



Государственный комитет  
СССР  
по делам изобретений  
и открытий

# О П И С А Н И Е ИЗОБРЕТЕНИЯ

## К АВТОРСКОМУ СВИДЕТЕЛЬСТВУ

(11) 953638

(61) Дополнительное к авт. свид-ву -

(22) Заявлено 13.03.81 (21) 3259180/18-24

с присоединением заявки № -

(23) Приоритет -

, Опубликовано 23.08.82. Бюллетень № 31

Дата опубликования описания 23.08.82

(51) М. Кл.<sup>3</sup>

G 06 F 7/58

(53) УДК 681.325  
(088.8)

(72) Автор  
изобретения

М. М. Юрцевич

(71) Заявитель

Минский радиотехнический институт

### (54) ГЕНЕРАТОР ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

1  
Изобретение относится к вычислительной технике и может найти применение при моделировании случайных процессов и исследовании помехоустойчивости различных систем, а также в бортовых и наземных системах радиосвязи и радионавигации для измерения параметров движущегося объекта в качестве модулирующих сигналов.

Известно устройство формирования псевдослучайных последовательностей, содержащее регистр сдвига и сумматор по модулю два в цепи обратной связи, позволяющее получить псевдослучайную последовательность максимальной длины с периодом  $2^n - 1$  [1].

Недостаток этого устройства - наличие корреляции между генерируемой последовательностью и задержанной последовательностью относительно самой себя на некоторое число дискретов, а также узость класса формируемых псевдослучайных последовательностей.

2  
Известен формирователь псевдослучайных последовательностей, содержащий  $n$ -разрядный регистр сдвига с сумматором по модулю два в цепи обратной связи и  $r$  дополнительных сумматоров по модулю два, на выходах которых формируются псевдослучайные последовательности, причем  $r \leq n/2$ . Дополнительные сумматоры по модулю два позволяют получить псевдослучайные последовательности с различным фазовым сдвигом [2].

Это устройство позволяет формировать псевдослучайные последовательности с равномерным спектром, но оно имеет неравный нулю коэффициент корреляции между сдвинутыми копиями последовательности.

Наиболее близким по технической сущности к предлагаемому является устройство формирования псевдослучайных последовательностей (ПСП), содержащее генератор тактовой частоты, выход которого связан с входами фазовращателя и первого датчика псевдослучайной последовательности.

ности, один выход которого связан с первым входом коррелятора, а другие выходы первого датчика псевдослучайной последовательности связаны с дешифратором, выход которого с одной стороны связан с другим входом коррелятора, а с другой стороны через фазовращатель связан с входом другого датчика псевдослучайной последовательности, выход которого подключен к третьему входу коррелятора [3].

Сущность работы данного устройства заключена в том, что первый и второй датчики псевдослучайных последовательностей формируют последовательности длины  $N = p^n - 1$  ( $p$  — простое число различной фазовой структуры), т.е. на основе различных неприводимых и примитивных полиномов, причем фаза второго датчика псевдослучайной последовательности сдвигается на один символ после каждого периода псевдослучайной последовательности генерируемой первым датчиком псевдослучайной последовательности. За период ПСП вычисляется взаимокорреляционная функция при  $i$ -ом сдвиге между ПСП, генерируемыми первым и вторым датчиками псевдослучайных последовательностей. В общем случае на выходе устройства формирования псевдослучайных последовательностей образуется многоуровневая ПСП длины  $N = p^n - 1$  с двузначной функцией автокорреляции.

$$\begin{cases} R(m) = N^2 + N - 1 & m \equiv 0 \pmod{N} \\ R(m) = -(N+2) & m \not\equiv 0 \pmod{N} \end{cases} \quad (1)$$

а значение каждого символа многоуровневой последовательности определяется по формуле

$$\alpha_m = \sum_{i=0}^{N-1} X_i Y_{i+m} \quad (2)$$

где  $X_i$  и  $Y_{i+m}$  — псевдослучайные последовательности, генерируемые соответственно первым и вторым датчиками псевдослучайных последовательностей.

Особый интерес представляют образующие на выходе устройства формирования последовательности  $\{\alpha_i\}$ , когда  $\alpha_i$  принимает только три уровня.

1. Пусть  $p=2$ , тогда следует, что уровни принимают следующие значения

а)  $\alpha_i = -1 + 2^{(n+l)/2}$  — встречается на периоде  $2^{n-l-1} + 2^{(n-l-2)/2}$  раз;

б)  $\alpha_i = -1$  — встречается на периоде последовательности  $2^n - 2^{n-l} - 1$  раз;

в)  $\alpha_i = -1 - 2^{(n+l)/2}$  — встречается на периоде последовательности  $2^{n-l-1} - 2^{(n-l-2)/2}$  раз.

При  $d = 2^k + 1$  или  $d = 2^{2k} - 2^k + 1$ ,  $cl = n$  н.о.д. ( $n, k$ ) — нечетное, а  $X_{i+k} = Y_{d_i}$

2. Пусть  $p \neq 2$ , простое, получаем а)  $\alpha_i = -1 + p^{(n+l)/2}$  — встречается на периоде многоуровневой последовательности  $1/2(p^{n-l} + p^{(n-l)/2})$  раз;

б)  $\alpha_i = -1$  — встречается на периоде многоуровневой последовательности  $p^n - p^{n-l} - 1$  раз.

с)  $\alpha_i = -1 - p^{(n+l)/2}$  — встречается на периоде многоуровневой последовательности  $1/2(p^{n-l} - p^{(n-l)/2})$  раз, где  $l = \text{н.о.д.}(n, k)$

$n/l$  — нечетное;  $d = 1/2(p^k - 1)$  или  $d = p^{2k} - p^k + 1$ , причем  $d \not\equiv p^i \pmod{p^n - 1}$ ;  $X_{i+k} = Y_{d_i}$ .

Если на выходе коррелятора со сбросом каждому символу поставить в соответствие (6)

$$\begin{cases} b_i = 0, & \text{если } \alpha_i = -1; \\ b_i = 1, & \text{если } \alpha_i = -1 + p^{(n+l)/2}; \\ b_i = -1, & \text{если } \alpha_i = -1 - p^{(n+l)/2}; \end{cases} \quad (3)$$

то пик-фактор выходной последовательности может определяться простой формулой (которая приближенно выполняется и для многоуровневой псевдослучайной последовательности)

$$\gamma = N/E, \quad (4)$$

где  $N$  — длина последовательности (период);

$E$  — энергия последовательности, определяемая числом не нулевых элементов последовательности на ее периоде.

Автокорреляционная функция выходной ПСП, формируемой в известном устройстве, при отображении ее уровнями (+1, -1, 0) имеет следующее значение

$$\begin{cases} R(m) = E = p^{n-l} & m \equiv 0 \pmod{N} \\ R(m) = 0 & m \not\equiv 0 \pmod{N} \end{cases} \quad (5)$$

Пик-фактор псевдослучайной последовательности, формируемой в известном устройстве имеет значение

$$\gamma = \frac{2^n - 1}{2^{n-l}} \quad (6)$$

В лучшем случае ( $l=1$ ) пик-фактор имеет значение  $\gamma = p$ .

ПСП, формируемые в известном устройстве, могут иметь минимальное значение пик-фактора  $\gamma = 2$  в случае, когда формируемые датчиками бинарные псевдослучайные последовательности имеют нечетную степень  $n = 3, 5, 7, \dots$ . Это значение

пик-фактора хуже значений, которые имеют псевдослучайные последовательности.

Недостатком известного устройства является также узкий класс формируемых последовательностей. Это объясняется тем, что период последовательностей при  $\rho \neq 2$  может иметь только одно из следующих значений:

- $N = 2^n - 1$  - когда датчиками формируются ПСП типа М-последовательностей;
- $N = 4x + 2$ ,  $N$  - простое,  $x = 1, 2, \dots$
- $N = 4x^2 + 27$ ,  $N$  - простое число,  $x = 1, 2, \dots$ ;
- $N_{x_2 x_1}, x_1, x_2$  - простые числа.

Цель изобретения - уменьшение пик-фактора формируемой псевдослучайной последовательности, что позволит повысить его точность, и увеличение класса формируемых псевдослучайных последовательностей.

Поставленная цель достигается тем, что в генератор псевдослучайных последовательностей, содержащий генератор тактовых импульсов, выход которого соединен с первым входом фазовращателя и с входом первого генератора М-последовательности, выход которого соединен с первым входом коррелятора, второй вход которого подключен к выходу дешифратора и к второму входу фазовращателя, выход которого соединен с входом второго генератора М-последовательности, разрядные выходы первого генератора М-последовательности соединены с входами дешифратора соответственно, введены компаратор, сумматор и блок задержки, входы которого подключены к разрядным выходам второго генератора М-последовательности соответственно, выход которого соединен с третьим входом коррелятора, выход которого соединен с входом компаратора, выход которого является выходом генератора, выходы блока задержки соединены с соответствующими входами группы сумматора.

На чертеже изображен генератор псевдослучайных последовательностей.

Устройство содержит генератор 1 тактовых импульсов, выход которого связан с входами фазовращателя 2 и первого генератора 3 М-последовательности, один выход которого соединен с первым входом коррелятора 4, а другие выходы первого генератора 3 М-последовательности связаны с дешифратором 5, выход которого соединен с другим входом коррелятора 4 и через фазовращатель 2 связан с входом второго генератора 6 М-последовательности, выходы которого

через блок 7 задержки и сумматор 8 соединены с третьим входом коррелятора 4, причем второй вход сумматора 8 соединен с основным выходом второго генератора 6 М-последовательности, а выход коррелятора 4 подключен к входу компаратора 9.

Генератор 1 тактовых импульсов выполняет операцию генерирования импульсов заданной частоты, с помощью которых осуществляется синхронная работа всех элементов и блоков устройства формирования псевдослучайных последовательностей.

Фазовращатель 2 осуществляет изменение фазы (задержку фазы) по сигналу с дешифратора 5. Выходное значение напряжения фазовращателя подчиняется выражению

$$\psi(Y) = \begin{cases} U(t) & Y=0 \\ 0 & Y=1, \end{cases}$$

где  $Y$  - значение выхода дешифратора;  $U(t)$  - выходное напряжение генератора тактовой частоты.

Первый генератор 3 М-последовательности выполняет операцию генерирования псевдослучайной последовательности с основанием  $\rho$  которая удовлетворяет некоторому полному значению задержки

$$f(x) = \sum_{i=0}^n C_i \cdot x^i, \text{ где } C_i = \{0, 1, \dots, -1\}.$$

Компектор 4 выполняет операцию следующего вида:

$$R(m) = \sum_{i=0}^{N-1} X_i \cdot Y_{i+m}$$

для дискретных величин  $X$  и  $Y$  и

$$R(m) = \int_0^T X(t+\tau) Y(t+\tau') dt$$

для непрерывных значений  $X$  и  $Y$ .

При  $\rho = 2$  коррелятор аналогичен коррелятору известного устройства. При  $\rho \neq 2$  коррелятор осуществляет перемножение с весом по правилу  $X_i \cdot Y_{i+m} = 1$ , если  $X_i = Y_{i+m}$  и  $X_i \cdot Y_{i+m} = 0$ , если  $X_i \neq Y_{i+m}$ . В общем случае коррелятор 4 имеет следующие узлы: весовой множитель; интегратор или сумматор.

Дешифратор 5 представляет собой  $n$ -входную схему совпадения на определенное кодовое состояние псевдослучайной последовательности, генерируемой первым датчиком 3 псевдослучайной последова-

тельности. Если значение  $n$  -разрядного слова ПСП совпадает с кодом схемы совпадения, на выходе Дешифратора будет напряжение, которое соответствует логической "1".

Второй генератор 6 М-последовательности выполняет операцию генерирования псевдослучайной последовательности с основанием  $p$ , но полином задержки отличается от полинома задержки первого датчика 3 псевдослучайной последовательности.

Блок 7 задержки осуществляет формирование ПСП, имеющих фазовый сдвиг относительно ПСП, генерируемой вторым датчиком 6 псевдослучайной последовательности. Число формируемых копий для каждого периода  $N$  ПСП выбирается в соответствии с разложением на множители,  $m = 0, 1, 2, \dots$

Сумматор 8 осуществляет операцию сложения  $m + 1$  величин. Сложение может быть проведено аналоговым или дискретным методами.

Компаратор 9 осуществляет преобразование уровней коррелятора 4 в три уровня (1, 0, -1).

Генератор работает следующим образом.

В момент включения в первый 3 и второй 6 генераторы М-последовательности вводятся состояния, отличные от нуля, а дешифратор 5 настроен на комбинацию символов, которые вводятся в первый генератор 3 М-последовательности в начальный момент времени. Это позволяет на выходе дешифратора 5 получить импульс, который осуществляет установку коррелятора 4 в нулевое состояние, а также производит задержку изменения фазы второго генератора 6 М-последовательности, за счет того, что логическая "1" на выходе дешифратора 5 не пропускает тактовый импульс через фазовращатель 2 на вход второго генератора 6 М-последовательности. Затем происходит формирование символов псевдослучайных последовательностей в первом 3 и втором 6 генераторах М-последовательности, а в блоке 7 задержки осуществляется формирование  $m$  -копий псевдослучайных последовательностей, которые имеют такую же форму, как и псевдослучайная последовательность, генерируемая вторым генератором 6 М-последовательности, но имеющие фазовый сдвиг, кратный значению  $\ell = \frac{n}{p^i - 1}, i = 1, 2, \dots$ . Символы с выхода второго генератора 6 М-последовательности и ее копии, сдвинутые на  $i$  символов одна

относительно другой, поступают на сумматор 8, выполняющий арифметическое суммирование.

Результат суммы сдвинутых псевдослучайных последовательностей поступает на коррелятор 4 со сбросом, на другой вход которого поступает ПСП, формируемая первым генератором 3 М-последовательности. За время  $N - \zeta_n$  ( $\zeta_n$  - длительность элементарного дискрета формируемых ПСП) вычисляется значение взаимокорреляционной функции между ПСП, генерируемой первым генератором 3 М-последовательности, и последовательностью, образованной суммой  $(m+1)$  копий ПСП такой же формы, как ПСП, генерируемая вторым генератором 6 М-последовательности. В соответствии с избранным правилом в компараторе 9 происходит отображение значения ВКФ в уровни (1, -1, 0). Одновременно с отображением уровней происходит сброс коррелятора 4 в нулевое состояние, так как ровно через период ПСП на выходе дешифратора 5 появится логическая "1", которая производит сброс коррелятора 4 в нуль раз за период. Кроме того, логическая "1" производит изменение фазы ПСП, генерируемой вторым генератором 6 М-последовательности. Далее цикл работы устройства повторяется. Через  $n$  сдвигов фаза ПСП, генерируемая другим датчиком псевдослучайной последовательности, примет исходное состояние и начнет выработываться второй период выходной псевдослучайной последовательности, состоящей из трех символов (+1, -1, 0).

Сущность работы предлагаемого устройства основана на новом свойстве взаимокорреляционной функции между одной М-последовательностью основания  $p$  и суммой  $m$  -копий другой М-последовательности такого же основания.

Если  $p^n - 1 = (p^i)^j - 1$ ,  $j$  - нечетное, то функция взаимной корреляции (ФВК) между псевдослучайной последовательностью и суммой  $p^i - 1$  копий другой псевдослучайной М-последовательности  $Y$  принимает всего три значения на периоде  $\frac{p^n - 1}{p^i - 1}$ .

50 Пусть  $p^i = 2$ , тогда

$$\left. \begin{aligned} \alpha_i = -(2^i - 1) & \text{ - встречается} \\ & \frac{(2^n - 1) - 1}{2^i - 1} \text{ раз} \\ \alpha_i = -(2^i - 1) + 2^{(n+\ell)/2} & \text{ - встречается} \\ & \frac{2^{n-\ell-1} - 2^{(n-\ell-2)/2}}{2^i - 1} \text{ раз} \\ \alpha_i = -(2^i - 1) - 2^{(n+\ell)/2} & \text{ - встречается} \\ & \frac{2^{n-\ell-1} - 2^{(n-\ell-2)/2}}{2^i - 1} \text{ раз} \end{aligned} \right\} (7)$$

55 где  $\ell = i = \text{н.о.д.}[n, k]$ ,  $n/\ell$  - нечетное;  
 $\delta = 2^k + 1$  или  $\delta = 2^{2k} - 2^{2k} + 1$ .



Увеличение класса формируемых псевдослучайных последовательностей происходит за счет того, что в предлагаемом устройстве образуется ряд псевдослучайных последовательностей не только периода  $P = -1$ , но и периода  $\frac{P^n - 1}{P^i - 1}$ .

В рассматриваемом выше примере число дополнительных фаз, формируемых в блоке генерирования  $m$  - дополнительных копий 7 другого датчика псевдослучайной последовательности, выбрано равным  $m = P^i - 2$ . Однако такое число формируемых копий является избыточным. Достаточно формировать всего  $m = \log_{P^i} P^i - 1$  дополнительных копий. Суммирование сумматора 8 тогда осуществляется по правилу

если  $\left\{ \sum_{i=0}^{m-1} Y_i^i \right\} = -m$ , то  $\left\{ \sum_{i=0}^{P^m} Y_i^i \right\} = -P^m - 1$ ;

если  $\left\{ \sum_{i=0}^{m-1} Y_i^i \right\} \neq -m$ , то  $\left\{ \sum_{i=0}^{P^m-2} Y_i^i \right\} = +1$ .

Эти формулы следуют непосредственно из свойств  $M$ -последовательностей.

Таким образом, предлагаемое устройство формирования псевдослучайных последовательностей имеет преимущества перед известным, заключающиеся в увеличении класса формируемых псевдослучайных последовательностей и уменьшении пик-фактора формируемых псевдослучайных последовательностей.

Введение блок задержки, сумматора и компаратора позволяют существенно расширить ансамбль псевдослучайных последовательностей с малым пик-фактором без существенного усложнения устройства.

20

Основание	Известное устройство		Предлагаемое устройство					
	Длина последовательности	$\gamma$	$i = 1$		$i = 2$		$i = 3$	
			Длина последовательности	$\gamma$	Длина последовательности	$\gamma$	Длина последовательности	$\gamma$
2	$2^n - 1$	2	$2^n$	2	$\frac{2^n - 1}{3}$	1,333	$2^n - 1$	1,142
3	$3^n - 1$	3	$\frac{3^n - 1}{2}$	1,5	$\frac{3^n - 1}{28}$	1,125	$\frac{3^n - 1}{2 \cdot 26}$	1,038
5	$5^n - 1$	5	$\frac{5^n - 1}{4}$	1,25	$\frac{5^n - 1}{4 \cdot 24}$	1,041	$\frac{5^n - 1}{4 \cdot 124}$	1,008
7	$7^n - 1$	7	$\frac{7^n - 1}{6}$	1,16	$\frac{7^n - 1}{6 \cdot 48}$	1,020	$\frac{7^n - 1}{6 \cdot 342}$	1,002
11	$11^n - 1$	11	$\frac{11^n - 1}{10}$	1,1	$\frac{11^n - 1}{10 \cdot 120}$	1,008	$\frac{11^n - 1}{10 \cdot 1330}$	1,0007
13	$13^n - 1$	13	$\frac{13^n - 1}{12}$	1,08	$\frac{13^n - 1}{12 \cdot 143}$	1,006	$\frac{13^n - 1}{12 \cdot 2196}$	1,0004
17	$17^n - 1$	17	$\frac{17^n - 1}{16}$	1,107	$\frac{17^n - 1}{16 \cdot 255}$	1,003	$\frac{17^n - 1}{16 \cdot 4912}$	1,0002
19	$19^n - 1$	19	$\frac{19^n - 1}{18}$	1,05	$\frac{19^n - 1}{18 \cdot 360}$	1,002	$\frac{19^n - 1}{18 \cdot 6858}$	1,0001

Ф о р м у л а   и з о б р е т е н и я

Генератор псевдослучайных последовательностей, содержащий генератор тактовых импульсов, выход которого соединен

55

с первым входом фазовращателя и с входом первого генератора  $M$ -последовательности, выход которого соединен с первым входом коррелятора, второй вход которого подключен к выходу дешифратора и к

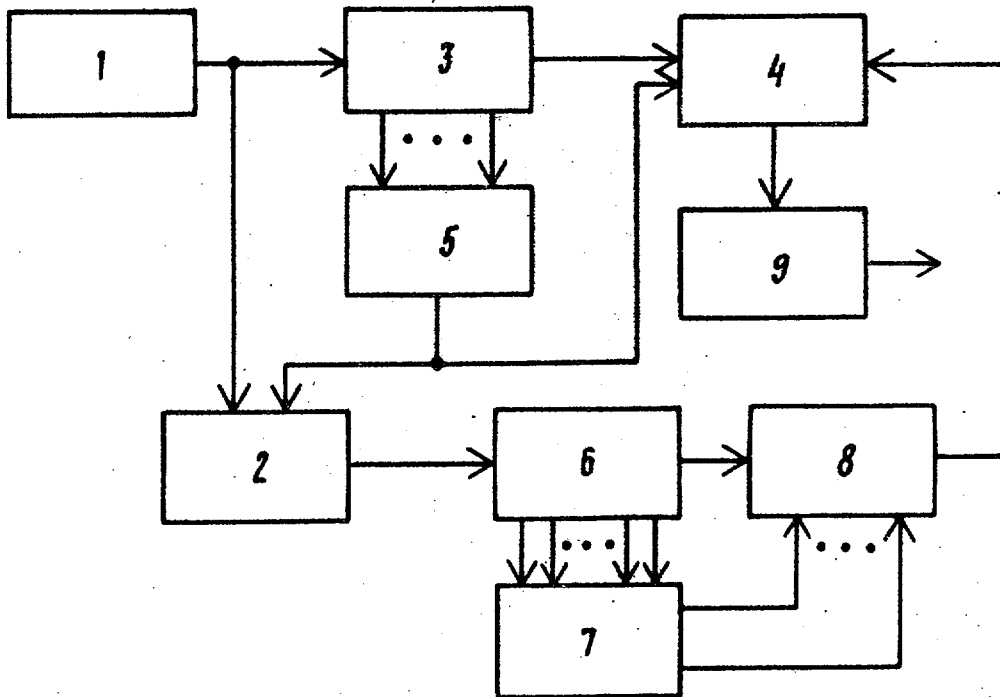
второму входу фазовращателя, выход которого соединен с входом второго генератора  $M$ -последовательности, разрядные выходы первого генератора  $M$ -последовательности соединены с входами дешифратора 5 соответственно, отличающийся тем, что, с целью повышения точности генератора, он содержит компаратор, сумматор и блок задержки, входы которого 10 подключены к разрядным выходам второго генератора  $M$ -последовательности соответственно, выход которого соединен с входом сумматора, выход которого соединен с третьим входом корректора, выход которого соединен с входом компаратора,

выход которого является выходом генератора, выходы блока задержки соединены с соответствующими разрядными входами сумматора.

Источники информации,

принятые во внимание при экспертизе

1. Патент США № 3700869, кл. 235-152, 1972.
2. Яковлев В. В., Федоров Р. Ф. Статистические вычислительные машины. Л. "Машиностроение", 1974, с. 253.
3. Авторское свидетельство СССР № 524174, кл. G 06 F 1/02, Н 03 В 29/00, 1974 (прототип).



Составитель А. Карасов

Редактор И. Николайчук Техред А. Ач

Корректор М. Шароши.

Заказ 6279/77

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