Курсовая работа
на тему:
«Тестирование генераторов случайных чисел»

Выполнил студент группы И-217А:
Ольховский Станислав
Руководитель работы, доцент:
Некрасова. М. В

Генераторы

Генераторы

- физические

Генераторы

- физические
- табличные

Генераторы

- физические
- табличные
- алгоритмические

Первые алгоритмы

«Всякий, кто питает слабость к арифметическим методам получения случайных чисел, грешен вне всяких сомнений»

Джон фон Нейман

Первые алгоритмы

- Метод серединных квадратов

Первые алгоритмы

- Метод серединных квадратов

Первые алгоритмы

- Метод серединных квадратов

Первые алгоритмы

- Метод серединных квадратов
- Метод серединных произведений

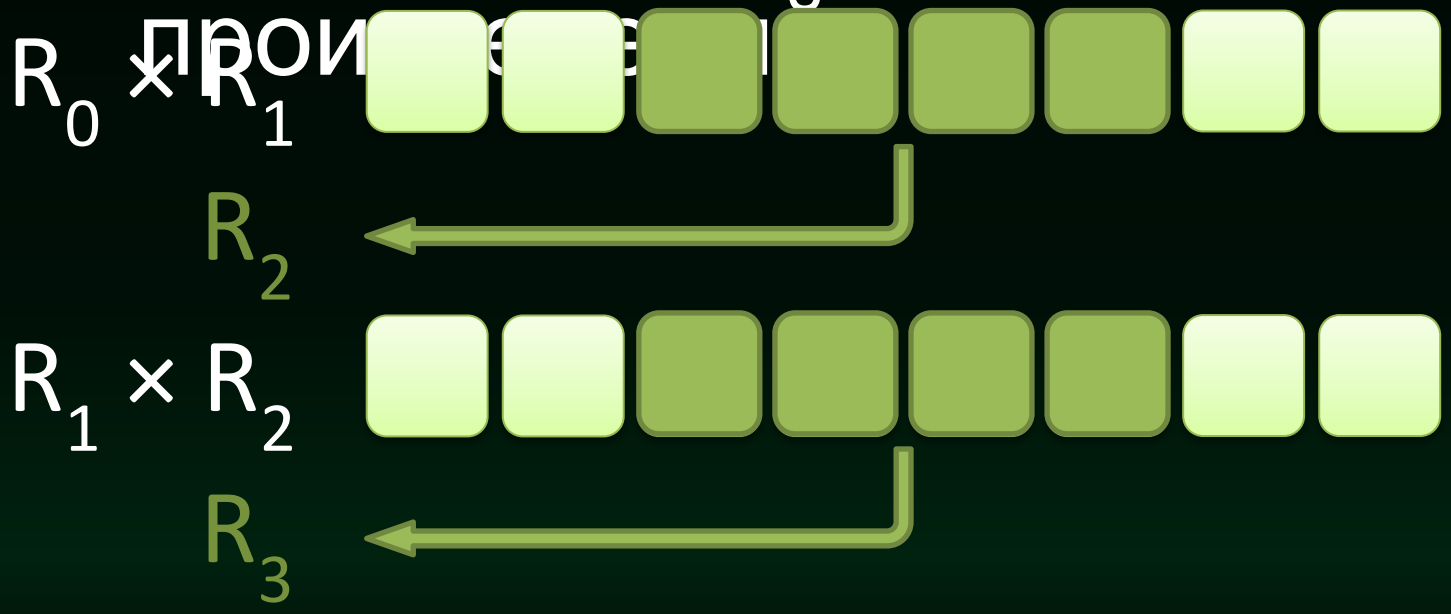
$R_0 \times R_1$ 

Первые алгоритмы

- Метод серединных квадратов
- Метод серединных произведений

Первые алгоритмы

- Метод серединных квадратов
- Метод серединных произведений

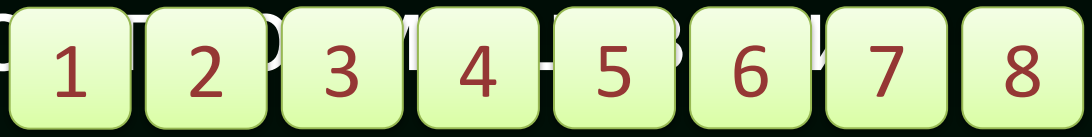


Первые алгоритмы

- Метод серединных квадратов
- Метод серединных произведений
- Метод перемешивания

Первые алгоритмы

- Метод серединных квадратов
- Метод серединных произведений
- Мето[illegible]

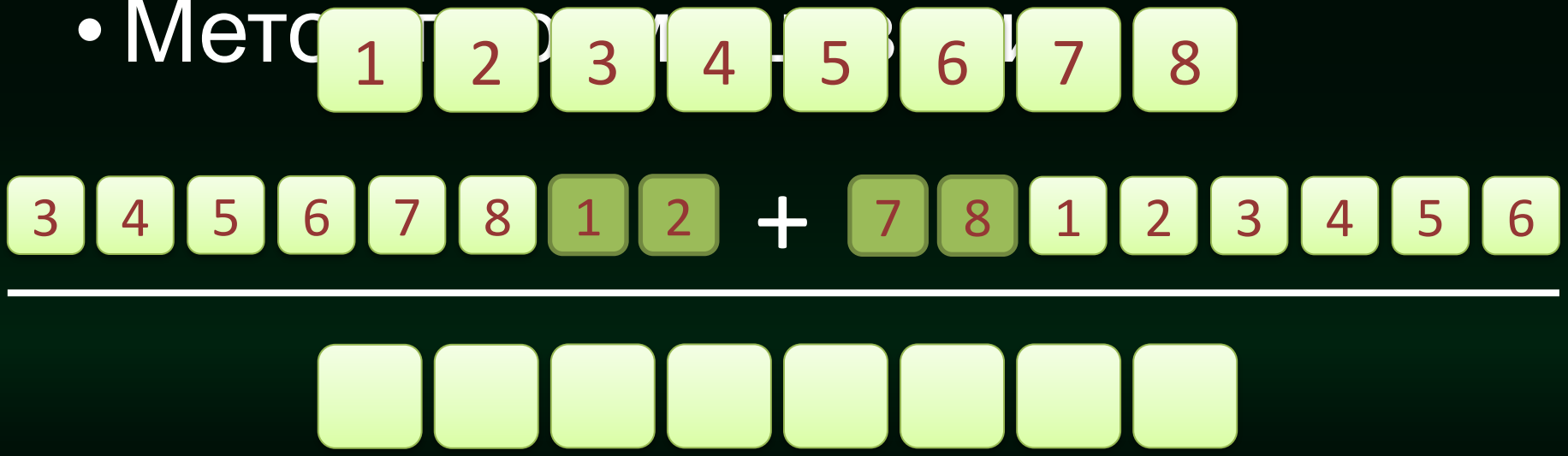


Первые алгоритмы

- Метод серединных квадратов
- Метод серединных произведений
- Мето[illegible]

Первые алгоритмы

- Метод серединных квадратов
- Метод серединных произведений
- Мето[illegible]



Тестирование

Тестирование

NIST

pLab Project

DIEHARD

TEST-U01

Dieharder

Knuth’s

CRYPT-X

ENT

Тестирование

NIST

pLab Project

DIEHARD

TEST-U01

Dieharder

Knuth’s

CRYPT-X

ENT

NIST

NIST

Частотный побитовый тест

NIST

Частотный побитовый тест

Частотный блочный тест

NIST

Частотный побитовый тест

Частотный блочный тест

Последовательность одинаковых бит

NIST

Частотный побитовый тест

Частотный блочный тест

Последовательность одинаковых бит

Самая длинная последовательность единиц в блоке

NIST

Ранговый тест

NIST

Ранговый тест

Спектральный тест

NIST

Ранговый тест

Спектральный тест

Тест на шаблоны

NIST

Ранговый тест

Спектральный тест

Тест на шаблоны

Тест на пересекающиеся шаблоны

NIST

Ранговый тест

Спектральный тест

Тест на шаблоны

Тест на пересекающиеся шаблоны

Тест Маурера

NIST

Тест на линейную сложность

NIST

Тест на линейную сложность

Тест на периодичность

NIST

Тест на линейную сложность

Тест на периодичность

Тест приблизительной энтропии

NIST

Тест на линейную сложность

Тест на периодичность

Тест приблизительной энтропии

Тест кумулятивных сумм

DIEHARD

DIEHARD

Тест на парковку

DIEHARD

Тест на парковку

Тест сжатия

DIEHARD

Тест на парковку

Тест сжатия

Тест игры в кости

Практическая часть

В программе выполняется построение диаграммы визуальной оценки равномерности случайных чисел. Числа – кружочки на диаграмме должны равномерно заполнить квадрат со стороной, равной единице. Далее приведен пример проверки случайной последовательности на равномерность распределения в интервале [0; 1]

Анализ качества Гсч системы Matlab

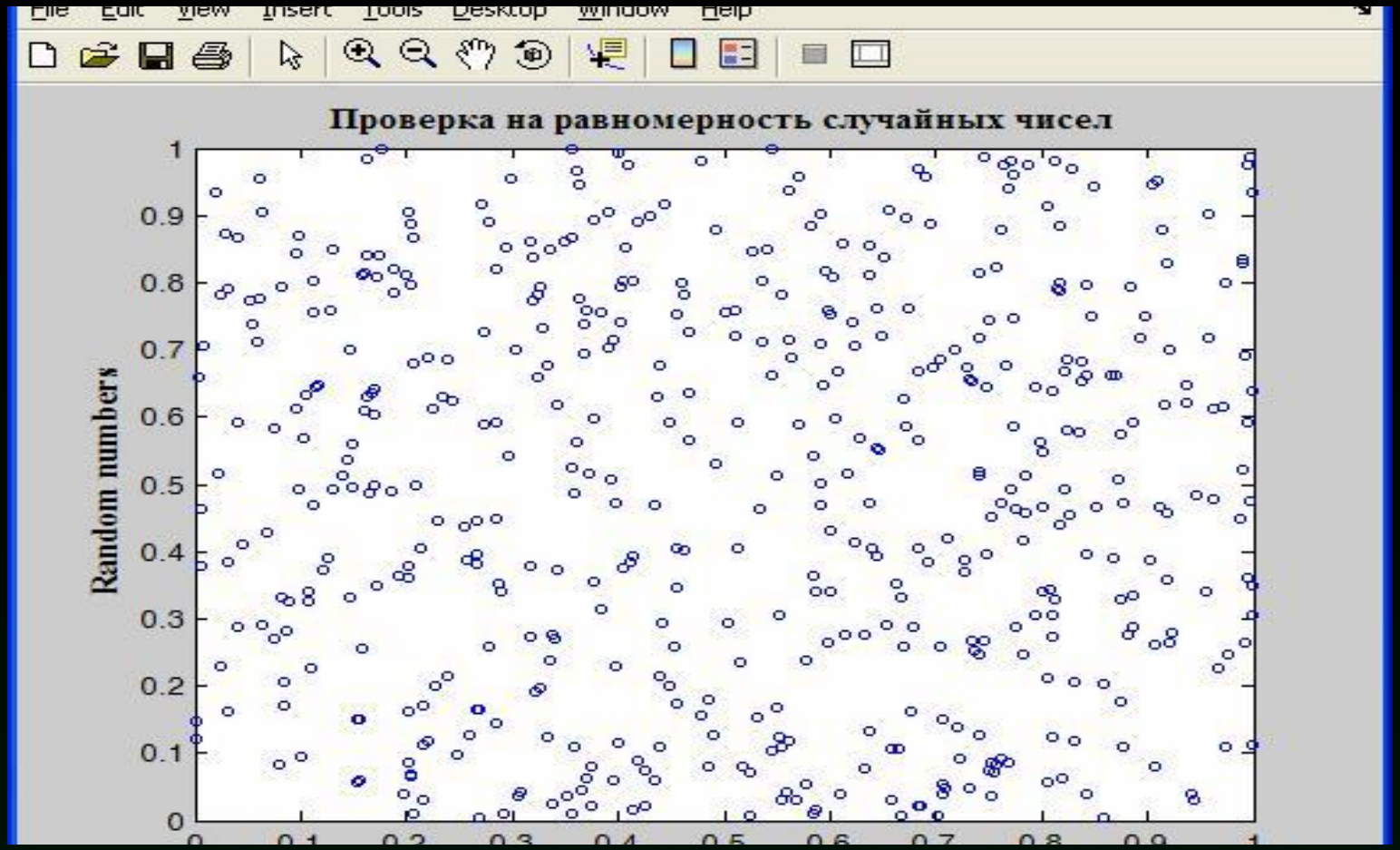
```
clear, clc
%% Генерирование выборки 500 случайных чисел
x = rand(500, 1);
%% Вычисление среднего значения выборки
m1 = mean(x)
%% Вычисление дисперсии данной выборки
s2 = var(x)
%% Вычисление среднего квадратического отклонения
s = std(x)

%% Расчет относительных погрешностей в процентах
%% по математическому ожиданию
m = 0.5;
Dm = abs((mean(x)- m)/m)*100;
fprintf('\n Относительная погрешность по математическому ожиданию:
%g%%\n', Dm);
%% по дисперсии
d = 1/12;
Dd = abs((var(x)- d)/d)*100;
fprintf(' Относительная погрешность по дисперсии: %g%%\n', Dd);
%% по среднему квадратическому отклонению
sd = sqrt(d);
Ds = abs((std(n1)- sqrt(1/12))/sqrt(1/12))*100;

fprintf(' Относительная погрешность по стандартному отклонению:
%g%%\n', Ds);

%% Генерирование дополнительной выборки
y = rand(500, 1);

%% Диаграмма оценки равномерности случайных чисел
fig1 = figure(1);
set(fig1, 'name', 'Случайные числа функции rand')
plot(x,y,'o', 'markersize', 4);
str = '\bf\fontsize{11}\fontname{times}Проверка на равномерность
случайных чисел';
title(str)
xlabel('\bf\fontsize{11}\fontname{times} Random numbers')
ylabel('\bf\fontsize{11}\fontname{times} Random numbers')
```



Проверка равномерности случайных чисел для функции rand

Заключение

В данной работе был изучен подход тестирования генераторов случайных чисел, позволяющий быть уверенным в корректности результатов тестов. Далее он был показан на практике на основе метода Пирсона и по критерию отклонения мат. ожидания.

Проблема генерации случайных и псевдослучайных последовательностей, применяемых в криптографии, остаётся актуальной на сегодняшний день. Существует большое количество статистических тестов для проверки генераторов.

Исследования в данной области продолжаются, и находятся более эффективные методы оценки качества генераторов случайных последовательностей.