Союз Советских Социалистических Республик

Государственный комитет СССР по делам изобретений и открытий

ОПИСАНИЕ ИЗОБРЕТЕНИЯ

К АВТОРСКОМУ СВИДЕТЕЛЬСТВУ

(11) 739603

(61) Дополнительное к авт. свид-ву –

(22) Заявлено 25.01.78 (21) 2571997/18-24

с присоединением заявки № –

(23) Приоритет –

Опубликовано 05.06.80. Бюллетень № 21

Дата опубликования описания 08.06.80

(51) М. Кл.^{2} G07 C 15/00 G06 F 1/02

(53) УДК 681.325 (088.8)

(72) Авторы изобретения В. Н. Ярмолик и А. И. Ковалев

(71) Заявитель Минский радиотехнический институт

(54) МНОГОКАНАЛЬНЫЙ ГЕНЕРАТОР ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ

1

Изобретение относится к вычислительной технике и может быть использовано в решающих блоках стохастических вычислительных машин, а также для моделирования случайных процессов на универсальных вычислительных машинах.

Известен генератор псевдослучайных чисел на основе m-разрядного регистра сдвига и сумматора по модулю два в цепи обратной связи. Подобный ГПСЧ состоит из генератора тактовых импульсов, m-разрядного регистра сдвига, сумматора по модулю два в цепи обратной связи.

Как известно, такая схема может генерировать циклическую двоичную последовательность максимальной длины (М-последовательность) с периодом $M = 2^m - 1$, где m-разрядность регистра сдвига, статистические свойства которой аналогичны свойствам последовательности равновероятных символов 0 и 1.

В случае выборки очередного псевдослучайного числа в каждый такт работы устройства наблюдается жесткая корреляция между последующими значениями многоразрядных кодов псевдослучайных чисел. Во избежание наличия корреляционной зависимости в таких устройствах необходимо осуществлять выборку выходных чисел только через $K \geq \ell$ тактов, где $\ell \leq m$-разрядность псевдослучайного числа. Следовательно, быстродействие устройства в предельном случае в m раз меньше тактовой частоты [1].

2

Однако такой генератор позволяет получить только один канал. При использовании псевдослучайных чисел в стохастических ВМ необходимо несколько каналов, независимых псевдослучайных чисел. Быстродействие ГПСЧ, при необходимости получения независимых ℓ-разрядных псевдослучайных чисел, оказывается в ℓ раз ниже его тактовой частоты.

Известен генератор псевдослучайных чисел на основе двух регистров сдвига с различным числом разрядов n и m,

генерирующих последовательности максимальной длины. Генератор содержит задающий генератор импульсов, n-разрядный регистр сдвига с сумматором по модулю два в цепи обратной связи, m -разрядный регистр сдвига с сумматором по модулю два в цепи обратной связи, r сумматоров по модулю два. В таком генераторе при условии, что периоды обеих последовательностей $N = 2^n - 1$ и $M = 2^m - 1$ являются взаимно простыми числами, можно получить некоррелированные в пределах N тактов работы, периода исходной последовательности большей длины (при $n > m$), псевдослучайные последовательности путем сложения по модулю два состояний двух разрядов регистров (по одному от каждого). Свойства таких последовательностей близки свойствам М-последовательностей. Максимальное число каналов, одновременно генерируемых таким ГПСЧ, равно $n + m - 1$. Число независимых каналов на основе двух регистров сдвига равно $n + m - 1$, [2].

При необходимости получения большого числа каналов, надо пропорционально ему увеличивать разрядности регистров сдвига n и m, что приводит к значительным аппаратурным затратам, неравномерности распределения псевдослучайных чисел, так как генерируемые последовательности являются участками последовательности $C_K = a_K \oplus b_K$, где a_K – последовательность периода N, а b_K – периода M, уменьшении периода работы генератора в $n + m - 1$ раз вследствие разбиения последовательности C_K на отдельные участки; однозначности соответствия значений периодов N и M, которые должны быть только взаимно простыми числами.

Наиболее близким к изобретению по технической сущности является генератор псевдослучайных чисел (многоканальный), содержащий задающий генератор импульсов, m -разрядный регистр сдвига с сумматором по модулю два в цепи обратной связи, r многовходовых сумматоров по модулю два. Генератор одновременно генерирует несколько участков полного кодового кольца М– последовательности, которое обеспечивается путем поразрядного сложения по модулю два отдельных последовательностей, снимаемых с соответствующих разрядов регистра сдвига. В этом генераторе отдельные каналы являются разрядами генерируемого числа. Для сдвига полного числового кольца М–последовательности на любое число символов С выходы определенных разрядов регистра сдвига подключают ко входу сумматора по модулю два. Структура связей определяется путем моделирования на ЭВМ исходной М–последовательности. Для этого в начальном состоянии генератора необходимо записать единицу в $i + 1$ разряд регистра сдвига (i -й разряд подключен ко входу сумматора 3 в цепи обратной связи регистра) и нули в остальные разряды. Тогда после каждых С тактов работы в регистре будут зафиксированы определенные m -разрядные коды. Наличие единицы в разряде регистра свидетельствует о том, что его выход подключается ко входу сумматора 4, а наличие нуля – о том, что не подключается. Для каждого канала необходим определенный сдвиг $K \cdot C$ (где $K = 1,2,\ldots r$), а следовательно ему присущ определенный код в регистре, строго определяющий структуру логических связей. Очевидно, что число разрядов, которые надо подключить ко входам сумматоров 4, зависит от числа единиц в коде регистра, который фиксируют через $K \cdot C$ тактов работы. В среднем число единиц в регистре сдвига за период М работы генератора равно $m/2$. Это значит, что для организации одного канала на основе m-разрядного регистра сдвига необходим сумматор по модулю два с $m/2$ входами. Обычно производят оптимизацию оборудования, что предусматривает при моделировании сдвиг не на $K \cdot C$ символов, а число близкое к нему. Целью является получение кода с минимальным числом единиц. В результате добиваются сокращения удельных затрат на канал до сумматора с $m/4$ входами. Лучшего результата добиться трудно [3].

Анализ данного генератора показывает, что при необходимости получения большого числа каналов К исходная М–последовательность разбивается на К одновременно генерируемых участков. При этом уменьшается период работы генератора до

$$M_K = \frac{M}{K} = \frac{2^m - 1}{K}.$$

Недостатком также является увеличение неравномерности распределения чисел при большом числе каналов. Это объясняется неравенством числа единиц

и нулей на отдельных участках М-последовательности.

Необходимы значительные удельные затраты оборудования на реализацию каждого канала. Для формирования таких каналов требуется использовать в среднем $m/4$ разрядов регистра сдвига, что приводит к необходимости применять либо сложные многовходовые сумматоры по модулю два, либо несколько двухходовых сумматоров (полусумматоров).

Попытка устранить два предыдущих недостатка путем увеличения разрядности m регистра сдвига, а следовательно и периода основной М-последовательности, приводит к увеличению числа входов сумматора по модулю два, необходимого для реализации одного канала.

Недостатком также является сложность подготовки к построению многоканального ГПСЧ, которая предусматривает моделирование на ЭВМ исходной М-последовательности.

Цель изобретения - сокращение удельного оборудования на один канал, увеличение периода работы генератора до максимальнс возможного для данной разрядности m регистра сдвига, а также уменьшения неравномерности распределения чисел при сохранении прежней корреляционной характеристики генератора.

Поставленная цель достигается тем, что в многоканальный генератор псевдослучайных чисел, содержащий задающий генератор импульсов, m-разрядный триггерный регистр сдвига с сумматором по модулю два в цепи обратной связи, причем выход задающего генератора подключен ко входам синхронизации триггеров регистра сдвига, вводятся две группы элементов И, группа элементов ИЛИ, группа сумматоров по модулю два, причем к первому входу i-го элемента И первой группы подключен прямой выход первого разряда регистра сдвига, а ко второму входу - прямой выход $i+1$-го разряда регистра сдвига ($i = 1, 2, 3, \ldots, m-1$), к первому входу i-го элемента И второй группы подключен инверсный выход первого разряда регистра сдвига, а ко второму - прямой выход j-го разряда регистра ($j = 2, 3, \ldots, m$; $j = m+1$), причем выходы i-х элементов И первой и второй групп подключены ко входам i-х элементов ИЛИ, выходы которых попарно подключены ко входам К сумматоров по модулю два, а выход o-го элемента ИЛИ - ко второму входу сумматора К (где $p = 1, 2, \ldots m-1$; $q = 1, 2 \ldots, m-1$; $p = q \ldots, k = 1, 2, \ldots \frac{m^2}{2} - \frac{3m}{2} + 1$).

На чертеже приведена схема предлагаемого генератора при $m = 8$.

Генератор содержит задающий генератор 1 импульсов, 8-разрядный регистр 2 сдвига с сумматором по модулю два в цепи 3 обратной связи, группу элементов 4 И, группу элементов 5 И; группу элементов 6 ИЛИ, группу сумматоров 7 по модулю два.

Задающий генератор импульсов предназначен для синхронизации работы всего устройства, регистр сдвига с сумматором по модулю два в цепи обратной связи - для получения псевдослучайной последовательности единиц и нулей с периодом, равным $2^m - 1$, две группы элементов И и группа элементов ИЛИ - для получения последовательностей нулей и единиц, вероятность появления, которых равна 0,5, а период последовательностей равен $2^m - 1$, группа сумматоров по модулю два - для получения большого числа каналов, генерирующих ПС числа.

Независимый канал, генерирующий ПС последовательность, получают, используя свойство М-последовательности, заключающееся в том, что вероятность появления двух определенных символов (11,10,01,00) в любых двух разрядах регистра сдвига равно 1/4.

Если обозначить прямой выход разряда регистра сдвига X, а инверсный выход $\bar{X}_i$ ($i = 1, 2, \ldots, m$), то реализацию таких последовательностей можно выразить математически следующим образом:

$$V_1 = X_1 X_2 + \bar{X}_1 X_4$$
$$V_2 = X_1 X_3 + \bar{X}_1 X_7$$
$$V_3 = X_1 X_4 + \bar{X}_1 X_8$$
$$V_4 = X_1 X_5 + \bar{X}_1 X_6$$
$$V_5 = X_1 X_6 + \bar{X}_1 X_3$$
$$V_6 = X_1 X_7 + \bar{X}_1 X_2$$
$$V_7 = X_1 X_8 + \bar{X}_1 X_5$$

Получают последовательности $V_1 - V_7$ с вероятностью появления 1 или 0, равной 1/2. Для получения V_i складывают последовательности $X_1 X_2$ и $X_1 X_4$ с вероятностью появления единицы, равной 1/4. Возможность появления единицы

одновременно в двух слагаемых исключена, так как первое слагаемое равно 1 при $X_1 = 1$, $X_2 = 1$, а второе – при $X_1 = 0$, $X_4 = 1$. Число таких последовательностей $N_1 = m - 1$. Простое сложение в выражениях эквивалентно суммированию по модулю два.

Функционирование устройства происходит следующим образом.

Производят запись начального кода в регистр 2 сдвига и по сигналам генератора 1 тактовых импульсов в нем начинает происходить смена состояний, определяемая структурой обратной связи. В зависимости от состояния разрядов регистра сдвига на выходах элементов 4,5,6,7 получают последовательности единиц и нулей, которые в каждом конкретном случае определяются структурой логических связей. Через $2^m - 1$ тактов работы состояния регистра сдвига начнут повторяться, а, следовательно, начнут повторяться последовательности на выходах элементов 4,5, 6,7. Отсюда следует, что период работы генератора равен $2^m - 1$.

Величина функции Φ_K корреляции между отдельными каналами

$$\Phi_{Kij} = -\frac{1}{M}.$$

Вывод о равномерности распределения чисел в данном генераторе следует из вывода о минимальной корреляции между каналами.

Таким образом, введение двух групп элементов И, группы элементов ИЛИ и группы сумматоров по модулю два позволяет значительно сократить затраты оборудования на реализацию многоканального ГПСЧ. Получаемая экономия оборудования будет тем более высокой, чем большее число каналов необходимо получить на основе регистра сдвига и чем больше разрядность m этого регистра.

Например, для построения 30 каналов по 15 разрядов на основе 32 разрядного регистра сдвига, удельные затраты оборудования в известном устройстве равны примерно одному восьмивходовому сумматору по модулю два (число входов равно $m/4$). Это эквивалентно семи полусумматорам по модулю два. Удельные затраты предлагаемого устройства равны примерно одному двухвходовому сумматору по модулю два. С ростом разрядного регистра сдвига m они не растут, а несколько уменьшаются.

Таким образом, получают семикратный выигрыш в оборудовании, а также период работы генератора возрастает в 450 раз по сравнению с известным равномерно распределенные и некоррелированные числа. Скорость работы генератора равна тактовой частоте.

Формула изобретения

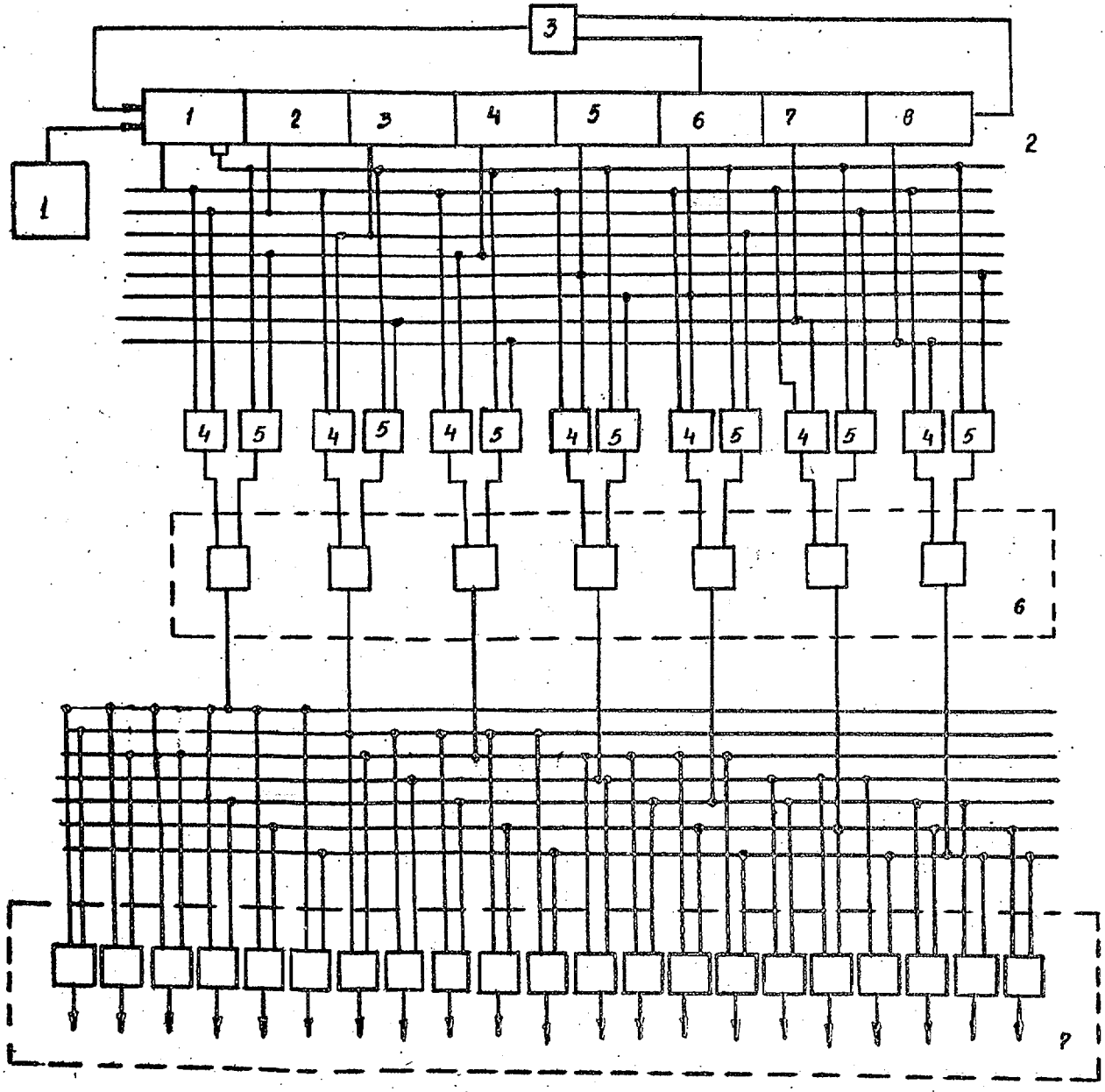
Многоканальный генератор псевдослучайных чисел, содержащий задающий генератор импульсов, m-разрядный триггерный регистр сдвига с сумматором по модулю два в цепи обратной связи, причем выход задающего генератора подключен ко входам синхронизации триггеров регистра сдвига, отличающийся тем, что, с целью сокращения аппаратурных затрат генератора, он содержит две группы элементов И, группу элементов ИЛИ, группу сумматоров по модулю два, причем к первому входу i-го элемента И первой группы подключен прямой выход первого разряда регистра сдвига, а ко второму входу – выход $i+1$-го разряда регистра сдвига ($i = 1,2,3,\ldots m-1$) к первому входу i-го элемента И второй группы подключен инверсный выход первого разряда регистра сдвига, а ко второму выход j-го разряда регистра ($j=2,3,m$; $j=m+1$), кроме того, выходы i-го элемента и первой группы и элемента И второй группы подключены ко входам i-го элемента ИЛИ, выход P-го элемента ИЛИ подключен к первому входу K-го сумматора по модулю два, а выход q-го элемента ИЛИ – ко второму входу сумматора К (где $p = 1,2,\ldots m-1$; $q = 1,2,\ldots m-1$; $p \neq q$; $k = 1,2,\ldots \left(\frac{m^2}{2} - \frac{3m}{2} 1\right)$.

Источники информации, принятые во внимание при экспертизе

1. Яковлев В. В., Федоров Р. Ф. Стохастические вычислительные машины Ленинград, "Машиностроение", 1974, с. 238-283.

2. Добрис Г. В. Метод синтеза генератора псевдослучайных чисел для стахостических вычислительных машин на основе двух регистров сдвига. Автоматика и вычислительная техника, 1973, № 2, с. 1-7.

3. Кирьянов Б. Ф. Многоканальный генератор псевдослучайных символов. "Техническая кибернетика". Известия АН СССР, 1970, № 4, с. 197-110 (прототип).



Составитель Загорбинина

Редактор Н. Кравцова Техред И. Асталош Корректор М. Пожо

Заказ 3049/8 Тираж 641 Подписное

ЦНИИПИ 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