Государственное бюджетное профессиональное образовательное учреждение города Москвы "Московский колледж управления, гостиничного бизнеса и информационных технологий "Царицыно" Отделение управления и информационных технологий

Доклад по теме:
Моделирование и визуализация случайных данных

Студент: Уколов Алексей

Группа: П2-3

Преподаватель: к.ф.-м.н. Мещеряков В.В.

Москва 2019

Линейный конгруэнтный метод — один из методов генерации псевдослучайных чисел. Применяется в простых случаях и не обладает криптографической стойкостью. Входит в стандартные библиотеки различных компиляторов.

Линейный конгруэнтный метод был предложен Д. Г. Лемером в 1949 году.Суть метода заключается в вычислении последовательности случайных чисел , полагая

$$X_{n+1} = (aX_n + C)\ mod\ m$$

Где m — модуль (натуральное число, относительно которого вычисляет остаток от деления;m ≥ 2), a — множитель (0≤a<m), C — приращение ($0 \leq C < m$), X_0 — начальное значение ($0 \leq X_0 < m$).

> Линейная конгруэнтная последовательность, определенная числами m,a ,c и X_0 периодична с периодом, не превышающим m . При этом длина периода равна m тогда и только тогда, когда:

1. Числа m и c **взаимно простые**;
2. b=a-1 кратно ρ для каждого простого ρ , являющегося делителем m ;
3. b кратно 4, если m кратно 4 .

Наличие этого свойства для случая , где — число **битов** в **машинном слове**, было доказано М. Гринбергом. Наличие этого свойства для общего случая и достаточность условий были доказаны Т. Е. Халлом и А. Р. Добеллом .

Наличие этого свойства для случая $m = 2^e$,е где — число **битов** в **машинном слове**, было доказано М. Гринбергом. Наличие этого свойства для общего случая и достаточность условий были доказаны Т. Е. Халлом и А. Р. Добеллом .

Метод генерации линейной конгруэнтной последовательности при C=0 называют **мультипликативным конгруэнтным методом**, а при $C \neq 0$ — **смешанным конгруэнтным методом**.

При C=0 генерируемые числа будут иметь меньший период, чем при C ≠ 0 , но при определенных условиях можно получить период длиной $m - 1$, если m — простое число. Тот факт, что условие $C \neq 0$ может приводить к появлению более длинных периодов, был установлен В. Е. Томсоном, и независимо от него А. Ротенбергом , Чтобы гарантировать максимальность цикла повторения последовательности при $C = 0$, необходимо в качестве значения параметра выбирать простое число. Самым известным генератором подобного рода является так называемый минимальный стандартный генератор случайных чисел, предложенный Стивеном Парком и Кейтом Миллером в 1988 году

Наиболее часто практикуемым методом генерации последовательностей псевдослучайных чисел является смешанный конгруэнтный метод

Mersenne Twister(Вихрь Мерсенна) — генератор псевдослучайных чисел (ГПСЧ), разработанный в 1997 году японскими учёными Макото Мацумото и Такудзи Нисимура . Вихрь Мерсенна основывается на свойствах простых чисел Мерсенна (отсюда название) и обеспечивает быструю генерацию высококачественных по критерию случайности псевдослучайных чисел.

Вихрь Мерсенна лишён многих недостатков, присущих другим ГПСЧ, таких как малый период, предсказуемость, легко выявляемые статистические закономерности.

Тем не менее, этот генератор не является криптостойким, что ограничивает его использование в криптографии.

Существуют по меньшей мере два общих варианта алгоритма, различающихся только величиной используемого простого числа Мерсенна, наиболее распространённым из которых является алгоритм *MT19937*, период которого составляет $2^{19937} - 1$ (приблизительно $4{,}3 \cdot 10^{6001}$).

Свойства

Вихрь Мерсенна является витковым регистром сдвига с обобщённой отдачей (TGFSR)[1] . «Вихрь» — это преобразование, которое обеспечивает равномерное распределение генерируемых псевдослучайных чисел в 623 измерениях (для линейных конгруэнтных генераторов оно ограничено 5 измерениями). Поэтому функция корреляции между двумя последовательностями выборок в выходной последовательности вихря Мерсенна пренебрежимо мала.

K-распределение

Было предложено много генераторов возможно «высокого качества», но только немногие могут быть использованы для серьёзного моделирования из-за отсутствия чёткого понятия «хаотичности» для генераторов псевдослучайных чисел, так как каждый исследователь концентрируется на конкретных параметрах хаотичности. Среди многих известных мер, тесты, основанные на более высоком равномерном распределении, таких как спектральный тест и тест на к-распределении, описанный ниже, считается сильнейшим.

Определние

Говорят, что псевдослучайная последовательность $\mathbf{x}_i$ периода P, состоящая из w-битных целых, имеет k-распределение с v-битной точностью, если она удовлетворяет следующему условию:

$$(trunc_{\cup}(X_I), \left(trunc_{\cup}(X_{I+1}), \ldots\ldots, trunc(x_{i+k-1})\right)(0 \leq i < P)$$

Тогда каждая из 2^{kv} возможных комбинаций битов встречается равное число раз, за исключением комбинации, состоящей полностью из нулей, которая встречается на один раз меньше.

Постановка задачи Бюффона

Задача Бюффона о бросании иглы — один из первых примеров применения метода Монте-Карло и рассмотрения понятия геометрической вероятности. Задача была сформулирована Бюффоном в 1777 году. Оказалось, что эта задача сделала возможным определение числа Пи вероятностными методами.

Вероятность становится лишь при условии, что r>L) того, что отрезок пересечет прямую, связана с числом Пи:

$$\rho = \int_0^{\pi} \int_0^{lsin\theta} \frac{1}{\tau\pi} \delta a \delta\theta$$

a-расстояние от начало иглы до ближайшей к ней точки

θ – угол иглы относительно прямых

При условии, что r > L получается решение: $\rho = \frac{2r}{2\pi}$

Таким образом, подсчитав долю отрезков, пересекающих прямые, можно приближенно определить число Пи. При увеличении количества попыток точность получаемого результата будет увеличиваться.

Теорема Колмогорова

Теоре́ма Колмого́рова в математической статистике уточняет скорость сходимости выборочной функции распределения к её теоретическому аналогу.

Формулировка

Пусть $X_1,\ldots\ldots,X_n,\ldots.$-бесконечная выборка из определения, задаваемого непрерывной функцией распределения , построенная на первых n элементах выборки , тогда

$$\sqrt{n}\ \sup_{x\epsilon R}|F_n(x)\text{-}F(x)\rightarrow k$$

по распределению при $n\rightarrow\infty$

где K — случайная величина, имеющая распределение Колмогорова.

Определение границ доверительной зоны

Теорема Колмогорова очень часто применяется, чтобы определить границы, в которые с заданной вероятностью попадает теоретическая функция F(x)

$$P(\sqrt{n}Dn \le k_{Y\prime}) = P(F_n(x) - \frac{K_{Y\prime}}{\sqrt{n}} \le F(x) \le F_n(x) + \frac{k_{Y\prime}}{\sqrt{n,}}; x \in R) \xrightarrow{n\rightarrow\infty} K(K_1)=y'$$

$D_n=\sup_x |F_n(x)\text{-}F(x)|$-где $k_{y\prime}$ квантиль уровня закона распределения Колмогорова.

Таким образом с вероятностью y' при n находится $n\rightarrow\infty$ F(x) в указанном интервале

.Вероятность y' называют *уровнем значимости*.

Область,определяемую этими границами, называют *асимптотической -доверительной зоной*для теоретической функции распределения.

SPYDER (IDE)

Spyder[3] (ранее **Pydee**) — свободная и кроссплатформенная интерактивная IDE для научных расчетов на языке Python, обеспечивающая простоту использования функциональных возможностей и легковесность программной части.

Spyder является частью модуля spyderlib для Python, основанного на PyQt4, pyflakes, rope и Sphinx, предоставляющего мощные виджеты на PyQt4, такие как редактор кода, консоль Python (встраиваемая в приложения), графический редактор переменных (в том числе списков, словарей и массивов).

Возможности

- Редактор с подсветкой синтаксиса Python, C/C++и Fortran
- Динамическая интроспекция кода (с помощью rope) — автодополнение, переход к определению объекта по клику мыши
- Нахождение ошибок на лету (с использованием pyflakes)
- Поддержка одновременного использования множества консолей Python (включая оболочку IPython)
- Просмотр и редактирование переменных с помощью GUI (поддерживаются различные типы данных - числа, строки, списки, массивы, словари)
- Встроенные средства доступа к документации (в формате Sphinx)
- Гибко настраиваемый интерфейс
- Интеграция с научными библиотеками Python - NumPy, SciPy, Matplotlib, Pandas
- Полный список возможностей доступен на официальном сайте [4].

Биномиальный коэффициент

В математике **биномиальные коэффициенты** — это коэффициенты в разложении бинома Ньютона$(1 + x_n)$ по степеням *x*. Коэффициент при x^kобозначается$\binom{n}{k}$ или C_k^n и читается «биномиальный коэффициент из *n* по *k*» ;

$$(1 + x_n)^n = \binom{n}{1} + \binom{n}{3}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n = \sum_{k=0}^{n} \frac{n}{k}(x^k)$$

для натуральных степеней n.

Биномиальные коэффициенты могут быть также определены для произвольных действительных чисел a . В случае произвольного действительного числа биномиальные коэффициенты определяются как коэффициенты разложения выражения$(1+x)^2$ в бесконечный степенной ряд:

$$(1+\mathrm{x})^a = \sum_{k=0}^{\infty} \binom{a}{k} x^k$$

Для неотрицательных целых *a* все коэффициенты с индексами *k>a* в этом ряду являются нулевыми , и поэтому данное разложение представляет собой конечную сумму

В комбинаторике биномиальный коэффициент $\binom{n}{k}$ для неотрицательных целых

чисел *n* и *k* интерпретируется как количество сочетаний из *n* по *k*, то есть количество всех подмножеств размера *k* в *n*-элементном множестве.

Биномиальные коэффициенты часто возникают в задачах комбинаторики и теории вероятностей. Обобщением биномиальных коэффициентов являются мультиномиальные коэффициенты.