Союз Советских Социалистических Республик

Государственный комитет Совета Министров СССР по делам изобретений и открытий

ОПИСАНИЕ ИЗОБРЕТЕНИЯ

К АВТОРСКОМУ СВИДЕТЕЛЬСТВУ

(11) 634329

(61) Дополнительное к авт. свид-ву –

(22) Заявлено 27.10.76 (21) 2415584/18-24

с присоединением заявки № –

(23) Приоритет –

(43) Опубликовано 25.11.78. Бюллетень № 43

(45) Дата опубликования описания 28.11.78

(51) М. Кл.[2] G 07 C 15/00 G 06 F 1/02

(53) УДК 681.325. (088.8)

(72) Авторы изобретения В. Н. Ярмолик и А. Н. Морозевич

(71) Заявитель Минский радиотехнический институт

(54) ГЕНЕРАТОР ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ

1

Изобретение относится к области вычислительной техники и может быть использовано для повышения эффективности больших ЦВМ, для расширения возможности малых ЦВМ при вероятностном моделировании, а также в качестве основного блока стохастических ЭВМ.

Известны генераторы псевдослучайных чисел, основанные на применении регистров сдвига. Простейшим генератором псевдослучайных чисел на базе регистра сдвига является последовательный генератор псевдослучайных чисел (ГПСЧ) [1]. В таком генераторе очередное двоичное число образуется на выходе ℓ разрядов регистра сдвига через $N \geq \ell$ импульсов сдвига. Частота выборки псевдослучайных чисел в N раз меньше, чем тактовая частота.

Другой из известных генераторов псевдослучайных чисел для повышения быстродействия на один разряд содержит $m + m\cdot\left(\frac{m-i}{1}\right)$ триггеров, что обуславливает его аппаратурную избыточность [2].

2

Наиболее близким техническим решением к данному изобретению является генератор псевдослучайных чисел, содержащий m сумматоров по модулю два и m триггеров, входы синхронизации которых подключены к выходу генератора тактовых импульсов [3].

Недостатком этого генератора также является аппаратурная избыточность.

Целью изобретения является упрощение генератора.

Для достижения поставленной цели единичные выходы триггеров подключены к первым входам сумматоров по модулю два соответственно, вторые входы i старших сумматоров по модулю два подключены к единичным выходам i младших триггеров соответственно, счетные входы $2i-m$ старших триггеров соединены с единичными выходами $2i-m$ младших триггеров соответственно, счетные входы $2m-2i$ младших триггеров соединены с выходами $2m-2i$ старших сумматоров по модулю два соответственно, вто-

рые входы $m-i$ младших сумматоров по модулю два подключены к выходам $m-i$ старших сумматоров по модулю два соответственно.

Блок-схема генератора для случая $m=5$ (m –число разрядов генератора) приведена на чертеже.

Генератор содержит m триггеров 1, входы синхронизации которых подключены к генератору тактовых импульсов 2, m сумматоров по модулю два 3, первые входы которых соединены с единичными выходами триггеров, а вторые входы i старших сумматоров по модулю два соединены с единичными выходами i младших триггеров, вторые входы $m-i$ младших сумматоров по модулю два соединены с $m-i$ выходами старших сумматоров по модулю два, счетные входы $2i-m$ старших триггеров соединены с единичными выходами $2i-m$ младших триггеров, а счетные входы $2m-2i$ младших триггеров соединены с выходами $2m-2i$ старших сумматоров по модулю два.

Работает генератор следующим образом. Начальное псевдослучайное число имеет вид $\xi_{10}=b_1^0 b_2^0 b_3^0 \ldots b_{2m}^0$, где m разрядность регистра сдвига, на базе которого основан генератор. Число $b_1^0, b_2^0 b_3^0 \ldots b_m^0$ снимается с выходов сумматоров по модулю два слева направо, а число $b_{m+1}^0 \ldots b_{2m}^0$ с выходов триггеров со счетным входом. При поступлении тактового импульса состояние триггеров и соответственно состояние выходов сумматоров по модулю два изменяется. По истечении переходных процессов на выходах сумматоров по модулю два и выходах триггеров получается очередное псевдослучайное число $\xi_{11}=b_1' b_2' \ldots b_{2m}'$. При поступлении очередного тактового импульса получается следующее число ξ_{12} и т. д. Из функционирования многоканального генератора псевдослучайных чисел очевидно, что данное устройство имеет максимальное быстродействие, т. е. за один такт получается следующее число. В данном случае быстродействие определяется только элементной базой. Структурный состав генератора показывает, что при минимальных затратах оборудования получается $2m$ разрядное псевдослучайное число. Данный генератор, как и все генераторы на базе регистра сдвига с сумматором по модулю два, генерирует M – последовательность, свойства которой хорошо изучены.

Аналитически функциональные связи для построения многоканального генератора псевдослучайных чисел для любого значения легко определить из следующей системы уравнений (1):

$$b_{m-j}^{K+1} = b_{2m-j}^{K} \oplus b_{m+i-j}^{K}, \quad j=0,1,2,\ldots m-1$$

$$b_{2m-j}^{K+1} = b_{2m-j}^{K} \oplus b_{2i-j}^{K}, \quad j=0,1,2,\ldots m-1$$

где b_{m-j}^{K+1} – содержимое или значение $m-j$ разряда ГСПЧ в К+1 такт работы устройства.

Для пояснения аналитической зависимости (1) и функционирования генератора на чертеже приведена конкретная структура для $m=5$. Легко видеть, что функциональные связи структуры подчиняются вышеприведенной системе уравнений (1). Так, например, для $m=5$, $i=3$ система уравнений (1) имеет вид

$$b_5 = b_{10} \oplus b_8 \qquad b_{10} = b_{10} \oplus b_6$$
$$b_4 = b_9 \oplus b_7 \qquad b_9 = b_9 \oplus b_5$$
$$b_3 = b_8 \oplus b_6 \qquad b_8 = b_8 \oplus b_4$$
$$b_2 = b_7 \oplus b_5 \qquad b_7 = b_7 \oplus b_3$$
$$b_1 = b_6 \oplus b_4 \qquad b_6 = b_6 \oplus b_2$$

что полностью соответствует функциональным связям между узлами многоканального генератора псевдослучайных чисел, приведенного на чертеже.

Все известные генераторы псевдослучайных чисел на базе регистра сдвига имеют одинаковые статистические свойства, отражающие равномерность и случайность появления двоичных цифр. Все эти свойства определяются свойствами последовательного генератора, что доказывается в ряде литературных источников.

Предлагаемый многоканальный генератор псевдослучайных чисел обладает аналогичными свойствами в силу того, что генерирует идентичную последовательность псевдослучайных чисел, как и последовательный генератор. Справедливость этого утверждения подтверждается функционированием последовательного генератора и предлагаемого генератора. Для генератора, приведенного на чертеже, последовательность псевдослучайных чисел будет иметь вид:

$\xi_7 = b_1 b_2 b_3 b_4 b_5 b_6 b_7 b_8 b_9 b_{10}$

$\xi_{70} = 1\ 1\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 0$

$\xi_{71} = 1\ 1\ 0\ 1\ 1\ 0\ 0\ 0\ 1\ 1$

. . . . . .

причем очередное число получается за один такт, и разрядность этого числа равняется 10, т. е. в общем случае $2m$. Для последовательного генератора последовательность состояний триггеров будет иметь вид:

1.	1	1	1	0	0	1	1	0	1	0
2.	1	1	1	1	0	0	1	1	0	1
3.	1	1	1	1	1	0	0	1	1	0
4.	0	1	1	1	1	1	0	0	1	1
5.	0	0	1	1	1	1	1	0	0	1
6.	1	0	0	0	1	1	1	1	1	0
7.	1	1	0	0	0	1	1	1	1	1
8.	0	1	1	0	0	0	1	1	1	1
9.	1	0	1	1	0	0	0	1	1	1
10.	1	1	0	1	1	0	0	0	1	1

Очевидно, что очередным псевдослучайным числом может являться только такое число, которое получается через $N \leq 10$ тактов, т. е. очередным после ξ'_{70} является число ξ^1_{71}. Из вышеприведенного легко видеть, что $\xi_0 = \xi^1_{70}$ и $\xi_1 = \xi'_{71}$, но получение ξ_7 сопряжено с большими временными затратами.

Таким образом, введение новых функциональных связей и сумматоров по модулю два позволяет получить быстродействующий, высоко экономичный многоканальный генератор псевдослучайных чисел. Если в прототипе удельные затраты оборудования на один разряд составляли один триггер со счетным входом, то в предлагаемом генераторе 1/2 триггера плюс 1/2 сумматора по модулю два. И в то же время быстродействие такого генератора максимально. Патентный поиск показал, что предлагаемый многоканальный генератор псевдослучайных чисел имеет максимальное быстродействие (т. е. это устройство однотактное) и самые минимальные удельные затраты оборудования по сравнению с известными.

Формула изобретения

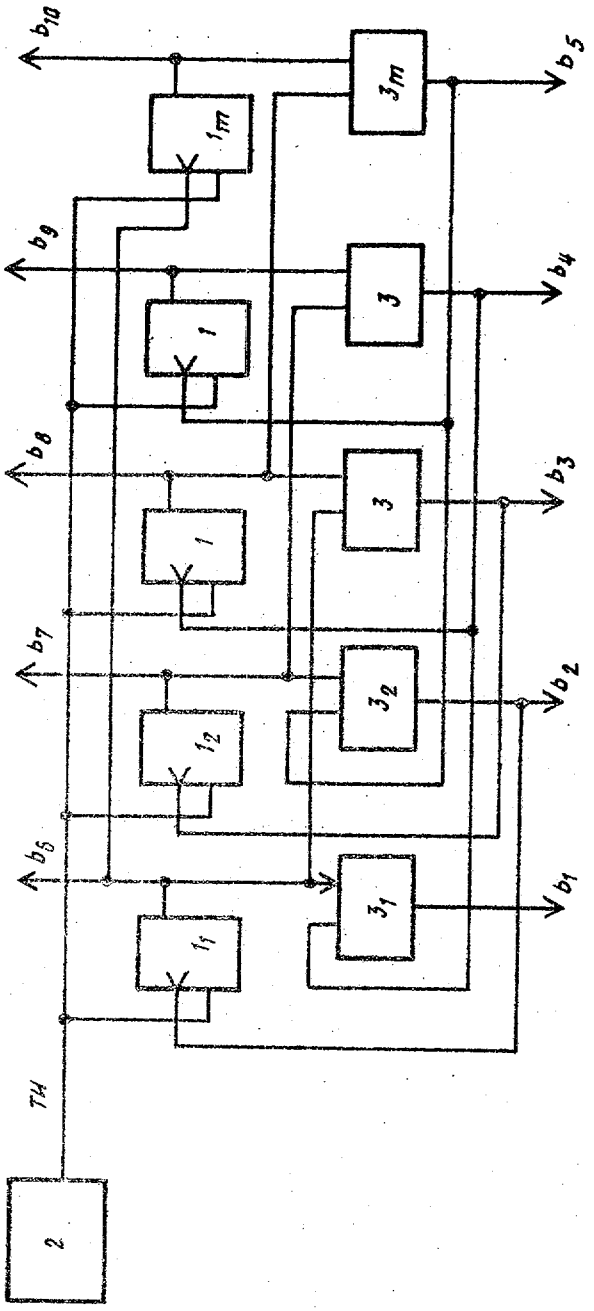
Генератор псевдослучайных чисел, содержащий m сумматоров по модулю два и m триггеров, входы синхронизации которых подключены к выходу генератора тактовых импульсов, отличающийся тем, что, с целью упрощения генератора, единичные выходы триггеров подключены к первым входам сумматоров по модулю два соответственно, вторые входы i старших сумматоров по модулю два подключены к единичным выходам i младших триггеров соответственно, счетные входы $2i - m$ старших триггеров соединены с единичными выходами $2i - m$ младших триггеров соответственно, счетные входы $2m - 2i$ младших триггеров соединены с выходами $2m - 2i$ старших сумматоров по модулю два соответственно, вторые входы $m - i$ младших сумматоров по модулю два подключены к выходам $m - i$ старших сумматоров по модулю два соответственно.

Источники информации, принятые во внимание при экспертизе:

1. Яковлев В. В., Федоров Р. Ф. Стахастические вычислительные машины. Л., "Машиностроение", 1974, с. 246-253.

2. Авторское свидетельство СССР №468231, кл. G 06 F 1/02, 14.09.73.

3. Авторское свидетельство СССР №543962, кл. G 07 C 15/00, 16,06.75.



Составитель А. Карасов
Редактор Д. Мепуришвили Техред М. Борисова Корректор А. Гриценко
Заказ 6767/50 Тираж 688 Подписное
ЦНИИПИ Государственного комитета Совета Министров СССР
по делам изобретений и открытий
113035, Москва, Ж-35, Раушская наб., д. 4/5
Филиал ППП "Патент", г. Ужгород, ул. Проектная, 4