НИТУ «МИСиС»
Кафедра Инженерной кибернетики

Имитационное моделирование

Лабораторная работа №1. «Генерация стандартных псевдослучайных чисел и проверка их статистических свойств»

Сенченко Р.В.

17 марта 2020 г.

I. Базовая часть. Требуется спроектировать и реализовать класс (или их совокупность) для моделирования и генерации стандартных псевдослучайных чисел $\varepsilon \rightsquigarrow \mathbf{U}[0,1]$ с помощью линейного конгруэнтного генератора $X_{k+1} = (aX_k + b) \bmod m$ (при этом, очевидно, $\varepsilon_k = X_k/m$). Параметры a, b, m и X_0 необходимо выбрать самостоятельно; доступные готовые комбинации параметров см. в работе *Entacher, Karl. (1999). A Collection of Selected Pseudorandom Number Generators With Linear Structures.* При этом выбранные параметры не должны совпадать с параметрами генератора в какой-либо другой работе[1].

Разработанные классы должны отвечать требованиям методологии ООП, иметь хорошо продуманную архитектуру, а также позволять реализовывать базовые (основные) статистические тесты проверки качества получаемых псевдослучайных чисел: *критерий частот*, *критерий серий*, *критерий интервалов* и *покер-критерий*. Каждый критерий должен быть подсчитан по крайней мере для одного значения параметра d преобразования $U_k = \lfloor d \cdot \varepsilon_k \rfloor$. Соответствие эмпирических данных должным теоретическим результатам следует проводить с помощью критерия согласованности χ^2; допускается лишь подсчет оценки критерия χ^2 и последующий "ручной" анализ с помощью таблиц.

Выбранный генератор должен быть проверен для генерации последовательности псевдослучайных чисел длины $\ell = 2^{31}$ или более (здесь речь идет о длине проверенной последовательности, а не о периоде генератора). Программные компоненты должны быть реализованы на языке программирования `c++`. Программный код должен быть снабжен достойными комментариями, обладать стройностью и читабельностью; функциональность разработанных программных компонентов должна быть продемонстрирована (например, в рамках метода main и/или любого другого подходящего участка кода).

[1] В том случае, если один и тот же набор параметров будет использован сразу в двух лабораторных работах — засчитывается та из лабораторных работ, которая первой была загружена в систему Canvas.

II. Дополнительная часть.

1. **Собственный генератор, 15☆.** Самостоятельно подобрать уникальные параметры a, b, m и X_0 линейного конгруэнтного генератора $X_{k+1} = (aX_k + b) \bmod m$. Найденные параметры должны отсутствовать в рекомендованной литературе из *Базовой части*, однако удовлетворять всем прочим ее требованиям (в том числе — удовлетворять статистическим критериям).

   Генератор с найденными параметрами должен быть теоретически исследован на предмет его периода с использованием теорем о максимальном периоде. Проведенные исследования должны быть оформлены в виде отчета (в формате .pdf, .docx или .tex) и прикреплены в качестве дополнительных материалов к лабораторной работе.

2. **Образование случайных векторов, 3☆.** Провести исследование выбранного генератора стандартных псевдослучайных чисел $\varepsilon \rightsquigarrow \mathbf{U}[0, 1]$ на предмет возможности формирования псевдослучайных векторов размерности $k = 2, 3, \ldots, 8$. Методологию исследования следует выбрать самостоятельно, описать в виде отчета (как всегда — в формате .pdf, .docx или .tex). В отчете должны содержаться ход и основные результаты исследования, описание выбранной методологии исследования, а также ее теоретическое обоснование.

   Программный код, позволяющий провести исследование генератора на возможность формирования псевдослучайных векторов, является обязательной частью задания и прикладывается к материалам лабораторной работы.

3. **Процедура перехода, 5☆.** Предусмотреть и эффективно реализовать в разрабатываемом программном обеспечении процедуру "перехода" в генераторе псевдослучайных чисел $X_{k+n} = (a^n X_k + (a^n - 1)c/b) \bmod m$, $b = a - 1$. (Основную формулу процедуры перехода необходимо уметь выводить.)

   Корректность работы процедуры должны быть обоснована:

   (a) Оформленными теоретическими выкладками и доказательствами, если предлагаемая реализация имеет под собой математические основания. (Например, привлечены специальные знания из теории чисел, арифметики вычетов и пр.) Выкладки должны быть аккуратно и строго изложены "на бумаге" (в формате .pdf, .docx или .tex) и прикреплены в качестве дополнительных материалов к лабораторной работе.

   При отсылке к теоремам и пр. теоретическим результатам, не охваченным и не освещенным учебными дисциплинами НИТУ «МИСиС», означенные теоремы и пр. теоретические результаты должны быть дополнительно приложены к лабораторной работе в электронном виде (сам ресурс при этом, разумеется, должен в известной степени "заслуживать доверия" и иметь надлежащее качество).

   Калибровочное замечание. *Принимаются только оригинальные теоретические выводы, не предложенные ранее в рамках других лабораторных работ. В тех случаях, когда*

теоретические выкладки были получены группой студентов совместно — баллы равномерно распределяются между участниками группы с округлением в меньшую сторону. (Например, при распределении 10 баллов между 3 студентами каждый студент получит по 3 балла, тогда как оставшийся 1 балл — "сгорает".)

(b) Отсылкой к официальной технической документации и спецификациям, если реализация процедуры основана на использовании особенностей микропроцессоров ЭВМ и/или операционной системы, спецификой работы компилятора языка программирования C++ и иных приемов технического характера. Сама техническая документация или спецификация должна прикладываться к лабораторной работе в качестве сопроводительного материала в электронном виде с указанием ссылки на официальный (или сопоставимый с официальным) интернет-ресурс.

Калибровочное замечание. *Использование специальных программных компонентов, обеспечивающих бóльшую битность (разрядность) числовых типов данных (например, 128-битных чисел и/или чисел большей битности), допускается с предъявлением убедительного и исчерпывающего объяснения принципа работы этих компонентов, подкрепленного отсылками к технической документации, спецификациям и пр. Калибровочное замечание не применяется ("принцип собственности"), если собственная ЭВМ студента обладает необходимой битностью, на ЭВМ установлена специальная операционная система с поддержкой используемой битности и иное решение, соответствующее обозначенному духу калибровочного замечания.*

(c) Вычислительным экспериментом и прямым сравнением элементов генерируемой линейной конгруэнтной последовательности $X_0, X_1, X_2, \ldots, X_n$ с помощью последовательных вычислений $X_0 \mapsto X_1$, $X_1 \mapsto X_2$, $\ldots$, $X_{n-1} \mapsto X_n$ и вычисления по процедуре перехода $X_0 \mapsto X_n$. Вычислительный эксперимент имеет обязательный характер в том случае, если процедура перехода реализована с применением специальных алгоритмов и структур данных (например, длинной арифметики). Используемые алгоритмы и структуры данных должны быть грамотно реализованы в рамках лабораторной работы самостоятельно; соответствующий исходный код прикладывается к материалам лабораторной работы и является ее неотъемлемой частью.

4. **Улучшенное вычисление χ^2, 1⋆.** Исключить использование "ручных" таблиц при проверке критерия согласованности χ^2 в базовой части лабораторной работы. Для этого необходимо реализовать соответствующий вычислительный метод на основе аппроксимации Голдштейна $\chi^2_p(f)$, см. подробнее в научной и инженерной литературе: *Кобзарь А. И. Прикладная математическая статистика. Для инженеров и научных работников. - М.: ФИЗМАТЛИТ, 2006. - 816 с.*.

5. **Исследование длинного периода, 2⋆.** Предусмотреть в программной реализации генератора псевдослучайных чисел возможность сохранения промежуточных результатов оценки критериев качества, их сериализации и десериализации.

С помощью и с применением указанных методов исследовать статистические качества генератора псевдослучайных чисел на линейной конгруэнтной последовательности $X_0, X_1, X_2, \ldots, X_\ell$ длиной $\ell \geqslant 2^{48}$.

6. **Механизм "Зерна", 2☆.** Продумать и реализовать возможность задания начального "зерна" (seed) в исследуемом и реализуемом генераторе псевдослучайных чисел. Предложенная схема должна гарантировать сохранение вероятностных качеств генерируемой последовательности псевдослучайных чисел. Необходимые обоснования должны быть приведены отдельно, в виде пояснительной записки (в виде комментариев в коде или — при необходимости более полного обоснования "с формулами" — в виде отдельного отчета в электронном виде).

7. **Независимые псевдослучайные числа, 1☆.** Продумать теоретические аспекты моделирования нескольких *независимых* псевдослучайных чисел $\varepsilon_1, \varepsilon_2 \rightsquigarrow \mathbf{U}[0,1]$ на основе линейного конгруэнтного метода. Описать и изобразить в виде UML-диаграммы (грамотный) объектно-ориентированный дизайн системы с n независимыми генераторами стандартных псевдослучайных чисел.

   Калибровочное замечание. *Здесь, как и ранее, принимаются только оригинальные подходы, а также возможные объектно-ориентированные дизайны систем. Предлагаемые подходы должны быть тщательно продуманы на предмет их использования на практике, удобства и технологичности предлагаемого решения, а также инкапсуляции особенностей и специфики работы с псевдослучайными числами.*