

Изобретение относится к вычислительной технике и может быть использовано для генерирования равномерно распределенных случайных чисел при решении задач вероятностного моделирования, реальных, процессов.

Известен управляемый преобразователь законов распределения вероятностей, содержащий  $n$  первичных датчиков случайных импульсов, генератор тактовых импульсов, первый выход которого соединен со входом "сдвиг" циклического регистра сдвига,  $(n-1)$  элементов И, выходы которых соединены со входами первого элемента ИЛИ, выход которого является выходом преобразователя и соединен со входом "сброс" циклического регистра сдвига, выходы которого соединены с первыми входами соответствующих элементов И [Авт.св. СССР № 898427, кл. G 06 F 7/58].

Недостатком данного устройства является функциональная сложность, что приводит к большим аппаратным затратам.

Известен генератор случайных чисел, содержащий блок памяти, сумматор, выход которого является выходом генератора и подключен к информационному входу блока памяти, выходы первой и последней ячейки которого соединены со входами сумматора [Рабинер Л., Голд Б. Теория и применение цифровой обработки сигналов. М., Мир, 1978].

Недостатком данного генератора является низкое быстродействие, так как после выработки очередного случайного числа необходимо выполнить сдвиг содержимого ячеек в блоке памяти.

Известен также генератор случайных чисел, содержащий генератор тактовых импульсов, реверсивный счетчик, выход которого соединен со входами первого и второго дешифраторов, два элемента И-НЕ, генератор случайной последовательности импульсов, выход которого соединен с первым входом второго элемента И-НЕ, выход которого соединен со входом управления направлением счета реверсивного счетчика, выход которого является выходом генератора, выход первого дешифратора соединен со вторым входом первого элемента И-НЕ, выход второго дешифратора соединен со вторым входом второго элемента И-НЕ, выход генератора тактовых импульсов подключен к счетному входу реверсивного счетчика [Патент РФ № 1661761, кл. G 06 F 7/58, 1992].

Недостатком этого генератора является его функциональная сложность, требующая больших аппаратных затрат.

Наиболее близким техническим решением является генератор случайных чисел, содержащий блок памяти, два счетчика, элемент задержки, регистр памяти и сумматор, выход которого является выходом генератора и соединен с информационным входом регистра памяти, выход которого соединен с информационным входом блока памяти и с первым входом сумматора, второй вход которого подключен к выходу блока памяти, синхронизирующий вход которого подключен к выходу источника тактовых импульсов и ко входу элемента задержки, выход которого соединен со счетными входами первого и второго счетчиков, информационные выходы которых соединены соответственно с адресным входом считывания и адресным входом записи блока памяти [Авт.св. СССР № 1388859, кл. G 06 F 7/58 (прототип)].

Недостатком данного генератора является то, что недостаточно точно соблюдается равномерность распределения случайных чисел и период повторения их серий небольшой.

В основу изобретения поставлена задача повышения качества генерируемых равномерно распределенных случайных чисел, для чего генератор случайных чисел совершенствуется путем обеспечения условий суммирования произвольного количества операндов за счет введения в генератор дополнительно  $(n-1)$  счетчиков адреса чтения.

Для решения поставленной задачи в генератор случайных чисел, содержащий блок памяти, суммирующий блок, регистр памяти, первый счетчик адреса чтения, счетчик адреса записи и элемент задержки, причем выход суммирующего блока является выходом генератора и соединен с информационным входом регистра памяти, выход которого соединен с информационным входом блока памяти, первый вход суммирующего блока соединен с первым выходом блока памяти, синхронизирующий вход которого подключен к выходу источника тактовых импульсов и к входу элемента задержки, - выход которого соединен со счетными входами первого счетчика адреса чтения и счетчика адреса записи, информационные выходы которых соединены соответственно с первым адресным входом чтения и адресным входом записи блока памяти, дополнительно введено  $(n-1)$  счетчиков адреса чтения, счетные входы которых подключены к выходу элемента задержки, а информационные выходы соединены соответственно со вторым по  $n$ -й адресными входами чтения блока памяти, выходы со второго по  $n$ -й которого соединены соответственно со вторым по  $n$ -й входами суммирующего блока.

Соответствующий сравнительный анализ с прототипом показывает, что заявляемый генератор случайных чисел отличается тем, что в нем подключены дополнительные счетчики, информационные выходы которых подключены к адресным входам блока памяти, что обеспечивает улучшение качества генерируемых случайных чисел за счет суммирования большого количества операндов.

Таким образом, заявляемый генератор соответствует критерию изобретения "новизна". Сравнение заявляемого решения не только с прототипом, но и с другими техническими решениями в данной области техники, не позволило выявить в них признаки, отличающие заявляемое решение от прототипа, что позволяет сделать вывод о соответствии критерию "существенные отличия",

На фиг.1, приведена функциональная схема генератора случайных чисел; на фиг.2 - примеры интерпретации двоичных кодов случайных чисел на выходе генератора.

На фиг.1 обозначены: суммирующий блок 1, регистр памяти 2, блок памяти 3, счетчики адреса чтения 4, счетчик адреса записи 5, элемент задержки 6, шина тактовых импульсов 7.

Выход суммирующего блока 1 является выходом генератора случайных чисел и подключен ко входу регистра памяти 2, выход которого соединен с информационным входом блока памяти 3,  $n$  выходов которого соединены со входами суммирующего блока 1, а каждый из  $n$  адресных входов подключены соответственно к выходу с первого по  $n$ -й выходов счетчиков адреса чтения 4, входы которых подключены к выходу элемента задержки 6 и ко входу счетчика адреса записи 5, выход которого подключен к адресному входу чтения блока

памяти 3, Шина тактовых импульсов 7 соединена с управляющим входом блока памяти 3 и со входом элемента задержки 6.

Предлагаемый генератор формирует очередное случайное число по соотношению

$$\xi(m) = [\xi(m-k_1) + \xi(m-k_2) + \dots + \xi(m-k_n)] \pmod{2^{M-1}}, \quad (1)$$

где  $M$  - разрядность двоичных чисел.

В настоящее время цифровая вычислительная техника использует двоичные числа с фиксированной точкой как целые числа в дополнительном коде, когда точка расположена после младшего разряда.

Выполнение суммирования случайных чисел  $\xi(m-k)$  по модулю  $(\text{mod } 2^{M-1})$  означает следующее.

Пусть производится суммирование двух чисел

$$X(m) = [X(m-k_1) + X(m-k_2)] \pmod{2^{M-1}}. \quad (2)$$

Тогда имеем соотношения

$$Y(m) = X(m-k_1) + X(m-k_2),$$

$$\begin{aligned} \text{если } -2^{(M-1)} \leq Y(m) < +2^{(M-1)}, \text{ то } X(m) &= Y(m); \\ \text{если } +2^{(M-1)} \leq Y(m) < +2^M, \text{ то } X(m) &= Y(m) - 2^M, \\ \text{если } -2^M < Y(m) \leq -2^{(M-1)}, \text{ то } X(m) &= Y(m) + 2^M. \end{aligned} \quad (3)$$

Реализация соотношений (3) упрощается для дополнительного кода представления целых двоичных чисел. В этом случае суммирование по алгоритму (3) производится путем выполнения операции сложения двух чисел без учета переполнения разрядной сетки.

Так для  $M=16$  имеем  $2^{(M-1)} = 32768$ .

Покажем выполнение формул (3) на примерах:

$$\begin{aligned} 16384 &= 0\ 100\ 000\ 000\ 000\ 000 \\ 8192 &= 0\ 010\ 000\ 000\ 000\ 000 \\ \hline 24576 &= 0\ 110\ 000\ 000\ 000\ 000 \end{aligned}$$

Переполнения нет.

$$\begin{aligned} 16384 &= 0\ 100\ 000\ 000\ 000\ 000 \\ 28672 &= 0\ 111\ 000\ 000\ 000\ 000 \\ \hline -20480 &= 1\ 011\ 000\ 000\ 000\ 000 \end{aligned}$$

$$-20480 = 16384 + 28672 - 65536$$

Сложение по  $(\text{mod } 2^{M-1})$  выполнено автоматически.

$$\begin{aligned} -16384 &= 1\ 100\ 000\ 000\ 000\ 000 \\ -8192 &= 1\ 110\ 000\ 000\ 000\ 000 \\ \hline -24576 &= 1\ 010\ 000\ 000\ 000\ 000 \end{aligned}$$

Переполнения нет, при этом перенос

"1" не учитывается.

$$\begin{aligned} -11264 &= 1\ 101\ 010\ 000\ 000\ 000 \\ -24576 &= 1\ 010\ 000\ 000\ 000\ 000 \\ \hline +29696 &= 0\ 111\ 010\ 000\ 000\ 000 \\ +29696 &= -11264 - 24576 + 65536 \end{aligned}$$

Сложение по  $(\text{mod } 2^{M-1})$  выполнено автоматически, при этом перенос "1" не учитывается.

Генератор случайных чисел реализует соотношение (1), когда суммируется по  $(\text{mod } 2^{M-1})$  произвольное количество целых двоичных чисел. Их можно просуммировать последовательно

$$X_1(m) = [X(m-k_1) + X(m-k_2)] \pmod{2^{M-1}};$$

$$X_2(m) = [X_1(m) + X(m-k_3)] \pmod{2^{M-1}};$$

$$\dots \dots \dots X(m) = [X_{n-2}(m) + X(m-k_n)] \pmod{2^{M-1}}. \quad (4)$$

Соотношение (4) автоматически выполняет  $n$ -входовой сумматор, в котором не учитывается перенос "1" из старшего разряда (этот перенос теряется).

В итоге получаем результат  $X(m)$  как целое двоичное число, лежащее в пределах

$$-2^{M-1} \leq X(m) < +2^{M-1}.$$

Известный генератор-прототип реализует алгоритм

$$X(q) = [X(q-1) + X(q-k)] \pmod{2^{M-1}}, \quad (5)$$

при  $k > 50$ .

Вырабатываемые случайные числа по алгоритму (5) имеют почти равномерный закон распределения с периодом цикличности  $T_c > 2^M$  [Крут Д. Искусство программирования на ЭВМ. М., Мир, 1977, т. 2]. Алгоритм (1) при  $n > 4$  формирует равномерно распределенные случайные числа, которые имеют практически

безграничный период цикличности. Предлагаемый генератор, быстродействие которого, как и у известного, равно быстродействию суммирующего блока можно с успехом использовать для цифровой обработки сигналов, а также при решении задач вероятностного моделирования реальных процессов.

В блоке 3 памяти хранится  $K \geq K_n$  равномерно распределенных случайных чисел, при этом, в процессе реализации соотношения (1) блок памяти самообновляется. Для первоначального запуска генератора равномерно распределенные случайные числа можно взять из любой готовой таблицы.

В вышеупомянутой книге Крут Д. Искусство программирования для ЭВМ. М., Мир, 1977 рекомендует индексы  $k_1; k_2; \dots; k_n$  в соотношении (1) выбирать по правилу  $k_j - k_{j-1} > 50$ , где  $(k_j - k_{j-1})$  - числа простые, считая  $K_0 = 0$ .

Для примера можно ограничиться случаем  $n = 4$ , при этом индексам присвоить значения:

$$k_1 = 53; k_2 = 59 + k_1 = 112; k_3 = 67 + k_2 = 179; k_4 = 73 + k_3 = 252.$$

Тогда в блоке памяти 3 можно хранить  $2^8 = 256$  равномерно распределенных случайных чисел, и этого достаточно для реализации алгоритма (1) при суммировании четырех операндов

$$\xi(m-k_1); \xi(m-k_2); \xi(m-k_3); \xi(m-k_4).$$

Аналогично можно определить объем блока памяти 3 при суммировании произвольного количества чисел  $\xi(m-K_j)$ .

Для обеспечения высокого качества случайных чисел следует использовать блоки генератора повышенной разрядности, а сами числа перед выходом усекают до заданной разрядности.

В настоящее время наибольшее распространение получила 16-разрядная вычислительная техника, поэтому следует суммировать 32-разрядные операнды  $\xi(m-k_j)$  с округлением результата  $\xi(m)$  до 16-разрядного числа.

На фиг.2 приведены примеры интерпретации 16-разрядных двоичных чисел  $\xi(m)$  с фиксированной запятой в зависимости от принятых правил размещения точки.

Если точка расположена после младшего разряда (целые числа), то числа  $\xi(m)$  равномерно распределены в пределах: на фиг.2а имеем  $(-32768 \leq \xi(m)) < +32768$ ; на фиг.2б имеем  $(0 \leq \xi(m)) < +65536$ , при этом знак + (код "0" только подразумеваемые).

При интерпретации дробных чисел точка располагается после знакового разряда, в том числе при условном кодировании знака.

На фиг.2а,б,в представлена интерпретация дробных чисел соответственно:  $(-1,0 \leq \xi(m) < +1,0)$ ;  $(+0,0 \leq \xi(m) < 1,0)$ ;  $(0,5 \leq \xi(m) < +0,5)$ .

Предлагаемый генератор случайных чисел работает следующим образом.

В блоке памяти 3 хранится  $L - 2^P$  случайных чисел  $\xi(m)$ , которые были сформированы ранее. Первоначально эти числа вводятся заранее. Счетчики 4 адреса чтения находятся в состоянии соответственно  $(m-k_1); (m-k_2); \dots; (m-k_n)$  по модулю  $L - 2^P$ , где  $L$  - объем блока памяти 3. Счетчик 5 адреса записи находится в состоянии  $0 \leq L$ . При первоначальном запуске можно принять  $m = (L-1)$ . В регистре 2 находится ранее сформированное случайное число  $\xi(m-1)$ .

Формирование очередного случайного числа  $\xi(m)$  начинается с поступлением в генератор через управляющий вход блока памяти 3 очередного тактового импульса по шине 7. По этому импульсу в суммирующий блок 1 поступает  $n$  операндов  $\xi(m-k_1); \xi(m-k_2); \dots; \xi(m-k_n)$ , из блока памяти 3 по адресам чтения, выбираемого с выходов соответствующих счетчиков 4. На выходе суммирующего блока 4 вырабатывается очередное случайное число  $\xi(m)$ , имеющего повышенную разрядность. Результат  $\xi(m)$  на выходе генератора округляется до заданной разрядности, а без изменения разрядности поступает в регистр памяти 2, с выхода которого ранее хранимое число  $\xi(m-1)$  записывается в блок памяти 3 по адресу, считываемого с выхода счетчика 5 адреса записи.

Тактовый импульс с шины 7 также поступает на вход элемента задержки 6, с выхода которого тактовый импульс поступает на счетные входы всех  $m$  счетчиков 4 адреса чтения и счетчика 5 адреса записи задержка тактового импульса в элементе задержки 6 необходима для разнесения по времени считывания адресов с их выходов, а затем изменения их состояния на "1" по модулю  $L = 2^P$ .

Темп поступления тактовых импульсов в генератор по шине 7 согласован с быстродействием суммирующего блока 1. В итоге быстродействие предлагаемого генератора случайных чисел  $\xi(m)$  равно быстродействию суммирующего блока на  $n$  выходов и не зависит от объема блока памяти 3.

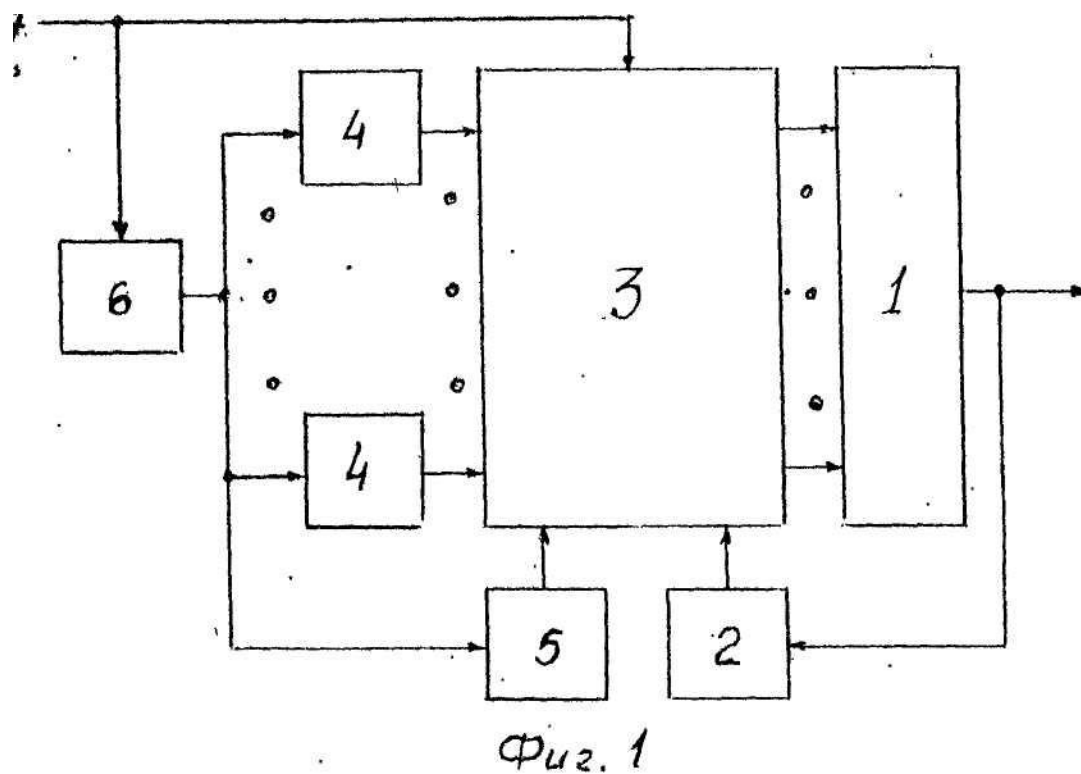
В настоящее время электронная технология микросхем позволяет создавать, например, четырехходовые 32-разрядные сумматоры с быстродействием до 100 млн. операций в секунду. С таким быстродействием можно генерировать высококачественные равномерно распределенные случайные числа  $\xi(m)$  с помощью предлагаемого технического решения.

Положительный эффект изобретения заключается в том, что за счет увеличения количества суммируемых операндов, разнесенных по времени на достаточно большие расстояния улучшается равномерность распределения генерируемых случайных чисел, при этом быстродействие по сравнению с прототипом не изменяется.

В известном генераторе суммируется два операнда  $\xi(m-1)$  и  $\xi(m-k)$  при  $k > 50$ , а операнд  $\xi(m-1)$  отстоит всего на один такт, от вырабатываемого числа  $\xi(m)$ . Это приводит к неравномерности закона распределения. Увеличив количество суммируемых чисел  $\xi(m-k_j)$  по соотношению (1) неравномерность закона распределения случайных чисел  $\xi(m)$  устраняется, а период цикличности становится практически безграничным.

Для достижения такого эффекта дополнительно введено  $(n-1)$  счетчиков, адреса чтения операндов.

Таким образом, введение  $(n-1)$  счетчиков позволяет увеличить количество суммируемых операндов с двух до  $n$  при генерировании очередных случайных чисел без изменения быстродействия генератора. Качество случайных чисел  $\xi(t)$  повышается за счет улучшения равномерности распределения и особенно резкого увеличения периода цикличности.



a)

$x_{15}$	$x_{14}$	$x_{13}$	$x_{12}$	$x_{11}$	$x_{10}$	$x_9$	$x_8$	$x_7$	$x_6$	$x_5$	$x_4$	$x_3$	$x_2$	$x_1$	$x_0$
----------	----------	----------	----------	----------	----------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------

б)

0	$x_{15}$	$x_{14}$	$x_{13}$	$x_{12}$	$x_{11}$	$x_{10}$	$x_9$	$x_8$	$x_7$	$x_6$	$x_5$	$x_4$	$x_3$	$x_2$	$x_1$	$x_0$
---	----------	----------	----------	----------	----------	----------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------

в)

$x_{15}$	$x_{14}$	$x_{13}$	$x_{12}$	$x_{11}$	$x_{10}$	$x_9$	$x_8$	$x_7$	$x_6$	$x_5$	$x_4$	$x_3$	$x_2$	$x_1$
----------	----------	----------	----------	----------	----------	-------	-------	-------	-------	-------	-------	-------	-------	-------

$\Phi_{u2.2}$