11. Понятие о генераторах псевдослучайной последовательности. Алгоритмы генерации

Случайное число – число, представляющее собой реализацию случайной величины.

Детерминированный алгоритм – алгоритм, который возвращает те же выходные значения при тех же входных значениях.

Псевдослучайное число – число, полученное детерминированным алгоритмом, используемое в качестве случайного числа.

Физическое случайное число (истинно случайное) – случайное число, полученное на основе некоторого физического явления.

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

Линейный конгруэнтный генератор псевдослучайных чисел

Генераторы псевдослучайных чисел могут работать по разным алгоритмам. Одним из простейших генераторов является так называемый линейный конгруэнтный генератор, который для вычисления очередного числа k_i использует формулу

$k_i=(a*k_{i-1}+b) \bmod c$,

где a, b, c — некоторые константы, а k_{i-1} — предыдущее псевдослучайное число.

Для получения k_1 задается начальное значение k_0. Возьмем в качестве примера a=5,b=3,c=11 и пусть k_0= 1. В этом случае мы сможем по приведенной выше формуле получать значения от 0 до 10 (так как c = 11). Вычислим несколько элементов последовательности:

$k_1 = (5 * 1 + 3) \bmod 11 = 8$;

$k_2 = (5 * 8 + 3) \bmod 11 = 10$;

$k_3 = (5 * 10 + 3) \bmod 11 = 9$;

$k_4 = (5 * 9 + 3) \bmod 11 = 4$;

$k_5 = (5 * 4 + 3) \bmod 11 = 1$.

Полученные значения (8, 10, 9, 4, 1) выглядят похожими на случайные числа. Однако следующее значение k_6 будет снова равно 8:

$k_6 = (5 * 1 + 3) \bmod 11 = 8$,

а значения k_7 и k_8 будут равны 10 и 9 соответственно:

$k_7 = (5 * 8 + 3) \bmod 11 = 10$;

$k_8= (5 * 10 + 3) \bmod 11 = 9$.

Выходит, наш генератор псевдослучайных чисел повторяется, порождая периодически числа 8, 10, 9, 4, 1. К сожалению, это свойство характерно для всех линейных конгруэнтных генераторов. Изменяя значения основных параметров a, b и c, можно влиять на длину периода и на сами порождаемые значения k_i. Так, например, увеличение числа c в общем случае ведет к увеличению периода. Если параметры a, b и c выбраны правильно, то генератор будет порождать случайные числа с максимальным периодом, равным c. При программной реализации значение c обычно устанавливается равным 2^{b-1} или 2^b, где b — длина слова ЭВМ в битах.

Достоинством линейных конгруэнтных генераторов псевдослучайных чисел является их простота и высокая скорость получения псевдослучайных значений. Линейные конгруэнтные генераторы находят применение при решении задач моделирования и математической статистики, однако в криптографических целях их нельзя рекомендовать к использованию, так как специалисты по криптоанализу научились восстанавливать всю последовательность ПСЧ по нескольким значениям. Например, предположим, что противник может определить значения k_0, k_1, k_2, k_3. Тогда:

$k_1=(a*k_0+b) \bmod c$

$k_2=(a*k_1+b) \bmod c$

$k_3=(a*k_2+b) \bmod c$

Решив систему из этих трех уравнений, можно найти a, b и c.

Для получения псевдослучайных чисел предлагалось использовать также квадратичные и кубические генераторы:

$k_i=(a_1^2*k_{i-1}+a_2*k_{i-1}+b) \bmod c$

$k_i=(a_1^3*k_{i-1}+a_2^2*k_{i-1}+a_3*k_{i-1}+b) \bmod c$

Однако такие генераторы тоже оказались непригодными для целей криптографии по той же самой причине "предсказуемости".

Метод Фибоначчи с запаздыванием

Известны и другие схемы получения псевдослучайных чисел.

Метод Фибоначчи с запаздываниями (Lagged Fibonacci Generator) — один из методов генерации псевдослучайных чисел. Он позволяет получить более высокое "качество" псевдослучайных чисел.

Наибольшую популярность фибоначчиевы датчики получили в связи с тем, что скорость выполнения арифметических операций с вещественными числами сравнялась со скоростью целочисленной арифметики, а фибоначчиевы датчики естественно реализуются в вещественной арифметике.

Известны разные схемы использования метода Фибоначчи с запаздыванием. Один из широко распространённых фибоначчиевых датчиков основан на следующей рекуррентной формуле:

$$k_i = \begin{Bmatrix} k_{i-a} - k_{i-b}, & если\ k_{i-a} \geq k_{i-b} \\ k_{i-a} - k_{i-b} + 1, & если\ k_{i-a} < k_{i-b} \end{Bmatrix}$$

где k_i — вещественные числа из диапазона [0,1], a, b — целые положительные числа, параметры генератора. Для работы фибоначчиеву датчику требуется знать max{a,b} предыдущих сгенерированных случайных чисел. При программной реализации для хранения сгенерированных случайных чисел необходим некоторый объем памяти, зависящих от параметров a и b.

Пример. Вычислим последовательность из первых десяти чисел, генерируемую методом Фибоначчи с запаздыванием начиная с k_5 при следующих исходных данных: a = 4, b = 1, k_0=0.1; k_1=0.7; k_2=0.3; k_3=0.9; k_4=0.5:

$k_5 = k_1 - k_4 = 0.7 - 0.5 = 0.2;$

$k_6 = k_2 - k_5 = 0.3 - 0.2 = 0.1;$

$k_7 = k_3 - k_6 = 0.9 - 0.1 = 0.8;$

$k_8 = k_4 - k_7 + 1 = 0.5 - 0.8 + 1 = 0.7;$

$k_9 = k_5 - k_8 + 1 = 0.2 - 0.7 + 1 = 0.5;$

$k_{10} = k_6 - k_9 + 1 = 0.1 - 0.5 + 1 = 0.6;$

$k_{11} = k_7 - k_{10} = 0.8 - 0.6 = 0.2;$

$k_{12} = k_8 - k_{11} = 0.7 - 0.2 = 0.5;$

$k_{13} = k_9 - k_{12} + 1 = 0.5 - 0.5 + 1 = 1;$

$k_{14} = k_{10} - k_{13} + 1 = 0.6 - 1 + 1 = 0.6.$

Видим, что генерируемая последовательность чисел внешне похожа на случайную. И действительно, исследования подтверждают, что получаемые случайные числа обладают хорошими статистическими свойствами.

Для генераторов, построенных по методу Фибоначчи с запаздыванием, существуют рекомендуемые параметры a и b, так сказать, протестированные на качество. Например, исследователи предлагают следующие значения: (a,b) = (55, 24), (17, 5) или (97,33). Качество получаемых случайных чисел зависит от значения константы a: чем оно больше, тем выше размерность пространства, в котором сохраняется равномерность случайных векторов, образованных из полученных случайных чисел. В то же время с увеличением величины константы a увеличивается объём используемой алгоритмом памяти.

В результате значения (a,b) = (17,5) рекомендуются для простых приложений. Значения (a,b) = (55,24) позволяют получать числа, удовлетворительные для большинства

криптографических алгоритмов, требовательных к качеству случайных чисел. Значения (a,b) = (97,33) позволяют получать очень качественные случайные числа и используются в алгоритмах, работающих со случайными векторами высокой размерности.
Генераторы ПСЧ, основанные на методе Фибоначчи с запаздыванием, использовались для целей криптографии. Кроме того, они применяются в математических и статистических расчетах, а также при моделировании случайных процессов. Генератор ПСЧ, построенный на основе метода Фибоначчи с запаздыванием, использовался в широко известной системе Matlab.