Союз Советских Социалистических Республик

Государственный комитет СССР по делам изобретений и открытий

ОПИСАНИЕ ИЗОБРЕТЕНИЯ

К АВТОРСКОМУ СВИДЕТЕЛЬСТВУ

(11) 907548

(61) Дополнительное к авт. свид-ву -

(22) Заявлено 08.07.80 (21) 2958815/18-24

с присоединением заявки № -

(23) Приоритет -

Опубликовано 23.02.82. Бюллетень № 7

Дата опубликования описания 25.02.82

(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, а также для построения генераторов случайных процессов с заданными характеристиками, кроме того, применение подобных устройств может быть использовано 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. Кроме того, при построении генератора необходимо выбирать структуры исходных генераторов такими, чтобы их периоды являлись взаимно

2

простыми числами, что не всегда оказывается возможным.

Наиболее близким по технической сущности к изобретению является генератор псевдослучайных чисел, содержащий первую и вторую группы двухвходовых сумматоров по модулю два, первую и вторую группы трехвходовых сумматоров по модулю два, первую и вторую группы элементов И, группу элементов ИЛИ, группу триггеров и генератор равновероятной двоичной цифры [2].

Известный генератор предназначен для генерирования за один такт двух m разрядных псевдослучайных чисел, причем вероятность появления нуля или единицы в разрядах псевдослучайных чисел по первому и второму каналам равняется 0,5.

Недостаток известного устройства - низкое быстродействие.

Цель изобретения - увеличение быстродействия генератора псевдослучайных чисел.

Поставленная цель достигается тем, что в генератор псевдослучайных чисел, содержащий первую и вторую группы трехвходовых сумматоров по модулю два, первую и вторую группы элементов И, группу элементов ИЛИ, группу триггеров и генератор равновероятной двоичной цифры, ко входу которого подключен выход генератора тактовых импульсов, а единичный и нулевой выходы генератора равновероятной двоичной цифры подключены к первым входам элементов И первой и второй группы соответственно, ко второму входу j (j - число сумматоров по модулю два в первой группе) старших элементов И первой группы подключены выходы j старших трехвходовых сумматоров по модулю два первой группы, ко второму входу m-j (m - число элементов И в каждой группе, а число элементов ИЛИ в группе - число триггеров в группе) старших элементов И второй группы подключены выходы m-j старших трехвходовых сумматоров по модулю два второй группы, выходы i-ых (i=1,2,...) элементов И первой и второй группы подключены ко входам i-го элемента ИЛИ, выход которого подключен к D входу i-го триггера, к синхровходу которого подключен выход генератора тактовых импульсов, к первым входам i-ых трехвходовых сумматоров по модулю два первой и второй групп подключены единичные выходы (m-j+i) и (j+i)-ых триггеров соответственно, ко вторым входам j трехвходовых сумматоров по модулю два первой группы подключены выходы младших триггеров, ко вторым входам m-j трехвходовых сумматоров по модулю два второй группы подключены выходы m-j младших триггеров, к третьим входам j трехвходовых сумматоров по модулю два первой группы подключен нулевой выход генератора равновероятной двоичной цифры, к третьим входам m-j трехвходовых сумматоров по модулю два второй группы подключен нулевой и единичный выход генератора равновероятной двоичной цифры, соответственно введены группа четырехвходовых сумматоров по модулю два, n групп сумматоров по модулю два, по j(i+3)-входовых сумматоров по модулю два в i-ой группе и m-n·j (n+3)-входовых сумматоров по модулю два в n-ой группе, причем к первым, вторым и третьим входам (m-i)-ых четырехвходовых сумматоров по модулю два подключены выходы (2m-2j-i)-ых, (2m-j--i)-ых и (m-i)-ых триггеров (i=m-j, m-1) соответственно, а выходы j четырехвходовым сумматором по модулю два подключены ко второму входу j младших элементов И второй группы, к четвертым входам j четырехвходовых сумматоров по модулю два подключен единичный выход генератора равновероятной двоичной цифры, на первый, второй и третий входы ℓ-го (i+3) входового сумматора по модулю два i-ой группы заведены выходы (m+1-i)-ых (j+1-ℓ)-ых триггеров и нулевого выхода генератора равновероятной двоичной цифры соответственно, а на (K+3)-ие входы ℓ-го (i+3)-входового сумматора по модулю два заведены входы (m-j+1-K)-го триггера, кроме того, вторые входы m-j младших элементов И первой группы подключены к выходам m-j (i+3) входовых сумматоров по модулю два.

На фиг. 1 приведена функциональная схема генератора псевдослучайных чисел при m = 4 и j = 1; на фиг. 2 - временная диаграмма его работы.

Генератор псевдослучайных чисел состоит из m триггеров 1, m элементов ИЛИ 2, первой группы из m элементов И 3, второй группы из m элементов И 4, генератора 5 равновероятной двоичной цифры, $n \approx m/j-1$ по j i + 3 входовых сумматоров по модулю два в i-ой группе и m-n j n+3 входовых сумматоров по модулю два в n-ой группе 6, j четырехвходовых сумматоров по модулю два 7, первой группы из j трехвходовых сумматоров по модулю два 8, второй группы из m-j трехвходовых сумматоров по модулю два 9.

Количество трехвходовых сумматоров по модулю два в первой группе равняется j, а во второй группе - m-j. В то же время количество (i+3) входовых сумматоров по модулю два 6 равняется m-j, а количество четырехвходовых - j. На выходах (i=3) входовых сумматоров по модулю два блока 6 и трехвходовых сумматоров по модулю два 8 получается значение

псевдослучайного числа $\xi_1 = a_0, a_1 \ldots, a_m$, а на выходах четырехвходовых сумматоров по модулю два 7 и трехвходовых второй группы 3 значение псевдослучайного числа $\xi_2 = a'_1, a'_2, \ldots, a'_m$. Числа ξ_1 и ξ_2 представляют собой m-разрядные коды или их инверсии М последовательностей, порождаемых следующими полиномами $\varphi(Z) = Z^m + Z^8 + 1$ и $\varphi(Z) = Z^m + Z^{m-j} + 1$, причем периоды обоих последовательностей одинаковы. Последовательность следования кодов отлична и случайна как в первой, так и во второй М последовательности. Появление прямого кода М последовательности или его инверсии по первому и второму каналу определяется значением очередного отсчета на выходе генератора равновероятной двоичной цифры. Выходы D-триггеров и генератора равновероятной двоичной цифры соединены со входами трехвходовых сумматоров по модулю два первой и второй группы.

Выходы D-триггеров соединены со входами m-j многовходовых сумматоров по модулю два 6.

В зависимости от значения равновероятной двоичной цифры на выходе генератора 5 равновероятной двоичной цифры код псевдослучайного числа ξ_1 или ξ_2 с выходов сумматоров по модулю два через элементы ИЛИ 2 записывается на D-триггеры. Генератор 5 представляет собой простой датчик равновероятной двоичной цифры.

Функционирование генератора псевдослучайных чисел происходит следующим образом.

В начальный момент на D-триггеры записывается ненулевой код. На выходах сумматоров по модулю два 6 и 8 образуется очередной код псевдослучайного числа первой М последовательности в том случае, если x(K) в данный момент времени равняется 0, а на выходе сумматоров по модулю два 7 и 9 образуется обратный код псевдослучайного числа, второй М последовательности, так как $\overline{x(K)}=1$. В случае, когда x(K)=1, на выходе блоков 6 и 8 образуется обратный код, в котором проинвертированы значения разрядов псевдослучайного числа, а на выходе блоков 7 и 9 соответственно прямой, так как $\overline{x(K)}=0$. В зависимости от значения очередной двоичной цифры на выходе генератора $5 x(K) \in \{0,1\}$ по приходу тактового импульса на синхронизирующие входы триггеров 1 на их D-входы через первую или вторую группы элементов И 3, 4 и через элементы ИЛИ 2, определяющие выходы обоих групп элементов И, подается очередной код первой или второй М последовательности. С приходом очередного тактового импульса процесс повторяется.

Временная диаграмма работы предлагаемого генератора псевдослучайных чисел полностью соответствует временной диаграмме работы известного генератора, т.е. они генерируют абсолютно идентичные последовательности.

В то же время предлагаемое устройство отличается значительно большим быстродействием. Частота следования тактовых импульсов будет определяться временем прохождения электрического сигнала по самому длинному пути, т.е. величиной $T = 4t_э$, причем величина T не зависит от значения m. При любом m величина T неизменна. Для случая m = = 10 и j = 3 величина задержки для известного устройства определяется выражением $T = 1it$, что в $\frac{1}{4} = 2\frac{3}{4}$ раза больше чем в предлагаемом устройстве, а для $m_1 = 20$ $T = 17t_э + 4t_э = 21t_э$, т.е. $\frac{21}{4} = 1\frac{1}{4}$ раз больше, чем в предлагаемом устройстве. Таким образом видно, что быстродействие предлагаемого устройства существенно увеличилось по сравнению с известным для любых m, так при m = 10 и m = 20 быстродействие увеличивается более чем в два и более чем в пять раз соответственно.

Таким образом, природа выходных псевдослучайных последовательностей предлагаемого генератора максимально приближена к истинно случайным числам, он отличается высоким быстродействием и простотой технической реализации.

Удельные аппаратурные затраты на один разряд псевдослучайного числа составляют незначительный объем элементов И, ИЛИ, m_2 и триггеров. Данный генератор псевдослучайных чисел позволяет получать числа по двум каналам, кроме того, его применение позволяет повысить точность и достоверность решения задачи методом Монте-Карло и получать истинно белый шум для построения генератора случайных процессов.

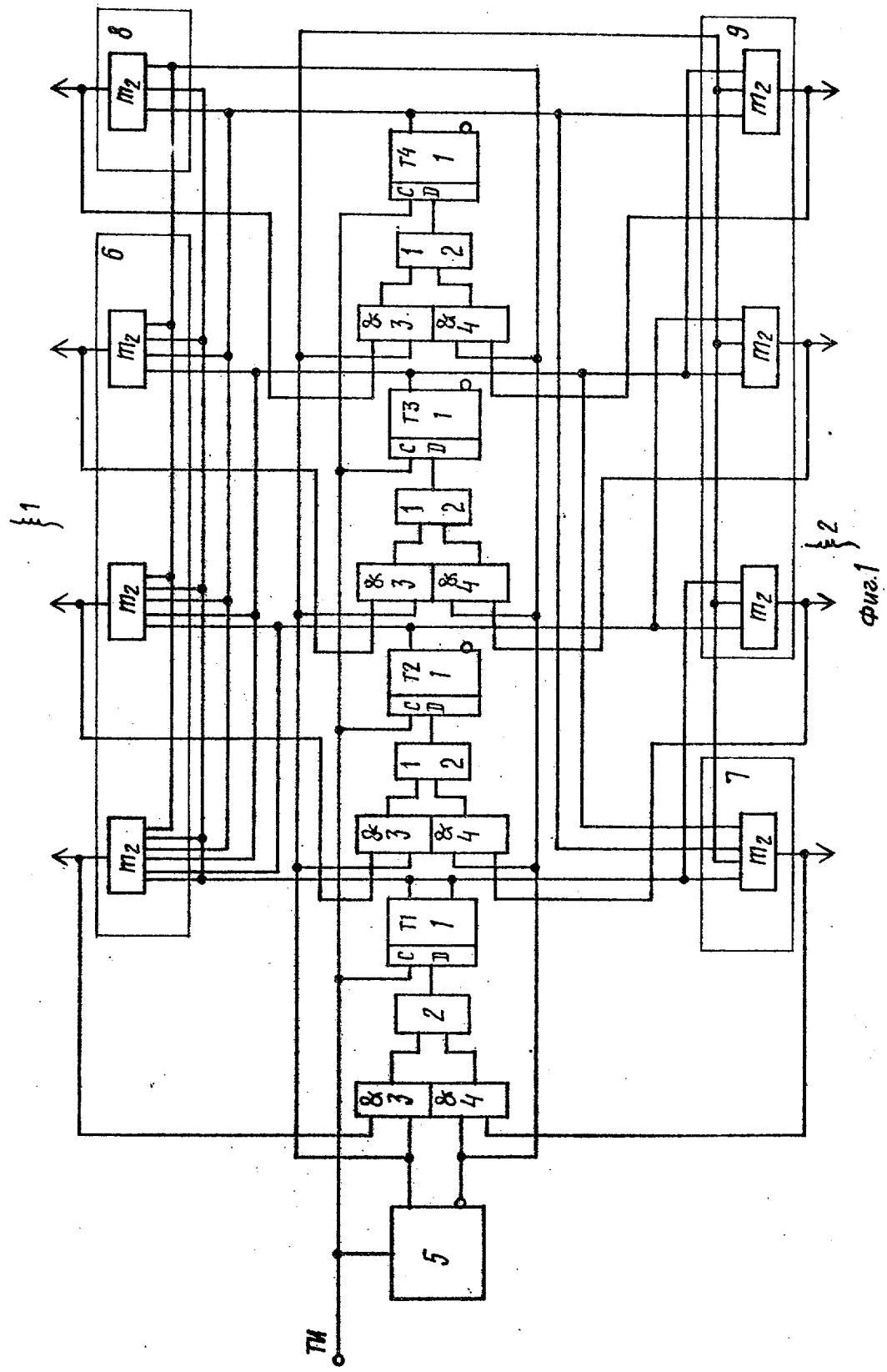
Формула изобретения

Генератор псевдослучайных чисел, содержащий первую и вторую группы трехвходовых сумматоров по модулю два, первую и вторую группы элементов И, группу элементов ИЛИ, группу триггеров и генератор равновероятной двоичной цифры, ко входу которого подключен выход генератора тактовых импульсов, а единичный и нулевой выходы генератора равновероятной двоичной цифры подключены к первым входам элементов И первой и второй группы соответственно, ко второму входу j (j - число сумматоров по модулю два в первой группе) старших элементов И первой группы подключены выходы j старших трехвходовых сумматоров по модулю два первой группы, ко второму входу m-j (m - число элементов И в каждой группе, а число элементов ИЛИ в группе - число триггеров в группе) старших элементов И второй группы подключены выходы m-j старших трехвходовых сумматоров по модулю два второй группы, выходы i-ых (i = =1,2,...) элементов И первой и второй группы подключены ко входам i-го элемента ИЛИ, выход которого подключен к D-входу i-го триггера, к синхровходу которого подключен выход генератора тактовых импульсов, к первым входам i-ых трехвходовых сумматоров по модулю два первой и второй групп подключены единичные выходы (m-j+i) и (j+i)-ых триггеров соответственно, ко вторым входам j трехвходовых сумматоров по модулю два первой группы подключены выходы j младших триггеров, ко вторым входам m-j трехвходовых сумматоров по модулю два второй группы подключены выходы m-j младших триггеров, к третьим входам j трехвходовых сумматоров по модулю два первой группы подключен нулевой выход генератора равновероятной двоичной цифры, к третьим входам m-j трехвходовых сумматоров по модулю два второй группы подключен нулевой и единичный выход генератора равновероятной двоичной цифры соответственно, о т л и ч а ю щ и й с я тем, что, с целью увеличения быстродействия генератора псевдослучайных чисел, он содержит группу четырехвходовых сумматоров по модулю два, n групп сумматоров по модулю два, по j(i+3)-входовых сумматоров по модулю два в i-ой группе и m-n x x j(n+3)-входовых сумматоров по модулю два в n-ой группе, причем к первым, вторым и третьим входам(m-i)-ых четырехвходовых сумматоров по модулю два подключены выходы (2m-2j-i)-ых, (2m-j-i)-ых и (m-i)-ых триггеров ($\overline{i=m-j,m-1}$) соответственно, а выходы j четырехвходовых сумматоров по модулю два подключены ко второму входу j младших элементов И второй группы, к четвертым входам j четырехвходовых сумматоров по модулю два подключен единичный выход генератора равновероятной двоичной цифры, на первый, второй и третий входы ℓ-го (i+3) входового сумматора по модулю два i-ой группы заведены выходы(m+1-i)-ых (j+1-i)-ых триггеров и нулевого выхода генератора равновероятной двоичной цифры соответственно, а на (K+3)-ие входы ℓ-го (i+3)-входного сумматора по модулю два заведены входы (m-j+ +1-K)-го триггера, кроме того, вторые входы m-j младших элементов И первой группы подключены к выходам m-j(i+3)-входовых сумматоров по модулю два.

Источники информации, принятые во внимание при экспертизе

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

2. Авторское свидетельство СССР по заявке № 2815712/18-24, кл. G 06 F 1/02, 19.03.80 (прототип).



Фиг.1

K	X (K)	$\xi(K)$	$\xi 1(K)$	$\xi 2(K)$
1	0	0001	(0000)	1001
2	1	1001	1000	(1010)
3	1	1000	0111	(0011)
4	1	0111	(0010)	0100
5	1	0100	(0011)	0110
6	0	0110	(1101)	1101
7	1	1101	0100	(1100)
8	1	0100	1100	(1001)
9	0	1100	(0100)	1010
10	1	1010	1001	(1000)

Фиг.2

Составитель А. Карасов
Редактор В. Лазаренко Техред А.Бабинец Корректор С. Шекмар

Заказ 592/58 Тираж 732 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