И. С. Кижватов

Особенности распределения выходных последовательностей усечённых конгруэнтных генераторов

Дипломная работа

Научный руководитель
д. ф.-м. н., проф. В. С. Анашин

Структура работы

Часть 1.

Сравнительная оценка равномерности распределения псевдослучайных последовательностей

Исследование эффективности критериев оценки

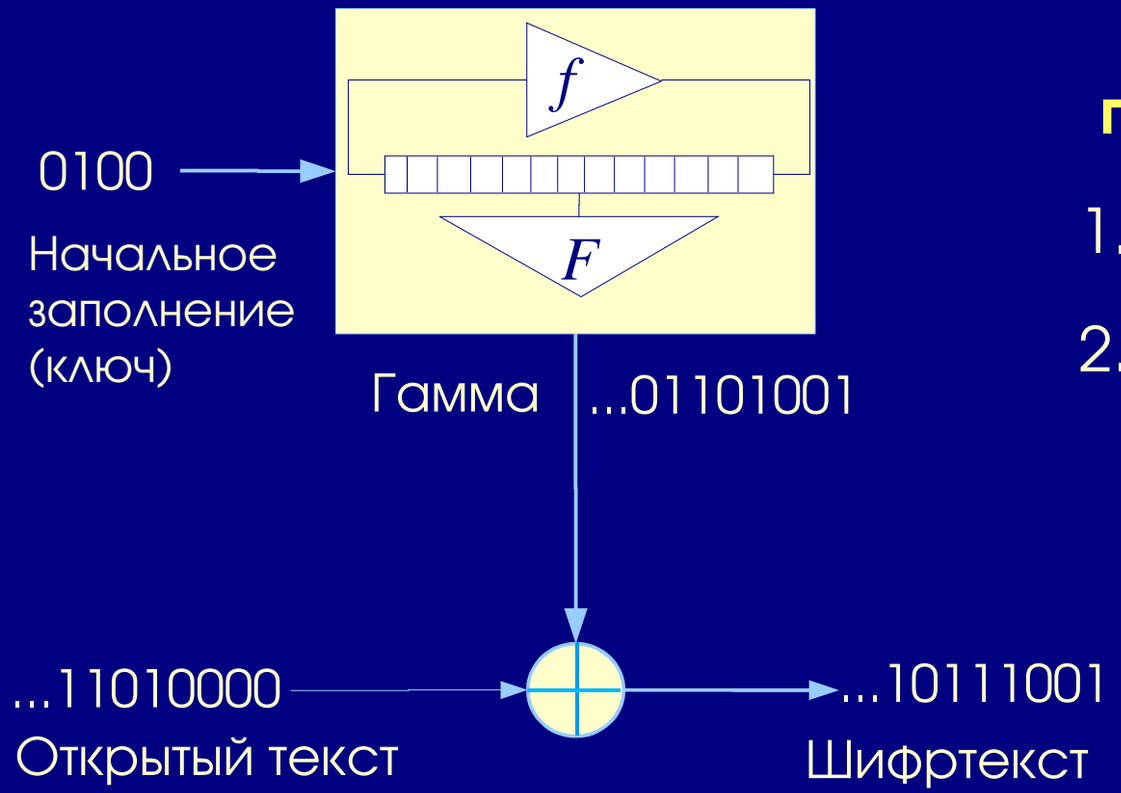
Часть 2.

Доказательство теоремы об условиях максимальности периода последовательности.

Результаты работы

Построение псевдослучайных генраторов большого периода для схем поточного шифрования с простой программной реализацией.

Псевдослучайные генераторы в поточных шифрах

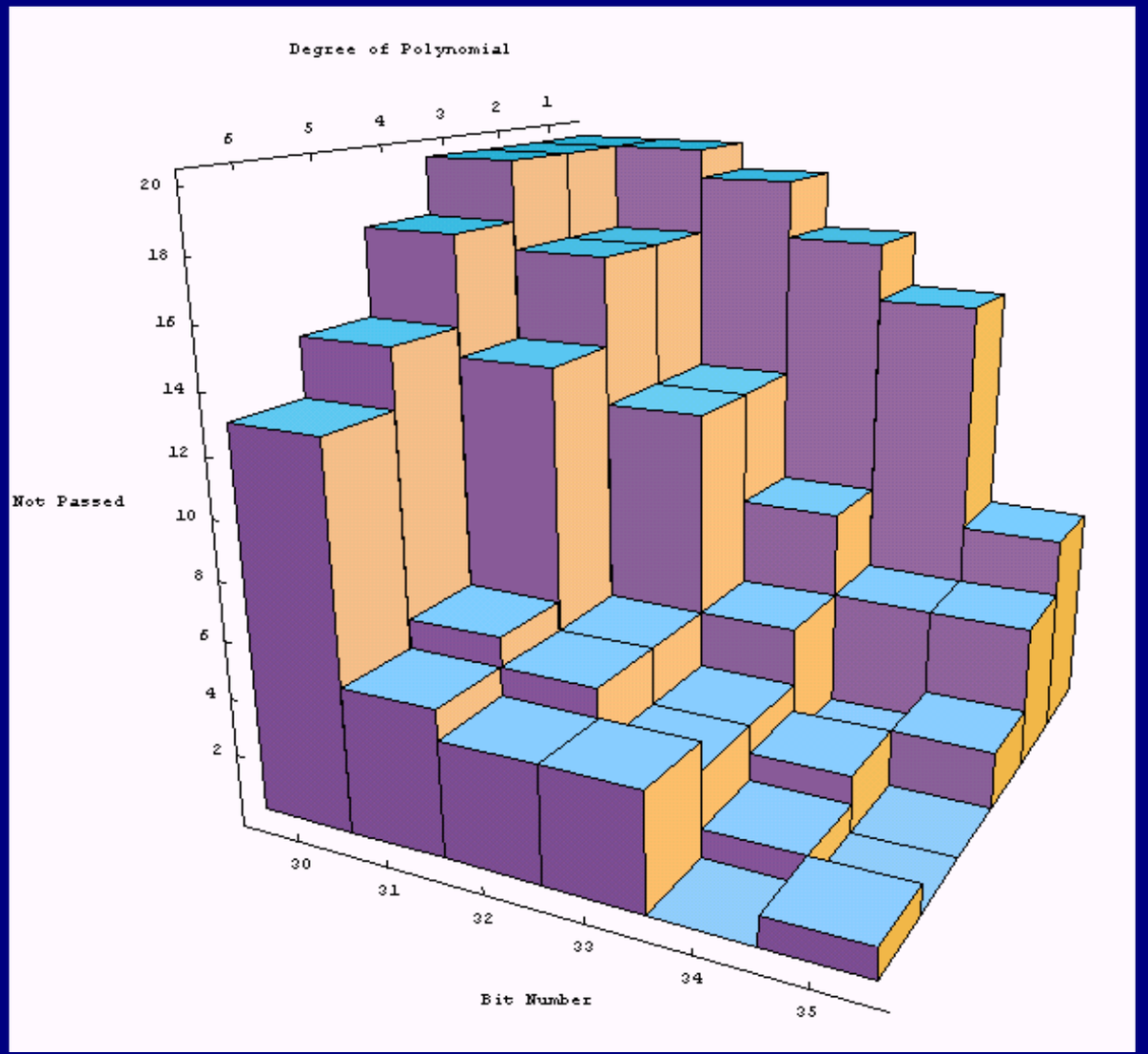


Требования к последовательности

1. Большой период
2. Равномерное распределение

Особенности распределения выходных последовательностей усечённых конгруэнтных генераторов

Часть первая. Сравнительная характеристика распределения последовательностей



Число не прошедших батарею тестов **DIEHARD** последовательностей

Генераторы – транзитивные (mod 2^{64}) полиномы с целыми коэффициентами степени 1–6.

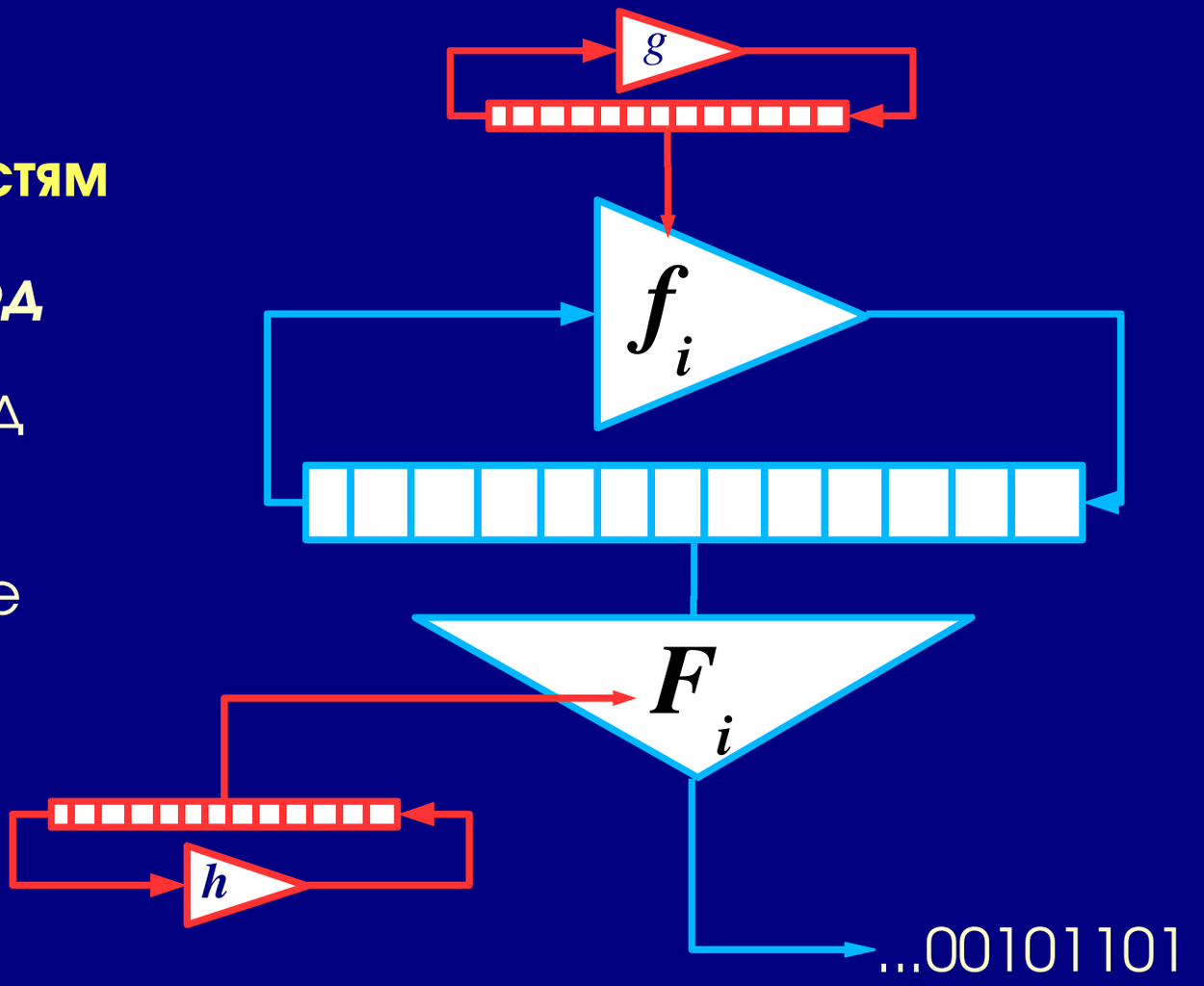
20 генераторов каждой степени

Съём последовательностей с разрядов 30–35.

Генератор с изменяющимися функциями перехода и выхода (неавтономный генератор)

Требования к управляющим последовательностям

1. ***Нечётный период***
2. Большой период
2. Равномерное распределение



Часть вторая. Доказательство теоремы об условиях максимальности периода последовательности.

Теорема (троичный случай).

Функция обладает максимальным периодом по модулю 3^k при любой натуральной k, если она представима в виде

$$f(x) = c_0 + x + \sum_{i=1}^{\infty} c_i 3^{\lfloor \log_3 i \rfloor + 1} \binom{x}{i},$$

$$c_i \in \mathbb{Z}_3,$$

$$c_0 \not\equiv 0 \pmod 3.$$

Теорема (общий случай).

Функция обладает максимальным периодом по модулю p^k при любой натуральной k, если она представима в виде

$$f(x) = c_0 + x + \sum_{i=1}^{\infty} c_i p^{\lfloor \log_p (i+1) \rfloor + 1} \binom{x}{i},$$

$$c_i \in \mathbb{Z}_p,$$

$$c_0 \not\equiv 0 \pmod p.$$

Часть вторая. Доказательство теоремы об условиях максимальности периода последовательности.

Теорема (критерий максимальности периода по модулю 9).

Функция, представленная в виде

$$f(x) = b_0 + \sum_{i=1}^{8} b_i 3^{\lfloor \log_3 i \rfloor} \binom{x}{i} \pmod 9,$$

обладает максимальным периодом по модулю ***9,*** если

$$\begin{aligned} b_0 &\not\equiv 0, \\ b_1 &\equiv 1, \pmod 3 \\ b_2 \equiv b_6 \equiv b_7 \equiv b_8 &\equiv 0, \end{aligned}$$

и одновременно выполняются сравнения по модулю 3 одного из наборов

(1)

$$b_3 \equiv b_4 \equiv b_5 \equiv 0,$$
$$\delta_0(b_0) + \delta_1(b_2) \not\equiv 0,$$

(2)

$$b_3 \equiv 0,$$
$$b_4 \equiv 1,$$
$$b_5 \equiv -1,$$
$$\delta_1(b_0) + \delta_0(b_0) \cdot [\delta_1(b_1) + \delta_1(b_2) - 1] - (\delta_0(b_0))^2 \not\equiv 0,$$

(3)

$$b_3 \equiv 1,$$
$$b_4 \equiv -1,$$
$$b_5 \equiv -1,$$
$$\delta_1(b_0) + \delta_0(b_0) \cdot [\delta_1(b_1) - \delta_1(b_2)] + (\delta_0(b_0))^2 \cdot [\delta_1(b_1) - 1] \not\equiv 0,$$

(4)

$$b_3 \equiv 1,$$
$$b_4 \equiv 0,$$
$$b_5 \equiv -1,$$
$$\delta_1(b_0) + \left[\delta_0(b_0) + (\delta_0(b_0))^2\right][\delta_1(b_1) - 1] \not\equiv 0.$$

Особенности распределения выходных последовательностей усечённых конгруэнтных генераторов

Результаты работы

1. Выработаны рекомендации по выбору соотношения длины регистра и степени генератора.

2. Установлено, что алгоритм машинного обучения не является жёстким критерием оценки равномерности распределения

3. Расширен класс функций, порождающих последовательности максимальной длины по модулю 3^k.

Продолжение работы

Описание всего класса функций, обладающих максимальным периодом 3^k, изучение свойств построенных на их основе генераторов.

Практическое применение результатов

Построение функций, обладающих максимальным периодом

$$f(x) = 3141592 + 271828 \cdot x + 372 \cdot \binom{x}{2} + 21789 \cdot \binom{x}{8}$$

Функция порождает последовательности максимальной длины 3^k по модулю 3^k при любой натуральной k.

Особенности распределения выходных последовательностей усечённых конгруэнтных генераторов

Практическое применение результатов

Построение функций, обладающих максимальным периодом

$$f(x) = 8 + 7 \cdot x + 9 \cdot \binom{x}{6} + 3483 \cdot \binom{x}{80}$$

Функция порождает последовательности максимальной длины 3^k по модулю 3^k при любой натуральной k.

Случайная последовательность

- последовательность ***независимых*** случайных чисел с ***заданным распределением***

... 0 1 1 0 1 0 0 1

ближе к ***ожидаемому среднему повдению*** случайной последовательности, чем

... 1 0 0 0 0 0 0 1

Часть первая. Сравнительная оценка качества последовательностей

Критерии оценки качества распределения последовательности

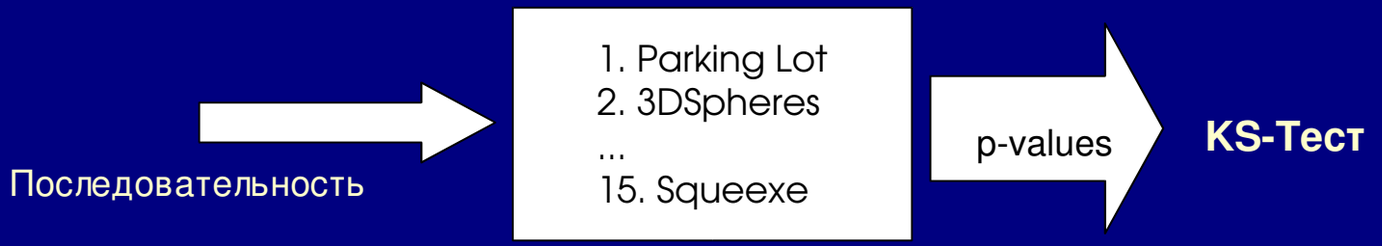
1. Теоретические (строгие)

2. Эмпирические (применяютя к любой последовательности)

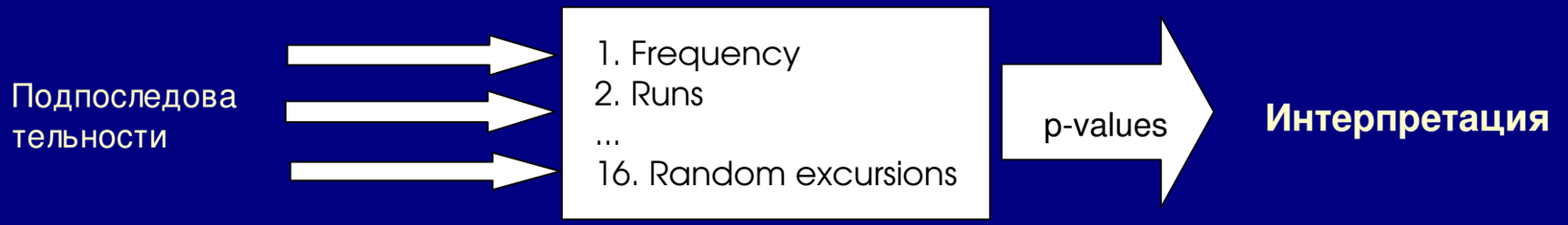
Часть первая. Сравнительная оценка качества последовательностей

Пакеты эмпирических тестов:

1. DIEHARD (*George Marsaglia*)

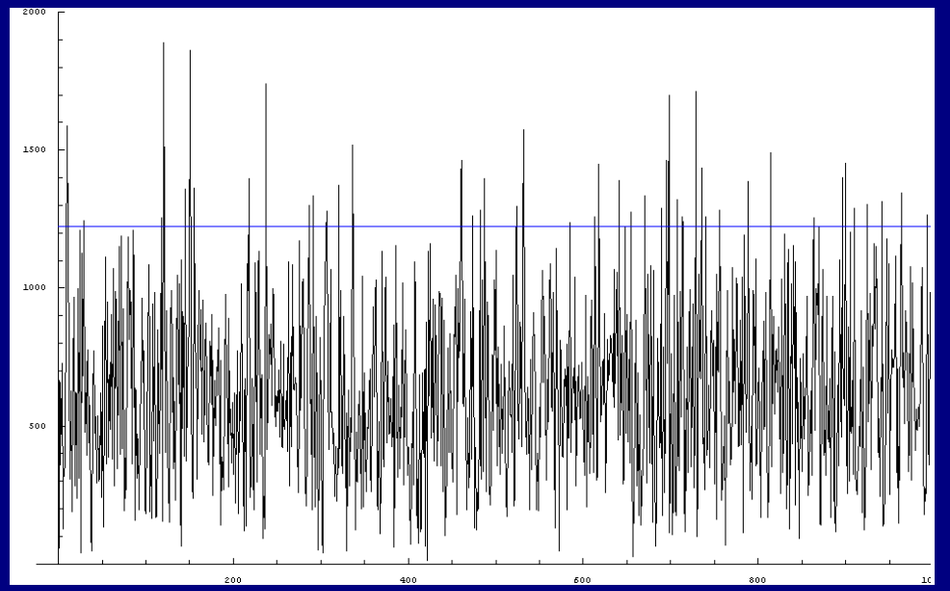


2. NIST statistical Test Suite (*A. Rukhin et al*)

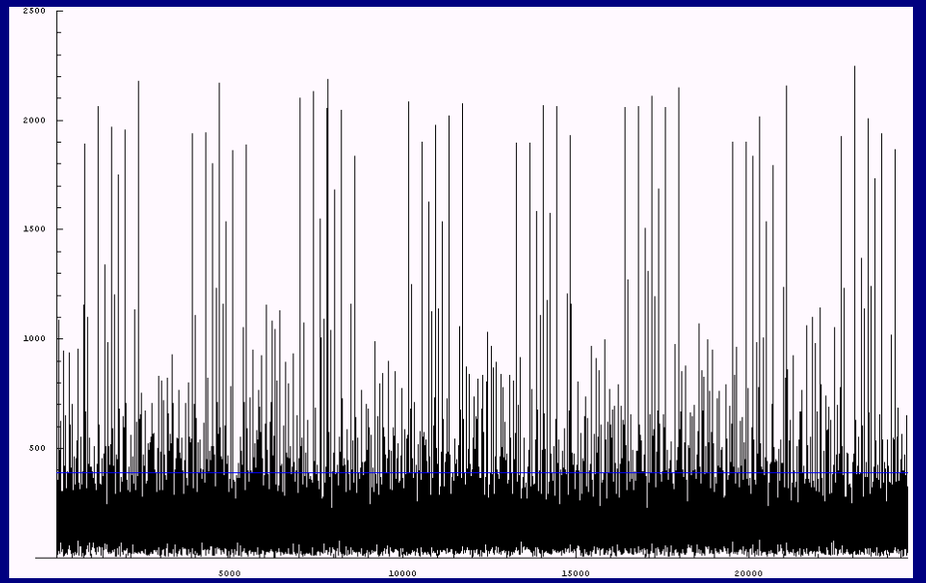


Особенности распределения выходных последовательностей усечённых конгруэнтных генераторов

Результаты тестов NIST: FFT.

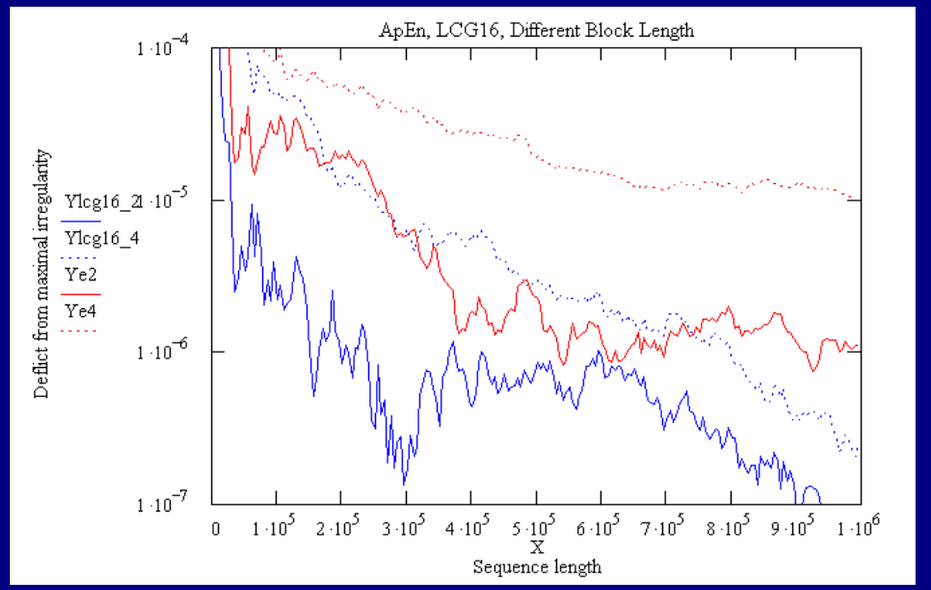


Генератор 6 степени

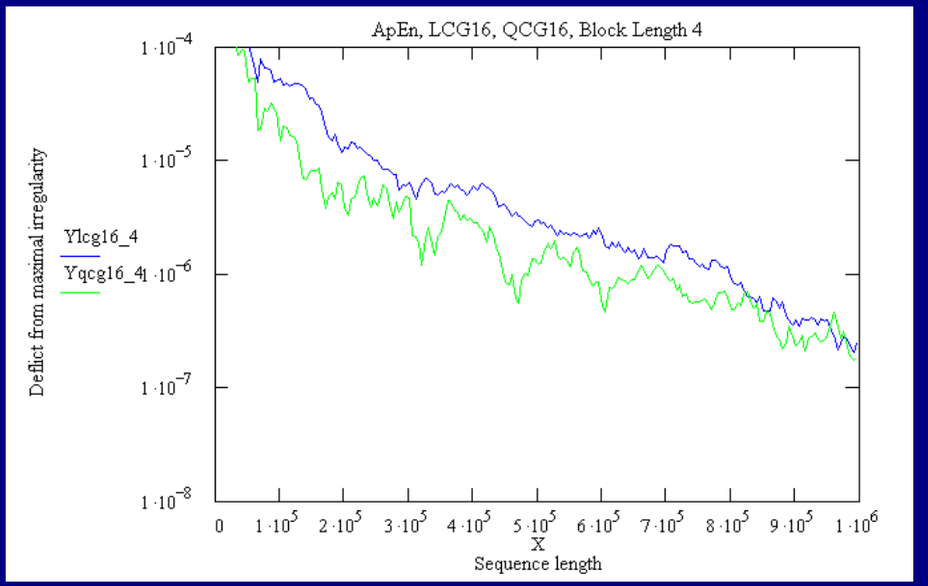


Линейный конгруэнтный генератор

Результаты тестов NIST: Approximate Entropy



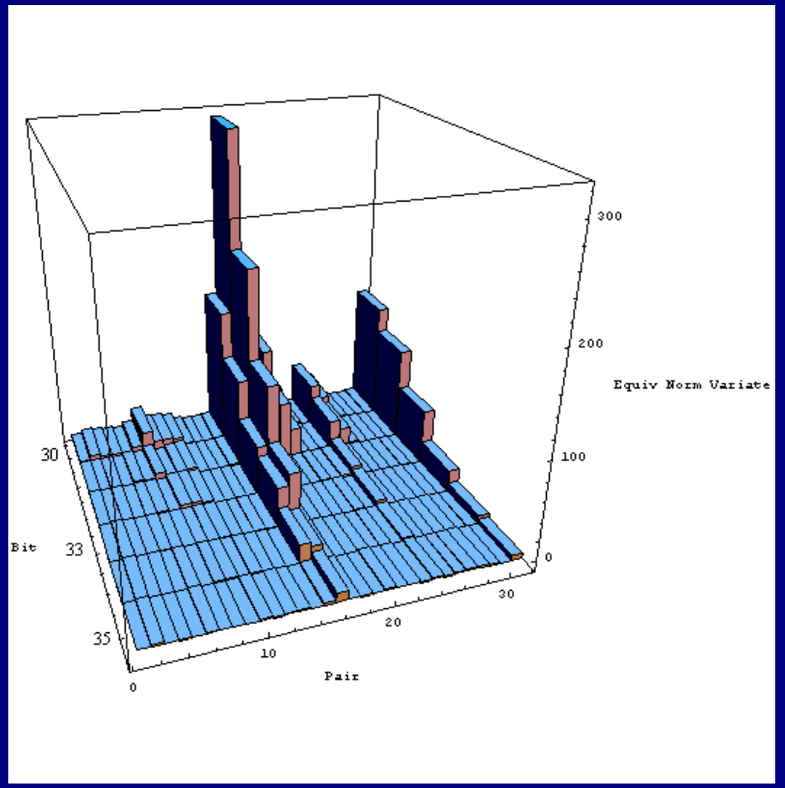
Линейный генератор и число ***e***



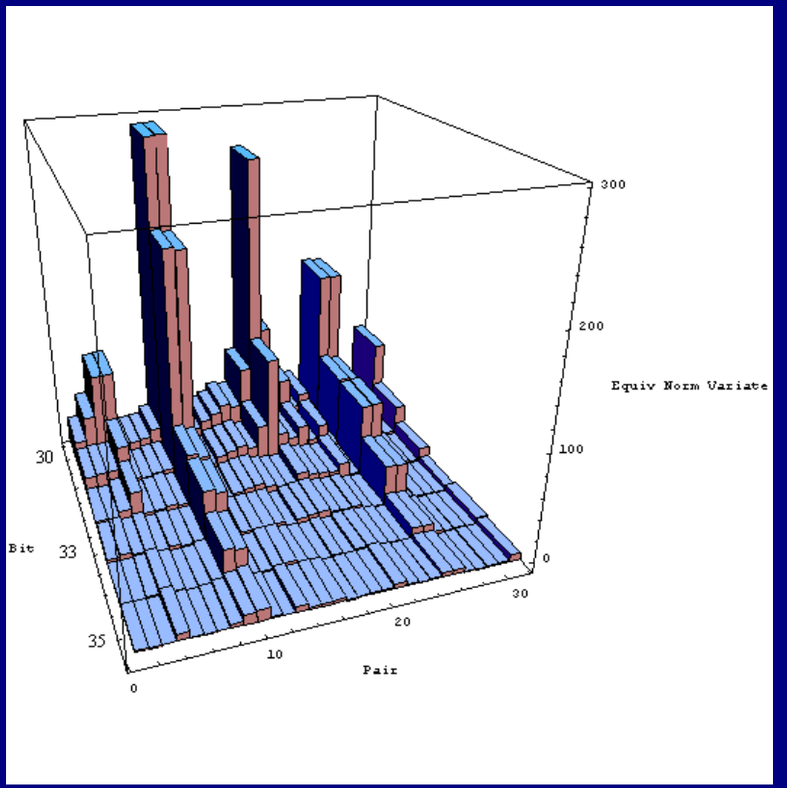
Линейный и квадратичный генераторы

Особенности распределения выходных последовательностей усечённых конгруэнтных генераторов

Результаты тестов DIEHARD: DNA



Генератор 4 степени



Генератор 6 степени