Союз Советских Социалистических Республик

Государственный комитет СССР по делам изобретений и открытий

ОПИСАНИЕ ИЗОБРЕТЕНИЯ

К АВТОРСКОМУ СВИДЕТЕЛЬСТВУ

(11) 868734

(61) Дополнительное к авт. свид-ву –

(22) Заявлено 10.09.79 (21) 2815712/18-24

с присоединением заявки № –

(23) Приоритет –

Опубликовано 30.09.81. Бюллетень № 36

Дата опубликования описания 30.09.81

(51) М. Кл.³ G 06 F 1/02
G 07 C 15/00

(53) УДК 681.325 (088.8)

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

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

Недостатком такого генератора является наличие периода в формулируемой последовательности.

Известно также устройство, в котором для приближения свойств псевдослучайных чисел к свойствам истинно случайных, полученных физическими способами, период повторения последовательности увеличен до величины 2^{2m} [2].

Однако периодичность в указанном устройстве сохраняется.

Наиболее близким к предлагаемому является генератор псевдослучайных чисел, содержащий первую и вторую группы двухвходовых сумматоров по модулю два, первую и вторую группы элементов И, группу элементов ИЛИ, группу триггеров и генератор равновероятной двоичной цифры. Подобный генератор предназначен для генерирования за один такт двух m-разрядных псевдослучайных чисел [3].

2

Недостаток описанного устройства - отличие вероятности появления нуля или единицы в разрядах чисел от 0,5 по обоим каналам. Так, вероятность появления нуля или единицы в любом разряде псевдослучайного числа по обоим каналам определяется из выражений

$$P(a_k=1) = \frac{1}{2} + \frac{1}{2^{m-1}}; \quad (1)$$

$$P(a_k=0) = \frac{1}{2} - \frac{1}{2^{m-1}} \quad (2)$$

Известно, что построение таких высокоэффективных устройств, какие приведены в [2], имеет смысл при небольших значениях величины m. В этом случае выражение $\eta = \frac{1}{2^{m-1}}$, характеризующее отклонение от равновероятности, принимает значение, величина которого в ряде случаев оказывается недопустимой. Даже при $m=10$, $\eta = 0{,}001$.

Цель изобретения - повышение точности генератора за счет приближе-

ния вероятности нуля или единицы в разрядах псевдослучайности чисел по первому и второму каналам к 0,5.

Поставленная цель достигается тем, что генератор, 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, ко входу которого подключен выход генератора тактовых импульсов, а единичный и нулевой выходы генератора равновероятной двоичной цифры подключены к первым входам первой и второй групп элементов И соответственно, второй вход m-j младших элементов И первой группы подключен к выходам m-j младших двухвходовых сумматоров по модулю два первой группы, второй вход j младших двухвходовых сумматоров по модулю два второй группы, выходы i-х элементов И первой и второй группы подключены ко входам i-го элемента ИЛИ, выход которого подключен ко входу i-го триггера, к первым входам i-х двухвходовых сумматоров по модулю два первой и второй групп подключены единичные выходы i-х триггеров, ко вторым входам m-2j младших двухвходовых сумматоров по модулю два первой группы подключены выходы m-2j старших сумматоров по модулю два первой группы, выход генератора тактовых импульсов подключен к синхровходам триггеров, содержит первую группу из j трехвходовых сумматоров по модулю два и вторую группу из m-j трехвходовых сумматоров по модулю два, к первым входам i-х трехвходовых сумматоров по модулю два первой и второй групп подключены единичные выходы (m-j+i)=x и (j+i)=x триггеров, соответственно, вторые входы j трехвходовых сумматоров по модулю два первой группы подключены к выходам j младших триггеров, вторые входы m-j трехвходовых сумматоров по модулю два второй группы подключены к выходам m-j младших триггеров, третьи входы j трехвходовых сумматоров по модулю два первой группы подключены к нулевому выходу генератора равновероятной двоичной цифры, третьи входы j трехвходовых сумматоров по модулю два второй группы подключены к единичным выходам генератора равновероятной цифры, выходы j трехвходовых сумматоров по модулю два первой группы подключены соответственно ко вторым входам j старших двухвходовых сумматоров по модулю два первой группы, а выходы j старших трехвходовых сумматоров по модулю два второй группы подключены соответственно ко вторым входам j младших двухвходовых сумматоров по модулю два второй группы, кроме того, выход i-го трехвходового сумматора по модулю два первой группы подключен ко второму входу (m-j+i)-го элемента И первой группы, выход i-го трехвходового сумматора по модулю два второй группы подключен ко второму входу (j+i)-го элемента И второй группы.

На фиг.1 приведена структурная схема генератора для случая, когда m=7; на фиг.2 - функциональная схема генератора псевдослучайных чисел для m=4; на фиг.3 - временная диаграмма работы генератора для m=4.

В общем случае генератор псевдослучайных чисел состоит из m триггеров 1, m элементов ИЛИ 2, первой группы m элементов И 3, второй группы m элементов И 4, генератора 5 равновероятной двоичной цифры, первой группы m-j двухвходовых сумматоров 6 по модулю два, второй группы j двухвходовых сумматоров 7 по модулю два, первой группы j трехвходовых сумматоров 8 по модулю 8, второй группы m-j трехвходовых сумматоров 9 по модулю два.

Количество двухвходовых сумматоров по модулю два в первой группе равняется m-j, а во второй группе j. В тоже время количество трехвходовых сумматоров по модулю два в первой и второй группе равняется j и m-j соответственно. На выходах двухвходовых и трехвходовых сумматоров по модулю два первых групп получаются значения псевдослучайного числа $\xi 1 = a_1, a_2, \ldots, a_m$, а на выходах вторых групп получаются значения псевдослучайного числа $\xi 2 = a_1', a_2', \ldots, a_m'$. Числа $\xi 1$ и $\xi 2$ представляют собой m-разрядные коды или их инверсии М-последовательностей, порождаемых случайными полиномами $\varphi(z) = z^m + z^j + 1$ и $\varphi(z) = z^m + z^{m-1} + 1$, причем периоды обоих их 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 цифры соединены со входами трехвходовых сумматоров по модулю два первой и второй группы согласно выражениям:

$$a_{m-i}(k) = b_{m-i}(k) \oplus b_{j-i}(k) \oplus \oplus \overline{x(k)}, i = \overline{0, j-1}; \quad (3)$$

$$a'_{m-i}(k) = b_{m-i}(k) \oplus b_{m-j-i}(k) \oplus \oplus x(k), i = \overline{0, m-j-1}, \quad (4)$$

где $b_{m-i}(k)$ - значение на единичном выходе (m-i)-го триггера в k-ый такт работы устройства;

$x(k)$ и $\bar{x}(k)$ - значения на единичном и нулевом выходах генератора равновероятной двоичной цифры;

$a_{m-i}(k)$ и $a'_{m-i}(k)$ - значения на выходах трехвходовых сумматоров по модулю два первой и второй группы;

знак $\oplus$ означает операцию суммирования по модулю два.

Выходы D-триггеров и выходы сумматоров по модулю два соединены со входами двухвходовых сумматоров по модулю два первой и второй групп согласно выражениям

$$a_{m-i}(k) = b_{m-i}(k) \oplus a_{m+j-i}(k), \; i = \overline{j,m}; \quad (5)$$

$$a'_{m-i}(k) = b_{m-i}(k) \oplus a'_{2m-j-i}(k), \; i = \overline{m-j,m-1} \quad (6)$$

При использовании выражений (3)-(6) для организации связей в генераторе псевдослучайных чисел для нумерации сумматоров по модулю два первых групп и вторых групп используются единые сквозные нумерации. Для случая m=5, j=1 на выходы сумматоров по модулю два. На фиг.1 представлены связи в соответствии с системой

$$a_7 = b_7 \oplus b_1 \oplus \bar{x}; \; a_6 = b_6 \oplus a_7; \; a_5 = b_5 \oplus a_6; \; a_4 = b_4 \oplus a_5;$$
$$a_3 = b_3 \oplus a_4; \; a_2 = b_2 \oplus a_3; \; a_1 = b_1 \oplus a_2. \quad (7)$$

по первому каналу и в соответствии с системой

$$a'_7 = b_7 \oplus b_6 \oplus x; \; a'_6 = b_6 \oplus b_5 \oplus x; \; a'_5 = b_5 \oplus b_4 \oplus x;$$
$$a'_4 = b_4 \oplus b_3 \oplus x; \; a'_3 = b_3 \oplus b_2 \oplus x; \; a'_2 = b_2 \oplus$$
$$\oplus b_1 \oplus x; \; a'_1 = b_1 \oplus a'_7 \quad (8)$$

по второму каналу. В зависимости от значения равновероятной двоичной цифры на выходе генератора 5 равновероятной двоичной цифры код псевдослучайного числа $\xi 1$ или $\xi 2$ с сумматоров по модулю два через элементы ИЛИ 2 записывается на D-триггеры. Генератор 5 представляет собой простейший датчик равновероятной двоичной цифры, построенной на физических принципах.

Генератор псевдослучайных чисел работает следующим образом.

В начальный момент на D-триггеры 1 записывается ненулевой код (фиг.1). На выходах сумматоров 6 и 8 по модулю два образуется очередной код псевдослучайного числа первой М-последовательности в том случае, если $x(k)$ в данный момент времени равняется 0, а на выходе сумматоров 7 и 9 по модулю два образуется обратный код псевдослучайного числа второй М-последовательности, так как $\bar{x}(k) = 1$. 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 $\bar{x}(k)=0$. 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 входы через первую или вторую группы элементов И 3 и 4 и через элементы ИЛИ 2, объединяющие выходы обоих групп И, подается очередной код первой или второй М-последовательности. С приходом очередного тактового импульса процесс повторяется.

На фиг.3 для каждого такта работы $k=\overline{1,10}$ показаны соответствующие значения выходных псевдослучайных чисел $\xi 1$ и $\xi 2$ и содержимое триггерного регистра $1\xi(k)$. В первоначальный момент на триггерах записан код 0001, а значения $\xi 1(1)=0000$ и $\xi 2(1)=1001$, причем $\xi 1$ есть инвертированный код первой М-последовательности, так как $x(1)=0$. По приходу тактового импульса на триггеры записывается код числа $\xi 2$ (1), таким образом во втором такте исходной информацией для формирования $\xi 1(2)$ и $\xi 2(2)$ является 1001. Так как $x(2)=1$, то $\xi 1(2)$ принимает неинвертированное значение кода первой М-последовательности, а $\xi 2(2)$ - инвертированное значение кода второй М-последовательности. В следующий момент $\xi(k)$ содержимое триггерного регистра принимает значение 1000. Подобным образом триггеры меняют свое состояние в зависимости от значения $x(k)$ на выходе генератора равновероятной двоичной цифры по приходу последующих импульсов.

Из описанного выше следует, что значения $\xi 1$ и $\xi 2$, генерируемые на выходах первой и второй групп сумматоров по модулю два, в каждый конкретный такт являются значениями кодов или их инверсий из двух отличных М-последовательностей. $\xi 1$ и $\xi 2$ принимают значения из двух различных М-последовательностей (но имеющих одинаковый состав кодов), порядок последования которых случаен. Автокорреляционная функция выходных последовательностей по обоим каналам имеет ненулевое значение только при $t < \tau$, где τ - длительность выходного сигнала между очередными тактовыми импульсами. Вероятность появления нуля или единицы на выходе любого разряда псевдослучайного числа по любому каналу определяется вероятностью равенства единице суммы по модулю два псевдослу-

чайной последовательности с последовательностью отсчетов равновероятной двоичной цифры. Это следует из такого факта, что выражение для формирования значения любого разряда выходного псевдослучайного числа по обоим каналам на основании (3)-(6) представляется в виде выражений

$$a_i(k)=a_s(k)\oplus\bar{x}(k),\quad i=\overline{1,m};\quad (9)$$

$$a'_i(k)=a'_s(k)\oplus x(k),\quad i=\overline{1,m},\quad (10),$$

где $s\neq i$; так, например, для $a'_1=b_1\oplus a'_7=b_1\oplus b_7\oplus b_6\oplus x=a'_s\oplus x$. Здесь в преобразованиях используется свойство сдвига и сложения М-последовательности.

Таким образом, вероятность появления нуля или единицы на выходе любого разряда псевдослучайного числа по любому каналу определяется следующим образом:

$$P(a_i=1)=P(a_s\oplus x=1)=P(a_s\oplus\bar{x}=1)=$$
$$=P(\bar{a}_s x)+a_s\bar{x}=1) \quad (11)$$

Учитывая, что a_s и x независимы, выражение (11) принимает вид

$$P(a_i=1)=P(a_s=0)P(x=1)+$$

$$+P(a_s=1)P(x=0)=0{,}5-\frac{\eta_x}{2^{m-1}} \quad (12)$$

Анализ выражения (12) показывает, что вероятность появления единицы или нуля на выходе генератора отличается от 0,5 на величину

$$\frac{\eta_x}{2^{m-1}},$$

где η_x - отклонение от 0,5 вероятности появления единицы на выходе генератора равновероятной двоичной цифры.

Так как величина $\eta_x=0{,}01-0{,}001$ для известных устройств [1], то значение $P(a_i=1)$ незначительно отличается от 0,5. Таким образом, вероятность появления нуля или единицы в разрядах псевдослучайных чисел по обоим каналам в предлагаемом устройстве максимально приближена к 0,5, Для случая $m=10$ величина, характеризующая отклонение от 0,5, равна 0,00001-0,000001.

Таким образом, природа выходных псевдослучайных последовательностей максимально приближена к истинно случайным числам. Предлагаемый генератор отличается простотой технической реализации. Удельные аппаратные затраты на один разряд псевдослучайного числа составляют один элемент И, $\frac{1}{2}$ элемента ИЛИ, $\frac{1}{2}$ двухвходового сумматора по модулю два, $\frac{1}{2}$ трехвходового сумматора по модулю два, $\frac{1}{2}$ триггера и $\frac{1}{2}$ генератора равновероятной двоичной цифры. Предлагаемый генератор псевдослучайных чисел позволяет получать числа по двум каналам.

Применение предлагаемого генератора псевдослучайных чисел позволяет повысить точность и достоверность решения задач методом Монте-Карло. Кроме того, подобные устройства позволяют получать истинно "белый" шум для построения генератора случайных процессов.

Формула изобретения

Генератор псевдослучайных чисел, содержащий первую группу из m-j двухвходовых сумматоров по модулю два, вторую группу из j двухвходовых 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 групп соответственно, вторые входы m-j младших элементов И первой группы подключены, соответственно, к выходам m-j двухвходовых сумматоров по модулю два первой группы, вторые входы j младших элементов И второй группы подключены соответственно к выходам j младших двухвходовых сумматоров по модулю два второй группы, выходы i-х элементов И первой и второй групп подключены к соответствующим входам i-го элемента ИЛИ, выход которого подключен ко входу i-го триггера, к первым входам i-х двухвходовых сумматоров по модулю два первой и второй групп подключены соответственно единичные выходы i-х триггеров, вторые входы m-2j младших двухвходовых сумматоров по модулю два первой группы подключены соответственно к выходам m-2j старших сумматоров по модулю два первой группы, выход генератора тактовых импульсов подключен к синхровходам триггеров, о т л и ч а ю щ и й с я тем, что, с целью повышения точности генератора, он содержит первую группу из j трехвходовых сумматоров по модулю два и вторую группу из m-j трехвходовых сумматоров по модулю два, к первым входам i-х трехвходовых сумматоров по модулю два первой и второй групп подключены единичные выходы (m-j+i)-х и (j++i)-х триггеров, соответственно, вторые входы j трехвходовых сумматоров по модулю два первой группы подключены к выходам j младших триггеров, вторые входы m-j трехвходовых сумматоров по модулю два второй группы подключены к выходам m-j младших триггеров, третьи входы j трехвходовых сумматоров по модулю два первой группы подключены к нулевому выходу генератора равновероятной двоичной цифры, третьи входы j трех-

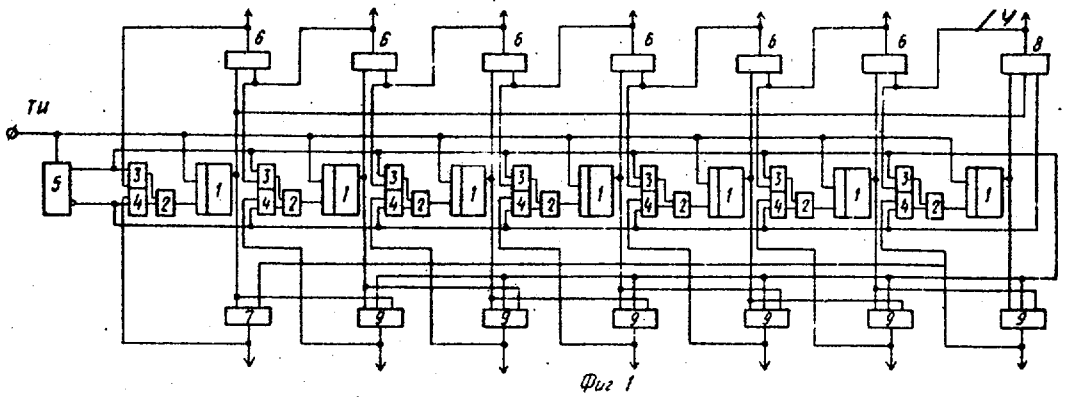
входовых сумматоров по модулю два второй группы подключены к единичному выходу генератора равновероятной двоичной цифры, выходы j трехвходовых сумматоров по модулю два первой группы подключены соответственно ко вторым входам j старших двухвходовых сумматоров по модулю два первой группы, а выходы j старших трехвходовых сумматоров по модулю два второй группы подключены соответственно ко вторым входам j младших двухвходовых сумматоров по модулю два второй группы, кроме того, выход i-го трехвходового сумматора по модулю два первой группы подключен ко второму входу (m-j+i)-го элемента И первой группы, выход i-го трехвходового сумматора по модулю два второй группы подключен ко второму входу (j+i)-го элемента И второй группы.

Источники информации, принятые во внимание при экспертизе

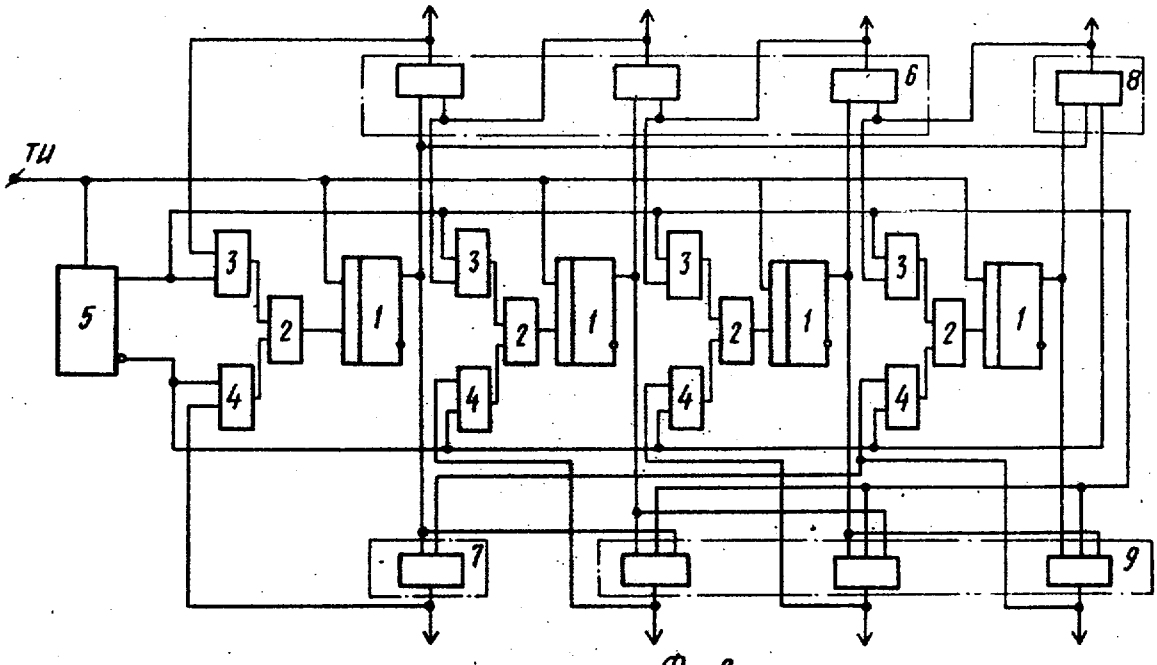
1. Яковлев В.В., Федоров Р.Ф. Вероятностные вычислительные машины. Л., "Машиностроение", 1974, с.344.

2. Авторское свидетельство СССР № 524175, кл. G 06 F 1/02, 1975.

3. Авторское свидетельство СССР по заявке № 2505976/18-24, кл. G 06 F 1/02, 1978 (прототип).



Фиг 1



Фиг 2

k	x(k)	f(k)	f1(k)	f2(k)
1	0	0001	0000	1001
2	1	1001	1000	1010
3	1	1000	0111	0011
4	0	0111	0010	0100
5	0	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.3

Составитель А.Карасов
Редактор И.Михеева Техред Т.Маточка Корректор М.Коста

Заказ 8329/70 Тираж 748 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