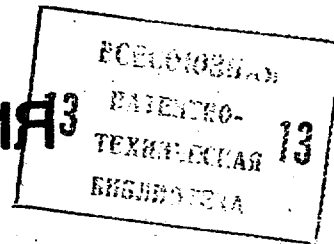




ГОСУДАРСТВЕННЫЙ КОМИТЕТ СССР
ПО ДЕЛАМ ИЗОБРЕТЕНИЙ И ОТКРЫТИЙ

ОПИСАНИЕ ИЗОБРЕТЕНИЯ И АВТОРСКОМУ СВИДЕТЕЛЬСТВУ



- (21) 3414278/18-24.
- (22) 29.03.82
- (46) 07.06.83. Бюл. № 21
- (72) В. Н. Ярмолик и И. П. Кобяк.
- (71) Минский радиотехнический институт
- (53) 681.325 (088.8)
- (56) 1. Яковлев В. В., Федоров Р. Ф. Вероятностные вычислительные машины. Л., "Машиностроение", 1974, с. 228.
2. Кирьянов Б. Ф. Многоканальный генератор псевдослучайных символов. - "Известия АН СССР. Техническая кибернетика", 1970, № 4, с. 107.
3. Авторское свидетельство СССР № 572823, кл. G06F 7/58, 1975 (прототип).

(54) (57) ГЕНЕРАТОР ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ, содержащий генератор тактовых импульсов, регистр сдвига, в цепь обратной связи которого включен сумматор по модулю два, отличающийся тем, что, с целью упрощения генератора, содержит элемент И-НЕ, первый вход которого соединен с его выходом и с тактовым входом регистра сдвига, а второй вход элемента И-НЕ подключен к выходу генератора тактовых импульсов.

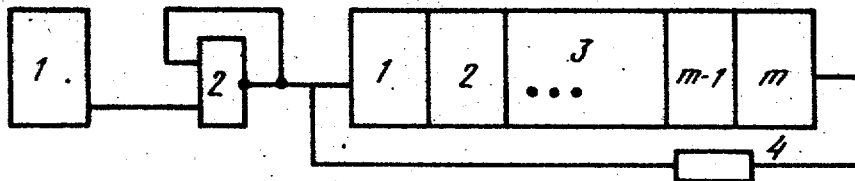


Fig. 1

Изобретение относится к вычислительной технике и может быть использовано для построения задающих блоков вероятностных вычислительных машин при решении задач статистическими методами, а также для построения генераторов случайных процессов с заданными характеристиками, которые широко применяются при испытании эффективности различных алгоритмов для вычислительных машин, для измерения дальности в радиолокации, для кодирования речи, обнаружения ошибок, идентификации систем, в испытательной и контрольной аппаратуре при выпуске изделий вычислительной техники.

Известны генераторы псевдослучайных чисел, основанные на применении регистров сдвига. Простейшим генератором на базе регистра сдвига является последовательный генератор псевдослучайных чисел [1].

Для получения многозарядного двоичного числа работу данного устройства следует моделировать N/m число тактов, где m - разрядность регистра сдвига. Частота выборки псевдослучайных чисел в N раз меньше тактовой частоты.

Для достижения максимального быстродействия генераторов псевдослучайных чисел обычно используют параллельный принцип формирования разрядов псевдослучайного двоичного числа, что приводит к усложнению генератора.

Известен также генератор псевдослучайных чисел, содержащий регистр сдвига и блок сумматоров по модулю два, что также обуславливает большие аппаратные затраты [2].

Наиболее близким к предлагаемому является генератор псевдослучайных чисел, содержащий m триггеров, входы которых подключены к тактовому входу генератора, а выходы являются выходами генератора, и $(m-1)$ сумматоров по модулю два, где i - номер ячейки регистра сдвига, образующий обратную связь [3].

Однако данное устройство содержит избыточное количество сумматоров по модулю два, а методика построения ГПСЧ применима лишь для частного случая, когда цепь обратной связи генератора состоит только из одного полусумматора.

Цель изобретения - упрощение генератора за счет уменьшения объема используемого оборудования, повышения надежности устройства, повышения качества выходной последовательности и расшире-

ния функциональных возможностей устройства, за счет увеличения разрядности псевдослучайных кодов, увеличения периода последовательностей.

Поставленная цель достигается тем, что в генератор псевдослучайных чисел, содержащий генератор тактовых импульсов, регистр сдвига, в цепь обратной связи которого включен сумматор по модулю два, введен элемент И-НЕ, первый вход которого соединен с его выходом и с тактовым входом регистра сдвига, а второй вход элемента И-НЕ подключен к выходу генератора тактовых импульсов.

На фиг. 1 показана схема генератора; на фиг. 2 - диаграмма работы генератора.

Генератор содержит генератор 1 тактовых импульсов, элемент 2 И-НЕ и регистр 3 сдвига с сумматором 4 по модулю два в цепи обратной связи. Повышение качества выходной псевдослучайной последовательности происходит за счет флуктуации времен задержки фронтов тактовых импульсов генератора 1. Для многих параметров дискретных и логических элементов может быть принята гипотеза о нормальном законе распределения. Флуктуация параметров обусловлена действием внутренних шумов логических элементов. Так, в частности, время задержки на логическом элементе есть случайная величина, распределения, распределенная по нормальному закону распределения. Причина флуктуации времен задержки на логическом элементе заключается в дискретном характере зарядов, создающих электрический ток (дробовой эффект) в тепловом движении этих носителей зарядов (тепловой шум), в изменениях проводимости под воздействием некоторых случайных факторов (модуляционный шум и т. д.)

Устройство работает следующим образом.

Тактовый импульс от генератора 1 поступает на второй вход элемента И-НЕ 2 и является разрешающим импульсом для генерации пакета синхросигналов элементом 2. Очевидно, что количество синхросигналов в пакете будет случайным образом меняться от одного тактового импульса к другому за счет флуктуации длительности тактовых импульсов. Генерация пакета синхросигналов осуществляется элементом И-НЕ

в связи с логическим противоречием между первым входом элемента и его выходом в момент подачи тактового импульса на второй вход. Сформированный пакет синхросигналов поступает на синхровходы триггеров регистра сдвига, причем на средних и низких частотах количество синхросигналов в пакете значительно больше разрядности регистра 3 сдвига. Поэтому за один такт информация обновляется полностью. Кроме того, новое число соответствует числу, случайным образом взятому с кольца M-последовательности. Это позволяет практически неограниченно удлинить период формируемых чисел.

В элементе 2 можно использовать, кроме указанного элемента И-НЕ, двухвходовой сумматор по модулю два и другие элементы с соответствующей обратной связью.

Предлагаемый генератор псевдослучайных чисел реализуется с минимальными аппаратными затратами, причем реализация возможна для общего случая организации обратной связи регистра сдвига, что существенно расширяет возможности устройств данного типа. Минимизация оборудования ведет к повыше-

нию надежных характеристик. Важным достоинством технического решения является то, что выборка чисел проводится не жестко через определенное число тактов, а достаточно случайно, что позволяет неограниченно увеличить период следования чисел.

По сравнению с прототипом в предлагаемом ПСЧ аппаратные затраты не зависят от вида обратной связи регистра сдвига и составляют для любой структуры 1/4 микросхемы K155ЛА3. Прототипу же свойственна указанная зависимость, и при построении, например, 13-разрядного ПСЧ на 33-разрядном регистре сдвига избыточность аппаратуры будет составлять 13 элементов сложения по модулю два.

В сравнении с известным предлагаемый генератор псевдослучайных чисел обладает повышенным быстродействием и случайностью выборки псевдослучайных чисел.

Подобные устройства целесообразно использовать для построения генераторов случайных процессов с заданными характеристиками, а также в аппаратуре контроля и диагностики цифровых устройств при выпуске изделий для ЭВМ.

