Союз Советских Социалистических Республик

Государственный комитет СССР по делам изобретений и открытий

ОПИСАНИЕ ИЗОБРЕТЕНИЯ

К АВТОРСКОМУ СВИДЕТЕЛЬСТВУ

(11) 903872

(61) Дополнительное к авт. свид-ву -

(22) Заявлено 05.05.80 (21) 2920810/18-24

с присоединением заявки № -

(23) Приоритет -

(51) М. Кл.[3] G 06 F 7/58

Опубликовано 07.02.82. Бюллетень № 5

Дата опубликования описания 09.02.82

(53) УДК 681.325 (088.8)

(72) Автор изобретения В. Н. Ярмолик

(71) Заявитель Минский радиотехнический институт

ЗСССР 13 ПАТЕНТНО-ТЕХНИЧЕСКАЯ БИБЛИОТЕКА 13

(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, а также для построения генераторов случайных процессов с заданными характеристиками. Весьма важной областью применения подобных устройств является область генерирования случайных процессов с равномерным спектром, используемых для идентификации систем автоматического управления. Кроме того, генератор псевдослучайных чисел, позволяющий получать случайные числа с равномерным распределением, часто используется как составной блок для построения генераторов случайных чисел с произвольным законом распределения. При этом весьма важным оказывается качество первичных равномерно распределенных чисел, которое в первую очередь определяется законом распределения и автокорреляционной функцией.

2

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

Недостатком этого генератора является сложность структурного построения, а также усложненная методика синтеза. Кроме того, необходимым требованием для построения генератора псевдослучайных чисел является необходимость выбора таких структур исходных последовательностей, у которых периоды являются взаимно простыми числами, что не всегда оказывается возможным.

Наиболее близким по технической сущности к изобретению является генератор псевдослучайных чисел, содержащий m триггеров, $m-j$ двухвходовых сумматоров по модулю два. Выходы m триггеров соединены со счетными входами триггеров других разрядов и входами $m-j$ сумматоров по модулю два соответственно, выходы которых соединены со

счетными входами первых j триггеров. Для получения суммы по модулю два в описываемом генераторе используются свойства суммирования по модулю два хранений информации, поступающей на счетный вход триггера. В результате выполнения операций суммирования по модулю два на триггерах и сумматорах по модулю два за один такт формируется m-разрядное равномерно распределенное псевдослучайное число [2].

Недостатком этого устройства является невозможность получения на его выходе значения m-разрядного псевдослучайного числа $\xi_k = \underbrace{000\ldots0}_{m}$. Отсутствие комбинации $\xi_k = 000\ldots0$ приводит к искажению равномерного закона распределения, которое уменьшается с увеличением величины m.

Цель изобретения - расширение функциональных возможностей генератора и повышение точности генерирования выходных последовательностей равномерно распределенных m-разрядных псевдослучайных чисел, что достигается приближением вероятности к величине, равной 1/2.

Поставленная цель достигается тем, что в генератор псевдослучайных чисел, содержащий m триггеров, входы которых подключены к выходу генератора синхроимпульсов, дополнительно введены две группы по $m-2$ элементов ИЛИ, группа из $m-2$ элементов ИЛИ-НЕ, два элемента НЕ и m сумматоров по модулю два, причем выходы i-ных элементов ИЛИ в первой и второй группах подключены к первым входам $(i+1)$-ных элементов ИЛИ, к первым входам первых элементов ИЛИ в обоих группах подключены выход первого триггера и выход m-ого сумматора по модулю два соответственно, ко второму входу i-ого элемента ИЛИ первой и второй групп подключены квыход $(i+1)$-ого триггера и выход $(m-i)$-ого сумматора по модулю два соответственно, ко входам первого и второго элементов НЕ подключены выходы $(m-2)$-ных элементов ИЛИ первой и второй групп соответственно, выход i-ого элемента ИЛИ первой группы подключен к первому входу $(i+1)$-ого элемента ИЛИ-НЕ, а к первому входу первого элемента ИЛИ-НЕ подключен выход первого триггера, выход i-ого элемента ИЛИ второй группы подключен ко второму входу $(m-2-i)$-ого элемента ИЛИ-НЕ, ко второму входу $(m-2)$-ого элемента ИЛИ-НЕ подключен выход m-ого сумматора по модулю два, к первому входу i-ого сумматора по модулю два подключен выход i-ого триггера, ко входу которого подключен выход i-ого сумматора по модулю два, выход i-ого элемента ИЛИ-НЕ подключен ко второму входу $(i+1)$-ого сумматора по модулю два, ко второму входу i-ого и m-ого сумматора по модулю два подключены соответственно выходы второго и первого элементов НЕ, к третьим входам j-старших сумматоров по модулю два подключены выходы j-младших триггеров, а к третьим входам $m-j$-младших сумматоров по модулю два подключены выходы $m-j$-старших сумматоров по модулю два, выходы сумматоров по модулю два являются выходами генератора.

На фиг. 1 приведена функциональная схема генератора при $m = 5$ и $j = 3$; на фиг. 2 - временная диаграмма работы генератора.

Функциональная схема генератора псевдослучайных чисел, состоит из $m = 5$ триггеров 1, первой и второй группы по $m-2 = 3$ элементов ИЛИ 2 и 3, первого и второго элементов НЕ 4 и 5, группы из $m-2 = 3$ элементов ИЛИ-НЕ 6 и группы из $m=5$ сумматоров 7 по модулю два. Выходы i-ных элементов ИЛИ 2 и 3 в первой и второй группах подключены к первым входам $(i+1)$-ных элементов ИЛИ, к первым входам первых элементов ИЛИ 2 и 3 обеих групп подключены выход первого триггера группы триггеров 1 и выход m-ого сумматора 7 по модулю два соответственно, ко второму входу i-ого элемента ИЛИ 2 и 3 первой и второй группы подключен выход $(i+1)$-ого триггера 1 и выход $(m-i)$-ого сумматора 7 по модулю два соответственно, ко входам первого и второго элементов НЕ 4 и 5 подключены выходы $(m-2)$-ных элементов ИЛИ 2 и 3 первой и второй группы соответственно, выход i-ого элемента ИЛИ 2 первой группы подключен к первому входу $(i+1)$-ого элемента ИЛИ-НЕ 4, а к первому входу первого элемента ИЛИ-НЕ 4 подключен выход первого триггера 1, выход i-ого элемента ИЛИ второй группы подключен ко второму входу $(m-i-2)$-ого элемента ИЛИ-НЕ 4, ко второму входу $(m-2)$-ого элемента ИЛИ-НЕ 4 подключен выход m-ого сумматора 7 по модулю два, к первому входу i-ого сумматора 7 по модулю два подключен выход i-ого триггера 1, ко входу которого подклю-

чен выход i-ого сумматора 7 по модулю два, выход i-ого элемента ИЛИ-НЕ 4 подлкючен ко второму входу (i+1)-ого сумматора 7 по модулю два, ко второму входу i-ого и m-ого сумматора 7 по модулю два подключены соответственно выходы второго и первого элементов НЕ 3 и 2, к третьим входам j-старших сумматоров 7 по модулю два подключены выходы j-младших триггеров 1, а к третьим входам m-j-младших сумматоров 7 по модулю два подключены выходы m-j-старших сумматоров 7 по модулю два, к синхровходам триггеров 1 подключен выход генератора синхроимпульсов.

Функционирование генератора псевдослучайных чисел происходит следующим образом.

В исходном состоянии триггеры 1 генератора находятся в произвольном состоянии, т.е. значение К-ого разряда $X_K(0)$ может принимать значение нуля или единицы с равной вероятностью. В отличие от известного, в предлагаемом генераторе в первоначальный момент на триггерах может храниться нулевой код. В зависимости от начального кода на выходах трехвходовых сумматоров 7 по модулю два образуется псевдослучайное число. По приходу синхроимпульса информация с выходов сумматоров 7 записывается на триггере 1. Элементы ИЛИ 2 и 3, элементы ИЛИ-НЕ, элементы НЕ, а также сумматоры по модулю два выполняют операции логического произведения двух переменных, логического произведения с инверсией двух переменных, инверсии и суммирования по модулю два соответственно. При значениях содержимого m триггеров, обеспечивающих на выходе схем последовательность кодов $\xi_{\gamma K} \neq 000...0$, устройство генерирует на выходе сдвинутые участки по m символов из m-последовательности. В то же время в данном генераторе некоторому коду $\xi_{\gamma K}$, зависящему от m и j и хранящемуся на триггерах 1, соответствует нулевой код на выходе сумматоров по модулю два, который в очередном такте записывается на триггеры 1. Наличие нулевого кода на триггерах 1 позволяет получить на выходе устройства очередное значение ξ_K, в то время как появление нулевого кода в разрядах регистра известного генератора срывает генерирование псевдослучайных последовательностей.

Более подробно процесс работы предлагаемого ГПСЧ пояснен конкретным примером.

На фиг. 2а показана последовательность состояний последовательного генератора, где пунктирной стрелкой показана последовательность состояний регистра известного генератора. На фиг. 2б приведена последовательность состояний последовательного генератора, содержащего нулевой код после кода 000...1, а также пунктирной стрелкой показана последовательность состояний триггеров 1. Как видно на фиг. 2 последовательность кодов на выходе предлагаемого генератора отличается от последовательности, получаемой на выходе известного генератора, наличием кода 0000.

Возможность получения на выходе генератора комбинации 000...0 приводит к выравниванию вероятности $P(\xi_{\gamma K})$, которая равняется $1/2^m$. Таким образом, получение нулевой комбинации на выходе устройства расширяет его функциональные возможности и обеспечивает повышение качества выходных последовательностей. Отсутствие запрещенных кодов $\xi_{\gamma K}$ позволяет повысить надежность генератора, так наличие нуля на триггерах 1 не срывает генерирования псевдослучайной последовательности. Кроме того, дополнительные аппаратурные затраты на один разряд при построении генератора составляет всего $2 - \frac{4}{m}$ элементов ИЛИ, $(1 - \frac{2}{m})$ ИЛИ-НЕ, $\frac{2}{m}$ элементов НЕ, один сумматор по модулю два.

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

Формула изобретения

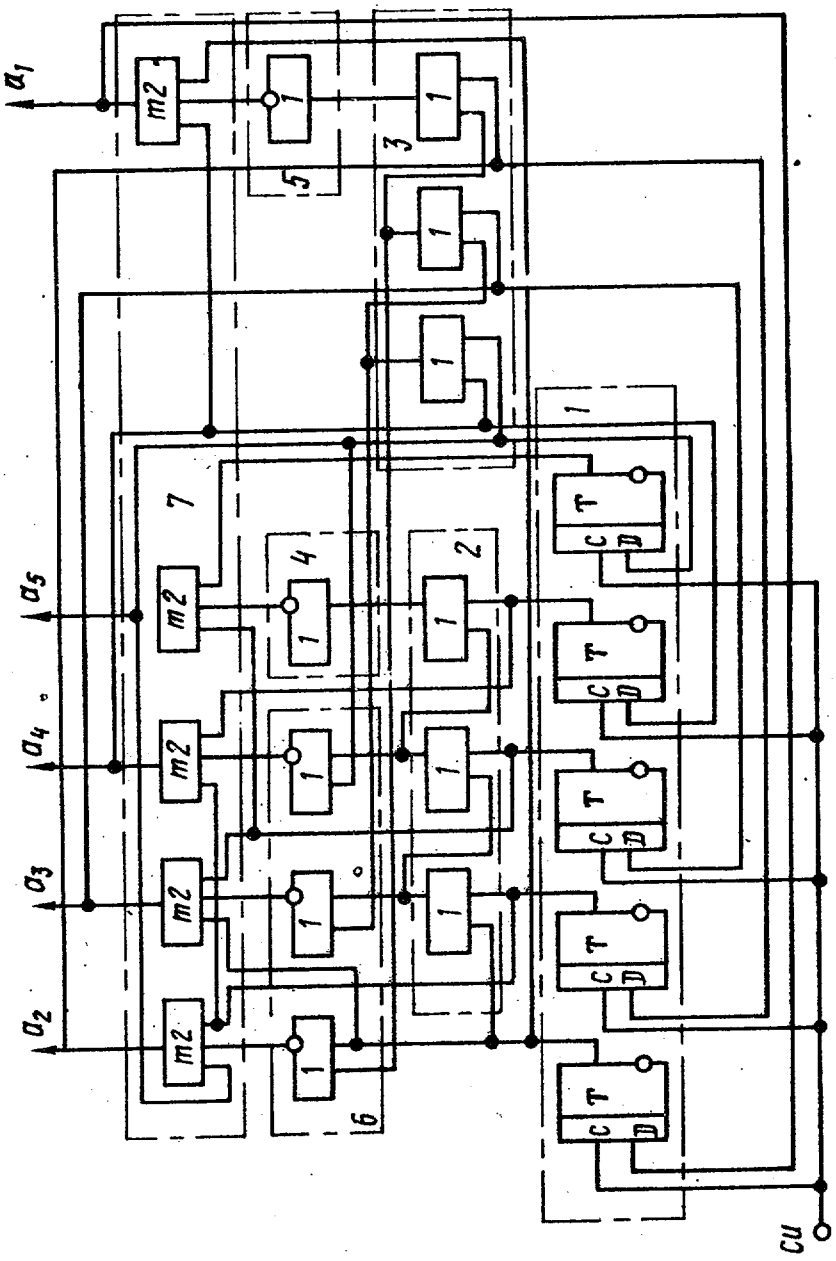
Генератор псевдослучайных чисел, содержащий m триггеров, входы которых подключены к выходу генератора синхроимпульсов, отличающийся тем, что, с целью повышения точности генерирования выходных последовательностей, дополнительно введены две группы по m-2 элементов ИЛИ, груп-

па из m-2 элементов ИЛИ-НЕ, два элемента НЕ и m сумматоров по модулю два, причем выходы i-ных элементов ИЛИ в первой и второй группах подключены к первым входам (i+1)-ных элементов ИЛИ, к первым входам первых элементов ИЛИ в обоих группах подключены выход первого триггера и выход m-ого сумматора по модулю два соответственно, ко второму входу i-ого элемента ИЛИ первой и второй групп подключены выход (i+1)-ого триггера и выход (m-i)-ого сумматора по модулю два соответственно ко входам первого и второго элементов НЕ подключены выходы (m-2)-ных элементов ИЛИ первой и второй групп соответственно, выход i-ого элемента ИЛИ первой группы подключен к первому входу (i+1)-ого элемента ИЛИ-НЕ, а к первому входу первого элемента ИЛИ-НЕ подключен выход первого триггера, выход i-ого элемента ИЛИ второй группы подключен ко второму входу $(m-2-i)$-ого элемента ИЛИ-НЕ, ко второму входу $(m-2)$-ого элемента ИЛИ-НЕ подключен выход m-ого сумматора по модулю два, к первому входу i-ого сумматора по модулю два подключен выход i-ого триггера, ко входу которого подключен выход i-ого сумматора по модулю два, выход i-ого элемента ИЛИ-НЕ подключен ко второму входу $(i+1)$-ого сумматора по модулю два, ко второму входу i-ого и m-ого сумматора по модулю два подключены соответственно выходы второго и первого элементов НЕ, к третьим входам j-старших сумматоров по модулю два подключены выходы j-младших триггеров, а к третьим входам m-j-младших сумматоров по модулю два подключены выходы m-j-старших сумматоров по модулю два, выходы сумматоров по модулю два являются выходами генератора.

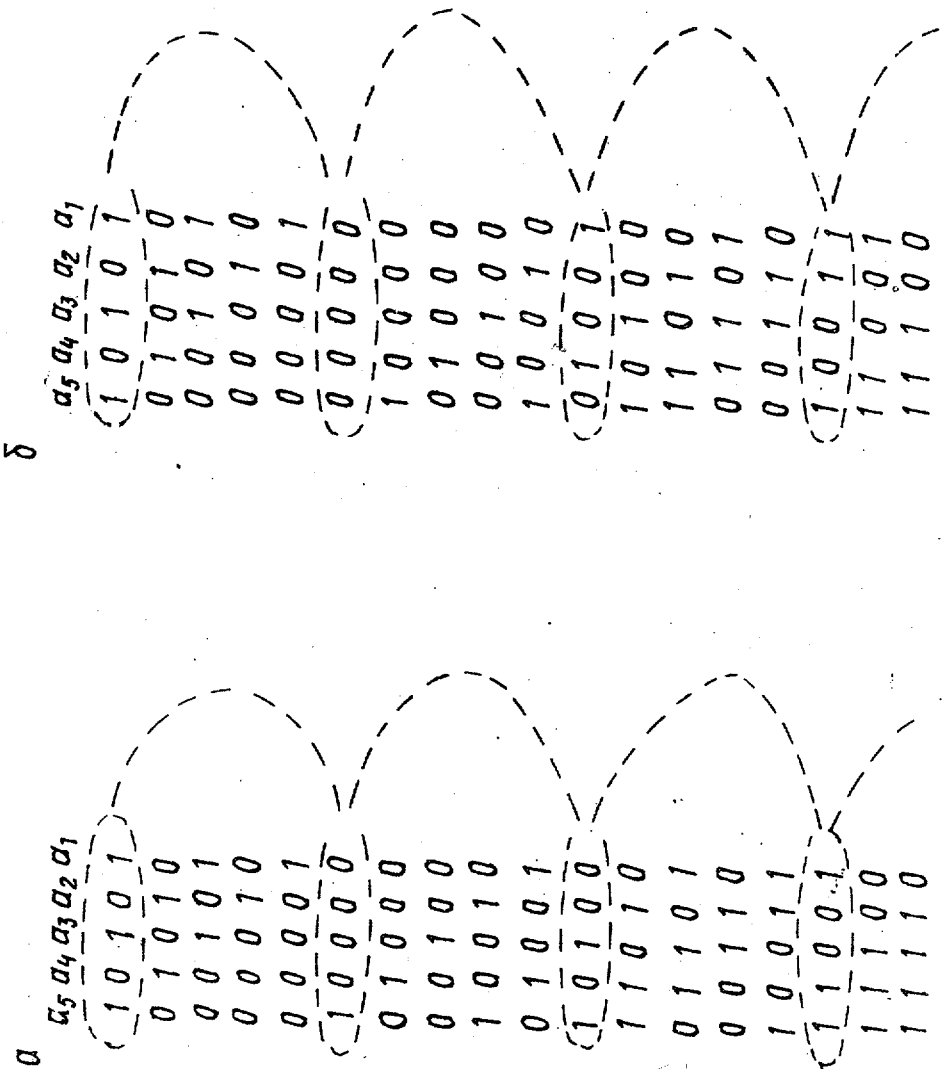
Источники информации, принятые во внимание при экспертизе

1. Яковлев В.В. и Федоров Р.Ф. Вероятностные вычислительные машины. Л., "Машиностроение", 1974, с. 344.

2. Авторское свидетельство СССР № 572823, кл. G 07 C 15/00, 1975 (прототип).



Фиг.1



Фиг.2

Составитель А. Карасов
Редактор Н. Лазаренко Техред М.Гергель Корректор Г. Огар
Заказ 121/30 Тираж 731 Подписное
ВНИИПИ Государственного комитета СССР
по делам изобретений и открытий
113035, Москва, Ж-35, Раушская наб., д. 4/5
Филиал ППП "Патент", г. Ужгород, ул. Проектная, 4