Союз Советских Социалистических Республик

Государственный комитет Совета Министров СССР по делам изобретений и открытий

ОПИСАНИЕ ИЗОБРЕТЕНИЯ

К АВТОРСКОМУ СВИДЕТЕЛЬСТВУ

(11) 572823

(61) Дополнительное к авт. свид-ву —

(22) Заявлено 09.09.75 (21) 2173579/24

с присоединением заявки № —

(23) Приоритет —

Опубликовано 15.09.77. Бюллетень № 34

Дата опубликования описания 28.09.77

(51) М. Кл.² G 07C 15/00
G 06F 1/02

(53) УДК 681.325(088.8)

(72) Авторы изобретения А. Е. Леусенко, В. Н. Ярмолик, А. Н. Морозевич и В. М. Цуриков

(71) Заявитель Минский радиотехнический институт

(54) ГЕНЕРАТОР ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ

1

Изобретение относится к вычислительной технике и может быть использовано для повышения эффективности больших ЦВМ, для расширения возможностей — малых при вероятностном моделировании, а также в качестве основного блока стахостических ЭВМ.

Известны генераторы псевдослучайных чисел, основанные на применении регистров сдвига. Простейшим генератором псевдослучайных чисел на базе регистра сдвига является последовательный генератор псевдослучайных чисел, в котором очередное двоичное число образуется на выходе l разрядов регистра сдвига через каждые $N \geqslant l$ импульсов сдвига. Частота выборки псевдослучайных чисел E в N раз меньше, чем тактовая частота. Для достижения максимального быстродействия ГПСЧ обычно используют параллельный принцип формирования разрядов псевдослучайного двоичного числа, что приводит к усложнению генератора [1]. Другой генератор псевдослучайных чисел содержит регистр сдвига и блок сумматоров по модулю, что также обуславливает большие аппаратурные затраты [2]. Наиболее близким к изобретению техническим решением является генератор псевдослучайных чисел, содержащий m триггеров, входы которых подключены к тактовому входу генератора, а выходы являются выходами генератора, и $(m-i)$ сумматоров по модулю два. В этом генераторе на один разряд формируемого числа приходится 0,5 сумматора по модулю два, что больше минимально возможной величины [3]. Целью изобретения является упрощение схемы. В описываемом генераторе это достигается тем, что в нем единичные выходы $(i-j)$-х триггеров соединены со счетными входами $(m-j)$-х триггеров, а единичные выходы $(2i-j)$-х и $(m+i-j)$-х триггеров подключены к первому и второму входам сумматоров по модулю два соответственно, выходы которых подключены к счетным входам $(m-j)$-х триггеров.

2

На чертеже приведена блок-схема описываемого генератора для случая m-5.

Он содержит m триггеров 1, выходы которых соединены со счетными входами триггеров других разрядов и входами j сумматоров 2 по модулю два соответственно, выходы которых соединены со счетными входами первых $(m-j)$ триггеров.

Количество сумматоров по модулю два и связи в генераторе определяется ключевым числом i по табл. 1.

Количество сумматоров $j=m-i$ для различных m приведены в табл. 2.

Таблица 1

m	i или $(m-i)$	m	i или $(m-i)$	m	i или $(m-i)$
4	1	11	2	22	1
5	2	15	1,4 или 7	23	5 или 9
6	1	17	3	25	3 или 7
7	1 или 3	18	7	28	3,9 или 13
9	4	20	3	31	3,6,7 или 13
10	3	21	2	33	13

Таблица 2

m	4	6	10	18	20	22
j	1	1	3	7	3	1

В исходном состоянии хотя бы один триггер должен находиться в ненулевом состоянии. Это требование справедливо для всех ГПСЧ на базе регистра сдвига. При поступлении синхросигнала СИ1 код, соответствующий состоянию $(i-j)$-х триггеров, поступает на счетные входы соответствующих $(m-j)$ триггеров (где i — ключевое число; m — номер старшего из используемых триггеров, который определяется разрядностью выходного псевдослучайного числа ($j=0, 1, 2, \ldots i-1$).

Таким образом, информация, хранящаяся на $(i-j)$-х триггерах, суммируется по модулю два на $(m-j)$-х триггерах с информацией, сформированной в предыдущем такте и хранящейся на $(m-j)$-х триггерах. На сумматорах по модулю два формируются суммы содержимого $(m+i-j)$-х разрядов с содержимым $(2i-j)$-х разрядов ($j=i, i+1, i+2, \ldots m-1$). При поступлении СИ1 эти суммы суммируются по модулю два с содержимым $(m-j)$-х разрядов и окончательная сумма остается на $(m-j)$-х разрядах ($j=i, i+1, i+2, \ldots m-1$).

Для получения суммы по модулю два в описываемом генераторе использовано свойство суммирования по модулю два хранимой информации с поступающей на счетный вход триггера со счетным входом. В результате приведенных операций за один такт формируется m-разрядное равномерно распределенное псевдослучайное число.

Формула изобретения

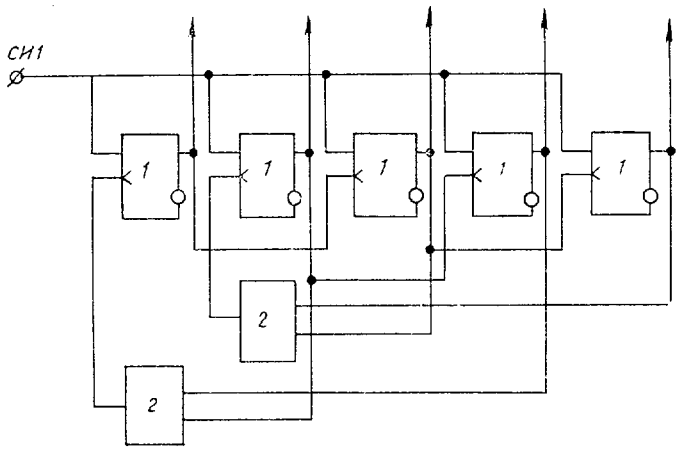
Генератор псевдослучайных чисел, содержащий m триггеров, входы которых подключены к тактовому входу генератора, а выходы являются выходами генератора, и $(m-i)$ сумматоров по модулю два, отличающийся тем, что, с целью упрощения генератора, единичные выходы $(i-j)$-х триггеров соединены со счетными входами $(m-j)$-х триггеров, а единичные выходы $(2i-j)$-х и $(m+i-j)$-х триггеров подключены к первому и второму входам сумматоров по модулю два соответственно, выходы которых подключены к счетным входам $(m-j)$-х триггеров.

Источники информации,
принятые во внимание при экспертизе

1. Яковлев В. В. и Федоров Р. Ф., Стахостические вычислительные машины, Л., Машиностроение, 1974, с. 246.

2. Кирьянов Б. Ф. Многоканальный генератор псевдослучайных символов. Известия АН СССР, «Техническая кибернетика», 1970, № 4, с. 107.

3. «Датчик псевдослучайных чисел». ЭИ приборы и элементы автоматики и вычислительной техники, 1973, № 7.



Заказ 2146/1 Изд. № 776 Тираж 738 Подписное
Типография, пр. Сапунова, 2