



3(51) G 06 F 7/58

ГОСУДАРСТВЕННЫЙ КОМИТЕТ СССР
ПО ДЕЛАМ ИЗОБРЕТЕНИЙ И ОТКРЫТИЙ

ОПИСАНИЕ ИЗОБРЕТЕНИЯ

К АВТОРСКОМУ СВИДЕТЕЛЬСТВУ

(21) 3350961/18-24

(22) 22.10.81

(46) 23.06.83. Бюл. № 23

(72) В. Н. Ярмолик

(71) Минский радиотехнический институт

(53) 681.325 (088.8)

(56) 1. Яковлев В. В., Федоров Р. Ф.

Вероятностные вычислительные машины.
Л., "Машиностроение", 1974, с. 247.

2. Авторское свидетельство СССР
№ 527012, кл. G 06 F 7/58, 1974.

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

(54)(57) ГЕНЕРАТОР ПСЕВДОСЛУЧАЙНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ, содержащий генератор тактовых импульсов, регистр сдвига, в цепь обратной связи которого включен сумматор по модулю два, группу из m элементов И (m - число разрядов генератора), m -входовой сумматор по модулю два, выход генератора тактовых импульсов подключен к С-входу регистра сдвига, выходы элементов И группы подключены к входам m -входового сумматора по модулю два соответственно, первый вход i -го, ($i = \overline{1, m}$), элемента И группы подключен к выходу i -го разряда регистра сдвига, отличающийся тем, что, с целью увеличения быстродействия генератора, он содержит RS-триггер, генератор одиночных импульсов, группу из m Д-триггеров, группу из $C = \lfloor \frac{m+1}{2} \rfloor$ сумматоров по модулю два, группу из $q = \lfloor \frac{m-1}{2} \rfloor$

элементов 2И-ИЛИ и элемент И, причем к второму входу i -го элемента И группы подключен выход i -го Д-триггера группы, к С-входам Д-триггеров группы подключен выход генератора одиночных импульсов, к первому входу r -го ($r = \overline{1, C}$) сумматора по модулю два группы подключен единичный выход r -го Д-триггера группы, к второму входу первого сумматора по модулю два группы подключен выход элемента И, к второму входу η -го ($\eta = \overline{2, C}$) сумматора по модулю два группы подключен выход ($\eta - 1$)-го элемента 2И-ИЛИ группы, выход r -го сумматора по модулю два группы подключен к входу $(2r-1)$ -го Д-триггера группы, единичный выход RS-триггера подключен к первым входам элементов 2И-ИЛИ группы, к вторым входам которых подключен нулевой выход RS-триггера, единичный выход $(C + \xi)$ -го ($\xi = \overline{1, q}$) Д-триггера группы подключен к Д-входу 2ξ -го Д-триггера группы и к третьему входу ξ -го элемента 2И-ИЛИ группы, а единичный выход $(C+1)$ -го Д-триггера группы подключен к первому входу элемента И, к второму входу которого подключен нулевой выход RS-триггера, единичный выход $(C + \xi + 1)$ -го Д-триггера группы подключен к четвертому входу ξ -го элемента 2И-ИЛИ группы, RS-входы RS-триггера являются первым и вторым входами генератора, а выход m -входового сумматора по модулю два является выходом генератора.

09 SU (11) 1024918 A

Изобретение относится к вычислительной технике и может быть использовано в качестве устройства для определения топологии связей многоходового сумматора по модулю два, на выходе которого формируются сдвинутые копии псевдослучайных последовательностей. Использование сдвинутых копий псевдослучайных последовательностей позволяет строить экономичные генераторы псевдослучайных чисел, а также организовывать автономные устройства для имитации случайных процессов с заданными характеристиками.

Известен генератор псевдослучайных чисел, содержащий регистр сдвига с сумматором по модулю два в цепи обратной связи [1].

Недостатком этого устройства является невозможность получения копий псевдослучайной последовательности сдвинутых более, чем на число тактов, равное разрядности регистра сдвига.

Известно также устройство для формирования сдвинутых копий псевдослучайного сигнала, состоящее из генератора тактовых импульсов, первого элемента "Запрет", регистра сдвига с сумматором по модулю два и элементами И в цепи обратной связи, дешифратора, второго элемента "Запрет", счетчика, блока памяти, сумматоров по модулю два и индикаторов [2].

Недостатком такого устройства является сложность аппаратного построения. Кроме того, наличие блоков памяти снижает быстродействие генератора.

Наиболее близким техническим решением к предлагаемому изобретению является генератор псевдослучайной последовательности, содержащий регистр сдвига с сумматором по модулю два в цепи обратной связи, элементы И и сумматор по модулю два [3].

Недостатком известного генератора является низкое быстродействие.

Целью изобретения является повышение быстродействия генератора.

Для достижения поставленной цели в генератор псевдослучайной последовательности, содержащий генератор тактовых импульсов, регистр сдвига с сумматором по модулю два в цепи обратной связи, группу из m элементов И (m - число разрядов генератора), m -входовой сумматор по модулю два, выход генератора тактовых импульсов подключен к С-входу регистра сдвига, выходы элементов И группы подключены к входам m -входового

сумматора по модулю два соответственно, первый вход i -го ($i = 1, m$) элемента И группы подключен к выходу i -го разряда регистра сдвига, введены RS-триггер, генератор одиночных импульсов, группу из m Δ -триггеров, группу из $C = \lfloor \frac{m+1}{2} \rfloor$ сумматоров по модулю два, группу из $Q = \lfloor \frac{m-1}{2} \rfloor$ элементов 2И-ИЛИ и элемент И, при этом к второму входу i -го элемента И группы подключен выход i -го Δ -триггера группы, к С-входам Δ -триггеров группы подключен выход генератора одиночных импульсов, к первому входу r -го ($r = 1, C$) сумматора по модулю два группы подключен единственный выход r -го Δ -триггера группы, к второму входу первого сумматора по модулю два группы подключен выход элемента И, к второму входу η -го ($\eta = 2, C$) сумматора по модулю два группы подключен выход $(\eta - 1)$ -го элемента 2И-ИЛИ группы, выход r -го сумматора по модулю два группы подключен к входу $(2r - 1)$ -го Δ -триггера группы, единственный выход RS-триггера подключен к первым входам элементов 2И-ИЛИ группы, к вторым входам которых подключен нулевой выход RS-триггера, единственный выход $(C + \xi)$ -го ($\xi = 1, Q$) Δ -триггера группы подключен к Δ -входу 2ξ -го Δ -триггера группы и к третьему входу ξ -го элемента 2И-ИЛИ группы, а единственный выход $(C + 1)$ -го Δ -триггера группы подключен к первому входу элемента И, к второму входу которого подключен нулевой выход RS-триггера, единственный выход $(C + \xi + 1)$ -го Δ -триггера группы подключен к четвертому входу ξ -го элемента 2И-ИЛИ группы, RS-входы RS-триггера являются первым и вторым входами генератора, а выход m -входового сумматора по модулю два является выходом генератора.

На чертеже приведена функциональная схема генератора псевдослучайной последовательности.

Схема состоит из генератора 1 тактовых импульсов, регистра 2 сдвига (с сумматором по модулю два в цепи обратной связи), m элементов И 3, m -входового сумматора 4 по модулю два, RS-триггера 5, генератора 6 одиночных импульсов, m Δ -триггеров 7, $C = \lfloor \frac{m+1}{2} \rfloor$ сумматоров 8 по модулю два, $Q = \lfloor \frac{m-1}{2} \rfloor$ элементов 2И-ИЛИ 9 и элемента И 10.

Функционирование устройства для получения сдвинутых копий псевдослучайной последовательности происходит следующим образом.

В первоначальный момент на Δ -триггера 7 записываются начальный код 100...001, т.е. только на первый и последний триггер записываются единичные значения. Таким образом содержимое m Δ -триггеров равняется $\alpha_i = \sigma_i(1)$, $i = 1, m$. На RS-триггер записывается единица, если m нечетно, и ноль, если четно. На RS-триггер 5 записывается ноль. С нулевого выхода RS-триггера на элемент И 10 и на третьи входы элементов 2И-ИЛИ подается разрешающий потенциал. В этом случае на выходе комбинационной части устройства, состоящей из элементов 8-10, т.е. на выходе сумматоров 8 по модулю два, формируются значения двоичных цифр согласно системы логических уравнений, определяемой структурой генератора.

Далее с выхода генератора 6 одиночных импульсов подается синхримпульс на С-входы всех Δ -триггеров 7. По приходу импульса с генератора 6 Δ -триггера изменяют свои состояния, таким образом на Δ -триггерах 7 записывается код 100011, т.е. $\sigma_1(2)=1$; $\sigma_2(2)=0$; $\sigma_3(2)=0$; $\sigma_4(2)=0$; $\sigma_5(2)=1$; $\sigma_6(2)=1$. Значения $\sigma_i(2)$, $i=1,6$ с единичных выходов Δ -триггеров подается на вход комбинационной части устройства, состоящей из блоков 8-10. По приходу очередного синхримпульса с выхода генератора 6 на С-входы Δ -триггеров 7 на триггера 7 запишется код 101111, который определяет значения $\sigma_i(4)$, $i=1,6$. Таким образом $\sigma_1(4)=1$; $\sigma_2(4)=0$; $\sigma_3(4)=1$; $\sigma_4(4)=1$; $\sigma_5(4)=1$; $\sigma_6(4)=1$. При поступлении следующего синхримпульса

...1 1 1 1 1 1 0 1 0 1 0 1 1 0 0 1 1 0 1 1 1 0...
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21

а на выходе сумматора 4 последовательность

...1 0 1 1 1 0 1 1 0 1 0 0 1 0 0...
16 17 18 19 20 21 22 23 24 25 26 27 28 29 30.

Преимущество предлагаемого устройства для получения сдвинутых копий псевдослучайной последовательности заключается в том, что в нем существенно увеличено быстродействие. Так для определения коэффициентов $\sigma_i(2)^K$, $i=1, m$, $K=0, 1, 2, \dots$ в предлагаемом устройстве необходимо выполнить только K тактов, в то время как в известном — 2^K тактов. Таким образом, быстродействие предлагаемого устройства увеличивается в $2^K/m$ раз. Так для $K=10$ быстродей-

с выхода генератора 6 получим, что $\sigma_1(8)=0$; $\sigma_2(8)=1$; $\sigma_3(8)=1$; $\sigma_4(8)=1$; $\sigma_5(8)=0$; $\sigma_6(8)=1$. Таким же образом получим, что $\sigma_1(16)=1$; $\sigma_2(16)=1$; $\sigma_3(16)=1$; $\sigma_4(16)=0$; $\sigma_5(16)=0$; $\sigma_6(16)=1$.

Анализ, состоящий из Δ -триггеров 7, показывает, что на них последовательно получают значения коэффициентов $\sigma_i(2^k)$; $i=1, m$; $K=0, 1, 2, \dots$. В случае, если необходимо получить копию псевдослучайной последовательности, сдвинутую на $\ell=8$ тактов, первоначально необходимо на Δ -триггера 7 записать значения $\alpha_i=1$; $\alpha_i=0$, $i=2, m-1$; $\alpha_m=1$. Далее с выхода генератора одиночных импульсов последовательно подаются три импульса, так как $8=2^3$. После прохождения переходных процессов на Δ -триггерах 7 хранятся коэффициенты $\sigma_i(8)$, $i=1, m$. С выходов Δ -триггеров 7 значения коэффициентов $\sigma_i(8)$ подаются на входы элементов И 3, на вторые входы которых подключены выходы разрядов регистра 2 сдвига (с сумматором по модулю два в цепи обратной связи). Предварительно по RS-входам триггеров регистра 2 записывается начальный код. Предположим, что на триггерах регистра 2 записан код 100000. При поступлении тактовых импульсов с выхода генератора 1 на входы триггеров регистра 2, на выходе m -входового сумматора 4 по модулю два формируется сдвинутая на восемь тактов копия псевдослучайной последовательности. На выходе первого разряда регистра 2 формируется последовательность

стие увеличится более, чем в 100 раз. Увеличение быстродействия устройства позволяет расширить его функциональные возможности. Так же является возможным определение коэффициентов, позволяющих получить копии псевдослучайной последовательности, сдвинутые на астрономическое количество тактов для $\ell = 2^K \gamma 2^{40}$. А это в свою очередь позволит строить высоконадежные, стабильные и высококачественные генераторы псевдослучайных чисел.

