Союз Советских Социалистических Республик

Государственный комитет СССР по делам изобретений и открытий

ОПИСАНИЕ ИЗОБРЕТЕНИЯ

К АВТОРСКОМУ СВИДЕТЕЛЬСТВУ

(11) 947856

(61) Дополнительное к авт. свид-ву —

(22) Заявлено 22.09.80 (21) 2985884/18-24

с присоединением заявки № —

(23) Приоритет —

Опубликовано 30.07.82. Бюллетень № 28

Дата опубликования описания 30.07.82

(51) М. Кл.³ G 06 F 7/58

(53) УДК 681.325 (088.8)

(72) Автор изобретения В.Н.Ярмолик

(71) Заявитель Минский радиотехнический институт

ВСЕСОЮЗНАЯ ПАТЕНТНО-ТЕХНИЧЕСКАЯ БИБЛИОТЕКА

(54) МНОГОКАНАЛЬНЫЙ ПАРАЛЛЕЛЬНЫЙ ГЕНЕРАТОР ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ

1

Изобретение относится к вычислительной технике и может быть использовано в качестве устройства для получения случайных чисел при решении задач методом Монте-Карло, для построения генераторов случайных процессов с заданными характеристиками, а также для идентификации систем автоматического управления. При этом весьма важным оказывается качество первичных равномернораспределенных чисел, их разрядность и количество каналов генератора.

Известен генератор псевдослучайных чисел, содержащий два регистра сдвига и группу сумматоров по модулю два [1].

Недостатком этого генератора является сложность структурного построения, а также усложненная методика синтеза. Кроме того, необходимым требованием для построения генератора псевдослучайных чисел является требование выбора таких структур исходных последовательностей, у которых периоды являются взаимно простыми числами, что не всегда оказывается возможным.

Известен также последовательный генератор псевдослучайных чисел, который с точки зрения простоты реализации не имеет себе равных. Необходимое для построения генератора оборудование состоит из регистра сдвига с сумматором по модулю два, генератора тактовых импульсов, счетчика и выходных вентилей [2].

2

Недостатком данного генератора является меньшая в n раз по сравнению с тактовой частотой регистра сдвига частота выдачи n разрядных псевдослучайных чисел. При больших n это накладывает существенные ограничения на скорость или связанную с ней точность стохастических вычислений.

Наиболее близким к предлагаемому является параллельный генератор псевдослучайных чисел, состоящий из m-разрядного регистра сдвига с двухвходовым сумматором по модулю два, m групп двухвходовых элементов И и mm-входовых сумматоров по модулю два. В основе построения данного генератора лежит идея использования в качестве независимых последовательностей, формируемых в разрядах генератора, различных участков одной и той же псевдослучайной последовательности максимальной длины. Достоинством этого метода является возможность

генерирования различных участков исходной последовательности с помощью несложных схем - дополнительного набора сумматоров по модулю два. На выходах этих сумматоров генерируются идентичные, но сдвинутые относительно друг друга, псевдослучайные двоичные последовательности [3].

Недостатком известного генератора псевдослучайных чисел является сложность синтеза и громоздкость подготовительных операций. Это объясняется тем фактом, что определение набора коэффициентов δ_{ie} по заданному сдвигу не имеет простого аналитического решения. Поэтому для определения коэффициентов используют непосредственное моделирование работы генератора на ЭВМ, причем в общем случае эта задача не поддается решению путем моделирования на ЭВМ. Только в частном случае, когда схема цепи обратной связи регистра сдвига состоит только из одного сумматора по модулю два с двумя входами, задача нахождения коэффициентов решается относительно несложно.

Кроме того, невозможно построение параллельного генератора псевдослучайных чисел для общего случая, т.е. для порождающего многочлена произвольной степени с любым набором коэффициентов δ_{ie}, т.е. подобно оказывается возможным построение параллельного генератора только для простейшего случая, когда в цепь обратной связи включен двухвходовой сумматор по модулю два, что существенно сужает функциональные возможности подобных устройств.

Цель изобретения - упрощение генератора.

Поставленная цель достигается тем, что в генератор псевдослучайных чисел, содержащий m триггеров, mm-входовых сумматоров по модулю два и m групп по m в каждой группе двухвходовых элементов И, дополнительно введены n групп по m в каждой группе m-входовых сумматоров по модулю два и n групп по m подгрупп, включающих по m двухвходовых элементов И, причем к входам i-го m-входового сумматора по модулю два подключены выходы двухвходовых элементов И i-ой группы по m двухвходовых элементов И, к первому входу j-ой двухвходовой элемента И i-ой группы по m-двухвходовых элементов И подключен единичный выход j-го триггера, к синхровходам которого подключен выход генератора тактовых импульсов, вторые входы двухвходовых элементов И i-ой группы по m-двухвходовых элементов И образуют первую группу входов генератора, выходы двухвходовых элементов И ℓ-ой группы (ℓ = 1,2...,n) i-ой подгруппы по m двухвходовых элементов И подключены к входам i-го m-входового сумматора по модулю два ℓ-ой группы, а выход k-го (k - входового сумматора по модулю два подключен к первому входу j-ой двухвходового элемента И (k-j)-ой подгруппы ℓ-ой группы и к D-входу k-го триггера, единичный выход (m+1-k)-го триггера подключен к первому входу (m+j-k)-ой двухвходового элемента И (m+1-j)-ой подгруппы ℓ-ой группы, вторые входы j-ых двухвходовых элементов И каждой подгруппы ℓ-ой группы образуют вторую группу входов генератора единичные выходы триггеров и выходы m-входовых сумматоров по модулю два n групп являются выходами генератора.

На фиг.1 приведена функциональная схема генератора при m =4; на фиг.2 - последовательность состояний регистра при m = 4.

Функциональная схема генератора псевдослучайных чисел состоит из m = 4 триггеров 1 регистра сдвига, mm- входовых сумматоров 2 по модулю два m групп по m двухвходовых элементов И 3, n групп по mm-входовых сумматоров 4 по модулю два и n групп по m подгрупп, включающих m двухвходовых элементов И 5, причем к входам i-го m-входового сумматора 2 по модулю два подключены выходы двухвходовых элементов И i-ой группы по m двухвходовых элементов И 3, к первому входу j-ой двухвходового элемента И i-ой группы 3 подключен единичный выход j-го триггера 1, к синхровходам которого подключен выход генератора тактовых импульсов, на вторые входы двухвходовых элементов И i-ой группы 3 поданы значения коэффициентов, принимающих значения 0 или 1, а выходы двухвходовых элементов И ℓ-ой группы i-ой подгруппы по m-двухвходовых элементов И 5 подключены к входам i-го m-входового сумматора 4 по модулю два ℓ-ой группы, выход k-го m-входового сумматора 2 по модулю два подключен к входу j-ой двухвходового элемента 3 И (k-j)-ой подгруппы ℓ-ой группы 5 и к D-входу k-го триггера 1, единичный выход (m+1-k)-го триггера 1 подключен к первому входу (m+j-k)-ой двухвходового элемента И (m+1-j)-ой подгруппы ℓ-ой группы 5, на второй вход j-ой двухвходового элемента И каждой подгруппы ℓ-ой группы 5 поданы значения коэффициентов, принимающих значения 0 или 1, а единичные выходы триггеров 1 и выходы m-входовых сумматоров по модулю два n групп 4 являются выходами устройства.

Значение коэффициентов $\alpha_{1j} \in \{0,1\}$, j = 1,m определяют из известных таблиц.

Функционирование многоканального параллельного генератора псевдослучайных чисел происходит следующим образом.

В исходном состоянии триггеры 1 генератора находятся в произвольном состоянии, кроме нулевого кода 000... 0, другими словами на триггерах регистра хранится с равной вероятностью любой код, кроме нулевого. В зависимости от начального кода на выходах сумматоров по модулю два образуются значения нуля или единицы. На выходах триггеров 1 регистра получается значение первого псевдослучайного числа по первому каналу, а на выходах mm-входовых сумматоров 2 по модулю два значение следующего псевдослучайного числа, получаемого по первому каналу, а на выходах m-входовых сумматоров по модулю два по m в n группах 4 образуются значения первого псевдослучайного числа по остальным n каналам. По приходе синхроимпульса на С-входы триггеров 1 информация с выходов сумматоров 2 по модулю два записывается на триггера 1, после чего на выходах сумматоров 2 и 4 по модулю два образуются новые коды, которые являются очередными значениями псевдослучайных чисел по остальным n 1 каналам (сумматоры 4) и последующим значениям по первому каналу (сумматоры 2). Подобным образом по приходе следующих синхроимпульсов процедура повторяется.

Достоинством генератора является существенное расширение его функциональных возможностей, что объясняется возможностью построения параллельного генератора для общего случая, т.е. для порождающего многочлена произвольной степени с любым набором коэффициентов. В данном случае оказывается возможным построение генератора не только для частного случая, когда в цепь обратной связи включен двухвходовой сумматор по модулю два, но и для случая многовходового сумматора по модулю два в цепи обратной связи. Реализация генератора при неизмененной жесткой структуре требует только m триггеров и n+1 группу по m сумматоров по модулю два со средним количеством входов, равном m триггеров, и выходы m-входовых сумматоров по модулю два n групп являются выходами устройства, так как при равенстве нулю какого-либо коэффициента по соответствующему входу сумматора эта связь отсутствует, а при равенстве единице всегда присутствует.

Применение предлагаемого многоканального псевдослучайного генератора позволяет повысить качество псевдослучайных последовательностей, а тем самым точность решения задач методом Монте-Карло.

Формула изобретения

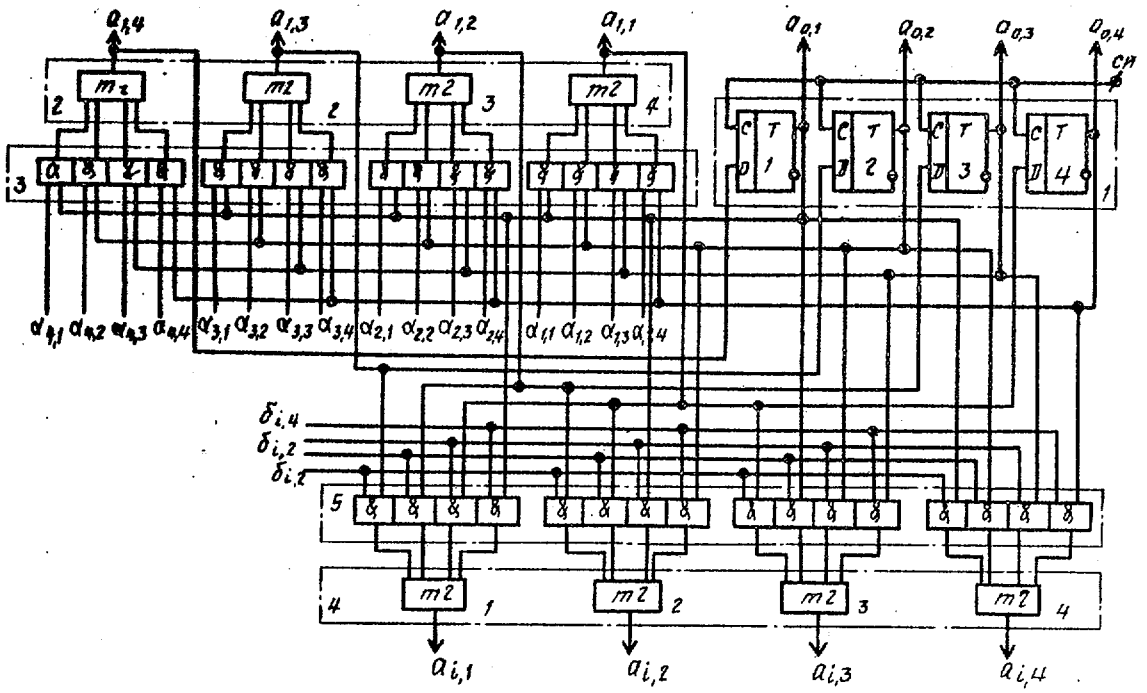
Многоканальный параллельный генератор псевдослучайных чисел, содержащий m триггеров, mm-входовых сумматоров по модулю два и m групп по m в каждой группе двухвходовых элементов И, причем к входам i-го (i = 1, 2,...,m) m-входового сумматора по модулю два подключены выходы двухвходовых элементов И i-й группы, к первому входу j-го (j = 1,2,...,m) элемента И i-й группы подключен единичный выход j-го триггера, к синхровходу которого подключен выход генератора тактовых импульсов, вторые входы элементов И i-й группы образуют первую группу входов генератора, о т л и ч а ю щ и й с я тем, что, с целью упрощения генератора, в него введены n групп по m в каждой группе m-входовых сумматоров по модулю два и n групп по m подгрупп, включающих по m-двухвходовых элементов И, причем выходы двухвходовых элементов И ℓ-ой группы (ℓ = 1,2...,n) i-й подгруппы по m-двухвходовых элементов И подключены к входам i-го m-входового сумматора по модулю два ℓ-й группы, а выход k-го (k = 1,2,...,m) m-входового сумматора по модулю два подключен к первому входу j-го двухвходового элемента И (k-j)-й подгруппы ℓ-й группы к D-входу k-го триггера, кроме того, единичный выход (m+1-k)-го триггера подключен к первому входу (m+j-k)-го двухвходового элемента И (m+1-j)-й подгруппы ℓ-й группы, вторые входы j-х двухвходовых элементов И каждой подгруппы ℓ-й группы образуют вторую группу входов генератора, единичные выходы триггеров и выходы m-входовых сумматоров по модулю два n групп являются выходами генератора.

Источники информации, принятые во внимание при экспертизе

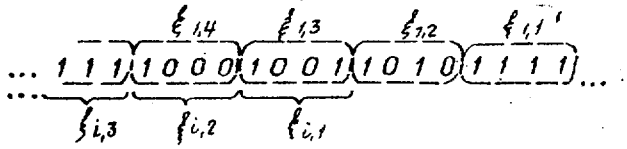
1. Яковлев В.В. и Федоров Р.Ф. Вероятностные вычислительные машины. Л., "Машиностроение", 1974, с.263.

2. Яковлев В.В. и Федоров Р.Ф. Вероятностные вычислительные машины. Л., "Машиностроение", 1974. с.247.

3. Яковлев В.В. и Федоров Р.Ф. Вероятностные вычислительные машины. Л., "Машиностроение", 1974, с.254 (прототип).



Фиг.1



Фиг.2

Составитель А.Карасов
Редактор Н.Ковалева Техред Т. Фанта Корректор О.Билак

Заказ 5652/72 Тираж 731 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