Лабораторная работа № 1

Генераторы псевдослучайных чисел

Цель работы – исследование свойств генераторов псевдослучайных чисел.

Задачи:

1. Разработать программу для создания и исследования линейных конгруэнтных генераторов (ЛКГ). Требования к программе приводятся далее.
2. Создать и исследовать несколько ЛКГ с указанными в задании характеристиками. План исследования приводится далее.

Требования к программе

1. Программа должна считывать **одну команду** из файла *input.txt* и выводить результаты вычисления в файл *output.txt*.
2. Команда состоит из ключевого слова и списка аргументов. Аргументы отделены от ключевого слова и друг от друга **одним или несколькими пробелами**. **Порядок следования аргументов** жестко не регламентируется и **может быть любым**. Длина строки с командой не регламентирована, строка может быть **сколь угодно длинной**.
3. Должны поддерживаться следующие команды со следующими аргументами:

3.1. **get_c cmin=ЧИСЛО cmax=ЧИСЛО m=ЧИСЛО** - подобрать все c - взаимно простые с m. 0 < c < m; cmin <= c <= cmax.

3.2. **get_a m=ЧИСЛО** - подобрать минимальное a такое что, a-1 делится на все простые делители m. Если m делится на 4 то и a-1 делится на 4; 0 < a < m, m <= 18446744073709551615 (2^{64}-1). Результат выводится в выходной файл. Если не найдено решения - вывести 'no solution'.

3.3. **lcg a=ЧИСЛО x0=ЧИСЛО c=ЧИСЛО m=ЧИСЛО n=ЧИСЛО** - сгенерировать n чисел с помощью указанного ЛКГ. Результат вывести в файл.

0 <= a,x0,c,m,n <= 18446744073709551615 (2^{64}-1); a,x0,c < m. Вывести 'no solution' если вычисления невозможны (например, n=0, или a,c,x0 >= m).

3.4. **test inp=ИМЯ_ФАЙЛА** - Проверить сгенерированную последовательность, представленную в файле, на случайность одним из тестов, представленных в книге «Искусство программирования» (Д. Кнут). Вывести в файл параметры, по которым делается вывод о случайности последовательности, а также сам вывод.

4. Если команда не распознана, либо были указаны не все аргументы, либо аргументы указаны некорректно (например, отрицательные числа или буквы в значении аргумента), то в output.txt должно быть выведено **incorrect command**.

План исследования

Провести исследование ЛКГ по приведенному ниже алгоритму:

1. Протестировать ЛКГ на случайном наборе параметров:

1.1. Взять любое число m, такое что m - простое, 0 <= m <= 2^{64}-1

1.2. Взять любое c, 0 < c < m.

1.3. Взять любое a, 0 < a < m, такое, что a-1 - простое.

1.4. Вычислить период полученного ЛКГ для различных x_0 (не менее 10). Например, возьмите разные x_0, идущие подряд: 1,2,3,4,5,… В отчете описать способ определения периода ЛКГ. Сравнить результат с теоремой об ЛКГ. Объяснить полученный результат.

1.5. Протестировать сгенерированную ЛКГ последовательность на случайность.

2. Протестировать ЛКГ на специально сгенерированном наборе параметров:

2.1. Взять m такое, что m - произведение нескольких (не менее 10) простых множителей.

2.2. Используя разработанную программу, подобрать c такое, что c - взаимно просто с m. В отчете представить полученный утилитой вывод.

2.3. Используя утилиту, подобрать такое a, чтобы выполнялось условие теоремы о максимальном периоде ЛКГ. В отчете представить полученный утилитой вывод.

2.4. Оценить период для 10 различных x_0 (см. п. 1.4), сделать выводы о соответствии полученного периода теореме об ЛКГ. Объяснить полученный результат.

2.5. Вычислить мощность полученного генератора.

2.6. Протестировать последовательность, полученную с помощью данного ЛКГ, на случайность. Объяснить, является ли полученный генератор «псевдослучайным». Если получаемая последовательность далека от идеально случайной, объяснить, что можно улучшить в генераторе.

3. Взять m и c из п.2. Взять a такое, что a-1 - составное, но **НЕ удовлетворяет** условию теоремы о максимальном периоде ЛКГ. Провести исследования периода и случайности сгенерированной последовательности аналогично п.1.

4. Взять m и a из п. 2. Взять c такое, что c - **НЕ взаимно простое** с m. Провести исследования периода и случайности сгенерированной последовательности аналогично п.1.

5. Взять m из п.2, a - из п.3, c - из п. 4. Провести исследования случайности сгенерированной последовательности аналогично п.1.

Содержание отчета

1. Цель работы.

2. Ход работы.

2.1. Описание алгоритмов и методов, которые были применены при решении задачи (разработке программы).

2.2. Описание произведенных исследований ЛКГ, в том числе:

2.2.1. Способ определения периода ЛКГ.

2.2.2. Результаты запуска (вывод программы) для команд get_a и get_c (для тех подпунктов, где это требовалось).

2.2.3. Результаты запуска (вывод программы) для команды test для каждого из подпунктов.

2.2.4. Результирующая таблица, содержащая значения для m, c, a-1 и выводы о периоде и случайности сгенерированных последовательностей.

3. Выводы. Описание полученных в ходе выполнения работы знаний, умений и навыков. Описание трудностей, которые были встречены в работе, совершенных ошибок и способов их устранения.

4. Текст программы.

Критерии оценивания

Обязательная часть работы: все п.п. «Требований к программе», п.п. 1-2 «Плана исследования». Оценивается в 8 баллов.

Дополнительные задания:

– п. 3 «Плана исследования» - 3 балла;
– п. 4 «Плана исследования» - 3 балла;
– п. 5 «Плана исследования» - 3 балла.

В случае несдачи обязательной части работы в установленный преподавателем строк из общего количества баллов за работу вычитается 5 баллов.