Союз Советских Социалистических Республик

Государственный комитет СССР по делам изобретений и открытий

ОПИСАНИЕ ИЗОБРЕТЕНИЯ

К АВТОРСКОМУ СВИДЕТЕЛЬСТВУ

(11) 1001097

(61) Дополнительное к авт. свид-ву –

(22) Заявлено 20.10.81 (21) 3348025/18-24

с присоединением заявки № –

(23) Приоритет –

Опубликовано 28.02.83. Бюллетень № 8

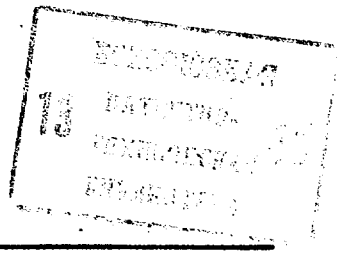
Дата опубликования описания 02.03.83

(51) М. Кл.[3] G 06 F 7/58

(53) УДК 681.325 (088.8)

(72) Автор изобретения 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.

Известен генератор псевдослучайных чисел, содержащий регистр сдвига с сумматором по модулю два в цепи обратной связи [1].

Недостатком этого генератора является невысокое быстродействие и наличие периода в формируемой последовательности.

Известен также генератор псевдослучайных чисел, содержащий группу сумматоров по модулю два и группу триггеров, выходы синхронизации которых подключены к выходу генератора тактовых импульсов [2].

В данном генераторе псевдослучайных чисел повышено быстродействие, но период генерируемой последовательности сохранен таким же как в [1].

2

Наиболее близким к предлагаемому по технической сущности является генератор псевдослучайных чисел, содержащий две группы сумматоров по модулю два, две группы элементов И, группу элементов ИЛИ, группу триггеров, входы синхронизации которых подключены к выходу генератора тактовых импульсов и входу генератора равновероятной двоичной цифры, причем к первым входам i-ых сумматоров по модулю два подключены единичные выходы i-ых триггеров, к вторым входам j старших сумматоров по модулю два подключены выходы j младших триггеров, к вторым входам $m-j$ младших сумматоров по модулю два подключены выходы $m-j$ старших сумматоров по модулю два [3].

В известном устройстве при высоком быстродействии практически отсутствует период последовательности, кодов форми-

руемых псевдослучайных чисел. Недостатком этого устройства является большой объем используемого оборудования.

Цель изобретения – сокращение объема используемого оборудования, т.е. упрощение генератора.

Поставленная цель достигается тем, что в генераторе псевдослучайных чисел, содержащем две группы из m сумматоров по модулю два и группу из m триггеров, синхронизирующие входы которых подключены к выходу генератора тактовых импульсов и входу генератора равновероятной двоичной цифры, а выходы триггеров группы подключены к первым входам соответствующих сумматоров по модулю два первой группы, причем выходы j ($j < m$) младших триггеров группы подключены к вторым входам j старших сумматоров по модулю два первой группы, а вторые входы $m-j$ младших сумматоров по модулю два первой группы подключены к выходам $m-j$ старших сумматоров по модулю два первой группы, информационные входы триггеров группы подключены к выходам соответствующих сумматоров по модулю два первой группы, третьи входы которых подключены к первому выходу генератора равновероятностной двоичной цифры, второй выход которого подключен к первым входам сумматоров по модулю два второй группы, вторые входы которых подключены к выходам соответствующих сумматоров по модулю два первой группы.

На фиг. 1 приведена структурная схема генератора псевдослучайных чисел при $m=5$; на фиг. 2 – функциональная схема генератора при $m=3$; на фиг. 3 – пример временной диаграммы сигналов, формируемых на выходе генератора тактовых импульсов (точка а), по приходу которых триггеры устройства меняют свое состояние, и на втором (прямом) выходе генератора равновероятной двоичной цифры (точка в); на фиг. 4 – граф состояний и последовательности переходов элементов памяти (триггеров) генератора псевдослучайных чисел при $m=3$ для порождающего полинома $\varphi(x)=x^3+x+1$ определенный начальным состоянием 101 и временной диаграммой (фиг. 3).

Генератор псевдослучайных чисел состоит из m сумматоров 1 по модулю два первой группы, m сумматоров 2 по модулю два второй группы, m триггеров 3, генератора 4 тактовых импульсов, генератора 5 равновероятной двоичной цифры. Причем входы сумматоров 1 по модулю два первой группы подключены к выходам триггеров 3 и генератора 5 равновероятной двоичной цифры таким образом, что на выходе сумматоров 1 формируются сигналы в соответствии со следующей системой логических уравнений:

$$\begin{aligned} a_{m-i} &= b_{m-i} \oplus b_{j-i} \oplus \bar{b}, \; i=0,1,\ldots,j-1; \\ a_{m-i} &= b_{m-i} \oplus a_{m+j-i} \oplus \bar{b}, \; i=j, j+1,\ldots,m, \end{aligned} \quad (1)$$

где b_{m-i} – единичный выход $(m-i)$-го триггера;

a_{m+j-i} – выход $(m+j-i)$-го сумматора по модулю два первой группы;

$\bar{b}$ – первый (инверсный) выход генератора 5 равновероятной двоичной цифры;

знак $\oplus$ – означает операцию суммирования по модулю два;

j – номер разряда регистра сдвига, выход которого вместе с выходом m-го разряда соединен с входами сумматора по модулю два в последовательных структурах.

Если $m=5$, $j=3$ и $\bar{b}=0$, то система (1) примет вид

$$a_5 = b_5 \oplus b_3; \; a_4 = b_4 \oplus b_2, \; a_3 = b_3 \oplus b_1$$

$$a_2 = b_2 \oplus a_5; \; a_1 = b_1 \oplus a_4.$$

Следовательно, при $\bar{b}=0$ предлагаемое устройство (фиг. 1) позволяет генерировать пятиразрядные коды псевдослучайных чисел М-последовательности, порождаемой полиномом $\varphi(x)=x^5+x^3+1$ (как в устройстве-прототипе). При $\bar{b}=1$ система (1) принимает вид

$$a_5 = \overline{b_5 \oplus b_3}; \; a_4 = \overline{b_4 \oplus b_2}; \; a_3 = \overline{b_3 \oplus b_1};$$

$$a_2 = \overline{b_2 \oplus a_5}; \; a_1 = \overline{b_1 \oplus a_4}.$$

Очевидно, что М-последовательности, генерируемые при $\bar{b}=0$ и $\bar{b}=1$, будут иметь одинаковые периоды, но очередность появления кодов и их состав различны (фиг. 4).

Входы сумматоров 2 по модулю два второй группы подключены к сумматорам 1 по модулю два первой группы и второму выходу генератора 5 в соответствии со следующей системой уравнений:

$$a^*_i = a_i \oplus b, \; i=1,2,\ldots,m, \quad (2)$$

где a^*_i – выход i-го сумматора по модулю два второй группы;

b – второй (прямой) выход генератора 5.

Кроме того, выход генератора 4 тактовых импульсов подключен к входу генератора 5 равновероятных двоичных цифр и первым входам триггеров 3.

Устройство функционирует следующим образом.

Исходное состояние триггеров – произвольное. В зависимости от значения двоичной цифры, сформированной генератором 5, на выходах сумматоров 1 появляется очередной код первой или второй М-последовательности. По переднему фронту тактового импульса в триггеры 3 записывается код с выходов сумматоров 1, по заднему фронту тактового импульса генератор 5 формирует очередное значение равновероятной двоичной цифры.

Генератор 5, как и в прототипе, может быть построен по простейшей схеме, например триггер с коммутируемым питанием, физических генераторов равновероятной двоичной цифры.

Более подробно процесс генерирования псевдослучайных чисел поясним на конкретном примере. Пусть в первоначальный момент времени на триггерах 3 (фиг. 2) записан код 101 и пусть генератор 5 на своем втором (прямом) выходе формирует сигнал, как это представлено на фиг. 3. Тогда до прихода первого тактового импульса на выходах сумматоров 1 в соответствии с (1) формируется код ξ_1 =010, а на выходах сумматоров 2 в соответствии с (2) – код ξ_2 = =101. По переднему фронту первого тактового импульса, пришедшего с выхода генератора 4 на первые (синхро–) входы триггеров 3, в триггера 3 записывается код 010. По заднему фронту первого тактового импульса (фиг. 3) значение сигнала на выходах генератора 5 меняется на противоположное. После окончания переходных процессов на выходах сумматоров 1 устанавливается код 100, на выходах сумматоров 2 – также код 100. Подобным образом триггеры меняют свое состояние в зависимости от значения сигналов на выходе генератора 5 и по приходу последующих импульсов. На фиг. 4 стрелками с номерами показана последовательность перехода состояний триггеров в течение первых девяти тактов работы устройства.

Из вышеприведенного описания функционирования генератора псевдослучайных чисел следует, что значения ξ_1, формируемые на выходах сумматоров 1 по модулю два первой группы, в каждый конкретный такт являются значениями кодов двух различающихся между собой М-последовательностей. Каждое последующее значение ξ_1 является следующим значением либо одной и той же М-последовательности, либо другой М-последовательности, что определяется значением двоичной цифры, формируемой на выходе генератора 5 равновероятной двоичной цифры. Нетрудно заметить, что при фиксировании на первом выходе генератора 5 значений "1" или "0" предлагаемый генератор генерирует одну из двух М-последовательностей, представленных на фиг. 4. На фиг. 4 пунктирами показаны для сравнения направления изменения состояний регистра сдвига последовательного генератора псевдослучайных чисел типа (1).

Преимущества предлагаемого генератора псевдослучайных чисел по сравнению с прототипом заключаются в сокращении объема используемого оборудования. Так удельные аппаратные затраты на один разряд псевдослучайного числа в прототипе составляют один сумматор по модулю два, один элемент И, 1/2 элемента ИЛИ, D –триггера, $1/2^m$ генератора равновероятной двоичной цифры и $1/2^m$ генератора тактовых импульсов. В предлагаемом же устройстве для этих целей требуется лишь один сумматор по модулю два, 1/2 D –триггера, $1/2^m$ генератора равновероятной двоичной цифры и $1/2^m$ генератора тактовых импульсов. Следует заметить, что в прототипе и предлагаемом устройстве значения ξ_1 и ξ_2 коррелированы, так как порождаются одним состоянием триггеров (в предлагаемом устройстве зависимость меньше, так как одно и тоже состояние триггеров может породить два значения ξ_1, два значения ξ_2, в прототипе – только по одному). В ряде случаев наличия корреляции ограничивает использование устройства в двухканальном режиме. При реализации одноканального режима, например при генерировании только последовательности ξ_1, в устройстве–прототипе все равно требуется две группы по m сумматоров по модулю два. В предлагаемом же устройстве m сумматоров по модулю два второй группы используются только для организации второго канала. Следовательно, в одноканальном режиме преимущества предлагаемого устройства более очевидны.

Кроме того, как это следует из (1) и (2) и видно из фиг. 4 в устройстве

генерируются последовательности из 2^m чисел (включая нулевую комбинацию), а не 2^m-1. Последнее также является отличительным положительным свойством устройства.

Предлагаемое устройство формирует последовательность практически неограниченной длины, так как период последовательности стремится к бесконечности даже при ограниченной разрядной сетке базового регистра сдвига. Кроме того, устройство позволяет воспроизводить три типа последовательности (в базовом – один) при одном и том же порождающем полиноме.

Предлагаемое устройство отличается высоким быстродействием: скорость формирования n -разрядного числа в n раз выше.

Формула изобретения

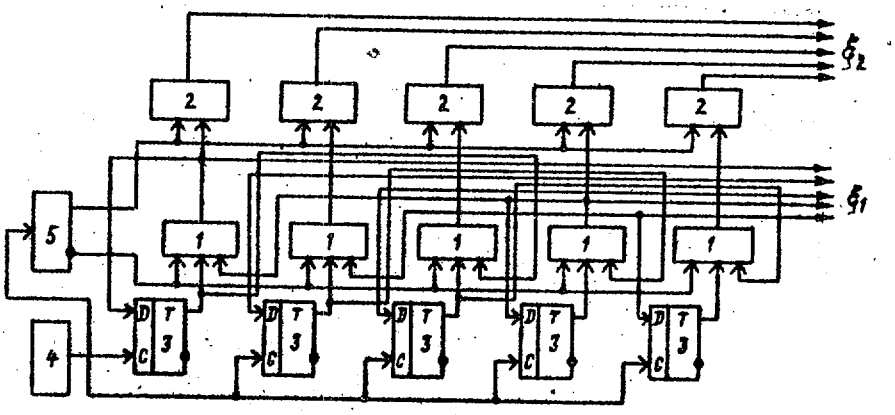
Генератор псевдослучайных чисел, содержащий две группы из m сумматоров по модулю два и группу из m триггеров, синхронизирующие входы которых подключены к выходу генератора тактовых импульсов и входу генератора равновероятной двоичной цифры, а выходы триггеров группы подключены к первым входам соответствующих сумматоров по модулю два первой группы, причем выходы j ($j < m$) младших триггеров группы подключены к вторым входам j старших сумматоров по модулю два первой группы, а вторые входы $m-j$ младших сумматоров по модулю два первой группы подключены к выходам $m-j$ старших сумматоров по модулю два первой группы, о т л и ч а ю щ и й с я тем, что, с целью упрощения генератора, информационные входы триггеров группы подключены к выходам соответствующих сумматоров по модулю два первой группы, третьи входы которых подключены к первому выходу генератора равновероятной двоичной цифры, второй выход которого подключен к первым входам сумматоров по модулю два второй группы, вторые входы которых подключены к выходам соответствующих сумматоров по модулю два первой группы.

Источники информации,
принятые во внимание при экспертизе

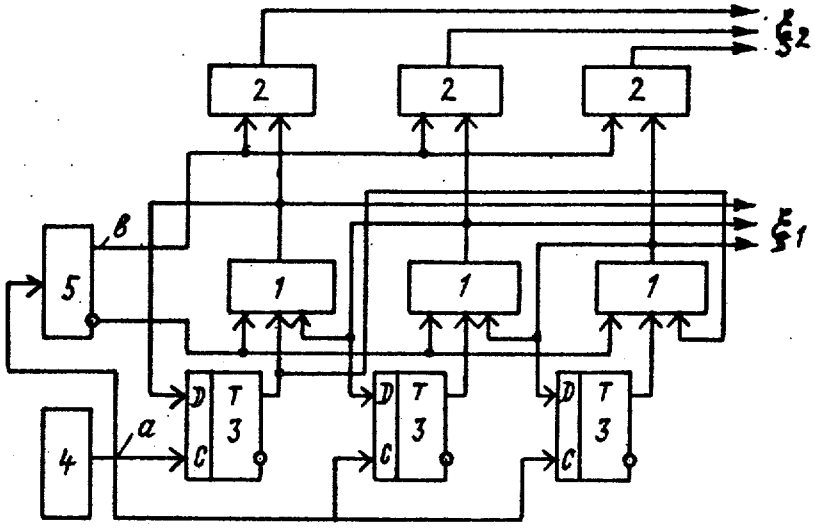
1. Яковлев В.В., Федоров Р.Ф. Вероятностные вычислительные машины. Л., "Машиностроение", 1974, с. 344.

2. Авторское свидетельство СССР № 634329, кл. G 06 F 7/58, 1976.

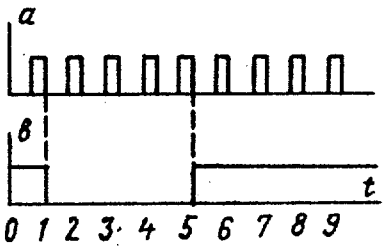
3. Авторское свидетельство СССР № 708381, кл. G 06 F 7/58, 1978. (прототип).



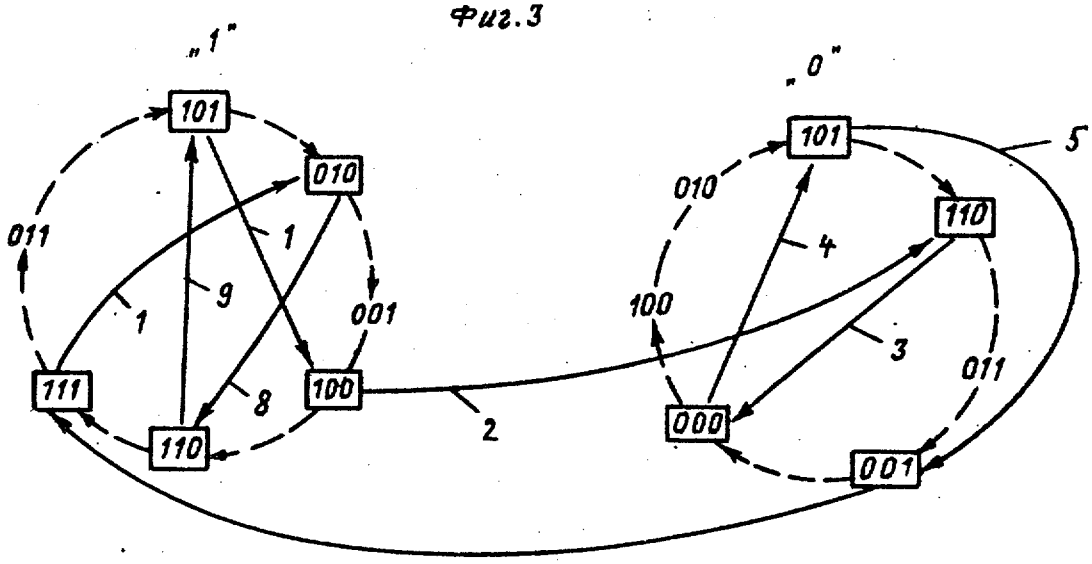
Фиг. 1



Фиг. 2



Фиг.3



Фиг.4

ВНИИПИ Заказ 1397/56 Тираж 704 Подписное
Филиал ППП "Патент", г. Ужгород, ул. Проектная, 4