|  |  |
| --- | --- |
|  | **Министерство науки и высшего образования Российской Федерации**  **Федеральное государственное бюджетное образовательное учреждение**  **высшего образования**  **«Московский государственный технический университет**  **имени Н.Э. Баумана**  **(национальный исследовательский университет)»**  **(МГТУ им. Н.Э. Баумана)** |

ФАКУЛЬТЕТ  *Информатика и системы управления*

КАФЕДРА *Программное обеспечение ЭВМ и информационные технологии*

**РАСЧЕТНО-ПОЯСНИТЕЛЬНАЯ ЗАПИСКА**

***К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ***

***НА ТЕМУ:***

***Метод генератор псевдослучайных чисел на основе автомата «игра Жизнь»***

Студент ИУ7-85Б **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Мирзоян С.А.**

(Группа) (Подпись, дата) (И.О.Фамилия)

Руководитель ВКР **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Ковтушенко А.П**

(Подпись, дата) (И.О.Фамилия)

Консультант **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

(Подпись, дата) (И.О.Фамилия)

Нормоконтролер **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

(Подпись, дата) (И.О.Фамилия)

*2022 г.*

# РЕФЕРАТ

Расчетно-пояснительная записка \_ с., \_ рис., \_ табл., \_ источников, \_ прил.

Объектом разработки является метод для генерации псевдослучайных чисел.

Цель работы – продолжить исследования в методе генерации псевдослучайных чисел на основе клеточного автомата, изучить новые способы применения, а также предложить модификации для улучшения качественно-скоростных характеристик.

Поставленная цель достигается за счет решения следующих задач:

* изучение методов генерации случайных и псевдослучайных чисел;
* изучение новых методик представления карты вселенной игры «Жизнь»;
* Модернизация правил игры «Жизнь»;
* Модернизация последних реализаций данного метода генерации.
* Исследование качественных характеристик приведенного метода генерации псевдослучайных чисел;
* Сравнительный анализ модернизированного метода генерации с изначальной итерацией на предмет улучшения качественно-скоростных характеристик;
* Сравнительный анализ приведенного метода с существующими, в том числе на основе технологии клеточных автоматов;
* разработка приложения, визуально демонстрирующая работу предложенного метода, а также выдающего на выход последовательность псевдослучайных чисел.

**СОДЕРЖАНИЕ**

[РЕФЕРАТ 2](#_Toc94137100)

[ВВЕДЕНИЕ 4](#_Toc94137101)

[1 Аналитический раздел 5](#_Toc94137102)

[1.1 Генераторы случайных и псевдослучайных чисел 5](#_Toc94137103)

[1.2 Описание предметной области 6](#_Toc94137104)

[1.2.1 Разновидности генераторов псевдослучайных чисел 7](#_Toc94137105)

[Линейный конгруэнтный 8](#_Toc94137106)

[Регистр сдвига с обратной линейной связью 11](#_Toc94137107)

[Вихрь Мерсенна 12](#_Toc94137108)

[ГПСЧ на базе клеточного автомата («правило 30») 13](#_Toc94137109)

[ГПСЧ на базе клеточного автомата (NESW) 15](#_Toc94137110)

[ГПСЧ на базе клеточного автомата (игра «Жизнь») 16](#_Toc94137111)

[1.2.2 Клеточные автоматы 17](#_Toc94137112)

[1.2.3 Игра «Жизнь» 18](#_Toc94137113)

[1.3 Вывод 19](#_Toc94137114)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 20](#_Toc94137115)

# ВВЕДЕНИЕ

Вокруг нас существует неисчерпаемый запас неизведанного знания. Чтобы получить более глубокий взгляд на мир, миллионы ученых всего мира работают ежедневно в своих лабораториях и исследуют живые организмы, как и химические соединения. Используя разнообразные методы и технологии, они проходят многолетние испытания и расширяют границы человеческого знания и науки.

Человечество достигло небывалых высот благодаря нашим научным открытиям и изобретениям, таким как колесо и компьютер. Компьютерное изобретение изменило наш мир, расширив границы человеческих возможностей во всех сферах жизни. Этот инструмент помог в завершении Второй Мировой Войны, создании программ для космонавтики, раскрытии научных теорий и моделировании процессов с использованием виртуальной реальности.

Многие научные исследования в области медицины или моделирования требуют поиска случайных чисел или последовательностей. Для этого существует множество способов, использующих различные технологии с разными достоинствами и недостатками.

В этой работе обсуждается метод генерации псевдослучайных чисел на основе клеточных автоматов. Уже существующие методы для генерации псевдослучайных чисел описаны и проанализированы в данной работе, а также предлагается использование критериев для оценки качества генераторов. Проведен сравнительный анализ между уже существующим линейно-конгруэнтным генератором псевдослучайных чисел, генератором на основе клеточных автоматов и предложенным новым генератором.

# Аналитический раздел

В аналитическом разделе выполнен анализ выбранной предметной области, определены ограничения, накладываемые предметной областью, поставлены требования к функционалу рассматриваемой системы взаимодействия модулей, а также рассмотрены существующие методы для выполнения одного или нескольких задач. Проведен разбор существующих решений для выполнения поставленной цели.

## **Генераторы случайных и псевдослучайных чисел**

Генерация случайных чисел — процесс, порождающий последовательность чисел, элементы которой независимы друг от друга.

Генератор псевдослучайных чисел (сокращенно ГПСЧ) — алгоритм, порождающий последовательность чисел, элементы которой почти независимы друг от друга и подчиняются заданному распределению.

Изначально, для получения последовательности случайно вычисленных чисел необходимо было прибегать к не самым удобным методам, таким как перемешивание костей и поочередное вынимание их из мешочка. В связи с развитием технологий, стали появляться и новые способы получения случайных данных. Таким образом, истинное число может быть получено путем наблюдения за шумом или количеством ног, прошедших по определенной плитке пола в определенное время. Однако, несмотря на то, что такой метод позволяет получать истинно случайные последовательности чисел, он требует специального оборудования для генерирования некоррелированных и статистически независимых чисел, что представляет собой сложную задачу. Кроме того, для защиты от внешних воздействий такой блок должен быть полностью изолирован от внешнего воздействия, что является весьма сложной задачей.

В дополнение к аппаратному методу генерации случайных чисел можно также создавать таблицы, которые будут проверяться на наличие некоррелированных последовательностей чисел. Этот метод называется табличным. Таким образом можно получить действительно случайные последовательности чисел, однако становятся очевидными и недостатки этого метода, а именно: ограниченность строк, занятая память, предопределенные значения в случае утечки таблицы.

Есть третий тип генераторов — алгоритмы. По сути, это комбинация физического генератора и детерминированного алгоритма. Он берет ограниченный набор входных данных от физического генератора и преобразует их в новое значение по определенному алгоритму. Этот метод отражает все достоинства и недостатки методов предыдущего поколения: быстрый, не потребляет памяти, не требует какого-либо специального оборудования, но генерирует последовательности псевдослучайных чисел, после чего вытекают все недостатки. исходя из этого, а также вычислить период и зависимость каждого последующего числа от предыдущих чисел.

Следует отметить, что в России существует ГОСТ на генераторы псевдослучайных чисел. Стандарт устанавливает методы генерации случайных чисел, подчиняющиеся другим и равномерным законам распределения, используемым при применении метода Монте-Карло, но в нем отсутствуют криптографические методы генерации. [6]

## **Описание предметной области**

Генераторов псевдослучайных чисел существует бесчисленное множество, и нет никакого смысла перечислять их все. Условно их можно разбить на несколько групп, отличающихся базовой логикой работы.

Из множества ГПСЧ можно выделить следующие группы:

* Линейно-конгруэнтные;
* Вихревые;
* На основе клеточных автоматов;
* На основе регистра сдвига.

Также в данной работе используется технология клеточных автоматов. Клеточные автоматы являют собой отдельную обширную тему для изучения и продолжают быть изучаемы и поныне, а посему будут рассматриваться лишь обобщенный клеточный автомат, а также его разновидность – игра «Жизнь».

В работе необходимо разработать метод генерации псевдослучайных чисел. Необходимо добиться того, чтобы данный метод проходил оценку качества, обеспечивающую уверенность в том, что данный метод имеет право на существование, результат его работы – это псевдослучайная последовательность чисел с редкой цикличностью.

И последнее, но не менее важное – это применимость данного метода. Необходимо изучить предложенный метод на прикладной характер. В качестве задач, например, могут выступать задачи поиска ключа шифрования в криптографии.

### Разновидности генераторов псевдослучайных чисел

В текущей подразделе рассматриваются различные виды методов генерации псевдослучайных чисел. Представленные ниже методы – это лишь малая часть от общего пантеона ГПСЧ.

В качестве примера можно рассмотреть следующие генераторы псевдослучайных чисел:

* Линейный конгруэнтный;
* Регистр сдвига с обратной линейной связью (РСЛОС);
* Вихрь Мерсенна;
* ГПСЧ на базе клеточного автомата (правило 30);
* ГПСЧ на базе клеточного автомата (NESW)
* ГПСЧ на базе клеточного автомата (игра «Жизнь»)

#### **Линейный конгруэнтный**

Линейная конгруэнтная схема генерации псевдослучайных чисел была предложена Д. Г. Лехмером в 1949 году и считается наиболее популярной. Согласно этой схеме последовательность случайных чисел можно получить, если положить, что

,

где

В приведенной выше формуле особое значение имеет выбор параметров. Например, для получится последовательность:

7, 5, 9, 1, 7, 5, 9, 1, …

Как можно заметить, данную последовательность с трудом можно назвать «случайной». В этом примере кроется проблема данного метода – линейный конгруэнтный метод всегда выдает последовательность, которая зацикливается.

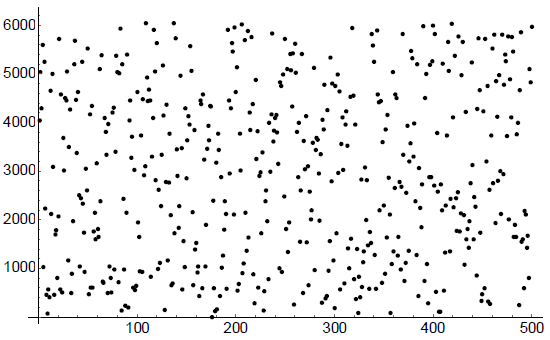
****

Рисунок 1.1. График ЛКП для X¬0= 7,a=106,c= 1283,m = 6075.

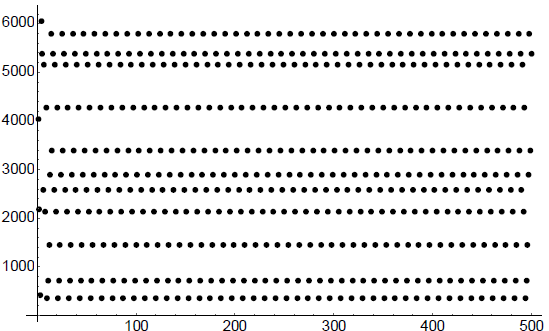


Рисунок 1.2. График ЛКП для X¬0= 7,a=105,c= 1283,m = 6075.

Также, ввиду свойств операций в конечном поле, применяемых в формуле (1), возникает «решетчатая структура» в последовательностях, что также является недостатком. Данный эффект можно наблюдать на рисунке 1.2.1.3

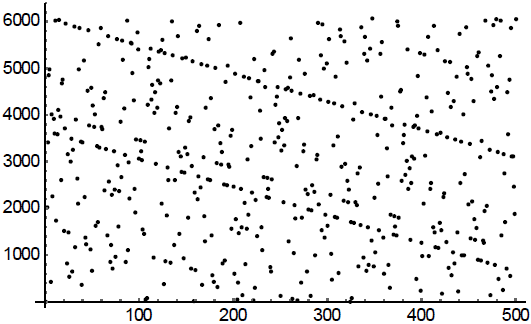
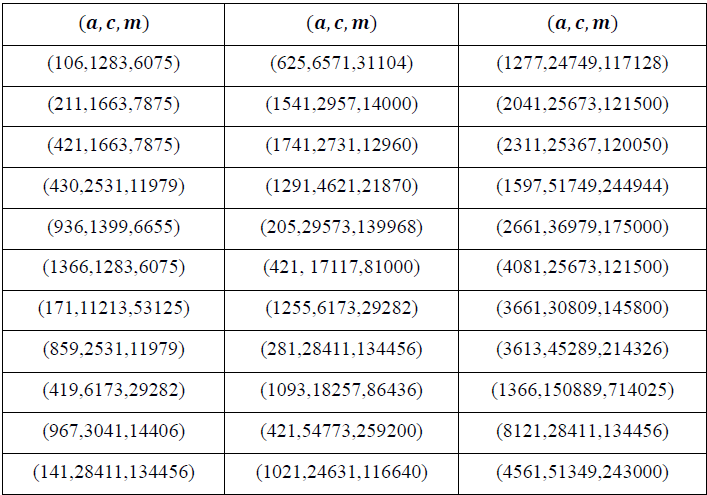


Рисунок 1.3. График ЛКП для X¬0= 7,a=106,c= 1284,m = 6075.

Ниже приведена таблица констант для линейных конгруэнтных генераторов. [4]

Таблица 1.1. Параметры ЛКГ для формулы 1.



Если подытожить, то можно в качестве преимуществ выделить простоту реализации и скорость работы данного генератора. Недостатком же будет являться цикличность значений последовательности.

#### **Регистр сдвига с обратной линейной связью**

Данный класс ГСПЧ основан на преобразовании бинарного представления некоторого числа. Такие генераторы имеют некоторые преимущества, как, например, скорость генерации чисел, хорошие статистические свойства псевдослучайных чисел, а также возможность простой реализации на аппаратном уровне.

Регистр сдвига с обратной линейной связью (РСЛОС) – регистр сдвига битовых слов, у которого входной (вдвигаемый) бит является линейной функцией остальных битов. Вдвигаемый вычисленный бит заносится в ячейку с номером 0. Количество ячеек p называют длиной регистра. [4]

Для натурального числа и , принимающих значения 0 или 1, определяют рекуррентную формулу

,

Из формулы можно заключить, что для РСЛОС функция обратной связи является линейной булевой функцией от состояний всех или некоторых битов регистра.

Одна итерация алгоритма, генерирующего последовательность, состоит

из следующих шагов:

1. Содержимое ячейки − 1 формирует очередной бит ПСП битов.

2. Содержимое ячейки 0 определяется значением функции обратной связи, являющейся линейной булевой функцией с коэффициентами . Его вычисляют по вышеприведенной формуле.

3. Содержимое каждого i-го бита перемещается в (*i* + 1)-й, 0 ≤ *i* < − 1.

4. В ячейку 0 записывается новое содержимое, вычисленное на шаге 2.

Наименьшее положительное целое N, такое, что для всех значений называют *периодом последовательности*. Эту последовательность называют М-последовательностью.

#### **Вихрь Мерсенна**

В 1997 году японскими учеными Макото Мацумото и Такудзи Нимисура был предложен метод генерации случайных чисел, основанный на свойствах простых чисел Мерсенна. Данный метод получил название «Вихревой генератор». «Вихрь» – это преобразование, которое обеспечивает равномерно распределение ПСЧ.

Числом Мерсенна называется натуральное число , определяемое формулой

Пример. Первые 17 чисел последовательности: 1, 3, 7, 15, 31, 63, 127, 255, 511,1023, 2047, 4095, 8191, 16 383, 32 767, 65 535, 131 071. [4]

Часто числами Мерсенна называют числа с простыми индексами n. Важным свойством чисел Мерсенна является то, что если является простым, то значит, что и n – также простое число. В общем случае обратное не верно, что не дает возможности просто и эффективно генерировать простые числа, но зато позволяет эффективно проверять число на простоту. Данное свойство лежит в основе теста на простоту Люка-Лемера. [1]

Существует несколько вариантов этого ГПСЧ. Мы рассмотрим наиболее распространенный, который имеет обозначение MT19937. По сути, данный ГПСЧ является РСЛОС, состоящим из 624 ячеек по 32 бита. Метод Вихрь Мерсенна позволяет генерировать последовательность двоичных псевдослучайных целых w-битовых чисел в соответствии со следующей рекуррентной формулой

где – целые константы, – степень рекуррентности, ;

– w-битовое двоичное целое число;

– двоичное целое число, полученное конкатенацией чисел и , когда первые (w-r) битов взяты из , а последние битов из в том же порядке;

– матрица размера w×w, состоящая из нулей и единиц, определенная по-

средством ;

– произведение, при вычислении которого сначала выполняют операцию (сдвига битов на одну позицию вправо), если последний бит равен

0, а затем, когда последний бит , вычисляют .

Вихрь Мерсенна имеет огромный период, равный числу Мерсенна (). Этот период достаточен для большинства возможных применений

алгоритма.

Метод обеспечивает равномерное распределение генерируемых псевдослучайных чисел в 623 измерениях. Поэтому корреляция между последовательными значениями в выходной последовательности Вихря Мерсенна пренебрежимо мала. Метод также хорошо проходит статистические тесты на «случайность».

Однако данный ГПСЧ не предназначен для получения криптографически стойких последовательностей случайных чисел. [12]

#### **ГПСЧ на базе клеточного автомата («правило 30»)**

В работах [7],[8],[9] и [10] описан метод генерации псевдослучайных чисел, предложенный Стивеном Вольфрамом. В его основе лежит клеточный автомат «правило 30».

Клеточный автомат – это устройство, состоящее из n-мерного массива ячеек и правил изменения значений ячеек. Каждая из ячеек имеет начальное состояние и изменяет свое состояние в дискретные моменты времени.

Правило, в соответствии с которым ячейка изменяет состояние, – это рекуррентная формула, в которой новое значение ячейки определяется исходя из предыдущих значений этой и соседних ячеек. В простом одномерном случае, когда массив ячеек состоит из n битов , правило выглядит так:

Этот генератор показывает хорошие статистические свойства. Однако он сильно зависим от начальных значений ячеек: при неудачном выборе начального состояния, клеточный автомат порождает циклические структуры. Кроме того, для него существует успешное вскрытие с известным открытым текстом. В [8, 9] показано, что вскрытие выполнимо на персональном компьютере с размером клеточного автомата вплоть до 500 битов.

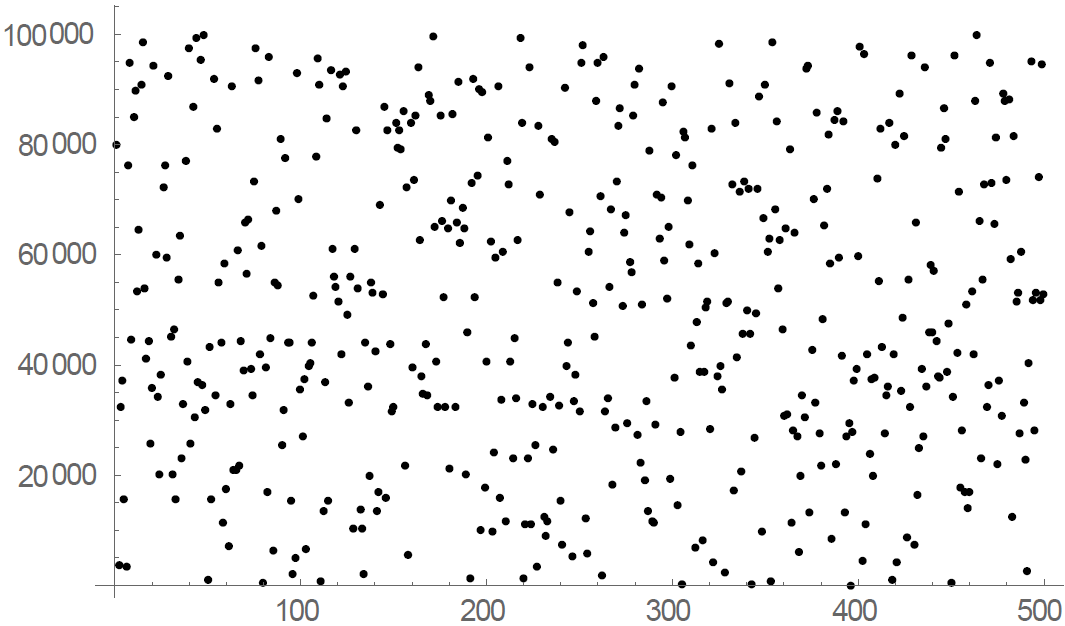


Рисунок 1.4. График ГПСЧ на базе клеточного автомата

#### **ГПСЧ на базе клеточного автомата (NESW)**

Одним из относительно молодых методов генерации псевдослучайных чисел, также основанном на технологии клеточного автомата, является метод, представленный университетом ИТМО за авторством Д. Д. Мухамеджанова, А. Б. Левиной. В сути своей данный метод является глубокой модификацией предыдущего метода. Сетка имеет размеры p и q , которые являются простыми числами (для улучшения периодичности). Изменения начинаются прямо с этого этапа: деление всей сетки на блоков, которые формируются как прямоугольники с размерами и , а каждый блок состоит из lbi wbi  ячеек (рис. 1.5).

Выбрав произведение сторон прямоугольников блоков lbi  wbi как начальную конфигурацию, необходимо заполнить ячейки таким образом, чтобы в каждой ячейке располагался один бит (состояние 0 или 1).

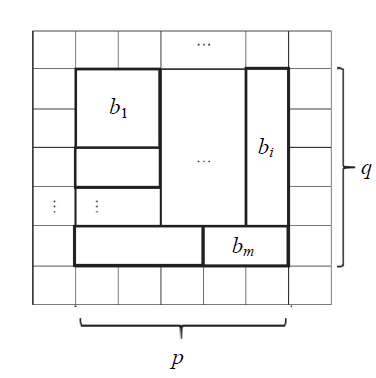


Рисунок 1.5. Разделение сетки клеточного автомата на блоки

Затем применяется алгоритм под названием NESW (North, East, South, West). Метод такого движения носит название по сторонам света (рис. 1.6). Суть способа в том, чтобы заполнять сетку блока согласно направлениям сторон света, т.е. мы циклически заполняем битами полученного числа сетку, начиная с левого нижнего угла, двигаясь сначала вверх, затем вправо, вниз и влево до конца сетки (или до заполненной ячейки).

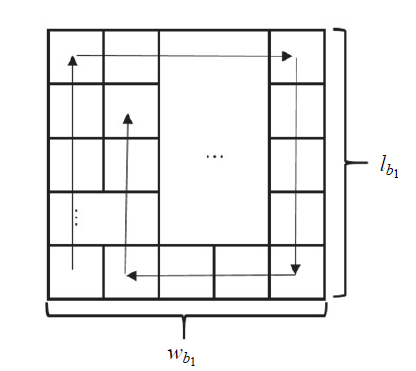


Рисунок 1.6. Метод NESW

Каждый блок может иметь свое собственное правило, что делает КА неоднородным и приводит к лучшим показателям критериев статистических свойств и лучшим периодическим свойствам. [11]

#### **ГПСЧ на базе клеточного автомата (игра «Жизнь»)**

Еще одним из методов генерации псевдослучайных чисел, основанном на клеточных автоматах, является метод, использующий в своей основе модернизированные правила игры «Жизнь». Далее будет представлено более точное представление о клеточных автоматах и игре «Жизнь» [13]. Стоит отметить, что метод генерации на момент написания данной работы имеет ряд недостатков, таких как отсутствие законов распределения, отсутствие возможности для ведения диапазона выходящих значений, а также сложности при подборе начальной конфигурации. Однако с этим данный ГПСЧ имеет потенциал для развития и улучшения.

### Клеточные автоматы

Клеточные автоматы – это дискретные динамические системы, поведение которых полностью определяется в терминах локальных зависимостей, в значительной в значительной степени так же обстоит дело для большого класса непрерывных динамических систем, определенных уравнениями в частных производных. [2]

КА можно формально описать как четверку

, (1)

где – множество мерных векторов, = - множество состояний одной ячейки в , – окрестность или шаблон соседства (упорядоченное множество различных -мерных векторов из , – локальная функция переноса.[3-4]

Из данного выше описания становится понятно, что на очередном шаге состояние каждой клетки зависит от состояния клеток вокруг нее – ее окрестности. Обычно различают два вида окрестностей: окрестность Мура и окрестность фон Неймана (рисунок 1.7). [3]

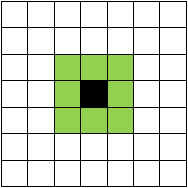
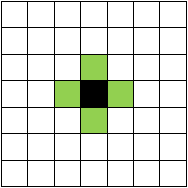


Рисунок 1.7 Окрестности фон Неймана (слева) и Мура (справа)

### Игра «Жизнь»

Игра «Жизнь» — это клеточный автомат, изобретенный в 1970 году английским математиком Джоном Конвеем, в котором соблюдается ряд определенных правил поведения системы.

Правила игры таковы:

* «Вселенная» игры — это размеченная на клетки поверхность или плоскость. Она может быть безграничная, ограниченная или замкнутая.
* Каждая клетка на этой поверхности может находиться в двух состояниях: быть «мёртвой» или «живой». Клетка имеет восемь соседей, окружающих её.
* Распределение живых клеток в начале игры называется первым поколением. Каждое следующее поколение рассчитывается на основе предыдущего по следующим правилам:
  + Если рядом с мёртвой клеткой рядом находятся ровно три живые клетки, то в данной клетке зарождается жизнь;
  + если вокруг живой клетки два или три живых соседки, то эта клетка не умирает;
  + клетка умирает, если соседей меньше двух («от одиночества») или больше трёх («от перенаселённости»);
* Игра прекращается, если
  + Во «вселенной» не останется ни одной живой клетки;
  + складывается периодическая конфигурация;
  + складывается стабильная конфигурация;

Благодаря этим простым правилам можно добиться большого разнообразия «форм жизни».

Стоит также отметить, что игрок занимает позицию наблюдателя и не принимает прямого участия в игре. Он может лишь формировать начальную конфигурацию живых клеток.

В результате выполнения классических условий игры через некоторое количество ходов по выбору методики генерирования получается последовательность псевдослучайных чисел из нулей и единиц. Эта особенность данного клеточного автомата и будет применяться в предложенном методе.

## **Вывод**

В разделе дано описание генераторов случайных и псевдослучайных чисел, а также клеточных автоматов. Рассмотрены особенности и проблемы генерации истинно случайных чисел, разновидности методов генерации псевдослучайных чисел. Среди разновидностей рассмотренных методов приведены три метода, основанных на технологии клеточных автоматов. Стоит отметить, что последний ГПСЧ из упомянутой тройки лежит в основе данной работы и именно он рассматривается как объект исследования. Также рассмотрены обобщенный клеточный автомат, а также частный случай его реализации – игра «Жизнь», которая лежит в основе предложенного метода. Приведены правила игры «Жизнь». Определены ограничения и требования.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Дональд Кнут. Искусство программирования, том 2. Получисленные алгоритмы = The Art of Computer Programming, vol.2. Seminumerical Algorithms.— 3-е изд. — М.: «Вильямс», 2007.
2. Т. Тоффоли, Н. Марголус, Машины клеточных автоматов// Мир 1991, стр. 8.
3. Aspray W. John von Neumann and the Origins of Modern Computing. MIT Press, 1990, стр. 376
4. Слеповичев И.И., ГЕНЕРАТОРЫ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ, май 21, 2017.
5. Документация Python 3.8 [Электронный ресурс]. URL: https://docs.python.org/3.8 (дата обращения 04.06.2021).
6. ГОСТ Р ИСО 28640-2012. [Электронный ресурс]. – Режим доступа: <http://files.stroyinf.ru/cgi-bin/ecat/ecat.fcgi?b=0&i=53898&pr=1>. Проверено 01.06.2021.
7. S. Wolfram, “Random Sequence generation by Cellular Automata”, Advances in Applied Mathematics, v. 7, 1986, pp.123-164.
8. W. Meier and O. Staffelbach, “Fast Correlation Attack on Stream Ciphers”, Journal of Cryptology v I n. 3, 1989, pp.159-176.
9. P.H. Bardell, “Analisis of Cellular Automata Used as Pseudorandom Pattern generators”, Proceedings of 1990 International Test Conference, pp. 762-768.
10. S. Wolfram, “Statistical mechanics of cellular automata”, Reviews of Modern Physics, Vol. 55, No. 3, July 1983, pp.8-13.
11. Мухамеджанов Д.Д., Левина А.Б. Генератор псевдослучайных чисел на основе клеточных автоматов // Научно-технический вестник информационных технологий, механики и оптики. 2018. Т. 18. № 5. С. 894–900. doi: 10.17586/22261494-2018-18-5-894-90
12. Деон А.Ф., Меняев Ю.А. Генератор равномерных случайных величин по технологии полного вихревого массива // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. 2017. № 2. C. 86–110. DOI: 10.18698/0236-3933-2017-2-86-110
13. Mirzoyan S.A. PSEUDORANDOM NUMBER GENERATOR BASED ON CELLULAR AUTOMATA AND THE GAME "LIFE" // International Scientific – Practical Conference «INFORMATION INNOVATIVE TECHNOLOGIES», 2021, стр. 280-285