Союз Советских Социалистических Республик

Государственный комитет СССР по делам изобретений и открытий

ОПИСАНИЕ ИЗОБРЕТЕНИЯ

К АВТОРСКОМУ СВИДЕТЕЛЬСТВУ

(11) 890391

(61) Дополнительное к авт. свид-ву -

(22) Заявлено 30.04.80 (21) 2919555/18-24

с присоединением заявки № -

(23) Приоритет -

Опубликовано 15.12.81. Бюллетень № 46

Дата опубликования описания 15.12.81

(51) М. Кл.[3] G 06 F 7/58

(53) УДК 681.325 (088.8)

(72) Авторы изобретения В.Н. Ярмолик, А.Е. Леусенко и А.Н. Морозевич

(71) Заявитель Минский радиотехнический институт

(54) ГЕНЕРАТОР ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ

1

Изобретение относится к вычислительной технике и может быть использовано в качестве устройства для получения случайных чисел при решении задач методом Монте-Карло, для построения генераторов случайных процессов с заданными характеристиками, а также для генерирования случайных процессов с равномерным спектром, используемых для идентификации систем автоматического управления.

Известен генератор псевдослучайных чисел, содержащий два регистра сдвига и группу сумматоров по модулю два [1].

Недостатком этого генератора является сложность структурного построения, методика синтеза подобного генератора псевдослучайных чисел значительно затруднена. Кроме того, для построения генератора псевдослучайных чисел необходимо выбирать такие структуры исходных генераторов, у которых периоды являются взаимно простыми числами.

2

Известен также параллельный генератор псевдослучайных чисел, который отличается максимальной величиной быстродействия и позволяет формировать многоразрядные псевдослучайные числа [2].

Недостаток этого генератора заключается в сложности схем формирования сдвинутых последовательностей, определяемой числом входов сумматоров по модулю два. Каждый сумматор в среднем имеет m/2 входов. При этом затраты оборудования, необходимые для схем формирования сдвинутых последовательностей, в несколько раз превышают затраты, идущие на построение кольцевого регистра сдвига.

Наиболее близким техническим решением к предлагаемому изобретению является генератор псевдослучайных чисел, содержащий m-разрядный регистр сдвига, два элемента И и элемент ИЛИ, которые реализуют операцию сложения по модулю два содержимого m-го и j-го

разряда регистра сдвига. Номер j-го разряда в зависимости от разрядности регистра сдвига m выбирается из таблицы [3].

Недостатком этого устройства является отличие вероятности появления нуля или единицы на его выходе от 0,5.

Цель изобретения - повышение точности генератора.

Поставленная цель достигается тем, что в генератор псевдослучайных чисел, содержащий m-разрядный регистр сдвига, первый элемент И, к первому входу которого подключен инверсный выход m-го разряда регистра сдвига RC, второй элемент И, к первому входу которого подключен прямой выход m-го разряда регистра сдвига, элемент ИЛИ, выход которого подключен ко входу первого разряда регистра сдвига, дополнительно введены третий элемент И, четвертый элемент И и элемент ИЛИ-НЕ, причем ко вторым входам первого и второго элементов И подключены инверсный и прямой выходы j-го разряда регистра сдвига соответственно, а выходы первого и второго элементов И подключены к первому и второму входам элемента ИЛИ-НЕ, ко входам четвертого элемента И подключены инверсные выходы m-1 первых разрядов регистра сдвига, а выход четвертого элемента И подключен к третьему входу элемента ИЛИ-НЕ и к первому входу третьего элемента И, ко второму входу которого подключен инверсный выход m-го разряда регистра сдвига, выход элемента ИЛИ-НЕ подключен к первому входу элемента ИЛИ, ко второму входу которого подключен выход третьего элемента И.

На фиг. 1 приведена функциональная схема генератора; на фиг. 2 - последовательность состояний известного (а) и предлагаемого (б) генераторов при m = 3 и j = 1.

Генератор состоит из регистра сдвига 1, первого, второго и третьего элементов И 2, 3, 4, четвертого элемента И 5, элемента ИЛИ-НЕ 6, и элемента ИЛИ 7. К первому входу первого элемента И 2 подключен инверсный выход m-го разряда регистра сдвига 1, к первому входу второго элемента И 3 подключен прямой выход m-го разряда регистра сдвига 1, а выход элемента ИЛИ 7 подключен ко входу первого разряда регистра сдвига 1. Ко вторым входам первого и второго элемента И 2 и 3 подключены инверсный и прямой выходы j-го разряда регистра сдвига 1 соответственно, а выходы первого и второго элементов И 2 и 3 подключены к первому и второму входам элемента ИЛИ-НЕ 6, ко входам четвертого элемента И 5 подключены инверсные выходы m-1 первых разрядов регистра сдвига 1, а его выход подключен к третьему входу элемента ИЛИ-НЕ 6 и первому входу третьего элемента И 4, ко второму входу которого подключен инверсный выход m-го разряда регистра сдвига 1, выход элемента ИЛИ-НЕ 6 подключен к первому входу элемента ИЛИ 7, а ко второму входу элемента ИЛИ 7 подключен выход третьего элемента И 4.

Генератор работает следующим образом.

В исходном состоянии регистр сдвига содержимое k-го разряда может принимать значение нуля или единицы. В отличие от известных генераторов в данном генераторе в первоначальный момент в разрядах регистра 1 может находиться нулевой код. В зависимости от начального кода на выходе комбинационной части, т.е. на выходе элемента ИЛИ 7, формируется символ, равный нулю или единице. По приходу тактового импульса содержимое регистра сдвига 1 сдвигается на один разряд вправо, а в первый разряд записывается символ, сформированный на выходе элемента ИЛИ 7. При значениях содержимого первых m-1 разрядов регистра сдвига 1, отличных от нуля, элементы 2, 3, 6 и 7 реализуют операцию суммирования по модулю два содержимого j-го и m-го разрядов регистров сдвига. В этом случае генерируется М-последовательность, как и в известном. Далее, при появлении в первых m-1 разрядах регистра 1 нулевой комбинации на выходе элемента 5 появляется единичный уровень, который обеспечивает появление на входе первого разряда регистра сдвига 1 нуля.

При поступлении очередного тактового импульса в регистре сдвига 1 находятся нулевые значения во всех разрядах. Появление нуля в m-ом разряде обеспечивает появление единицы на выходе элемента 4, которая через элемент 7 поступает на вход первого разряда регистра сдвига 1. Очередной тактовый импульс обеспечивает появление в регистре сдвига 1 комбинации 100...0, т.е. нулей во всех разрядах, кроме

первого. Далее, так же как и известном, генерируется М-последовательность. В этом случае содержимое первых m-1 разрядов регистра сдвига 1 отлично от нуля и элементы 2, 3, 6 и 7 реализуют операцию суммирования по модулю два.

Как видно из фиг. 2, последовательность на выходе предлагаемого генератора отличается от М-последовательности, полученной на выходе известного только кодом 000, следующим после кода 001.

Введение нулевой комбинации в М-последовательность позволяет приблизить вероятность нуля и единицы к 0,5. В силу того, что количество нулей и единиц в выходной последовательности генератора равняется 2^{m-1}, а количество символов 2^m, вероятность нуля и единицы на выходе системы равняется 0,5. Кроме того, дополнительные затраты оборудования составляют всего три логических элемента.

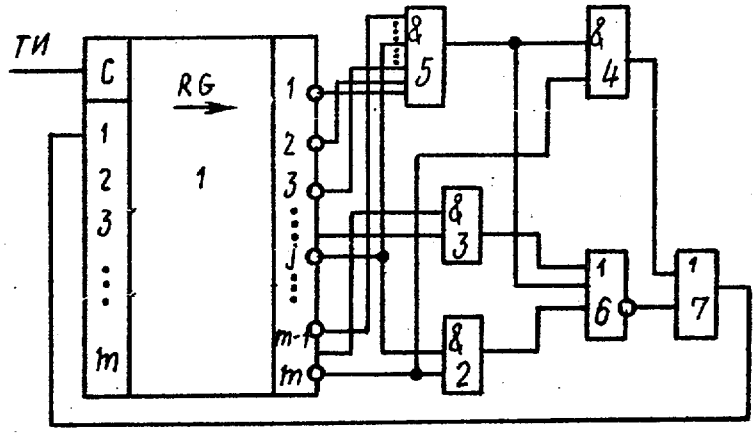
Применение подобного генератора псевдослучайных чисел позволит повысить качество псевдослучайных последовательностей, а тем самым точность и достоверность решения задач методом Монте-Карло.

Формула изобретения

Генератор псевдослучайных чисел, содержащий m-разрядный регистр сдвига, первый элемент И, к первому входу которого подключен инверсный выход m-го разряда регистра сдвига, второй элемент И, к первому входу которого подключен прямой выход m-го разряда регистра сдвига, элемент ИЛИ, выход которого подключен ко входу первого разряда регистра сдвига, *отличающийся* тем, что, с целью повышения точности генератора, он содержит третий элемент И, четвертый элемент И, элемент ИЛИ-НЕ, причем ко вторым входам первого и второго элементов И подключены инверсный и прямой выходы j-го разряда регистра сдвига соответственно, а выходы первого и второго элементов И подключены к первому и второму входам элемента ИЛИ-НЕ, ко входам четвертого элемента И подключены инверсные выходы m-1 первых разрядов регистра сдвига, а выход четвертого элемента И подключен к третьему входу элемента ИЛИ-НЕ и к первому входу третьего элемента И, ко второму входу которого подключен инверсный выход m-го разряда регистра сдвига, а выход элемента ИЛИ-НЕ подключен к первому входу элемента ИЛИ, ко второму входу которого подключен выход третьего элемента И.

Источники информации, принятые во внимание при экспертизе

1. Яковлев В.В., Федоров Р.Ф. Вероятностные вычислительные машины. Л., "Машиностроение", 1974, с. 263.
2. Там же, с. 254.
3. Там же, с. 247 (прототип).



Фиг.1

а	б
111	111
011	011
101	101
010	010
001	001
100	000
110	100
	110

Фиг.2

ВНИИПИ Заказ11007/78 Тираж 748 Подписное

Филиал ППП"Патент", г. Ужгород,ул. Проектная,4