СОЮЗ СОВЕТСКИХ СОЦИАЛИСТИЧЕСКИХ РЕСПУБЛИК

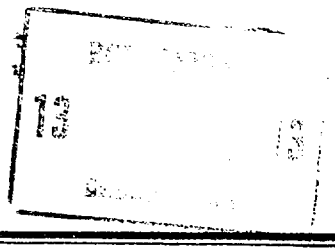
(19) SU (11) 1087993 A

3(51) G 06 F 7/58

ГОСУДАРСТВЕННЫЙ КОМИТЕТ СССР ПО ДЕЛАМ ИЗОБРЕТЕНИЙ И ОТКРЫТИЙ

ОПИСАНИЕ ИЗОБРЕТЕНИЯ

К АВТОРСКОМУ СВИДЕТЕЛЬСТВУ



(21) 3553801/18-24
(22) 15.02.83
(46) 23.04.84. Бюл. № 15
(72) А. И. Кузьмич, А. Г.Якубенко, В. А. Черников и А. С. Кобайло
(71) Минский радиотехнический институт
(53) 681.325(088.8)
(56) 1. Авторское свидетельство СССР № 590754, кл. G 06 F 15/36, 1976.
2. Авторское свидетельство СССР № 796856, кл. G 06 F 15/36, 1979.
3. Авторское свидетельство СССР № 822198, кл. G 06 F 15/36, 1979 (прототип).

(54)(57) УСТРОЙСТВО ДЛЯ КОНТРОЛЯ ГЕНЕРАТОРА СЛУЧАЙНЫХ ЧИСЕЛ, содержащее элемент И, блок управления, о т л и ч а ю щ е е с я тем, что, с целью повышения быстродействия и упрощения устройства, оно содержит дешифратор, группу триггеров, два счетчика, генератор тактовых импульсов, триггер и блок формирования интервала времени, а блок управления содержит элемент ЗАПРЕТ и элемент И, выход которого соединен с входом "Пуск" блока формирования интервала времени, с нулевыми входами триггеров группы и с нулевым входом триггера, единичный выход которого является выходом "Неисправность" устройства, выход генератора тактовых импульсов соединен со счетным входом первого счетчика, с первыми входами элемента ЗАПРЕТ и элемента И и с входом контролируемого генератора случайных чисел, выходы разрядов которого соединены с входами соответствующих разрядов дешифратора, выходы которого соединены с единичными входами соответствующих триггеров группы, выходы которых соединены с входами элемента И соответственно, выход которого соединен со счетным входом второго счетчика, с входом "Сброс" блока формирования интервала времени, с вторыми входами элемента И и элемента ЗАПРЕТ, выход которого соединен с синхронизирующим входом дешифратора, выход блока формирования интервала времени соединен с единичным входом триггера, выход переноса первого счетчика соединен с входом "Сброс" второго счетчика, информационные выходы первого и второго счетчиков являются соответственно первым и вторым информационными выходами устройства.

(19) SU (11) 1087993 A

Изобретение относится к вычислительной технике, предназначенной для оценки качества потока равномерно распределенных случайных чисел и может быть использовано для повышения достоверности работы аппаратуры, использующей последовательности случайных чисел, формируемых аппаратным способом.

Известно устройство для анализа вероятностных характеристик датчика случайных чисел, содержащее индикатор, первый вход которого подключен к выходу блока сравнения, а второй вход – к выходу блока управления, первая группа входов блока сравнения соединена с выходами коммутатора соответственно, первая группа входов которого является входами устройства, первый и второй регистры памяти, входы которых соединены с выходом блока управления, а выходы – с вторыми группами входов коммутатора и блока сравнения соответственно [1].

Недостатком данного устройства является недостаточно высокое быстродействие анализа характеристик генератора случайных чисел, не позволяющее делать оперативную оценку работоспособности, вызванное необходимостью накопления большого объема выборки для получения состоятельной оценки. Снижению быстродействия способствует также применению коммутатора, что предусматривает последовательный алгоритм анализа.

Известно также устройство для статистического анализа датчика случайных чисел, содержащее генератор тактовых импульсов, датчик случайных чисел, разрядный регистр сдвига, элемент И, блок трехпозиционных переключателей, счетчик числа испытаний, переключатель и триггер [2].

Недостатком этого устройства также является низкое быстродействие.

Кроме того, аппаратурные затраты на реализацию устройства значительно превышают затраты на реализацию самого датчика случайных чисел, причем устройство может оценивать качество только одного двоичного разряда потока.

Наиболее близким по технической сущности к данному изобретению является устройство для анализа вероятностных характеристик датчика случайных чисел, содержащее блок управления, датчик случайных чисел, первый регистр памяти, коммутатор, блок сравнения, второй регистр памяти, индикатор, схему сравнения и блок элементов И. Схема сравнения представляет собой одноразрядную схему сравнения, первый вход которой соединен со старшим разрядом датчика случайных чисел, второй вход – с выходом блока управления, выход блока соединен с первым регистром памяти. Первые входы каждого элемента И соединены с выходами коммутатора, вторые входы – с блоком управления, а выходы – со вторым регистром памяти. Выход индикатора является выходом устройства.

Работу устройства можно представить как процесс формирования событий, получаемых на выходе блока сравнения, состоящий в соединении входных случайных чисел в порядке их следования с датчика случайных чисел в двуплечные сцепленные группы, реализуемый на два такта работы устройства [3].

Однако известное устройство имеет ряд недостатков при использовании его для контроля работоспособности генератора случайных чисел. Например, большое время задержки обнаружения отказа, обусловленное временем накопления выборки в индикаторе для получения состоятельной оценки.

Недостатком является и то, что проверка осуществляется только для одного разряда.

Целью изобретения является повышение быстродействия устройства и его упрощение.

Для достижения поставленной цели в устройство для контроля генератора случайных чисел, содержащее элемент И и блок управления, введены дешифратор, группа триггеров, два счетчика, генератор тактовых импульсов, триггер и блок формирования интервала времени, а блок управления содержит элемент ЗАПРЕТ и элемент И, выход которого соединен с входом "Пуск" блока формирования интервала времени, с нулевыми входами триггеров группы и с нулевым входом триггера, единичный выход которого является выходом "Неисправность" устройства, выход генератора тактовых импульсов соединен со счетным входом первого счетчика, с первыми входами элементов ЗАПРЕТ и элемента И и с

входом контролируемого генератора случайных чисел, выходы разрядов которого соединены с входами соответствующих разрядов дешифратора, выходы которого соединены с единичными входами соответствующих триггеров группы, выходы которых соединены с входами элемента И соответственно, выход которого соединен со счетным входом второго счетчика, с входом "Сброс" блока формирования итервала времени и с вторыми входами элемента И и элемента ЗАПРЕТ выход которого соединен с синхронизирующим входом дешифратора, выход блока формирования интервала времени соединен с единичным входом триггера, выход переноса первого счетчика соединен с входом "Сброс" второго счетчика, информационные выходы первого и второго счетчиков являются соответственно первым и вторым информационными выходами устройства.

На фиг. 1 представлена структурная схема устройства; на фиг. 2 – схема блока управления.

Устройство содержит генератор 1 тактовых импульсов, генератор 2 случайных чисел, дешифратор 3, группу триггеров 4, элемент И 5, блок 6 управления, счетчик 7, блок 8 формирования интервала времени, триггер 9, счетчик 10. Блок управления содержит элемент И 11 и элемент ЗАПРЕТ 12.

В предлагаемом устройстве используется метод оценки качества некоторой равномерно распределенной случайной числовой последовательности, основанный на формировании "полного набора" событий и оценки отклонения от времени, в течение которого это событие должно произойти с заданной вероятностью.

Устройство работает следующим образом.

Началу работы устройства предшествует установка его в исходное состояние, т.е. сброс блока триггеров 4 и триггера 9 в "0" и запуск формирователя 8 временного интервала, что осуществляется импульсом с второго выхода блока 6 управления, а сброс счетчиков 7 и 10 происходит циклически в процессе работы. Количество триггеров блока триггеров 4 равно количеству выходов дешифратора 3 и равно множеству состояний выхода генератора 2 случайных чисел. Процесс формирования "полного набора" событий состоит в запоминании факта появления случайных чисел, представленных дешифратором в унитарном коде в порядке их следования с выхода генератора 2 случайных чисел на блоке триггеров 4. Происходит это следующим образом. Первый тактовый импульс поступает на первый вход блока управления, на вход счетчика 7 и на вход генератора 2 случайных чисел. Генератор 2 случайных чисел вырабатывает по этому импульсу некоторое случайное число U_i, которое поступает на информационные выходы дешифратора 3. При наличии на его втором входе нулевого уровня, поступающего с первого выхода блока 6 управления, происходит дешифрация данного случайного числа и на одном из выходов дешифратора в течение длительности тактового сигнала сохраняется низкий логический уровень, который поступает на S-вход соответствующего ему триггера из блока триггеров 4 и устанавливает его в "1". Остальные триггеры из блока триггеров 4 свое состояние не изменяют. Выходы всех триггеров заведены на входе элементов И 5. Данная схема сохраняет нулевой уровень на выходе при условии, что хотя бы один триггер из блока триггеров 4 находится в нулевом состоянии. Счетчик 7 суммирует количество тактовых импульсов, поступающих на его вход с генератора 1 тактовых импульсов, т.е. число сгенерированных случайных чисел. Появление "полного набора" событий соответствует установке всех триггеров 4 в состояние логической единицы, при этом на выходе элемента И 5 тоже появляется уровень логической единицы, а момент перехода из нуля в единицу фиксируется счетчиком 10, далее сигнал с выхода схемы И поступает на второй вход блока 6 управления, а также на второй вход формирователя 8 временного интервала, сбрасывая его в исходное состояние. После чего на время существования высокого логического уровня на выходе элемента И 5 запрещена работа дешифратора 3, а на второй выход блока 6 управления разрешается прохождение тактового импульса от генератора 1 тактовых импульсов, который устанавливает в исходное состояние блок триггеров 4 и триггер 9, а формирователь 8 временного интервала

запускает на новый цикл формирования временного интервала.

Требуемая длина временного интервала определяется как

$$T = r \cdot t,$$

где t – период следования тактовых импульсов с генератора тактовых импульсов;

r – длина последовательности случайных чисел вида U_i, формируемых генератором 2 случайных чисел, необходимая для накопления "полного набора" событий с вероятностью P.

Если "полный набор" событий появится за время меньшее T, то формирователь 8 временного интервала устанавливается в исходное состояние по первому входу и ожидает сигнал запуска на новый цикл формирования временного интервала. Если за время T "полный набор" событий не сформирован, то формирователь 8 временного интервала устанавливает триггер 8 в единичное состояние, что означает либо отклонение от нормального режима работы генератора случайных чисел, либо с вероятностью (1-P) ложное срабатывание. Выход триггера 9 должен использоваться для инициирования работы схемы более полного контроля, например, в случае работы генератора случайных чисел в составе ЭВМ к выходу инициации аппаратного прерывания для остановки текущей программы, а более точная проверка осуществляется дополнительными средствами при работе в составе ЭВМ программным тестом.

Достоинство предлагаемого устройства состоит в том, что при возникновении существенных отклонений в работе генератора случайных чисел (отказе) в процессе решения задачи исключается возможность потребления большим массивом чисел от неисправного генератора и распространение ошибки на уже полученные результаты. Это особенно важно при контроле генераторов случайных чисел, работающих в составе систем испытаний в масштабе реального времени, где задержка с обнаружением отказа грозит выходом в нерасчетный режим и необратимыми изменениями в объекте испытаний.

Для более полной оценки качества работы генератора случайных чисел имеется дополнительная информация:

n – число "полных наборов" событий на выходе счетчика 10;

L – общая длина последовательности случайных чисел, необходимых для формирования n "полных наборов", на первом выходе счетчика 7.

Полученные эмпирические значения n и L сравниваются с теоретическими значениями этих характеристик

$$L_{min} = n \cdot d;$$

$$L_{ср} = n \cdot d \cdot H_d;$$

$$k = \sqrt{n} \cdot \sqrt{d^2 H_d^{(2)} - d \cdot H_d};$$

где $d = 2^n$ – число возможных событий, которые могут появиться в данной числовой последовательности;

$H_d = \sum_d \frac{1}{d}$ – гармонический ряд;

$H_d^{(2)} = \sum_d \frac{1}{d^2}$;

k – стандартное отклонение длины числовой последовательности чисел вида U_i;

L_{min} – минимальная длина последовательности чисел вида U_i;

$L_{ср}$ – средняя длина последовательности чисел вида U_i.

Если длина числовой последовательности случайных чисел, полученная в результате анализа генератора случайных чисел, при условии, что было получено n "полных наборов", лежит в этих пределах, то вероятность P правильной работы генератора случайных чисел равна $P_{r^*} = \frac{d!}{d^{r^*}} \left\{ {r^* \atop d} \right\}$ где $r^* = L_{ср} + k_1$

$\left\{ {r^* \atop d} \right\}$ – число Стирлинга 2-го рода.

Таким образом, предлагаемое устройство позволяет упростить процедуру контроля качества работы генератора равномерно распределенных случайных чисел по сравнению с известными решениями. При этом повышается скорость (сокращается время) обнаружения отказа и одновременно уменьшаются аппаратурные затраты.

Повышение быстродействия предлагаемого устройства достигается за счет применения нового принципа контроля, обеспечивающего получение оценки ка-

чества работы генератора случайных чисел за время существенно меньшее, чем это делается в известных устройствах за время меньшее необходимого для состоятельного анализа.

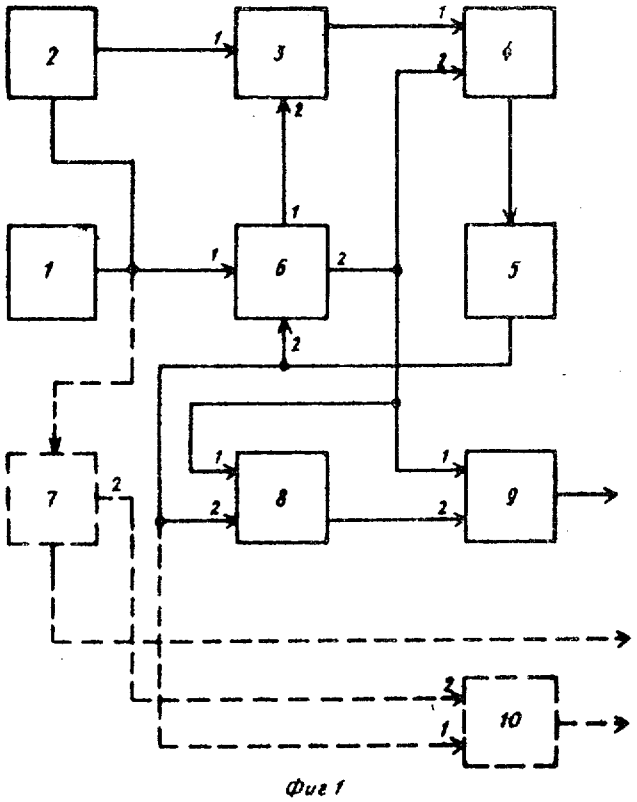
Для достижения поставленной цели в устройство контроля введены дешифратор, блок триггеров, формирователь временного интервала, триггер контроля. Оценка качества работы генератора происходит путем контроля за накоплением "полного набора" состояний за время T, определяемое вероятностью P появления последовательности U_i, содержащей "полный набор" событий. При непоявлении такого события за интервал времени И, отрабатываемый формирователем временных интервалов срабатывает триггер контроля, что вызывает необходимость проведения более тщательной проверки характеристик генератора, т.е. накопления выборки большего объема.

Для накопления состоятельной статистики "полных наборов" служит первый и второй счетчики. Производительность (быстродействие) предлагаемого устройства как средства контроля повышена и за счет того, что анализ потоков случайных чисел не поразрядный, а параллельный - все разряды числа U_i.

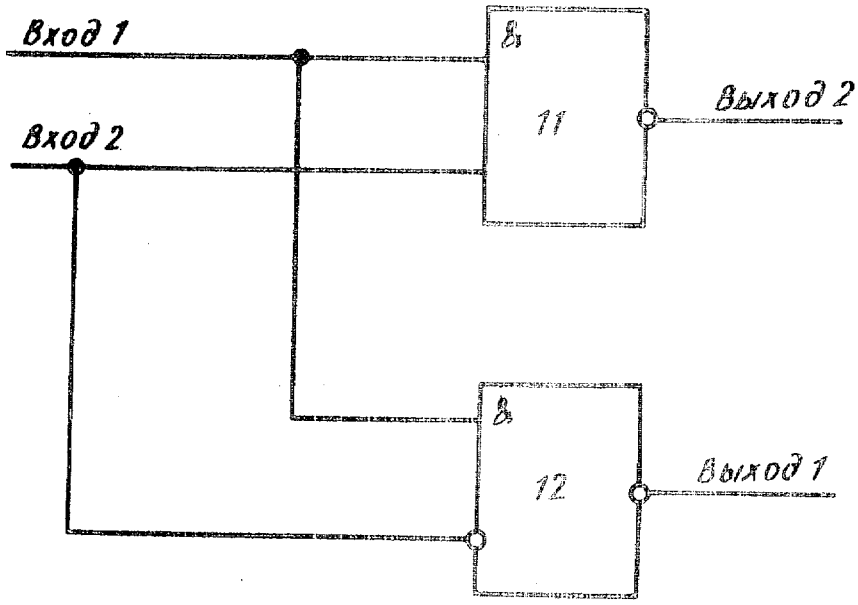
Упрощение аппаратурной реализации достигнуто за счет контроля при эквивалентном количестве оборудования не одного двоичного, а всех разрядов числа U_i. В противном случае для контроля n разрядов числа U_i пришлось бы использовать n устройств контроля, что потребовало бы пропорционального увеличения аппаратурных затрат.

Технико-экономическая эффективность предлагаемого устройства обусловлена сокращением затрат машинного времени и на тестовые проверки генератора.

Если в качестве базового образца использовать программный тест контроля, то экономический эффект будет определяться экономией машинного времени. Однако тестовый контроль - периодический. Эффект от организации непрерывного контроля работы генератора случайных чисел зависит от важности и характера решаемой задачи, поэтому оценить его трудно.



Фиг 1



Фиг. 2

Составитель А. Карасов
Редактор В. Иванова Техред Л.Коцюбняк Корректор Ю. Макаренко

Заказ 2674/46 Тираж 699 Подписное
ВНИИПИ 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