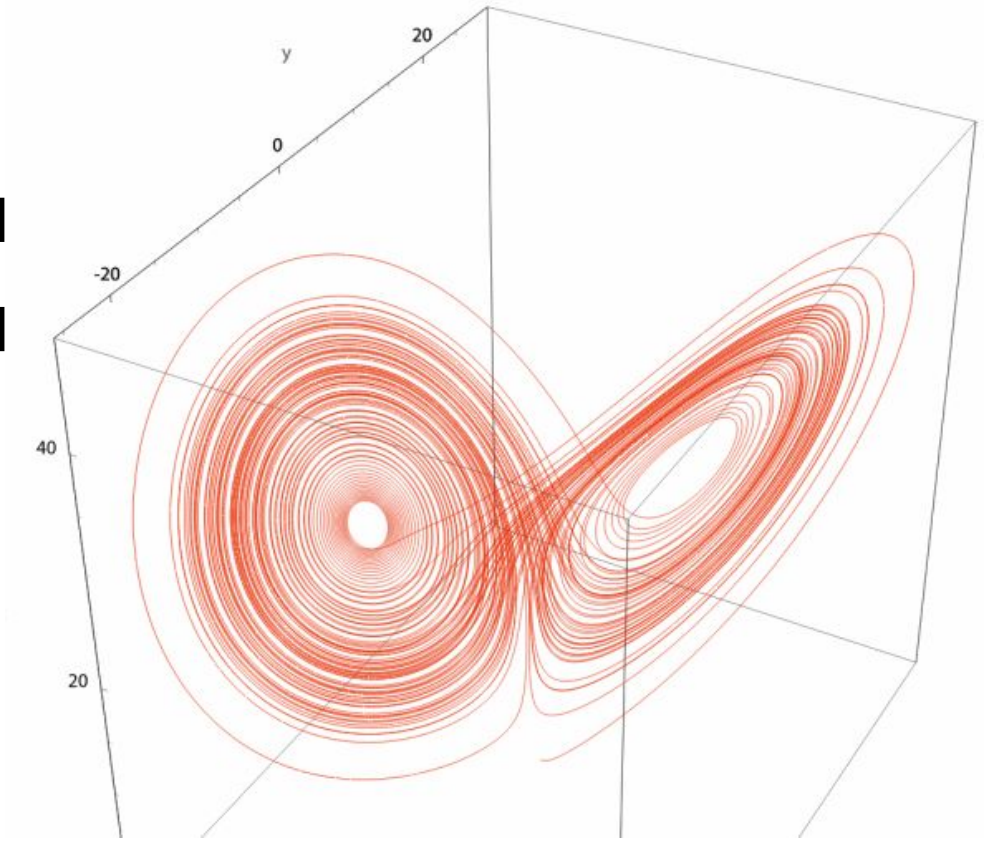
n=1000; (количество шагов)

k=10; (количество отрезков слежения)

T0=1;

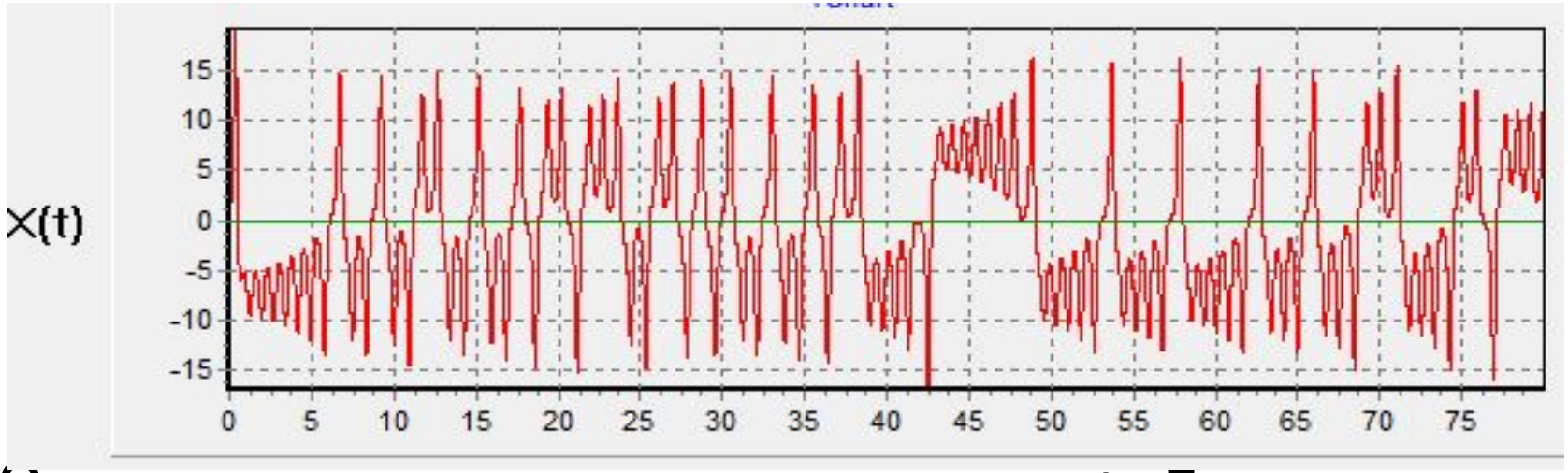
Фазовый портрет решения

С течением времен
решение выходит н
хорошо видимый
аттрактор и
хаотически
блуждает по нему.



Численный эксперимент

Решение приведем для X(t):



Заметим, что после значения t=5 наблюдается квазицикличность – решение вышло на аттрактор.

Численный эксперимент

- Для получения более длиной последовательности можно продлевать отрезок расчета.
- После подсчета и упрощения получим такую бинарную последовательность:

0000111100001110001000011110011100 0…

Значения статистик

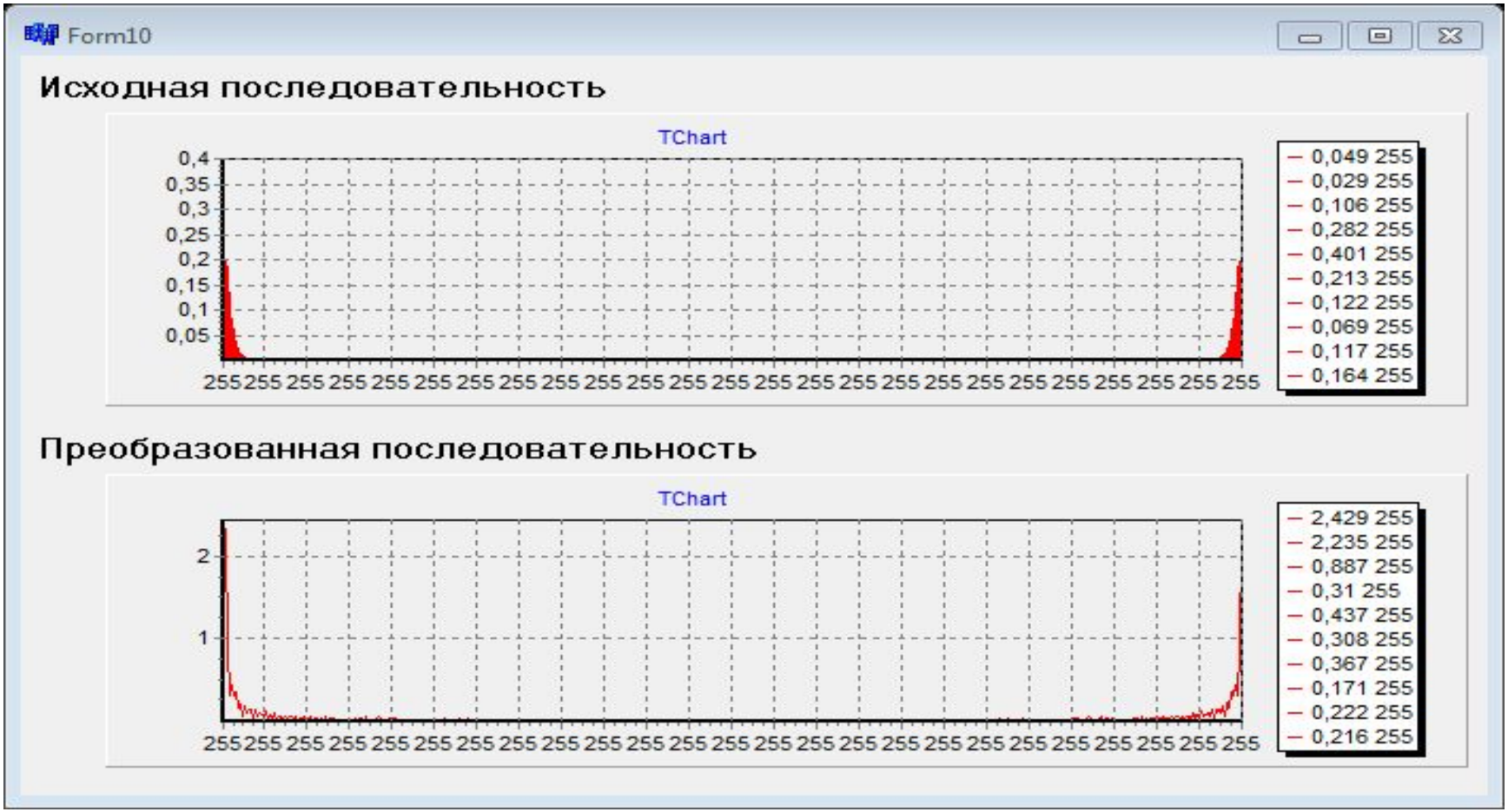
- Для определения статистических свойств полученной бинарной последовательности применяются следующие тесты.

1)Частотный тест

$$V_1 = \frac{(n_0 - n_1)^2}{n_0 + n_1}$$

Значения статистик

- Спектр Фурье будет выглядеть так:



Спасибо за внимание