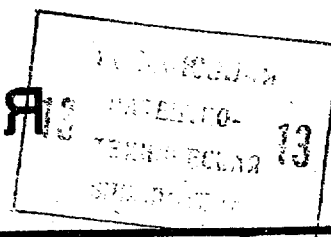




ГОСУДАРСТВЕННЫЙ КОМИТЕТ СССР
ПО ДЕЛАМ ИЗОБРЕТЕНИЙ И ОТКРЫТИЙ

ОПИСАНИЕ ИЗОБРЕТЕНИЯ

К АВТОРСКОМУ СВИДЕТЕЛЬСТВУ



- (21) 3252992/18-24
(22) 06.03.81
(46) 15.06.83. Бюл. № 22
(72) В. Н. Ярмолик
(71) Минский радиотехнический институт
(53) 681.325(088.8)

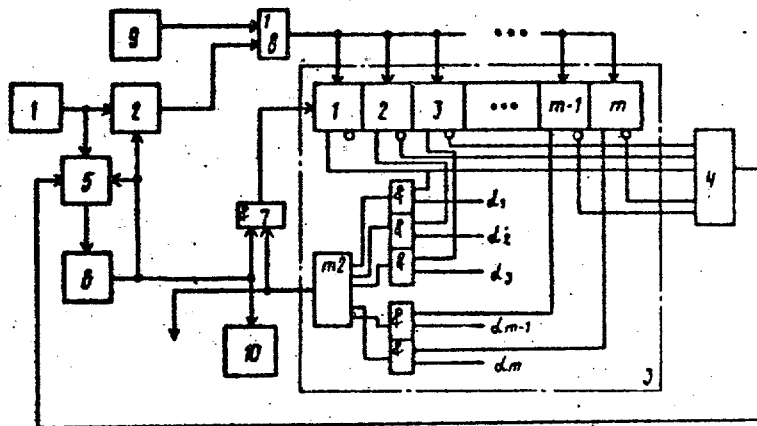
(56) 1. Яковлев В. В., Федоров Р. Ф. Вероятностные вычислительные машины. Л., "Машиностроение", 1974, с. 247.

2. Яковлев В. В., Федоров Р. Ф. Вероятностные вычислительные машины. 1974, с. 254.

3. Авторское свидетельство СССР № 527012, кл. Н 03 К 3/00, 1974 (прототип).

(54) (57) ГЕНЕРАТОР ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ, содержащий генератор тактовых импульсов, выход которого соединен с первыми входами первого и второго элементов ЗАПРЕТ, дешифратор, выход которого соединен с вторым входом второго элемента ЗАПРЕТ, выход которого соединен с входом счетчика, выход которого соединен с вторым входом первого элемента ЗАПРЕТ и с третьим входом вто-

рого элемента ЗАПРЕТ, регистр сдвига, инверсные выходы всех разрядов которого, кроме первого и последнего, соединены с соответствующими входами дешифратора, а прямые выходы всех разрядов регистра сдвига соединены соответственно с первыми входами элементов И группы, вторые входы которых являются группой входов генератора, а выходы элементов И группы соединены с соответствующими входами сумматора по модулю два, отличающийся тем, что, с целью упрощения генератора, он содержит элемент И, элемент ИЛИ, блок индикации и генератор одиночного импульса, выход которого соединен с первым входом элемента ИЛИ, второй вход которого подключен к выходу первого элемента ЗАПРЕТ, а выход элемента ИЛИ соединен с входом "Сдвиг" регистра сдвига, информационный вход которого подключен к выходу элемента И, первый вход которого объединен с входом блока индикации и подключен к выходу счетчика, выход сумматора по модулю два соединен с вторым входом элемента И и является выходом генератора.



Фиг. 1

Изобретение относится к вычислительной технике и может быть использовано в качестве устройства для определения топологии связей многоходового сумматора по модулю два, на выходе которого формируются сдвинутые копии псевдослучайных последовательностей. Использование сдвинутых копий псевдослучайных последовательностей позволяет строить экономичные генераторы псевдослучайных чисел, а также организовать автономные устройства для имитации случайных процессов с заданными характеристиками.

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

Недостатком этого устройства является невозможность получения копий псевдослучайной последовательности сдвинутых более, чем на m -тактов, где m - разрядность регистра сдвига.

Известен параллельный генератор псевдослучайных чисел, позволяющий получать копии псевдослучайной последовательности, сдвинутые на значительно большее, чем на m число тактов [2].

Однако данное устройство позволяет получать копии псевдослучайной последовательности только лишь для частного случая, когда схема цепи обратной связи регистра сдвига состоит только из одного полусумматора.

Наиболее близким к предлагаемому изобретению является устройство для формирования сдвинутых копий псевдослучайного сигнала, состоящее из генератора тактовых импульсов, первого элемента ЗАПРЕТ, регистра сдвига с обратной связью, дешифратора, второго элемента ЗАПРЕТ, счетчика, блоков памяти, сумматоров по модулю два и индикаторов [3].

Применение устройства для формирования сдвинутых копий псевдослучайного сигнала позволяет определить топологию связей m -ходового сумматора по модулю два, на выходе которого получается копия исходной псевдослучайной m -последовательности, сдвинутая на произвольное количество тактов. Причем, в данном устройстве эта задача решается для общего случая, т.е. для случая когда в цепи обратной связи регистра сдвига включен многоходовой сумматор по модулю два.

Недостатком данного устройства является сложность аппаратного построения, которая в основном определяется наличием

элементов памяти. Даже для сравнительно небольшой величины $m = 20$ дополнительное количество элементов памяти составит 171 элемент, что почти в 7 раз больше, чем затраты оборудования, идущие на другие блоки устройства. Кроме того, наличие блоков памяти снижает быстродействие устройства в целом. Это объясняется тем, что в данном случае необходимо время для записи и считывания информации на блоке памяти.

Цель изобретения - сокращение аппаратных затрат на построение устройства для получения сдвинутых копий псевдослучайной последовательности, т.е. упрощение генератора.

Поставленная цель достигается тем, что генератор псевдослучайных последовательностей, содержащий генератор тактовых импульсов, выход которого соединен с первыми входами первого и второго элементов ЗАПРЕТ, дешифратор, выход которого соединен с вторым входом второго элемента ЗАПРЕТ, выход которого соединен с входом счетчика, выход которого соединен с вторым входом первого элемента ЗАПРЕТ и с третьим входом второго элемента ЗАПРЕТ, регистр сдвига, инверсные выходы всех разрядов которого, кроме первого и последнего, соединены с соответствующими входами дешифратора, а прямые выходы всех разрядов регистра сдвига соединены с первыми входами соответствующих элементов И группы, вторые входы которых образуют группу входов генератора, а выходы группы элементов И соединены с соответствующими входами сумматора по модулю два, введены элемент И, элемент ИЛИ, блок индикации и генератор одиночного импульса, выход которого соединен с первым входом элемента ИЛИ, второй вход которого подключен к выходу первого элемента ЗАПРЕТ, а выход элемента ИЛИ соединен с входом "Сдвиг" регистра сдвига, информационный вход которого подключен к выходу элемента И, первый вход которого объединен с входом блока индикации и подключен к выходу счетчика, выход сумматора по модулю два соединен с вторым входом элемента И и является выходом генератора.

На фиг. 1 изображена блок-схема генератора; на фиг. 2 - схема генератора для случая $m = 5$; на фиг. 3 - диаграмма, поясняющая его работу.

Генератор псевдослучайных последовательностей состоит из генератора 1 тактовых импульсов, первого элемента "ЗАПРЕТ" 2, регистра 3 сдвига с сумматором по модулю два в цепи обратной связи, m -двухходовыми элементами И, дешифратора 4, второго элемента "ЗАПРЕТ" 5, счетчи-

$$(m-1)\left(\frac{m}{2}-1\right)=m^2/2-3m/2+1,$$

ка 6, двухвходового элемента И 7, двухвходового элемента ИЛИ 8, генератора 9 одиночных импульсов и элемента индикации 10.

Генератор тактовых импульсов 1, второй элемент ЗАПРЕТ 5, счетчик 6 и первый элемент ЗАПРЕТ 2 включены последовательно, к вторым входам первого и второго элемента ЗАПРЕТ 2 и 5, подключены выходы генератора тактовых импульсов 1 и счетчика 6 соответственно, к третьему входу второго элемента ЗАПРЕТ 5, подключен выход дешифратора 4, к входам которого подключены единичный выход первого разряда и нулевые выходы остальных разрядов регистра 3 сдвига, к первым входам m -двухвходовых элементов И схемы обратной связи регистра 3 сдвига подключены единичные выходы разрядов регистра 3 сдвига, а на вторые входы поданы постоянные коэффициенты, выходы m двухвходовых элементов И схемы обратной связи регистра 3 сдвига подключены к входам m -входового сумматора по модулю два цепи обратной связи регистра 3 сдвига, выход которого и выход счетчика 6 подключены к входам двухвходового элемента И 7, выход которого подключен к информационному входу первого разряда регистра 3 сдвига, а выходы генератора 9 одиночных импульсов и первого элемента ЗАПРЕТ 2 подключены к входам двухвходового элемента ИЛИ 8, выход которого подключен к синхровходам разрядов регистра 3 сдвига, а выход счетчика 6 подключен к входу элемента 10 индикации.

Элемент ЗАПРЕТ 2 подобно как и блок 7 представляет собой двухвходовой элемент И (фиг. 2). Генератор 1 тактовых импульсов выполнен по схеме с отрицательной обратной связью по току. Дешифратор 4 и двухвходовой элемент ИЛИ 8 представляют собой стандартные m -входовой элемент И и двухвходовой элемент ИЛИ (фиг. 2), кроме того, m -входовой сумматор по модулю два и m -двухвходовых элементов И в цепи обратной связи регистра 3 (фиг. 2) также являются стандартными элементами вычислительной техники. Второй элемент ЗАПРЕТ 5 (фиг. 2) состоит из RS-триггера двухвходового элемента И и инвертора, которые также являются типовыми элементами, блок 10 представляет собой элемент ИЛИ-НЕ с индикационной лампочкой (фиг. 2).

Значения коэффициентов $d_i \in \{0, 1\}$, $i = 1, m$, определяются из известных таблиц. Так, для случая $m = 4$, могут в частном случае принимать следующие значения $d_1 = 1, d_2 = 1, d_3 = 1, d_4 = 0, d_5 = 1$.

Устройство работает следующим образом.

Из генератора 1 тактовые импульсы через элемент ЗАПРЕТ 2 и блок 8 поступают на синхровходы регистра 3 сдвига, который генерирует псевдослучайную последовательность. В момент времени, когда в ячейках регистра 3 сдвига хранится комбинация 100 ... 0, т.е. первый триггер находится в единичном состоянии, а все остальные - в нулевом, дешифратор 4 вырабатывает разрешающий сигнал для второго элемента ЗАПРЕТ 5.

Это достигается тем, что дешифратор 4 представляет собой m -входной элемент И, к первому входу которого подключен прямой выход первого разряда регистра 3 сдвига, а к остальным $(m-1)$ входам, инверсные выходы оставшихся разрядов регистра сдвига. После того, как срабатывает элемент ЗАПРЕТ 5, тактовые импульсы с генератора 1 поступают на вход счетчика 6, на который перед началом работы устанавливается код числа $2^m - \ell$, где m - разрядность регистра 3 сдвига, а ℓ - число тактов, на которое необходимо получить сдвинутую последовательность. В момент времени, когда счетчик 6 хранит код $2^m - 1$, т.е. по истечении $\ell - 1$ тактов, на выходе счетчика 6 формируется сигнал, запрещающий прохождение импульсов счета через элемент 5 и элемент 2. Одновременно этим же выходным сигналом блокируется прохождение информации на первый разряд регистра 3 сдвига через двухвходовой элемент И 7 и включается элемент 10 индикации. По загоранию лампочки блока индикации оператор делает вывод о том, что информация, хранящаяся на регистре сдвига, является значениями символов m -последовательности через $\ell - 1$ такт. После этого на выходе устройства, т.е. на выходе сумматора по модулю два цепи обратной связи регистра 3 сдвига, фиксируется значение двойной цифры $b(0) \in \{0, 1\}$ равной $b(0) = \sum_{i=1}^m d_i \alpha_i (\ell - 1) = \alpha_1(\ell)$, где $\alpha_i(\ell - 1)$ - содержимое i -го разряда регистра сдвига в $\ell - 1$ такт работы, а знак Σ означает операцию суммирования по модулю два. Определив значение символа $b(0)$, содержимое регистра сдвига сдвигается на один разряд путем замыкания контакта генератора 9 одиночных импульсов, с выхода которого единичный импульс через элемент ИЛИ 8 поступает на синхровходы регистра 3 сдвига. При этом на первый разряд регистра сдвига записывается значение нуля. После того как информация, хранящаяся в регистре сдвинется на один разряд, значение цифры $b(i)$ равняется

$$b(i) = a_1(e+i) \oplus a_1(i) a_1(e) \quad (2)$$

После очередного замыкания контакта генератора 9 одиночных импульсов значение $b(2)$ имеет вид

$$b(2) = a_1(e+2) \oplus a_1(1) a_1(e+1) \oplus a_1(2) a_1(e) \quad (3)$$

И в общем случае для j -го замыкания контакта генератора одиночных импульсов 9 получим на выходе сумматора по модулю два, включенного в цепь обратной связи регистра сдвига 3, значение $b(j)$, определяемое согласно (4), где $j \in \{0, m-1\}$ - количество импульсов, генерируемое генератором 9; $a_1(i) \in \{0, 1\}$ - содержимое первого разряда регистра 3 сдвига,

$$b(j) = \bigoplus_{i=j+1}^m a_i a_{i-j}(e-1) = a_1(e+j) \oplus \bigoplus_{i=1}^j a_1(i) a_1(e+j-i)$$

в первые $(m-1)$ такты работы устройства. Значение коэффициентов $\delta_i(e) \in \{0, 1\}$, $i = 1, m$, определяющих топологию связей многоходового сумматора по модулю два, являются решением системы уравнений следующего вида

$$a_1(e) = a_1(0) \delta_1(e) \oplus a_2(0) \delta_2(e) \oplus \dots \oplus a_m(0) \delta_m(e);$$

$$a_1(e-1) = a_1(1) \delta_1(e) \oplus a_1(0) \delta_2(e) \oplus \dots \oplus a_{m-1}(0) \delta_m(e);$$

$$a_1(e+m-1) = a_1(m-1) \delta_1(e) \oplus \dots \oplus a_1(0) \delta_m(e) \quad (5)$$

При начальных условиях $a_1(0) = 1$ и $a_i(0) = 0$, $i = 2, m$, которые соответствуют начальным условиям работы предлагаемого устройства система логических уравнений (5), примет следующий вид

$$a_1(e) = \delta_1(e);$$

$$a_1(e+1) = a_1(1) \delta_1(e) \oplus \delta_2(e),$$

$$a_1(e+m-1) = a_1(m-1) \delta_1(e) \oplus \dots \oplus a_1(0) \delta_m(e) \quad (6)$$

Решением системы (6) является выражение (7)

$$\delta_i(e) = a_1(e-1+i) \oplus \bigoplus_{n=1}^{i-1} a_1(n) a_1(e+i-n) \quad (7)$$

Значение $b(j)$ равняется значению $b_{i-1}(e)$, что следует из тождественности уравнений (4) и (7). Таким образом, путем последовательного замыкания контактов генератора 9 одиночных импульсов на выходе сумматора по модулю два, включенного в цепь обратной связи регистра 3 сдвига, последовательно получают значения коэффициентов $\delta_i(e)$, определяющие топологию связей сумматора по модулю два, на выходе которого получается последовательность, сдвинутая на e тактов.

Пример. На фиг. 2 приведена функциональная схема предлагаемого устройства при $m = 5$ для случая, когда $a_1 = 1$, $a_2 = 1$, $a_3 = 1$, $a_4 = 0$, $a_5 = 1$.

Допустим требуется определить топологию связей многоходового сумматора, на выходе которого получается сдвинутая на $\varrho = 9$ тактов исходная m -последовательность. Предварительно на двоичный счетчик 6 записывается код числа $2^5 - 9 = 23$. Импульсы сдвига с блока 1 поступают на синхровходы триггеров регистра 3 через элемент И 2 и элемент ИЛИ 8. В момент времени, когда в ячейках регистра 3 сдвига хранится комбинация 10000, дешифратор 4 вырабатывает единичный разрешающий сигнал, который устанавливает триггер ЭЛЕМЕНТА 5 в единичное состояние и, таким образом, разрешает прохождение импульсов с генератора 1 тактовых импульсов через элемент И ЭЛЕМЕНТА 5 на вход счетчика 6. После восьми последующих тактов работы устройства в целом на счетчике 6 хранится код числа 31, т.е. все триггеры счетчика 6 находятся в нулевом состоянии. Сигнал, формируемый на выходе счетчика 6, запрещает прохождение тактовых импульсов через ЭЛЕМЕНТ 5 и ЭЛЕМЕНТ 2. Одновременно этим же сигналом блокируется прохождение информации на первый разряд регистра 3 сдвига через двухходовый элемент И 7 и включается лампочка индикации блока 10. В данный момент на резисторе сдвига 3 фиксируется двоичный код, равный 11001. На выходе сумматора по модулю два цепи обратной связи регистра 3 сдвига формируется значение первого коэффициента $\delta_1(9) = 1$. После того, как значение $\delta_1(9)$ зафиксировано, содержимое регистра сдвига сдвигается на один разряд путем замыкания контакта генератора 9 одиночных импульсов, с выхода которого одиночный импульс через элемент ИЛИ 8 поступает на синхровходы регистра сдвига. В результате на регистре сдвига хранится код 01100 и соответственно на выходе сумматора по модулю два цепи обратной связи $\delta_2(9) = 0$. После второго сдвига на регистре сдвига имеем код 00110 и на выходе сумматора по модулю два $\delta_3(9) = 1$. После третьего и четвертого сдвига на регистре имеем 00011 и 00001 и на выходе сумматора по модулю два соответственно $\delta_4(9) = 1$, $\delta_5(9) = 1$. Таким образом, коэффициенты, определяющие топологию связей многоходового сумматора по модулю два, на выходе которого получается сдвинутая на 9 тактов m -последовательность имеет следующий вид $\delta_1(9) = 1$,

$\sigma_2(9) = 0, \sigma_3(9) = 1, \sigma_4(9) = 1,$
 $\sigma_5(9) = 1$. На фиг. 3 приведена
 временная диаграмма последовательностей на выходе сумматора по модулю
 два, топология связей которого определяется коэффициентами $\sigma_i(9)$ и
 исходной m -последовательности.

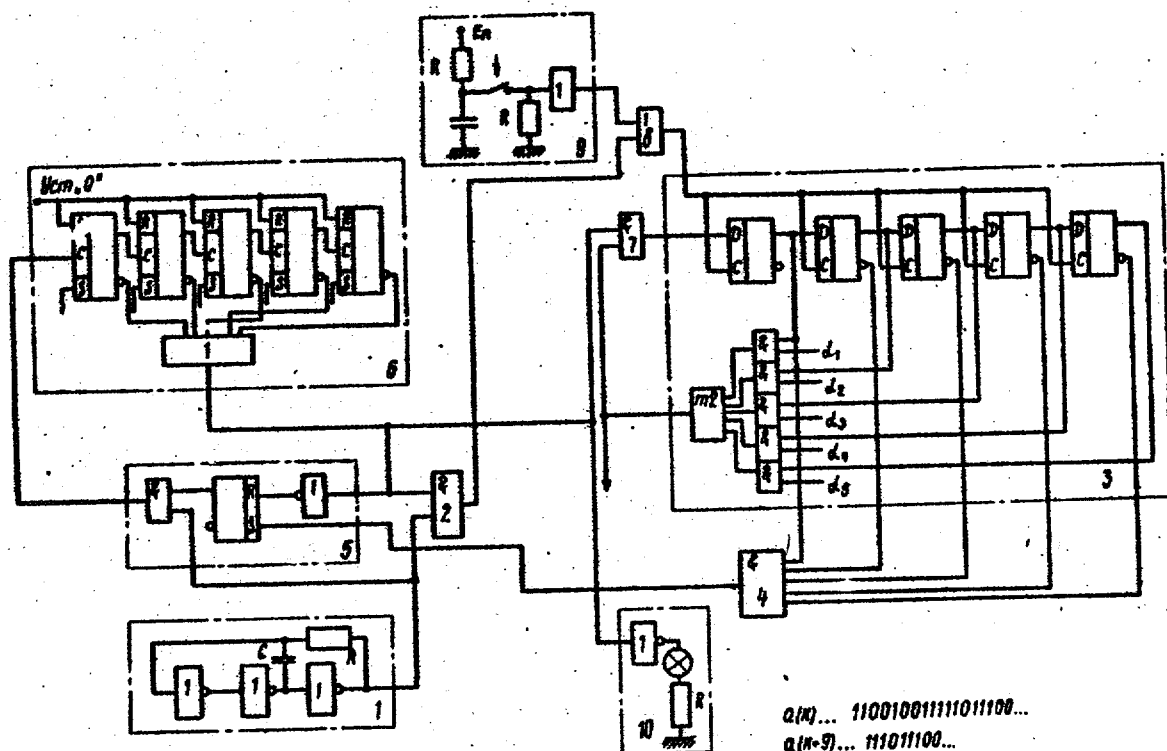
Как видно из фиг. 3 исходная и полученные последовательности сдвинуты на девять тактов.

Преимущества предлагаемого генератора псевдослучайных последовательностей заключаются в следующем.

Предлагаемый генератор псевдослучайностей существенно сокращает аппаратные затраты за счет отсутствия элементов памяти. Так для $m = 20$ необходимо было бы использовать 171 элемент памяти, что в

семь раз больше, чем затраты оборудования, идущие на другие блоки устройства. Дополнительное оборудование составляет весьма незначительный объем. Для любого m он состоит из одного двухвходового элемента И, одного двухвходового элемента ИЛИ, одного одноходового элемента ИЛИ, одного одноходового элемента ИЛИ-НЕ, трех сопротивлений, емкости и лампочки индикации.

Применение предлагаемого генератора псевдослучайных последовательностей, отличающегося уменьшенными аппаратными затратами, позволяет строить высоконадежные, стабильные и высококачественные генераторы псевдослучайных чисел, и тем самым повысить точность и достоверность решения задач методом Монте-Карло.



Фиг. 2

Фиг. 3

Редактор Н. Воловик Составитель А. Карасов Техред А. Ач Корректор Л. Боклан

Заказ 4213/33 Тираж 706 Подписное

ВНИПИ Государственного комитета СССР
 по делам изобретений и открытий
 113035, Москва, Ж-35, Раушская наб., д. 4/5

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