РАДИОТЕХНИКА И ЭЛЕКТРОНИКА, 2019, том 64, № 2, с. 160–167

ТЕОРИЯ И МЕТОДЫ ОБРАБОТКИ СИГНАЛОВ

УДК 621.396.4

ФОРМИРОВАНИЕ НЕЛИНЕЙНЫХ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ И ИХ СВОЙСТВА

© 2019 г. В. Б. Федоров[1, *], А. И. Стариковский[1, **], А. А. Парамонов[1], О. В. Тихонова[1]

[1]МИРЭА – Российский технологический университет,
Российская Федерация, 119454, Москва, просп. Вернадского, 78

**E-mail: fdorov@mail.ru*

***E-mail: starikovski@mirea.ru*

Поступила в редакцию 12.04.2018 г.
После доработки 01.06.2018 г.
Принята к публикации 11.06.2018 г.

Изложена основанная на теории *bent*-функций теория генератора периодических псевдослучайных двоичных *B*-последовательностей. Описан алгоритм построения генератора и приведены результаты компьютерного расчета для последовательностей некоторых периодов.

DOI: 10.1134/S0033849419020049

ВВЕДЕНИЕ

Псевдослучайные бинарные последовательности (ПСП) находят применение во многих радиоэлектронных системах, например, в многоканальных системах передачи цифровой информации с кодовым разделением каналов (CDMA), в криптосистемах и других. Например, используются, так называемые, *M*-последовательности, последовательности Голда и Касами, также формируемых на основе *M*-последовательностей. Это все примеры линейных последовательностей, поскольку их генерация основана на сдвиговом регистре с многоотводной линейной обратной связью и не использует нелинейных преобразований.

Известны и применяются на практике также нелинейные последовательности, так называемые *B*-последовательности. Методы генерирования *B*-последовательностей тоже основаны на теории конечного поля Галуа и используют сдвиговый регистр с линейной обратной связью. Однако при формировании *B*-последовательности содержимое сдвигового регистра подвергается уже некоторому нелинейному преобразованию с помощь одной из так называемых максимально-нелинейных булевых функций (*bent*-функций).

Это позволяет реализовать генератор, способный генерировать весьма широкий класс (и даже довольно много классов) *B*-последовательностей, равноценных по своим свойствам, что обеспечивается наличием целого ряда свободных параметров. При этом получаемые последовательности обладают следующими весьма привлекательными свойствами [1] (детальнее об этом см. в разд. 4).

1. Взаимно-корреляционные функции (ВКФ) и уровень боковых лепестков автокорреляционной функции (АКФ) *B*-последовательностей не превосходит величины $2^{n/2}+1$.

2. Последовательности хорошо “сбалансированы”, т.е. разность числа нулей и единиц в каждой последовательности равна 1.

3. Легко осуществляется “перенастройка” генератора с генерирования одной последовательности на генерирование другой, а также легко осуществляется временной сдвиг генерируемой последовательности.

4. Максимальная длина $n_{\text{экв}}$ (см. ниже) линейного эквивалентного генератора (ЛЭГ), способного генерировать такую же последовательность, при $n > 4$ значительно превышает число элементов памяти нелинейного генератора.

5. *B*-последовательности обладают высокой структурной сложностью, поэтому они трудно поддаются расшифровке и не могут быть быстро раскрыты и использованы для подавления радиосистемы.

В связи с этим практический интерес к *B*-последовательностям неуклонно возрастает [2, 3]. Однако по настоящее время отсутствует доступная литература, где бы подробно описывалась методика расчета генераторов *B*-последовательностей. И в тоже время в математическом отношении эти расчеты, основанные на теории конечного поля и теории нелинейных булевых функций, достаточно сложны и требуют подробного изложения, чтобы стать доступными более широкой аудитории, а не только специалистам-математикам.

В данной работе, в целях ликвидации указанного пробела, детально рассматривается процедура формирования *B*-последовательностей, из-

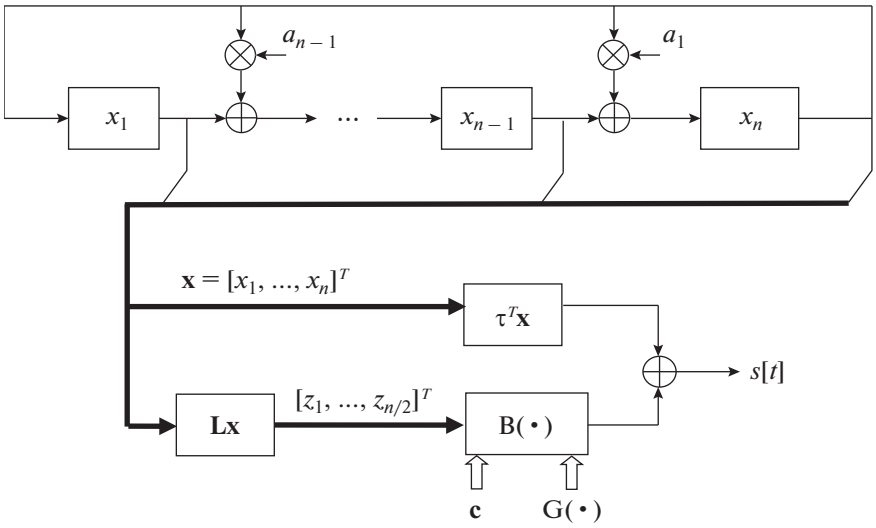

Рис. 1. Структурная схема генератора *B*-последовательностей.

лагается оригинальный алгоритм построения генератора и приводятся результаты компьютерных расчетов для значения периода последовательности $N = 2^n - 1$, при $n = 4, 8, 12, 16$, т.е. для $N = 15, 255, 4095, 65535$ соответственно.

Степень детализации описания алгоритма, местами доведенная до уровня псевдокода, позволяет легко запрограммировать все вычисления с использованием какой-либо библиотеки, поддерживающей вычисления в конечном поле. Имеется также соответствующая авторская компьютерная программа [4].

1. ОБЩАЯ СТРУКТУРА ГЕНЕРАТОРА *B*-ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Рассмотрим подробно процедуру формирования *B*-последовательности $\{s[t]\}_{t=0,1,2,\ldots}$ периода $N = 2^n - 1$, где n – длина используемого сдвигового регистра, над конечным полем Галуа 2-го порядка, $s[t] \in GF(2) = \{0,1\}$. При этом требуется, чтобы длина сдвигового регистра n была кратна 4.

Пусть $GF(2^n)$ – конечное поле Галуа порядка 2^n и α – его некоторый примитивный элемент с минимальным многочленом

$$\mathrm{M}_n(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + 1,$$

$a_k \in \{0,1\}$, так что $GF(2^n) = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{2^n-2}\}$.

Рассмотрим в $GF(2^n)$, как в n-мерном линейном пространстве над полем $\{0,1\}$, стандартный базис

$$\{\alpha^{k-1}\}_{k=1:n}. \qquad (1)$$

Тогда $\forall x \in GF(2^n)$

$$x = \sum_{k=1}^{n} x_k \alpha^{k-1}, \qquad (2)$$

где $x_k \in \{0,1\}$ – координаты элемента поля x в стандартном базисе.

В состав генератора *B*-последовательности входит n-элементный сдвиговый регистр, охваченный линейной обратной связью, соответствующей многочлену $\mathrm{M}_n(x)$, (см. рис. 1). В каждый момент дискретного времени t регистр содержит координаты какого-либо ненулевого элемента поля $x[t] = \alpha^t \in GF(2^n)$ в базисе (1), $t = 0, 1, 2\ldots$. Эти координаты обозначим $\mathbf{x} = [x_1, \ldots, x_n]^T \in \{0,1\}^n$, где T символ операции транспонирования. Чтобы не загромождать обозначения, зависимость от времени t элементов этого вектора мы явно не указываем, но подразумеваем, так что $\mathbf{x} = \mathbf{x}[t]$.

Очередной элемент генерируемой *B*-последовательности получается в результате применения к $\mathbf{x}[t]$ некоторой нелинейной булевой функции от n переменных $\mathrm{F}: \{0,1\}^n \to \{0,1\}$, т.е.

$$s[t] = \mathrm{F}(\mathbf{x}[t]), \qquad (3)$$

где $\mathbf{x}[t] = [x_1, \ldots, x_n]^T \in \{0,1\}^n$ – текущее содержимое сдвигового регистра.

Если бы функция $\mathrm{F}(\cdot)$ была линейной, то получился бы просто генератор некоторой *M*-последовательности. Однако в генераторе *B*-последовательностей эта функция представляет собой сумму некоторой линейной функции и композиции некоторого линейного отображения в пространство вдвое меньшей размерности и некоторой нели-

нейной функции, относящейся к классу так называемых *bent*-функций. А именно [1]

$$\mathrm{F}(\mathbf{x}) = \mathrm{B}(\mathbf{L}\mathbf{x}) + \boldsymbol{\tau}^T\mathbf{x}, \qquad (4)$$

где $\mathbf{L}$ – постоянная матрица над $\{0,1\}$ размера $n/2 \times n$, $\boldsymbol{\tau}$ –постоянный вектор-столбец длины n, с элементами из $\{0,1\}$, B: $\{0,1\}^{n/2} \to \{0,1\}$ – одна из *bent*-функций от $n/2$ логических переменных, имеющая следующую структуру:

$$\mathrm{B}(\mathbf{z}) = \mathbf{z}_{(1:n/4)}^T\mathbf{z}_{(n/4+1:n/2)} + \mathrm{G}\left(\mathbf{z}_{(1:n/4)}\right) + \mathbf{c}^T\mathbf{z}. \qquad (5)$$

Здесь $\mathbf{z} = \left[z_1,\ldots,z_{n/2}\right]^T$, $\mathbf{z}_{(1:n/4)} = \left[z_1,\ldots,z_{n/4}\right]^T$ – первая половина вектора $\mathbf{z}$, $\mathbf{z}_{(n/4+1:n/2)} = \left[z_{n/4+1},\ldots,z_{n/2}\right]^T$ – вторая его половина, $\mathbf{c} = \left[c_1,\ldots,c_{n/2}\right]^T \in \{0,1\}^{n/2}$ – вектор-столбец произвольных параметров, G: $\{0,1\}^{n/4} \to \{0,1\}$ – произвольная нелинейная булева функция от $n/4$ переменных.

Bent-функции относятся к классу, так называемых, максимально нелинейных функций, т.е. функций максимально далеких от аффинных булевых функций в смысле расстояния Хемминга [5]. Вообще, по определению [1], булева функция B: $\{0,1\}^m \to \{0,1\}$ называется *bent*-функцией, если она имеет преобразование Фурье $\tilde{B}$: $\{0,1\}^m \to \mathbb{R}$, все 2^m значений которого по модулю равны 1; преобразование Фурье (Уолша–Адамара) для булевых функций определяется формулой

$$\tilde{B}(\boldsymbol{\lambda}) = 2^{-m/2}\sum_{\mathbf{z}\in\{0,1\}^m}(-1)^{B(\mathbf{z})}(-1)^{\mathbf{z},\boldsymbol{\lambda}},$$

где $\mathbf{z},\boldsymbol{\lambda}$ – скалярное произведение в $\{0,1\}^m$ (можно говорить также, что это есть преобразование Фурье биполярной функции $(-1)^{B(\mathbf{z})}$). Доказано [1], что все функции вида (5) являются *bent*-функциями. Отметим также, что *bent*-функции – это максимально нелинейные функции четного порядка, хотя в общем случае максимально нелинейные функции могут иметь порядок любой четности [5].

Определения основных констант алгоритма, т.е. матрицы $\mathbf{L}$ и вектора-столбца $\boldsymbol{\tau}$, входящих в (4), и способ их вычисления приведены в следующем разделе. Общая структура алгоритма изображена на рисунке.

Как видно из (4), при заданном минимальном многочлене $\mathrm{M}_n(x)$ и при предварительно вычисленных основных константах $\mathbf{L}$, $\boldsymbol{\tau}$, вид генерируемой *B*-последовательности зависит лишь от выбора нелинейной функции G(·) и вектора параметров $\mathbf{c} = \left[c_1,\ldots,c_{n/2}\right]^T$.

Таким образом, для каждой фиксированной функции G(), получается семейство из $2^{n/2}$ различных *B*-последовательностей. Причем, если две нелинейные функции, скажем $\mathrm{G}_1(\cdot)$ и $\mathrm{G}_2(\cdot)$, различаются только линейным слагаемым, то они порождают один и тот же класс *B*-последовательностей, что непосредственно следует из (5). Порядок выбранной нелинейной функции влияет на длину сдвигового регистра ЛЭГ, способного генерировать такую же последовательность. Эта длина равна [1] $\sum_{k=1}^{m} C_m^k$, где $m \le n/4$ – порядок функции $\mathrm{G}(\cdot)$, а максимальная длина ЛЭГ $n_{\text{экв}}$ достигается при $m = n/4$. Уровень боковых лепестков периодической АКФ и уровень периодических ВКФ любых *B*-последовательностей, имеют максимальные значения равные $2^{n/2}+1$, при пиковом значении АКФ, равном $N = 2^n - 1$ [1].

Кроме того, описываемая далее процедура вычисления основных констант $\mathbf{L},\boldsymbol{\tau}$ имеет некоторые степени свободы (дополнительные параметры), о которых будет сказано ниже.

2. АЛГОРИТМ ПОСТРОЕНИЯ ГЕНЕРАТОРА *B*-ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Согласно [1, 6], введенный ранее вектор-столбец $\boldsymbol{\tau} = \left[\tau_1,\ldots,\tau_n\right]^T$ содержит коэффициенты линейной формы

$$\mathrm{tr}_n(\sigma x) = \boldsymbol{\tau}^T\mathbf{x}$$

в базисе (1), действующей из $GF(2^n)$ в $GF(2)$, где $\mathrm{tr}_n(z) = \sum_{k=0}^{n-1} z^{2^k}$ – след соответствующего элемента поля $z \in GF(2^n)$, $\sigma \in GF(2^n)\setminus\{0\} = \{\alpha^0,\alpha^1,\ldots,\alpha^{2^n-2}\}$ – произвольный не равный нулю элемент поля, т.е. $\sigma = \alpha^m$, $m = 0, 1,\ldots,2^n-2$.

Причем, как показано в [6], $\mathrm{tr}_n(\sigma\alpha^{k-1}) = \mathrm{tr}_n(\alpha^{m+k-1}) = \mathrm{tr}(\mathbf{A}_\alpha^{k+m-1})$, где

$$\mathbf{A}_\alpha = \begin{bmatrix} 0 & 0 & 0 & \ldots & 0 & 1 \\ 1 & 0 & 0 & \ldots & 0 & a_{n-1} \\ 0 & 1 & 0 & \ldots & 0 & a_{n-2} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 0 & a_2 \\ 0 & 0 & 0 & \ldots & 1 & a_1 \end{bmatrix} \qquad (6)$$

– матрица линейного оператора A:$GF(2^n) \to GF(2^n)$ в базисе (1), действующего по формуле:

$A(x) = \alpha x$, $\mathrm{tr}(\mathbf{A}_\alpha^{k+m-1})$ – след матрицы $\mathbf{A}_\alpha^{k+m-1}$. Таким образом, для $k = 1:n$

$$\tau_k = \mathrm{tr}\left(\mathbf{A}_\alpha^{k+m-1}\right), \tag{7}$$

где число $m \in \{0,1,\ldots,2^n - 2\}$ – может быть выбрано произвольно.

Далее отметим, что при любом n в поле $GF(2^n)$, как линейном пространстве над полем $\{0,1\}$, определено скалярное произведение

$$\langle x, y\rangle_n = \mathrm{tr}_n(xy).$$

В [6] показано, что в базисе (1)

$$\langle x, y\rangle_n = \mathbf{x}^T\mathbf{R}\mathbf{y},$$

где $\mathbf{x} = [x_1,\ldots,x_n]^T$, $\mathbf{y} = [y_1,\ldots,y_n]^T \in \{0,1\}^n$ – координатные вектор-столбцы произвольных элементов x и y поля $GF(2^n)$,

$$\mathbf{R} = [r_{km}]_{k,m=1:n}, \quad r_{km} = \mathrm{tr}\left(\mathbf{A}_\alpha^{k+m-2}\right). \tag{8}$$

Далее наряду с обозначением $\langle x, y\rangle_n$ скалярного произведения в $GF(2^n)$ также будет использоваться обозначение $\langle \mathbf{x}, \mathbf{y}\rangle = \mathbf{x}^T\mathbf{y}$ скалярного произведения в $\{0,1\}^n$.

Отметим, что $\mathbf{R}$ не является диагональной матрицей, поэтому базис (1) не является ортогональным. В работе [1] предлагалось использовать ортогональный базис, проведя процедуру ортогонализации базиса (1). Однако процедура ортогонализации достаточно громоздкая, и мы, следуя [6], обойдемся без нее.

Перейдем к определению введенной ранее матрицы $\mathbf{L}$. Согласно [1], это матрица линейного над $GF(2)$ отображения $L: GF(2^n) \to \{0,1\}^{n/2}$, такого, что сопряженное отображение $L^*: \{0,1\}^{n/2} \to GF(2^n)$ имеет вид:

$$L^*(\mathbf{y}) = \hat{x}y,$$

где $\hat{x} \in GF(2^n)$ – корень уравнения

$$x^2 + x = w. \tag{9}$$

В уравнении (9) $w \in GF(2^{n/2}) \subset GF(2^n)$ – произвольный параметр, удовлетворяющий условию $\mathrm{tr}_{n/2}(w) = 1$. При этом $y \in GF(2^{n/2})$ – элемент поля, которому соответствует вектор-столбец $\mathbf{y} \in \{0,1\}^{n/2}$ его координат в базисе подполя $GF(2^{n/2})$. Этот базис определим следующим образом: в $GF(2^{n/2})$ в качестве примитивного элемента выберем, элемент $\beta = \alpha^{2^{n/2}+1}$, тогда $GF(2^{n/2}) = \left\{0, 1, \beta, \beta^2,\ldots, \beta^{2^{n/2}-2}\right\}$, и среди перечисленных элементов подполя выберем стандартный базис

$$\left\{\beta^{k-1}\right\}_{k=1:n/2}. \tag{10}$$

То, что линейное отображение $L^*(\cdot)$ является сопряженным линейному отображению $L(\cdot)$, означает, что $\forall x \in GF(2^n)$, $\forall \mathbf{y} \in \{0,1\}^{n/2}$

$$\langle L(x), \mathbf{y}\rangle = \langle x, L^*(\mathbf{y})\rangle_n,$$

где $L(x) \in \{0,1\}^{n/2}$ – вектор-столбец координат элемента подполя $GF(2^{n/2})$ в базисе (10).

В матричном виде $L^*(\mathbf{y}) = \mathbf{L}^*\mathbf{y}$, где $\mathbf{L}^*$ – матрица сопряженного оператора, в которой каждый k-ый столбец состоит из коэффициентов разложения элемента поля $\hat{x}\beta^{k-1} \in GF(2^n)$ по базису (1). С учетом сказанного нетрудно показать [5], что

$$\mathbf{L} = \mathbf{L}^{*T}\mathbf{R}. \tag{11}$$

Требуемые здесь коэффициенты разложения элемента поля $\hat{x}\beta^{k-1} \in GF(2^n)$ по базису (1) получаются самым естественным образом. Как видно из (2), все элементы поля $GF(2^n)$ представляют собой многочлены степени не выше $n-1$ от примитивного элемента α, и произведение (в других случаях – сложение) элементов поля есть произведение (сложение) соответствующих многочленов, вычисляемое по модулю $\mathrm{M}_n(\alpha)$. В частности, в соответствии с этим вычисление $\hat{x}\beta^{k-1}$ дает искомое разложение вида (2). Все сказанное в равной мере относится и ко всем другим обсуждаемым нами вычислениям в поле $GF(2^n)$. Поэтому для компьютерной реализации рассматриваемых алгоритмов требуется использовать библиотеки программ, осуществляющих вычисления в конечном поле. Такие библиотеки содержатся во многих популярных пакетах программ, реализующих операции компьютерной алгебры.

Теперь остается только указать способ выбора параметра w уравнения (9) и метод решения самого уравнения. Найти подходящее значение параметра w можно простым перебором элементов поля $GF(2^{n/2})$, следуя алгоритму

$$\begin{aligned} &w = \beta \\ &\textbf{while} \quad \mathrm{tr}_{n/2}(w) \neq 1 \\ &\qquad w = w * \beta \\ &\textbf{end} \end{aligned} \tag{12}$$

% В результате w равно искомому значению, при котором $\mathrm{tr}_{n/2}(w) = 1$.

При этом на каждом шаге алгоритма функция

$$\mathrm{tr}_{n/2}(w) = w + w^2 + \ldots + w^{2^{n/2-1}} \quad (13)$$

вычисляется как выражение над $GF(2^n)$ описанным выше способом, поскольку $w \in GF(2^{n/2}) \subset \subset GF(2^n)$; то же относится и к строке (12) алгоритма.

При решении уравнения (9) используем метод, предложенный в [6]. Прежде всего, отметим, что, поскольку характеристика поля $GF(2^n)$ равна 2, то правая часть уравнения (9) $\mathrm{P}(x) = x^2 + x$ – линейный над $GF(2)$ оператор, действующий в $GF(2^n)$, т.е. уравнение (9) – линейное неоднородное уравнение, записанное в операторной форме. Рассмотрим сначала соответствующее однородное уравнение $\mathrm{P}(x) = 0$, которое в $GF(2^n)$ имеет ровно два решения: $x_{(1)} = 0$ и $x_{(2)} = 1$. Таким образом, ранг линейного оператора $\mathrm{P}(\cdot)$ и, следовательно, ранг его матрицы $\mathbf{P}$, в частности, в интересующем нас базисе (1), равен $n-1$. При этом из того, что $\mathrm{P}(1) = 0$, следует, что первый столбец матрицы $\mathbf{P}$ состоит из одних нулей. Обозначим подматрицу, состоящую из остальных $n-1$ столбцов матрицы $\mathbf{P}$, и содержащую n строк, символом $\mathbf{D}$. Эта подматрица имеет ранг $n-1$.

Уравнению (9) соответствует следующее неоднородное матричное уравнение

$$\mathbf{Px} = \mathbf{w}, \quad (14)$$

где $\mathbf{x} \in \{0,1\}^n$ – координаты искомого корня в базисе (1), $\mathbf{w} \in \{0,1\}^n$ – координаты свободного члена уравнения (9) в том же базисе. Следовательно, решение уравнения (14) сводится к решению системы уравнений вида

$$\mathbf{D}\mathbf{x}_{(2:n)} = \mathbf{w}, \quad (15)$$

где $\mathbf{x}_{(2:n)} = [x_2,\ldots,x_n]^T$. Эта система имеет единственное решение $\hat{\mathbf{x}}_{(2:n)} = [\hat{x}_2,\ldots,\hat{x}_n]^T$, которое можно найти, например, путем приведения расширенной матрицы системы (15), т.е. матрицы $[\mathbf{D},\mathbf{w}]$, к ступенчатому виду и с последующим исключением неизвестных стандартным способом. Полное решение системы (14) получается на основе решения системы (15) и имеет ровно два частных решения

$$\hat{\mathbf{x}} = [0,\hat{x}_2,\ldots,\hat{x}_n]^T, \quad \hat{\mathbf{x}} = [1,\hat{x}_2,\ldots,\hat{x}_n]^T. \quad (16)$$

Любое решение может быть использовано при вычислениях по формуле (11).

Остановимся теперь на способе вычисления элементов матрицы $\mathbf{D}$ или, что равнозначно, матрицы $\mathbf{P}$, в которой первый столбец уже был определен. Очевидно, что $\mathbf{P} = \mathbf{\Phi} + \mathbf{I}$, где $\mathbf{I}$ – единичная матрица, а $\mathbf{\Phi}$ – матрица оператора $\Phi(x) = x^2$. Воспользуемся разложением (2), а также учтем, что характеристика поля $GF(2^n)$ равна 2, и запишем x^2 в виде

$$x^2 = \left(\sum_{k=1}^{n} x_k \alpha^{k-1}\right)^2 = \sum_{k=1}^{n} x_k \alpha^{2(k-1)}.$$

Следовательно, матрица $\mathbf{\Phi}$ состоит из столбцов, каждый из которых содержит коэффициенты разложения соответствующего элемента $\alpha^{2(k-1)}$ по базису (1), т.е. k-ый столбец матрицы $\mathbf{\Phi}$ равен 1-му столбцу матрицы $\mathbf{A}_\alpha^{2(k-1)}$, причем матрица $\mathbf{A}_\alpha$ определена формулой (6).

3. РЕЗУЛЬТАТЫ КОМПЬЮТЕРНОГО РАСЧЕТА ГЕНЕРАТОРА ДЛЯ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НЕКОТОРЫХ ПЕРИОДОВ

В этом разделе приведены результаты компьютерных расчетов генератора по изложенной выше методике с помощью авторской компьютерной программы [4].

В программе для заданной длины сдвигового регистра n, или что эквивалентно, для заданного периода последовательности N и для заданного минимального многочлена $\mathrm{M}_n(x)$ вычисляются матрица $\mathbf{L}$ и вектор-столбец $\boldsymbol{\tau}$. Эти параметры мы называем основными параметрами, т.к. они являются общими (одинаковыми) для всех генераторов, формирующих последовательности данного периода. Чтобы переключить генератор на формирование какой-либо другой последовательности в пределах одного класса, необходимо лишь изменить свободный векторный параметр $\mathbf{c}$. А для того, чтобы переключить генератор на формирование какой-либо последовательности другого класса, требуется изменить вид нелинейной булевой функции $\mathrm{G}(\cdot)$ (при $n = 4$ в генераторе функция $\mathrm{G}(\cdot)$ не используется). В программе всегда используются максимально возможные степени этой функции, чтобы получить наибольшую длину ЛЭГ.

Отметим также, что при расчете основных параметров $\mathbf{L}$ и τ имеются некоторые степени свободы, которые для определенности всегда будут разрешаться одним и тем же способом. А именно, в формуле (7) положим $m = 0$ и из двух решений, представленных в (16), будем всегда выбирать первое. Базис (10) также определяется неоднозначно, т.е. этот базис можно было бы заменить другим, и от этого зависел бы результат, но мы остановимся на сделанном выборе. В принципе, можно было бы указанные неоднозначности

в (7), (16) и (10) разрешить и как-то иначе, например, задавшись целью минимизировать число единиц в $\mathbf{L}$ и τ [6].

В итоге для случаев $n = 4, 8, 12, 16$ получены следующие результаты.

1. При $n = 4$, $\mathrm{M}_4(x) = x^4 + x + 1$ имеем

$$\mathbf{L} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix}, \quad \boldsymbol{\tau} = [0\ 0\ 0\ 1]^T.$$

Весь ансамбль (класс) состоит из $2^{n/2} = 4$ последовательностей (каждая из них определяется соответствующим набором двоичных коэффициентов $c = [c_1, c_2]^T$, функция $\mathrm{G}(\cdot)$ – не используется). Сами эти последовательности (только один период) имеют вид:

0 0 0 1 0 1 0 1 1 1 0 1 0 1 1,
1 1 0 0 0 0 1 0 0 1 0 1 1 1 1,
0 0 1 1 0 0 1 1 0 1 1 0 1 0 1,
1 1 1 0 0 1 0 0 1 1 1 0 0 0 1.

Их период $N = 2^n + 1 = 15$, максимальная длина ЛЭГ $n_{\text{экв}} = 4$.

Приведенные для $n = 4$ результаты компьютерного расчета совпадают с результатами, полученными в [6] без использования компьютерных вычислений.

2. При $n = 8$, $\mathrm{M}_8(x) = x^8 + x^4 + x^3 + x^2 + 1$ имеем

$$\mathbf{L} = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}, \quad \boldsymbol{\tau} = [0\ 0\ 0\ 0\ 0\ 1\ 0\ 0]^T.$$

Весь ансамбль состоит из $2^{n/2} = 16$ последовательностей. Причем имеется единственная, с точностью до линейного слагаемого, нелинейная функция 2-го порядка $\mathrm{G}([z_1, z_2]) = z_1 z_2$. Период последовательностей $N = 255$, максимальная длина ЛЭГ $n_{\text{экв}} = 36$.

3. При $n = 12$, $\mathrm{M}_{12}(x) = x^{12} + x^6 + x^4 + x + 1$ имеем

$$\mathbf{L} = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \end{bmatrix},$$

$$\boldsymbol{\tau} = [0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1]^T.$$

В этом случае имеется восемь ансамблей последовательностей по $2^{n/2} = 64$ последовательности в каждом. Каждый ансамбль определяется одной из нелинейных функций 3-го порядка вида $\mathrm{G}([z_1, z_2, z_3]) = z_1 z_2 z_3 + g_1 z_1 z_2 + g_2 z_1 z_3 + g_3 z_2 z_3$, где $g_1, g_2, g_3 \in \{0,1\}$ – произвольные коэффициенты и всего имеется восемь различных комбинаций значений этих коэффициентов. Период последовательностей $N = 4095$, максимальная длина ЛЭГ $n_{\text{экв}} = 298$.

4. При $n = 16$, $\mathrm{M}_{12}(x) = x^{16} + x^{12} + x^3 + x + 1$ имеем

$$\mathbf{L} = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \end{bmatrix},$$

$$\boldsymbol{\tau} = [0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 1]^T.$$

В этом случае имеется уже 1024 ансамбля последовательностей по $2^{n/2} = 256$ последовательности в каждом. Каждый ансамбль определяется одной из нелинейных функций 4-го порядка вида

$$\mathrm{G}([z_1, z_2, z_3, z_4]) = z_1 z_2 z_3 z_4 + \sum_{\{k_1 k_2 k_3\} \subset \{1,2,3,4\}} g_{k_1 k_2 k_3} z_{k_1} z_{k_2} z_{k_3} + \sum_{\{m_1 m_2\} \subset \{1,2,3,4\}} g_{m_1 m_2} z_{m_1} z_{m_2}$$

где $g_{k_1 k_2 k_3}, g_{m_1 m_2} \in \{0,1\}$ – произвольные коэффициенты, причем суммирование в первой сумме осуществляется по всем трехэлементным подмножествам, а во второй – по всем двухэлементным подмножествам множества $\{1,2,3,4\}$. Таким образом, первая сумма дает $C_4^3 = 4$, а вторая – $C_4^2 = 6$, т.е. всего десять слагаемых с произвольными коэффициентами из {0,1}, что и дает 1024 варианта. Период последовательностей $N = 65535$, максимальная длина линейного эквивалентного генератора $n_{\text{экв}} = 2516$.

Ясно, что в общем случае при заданном n каждый ансамбль определяется одной из функций порядка $n/2$ за вычетом ее аффинной составляющей в представлении в виде многочлена Жегалкина.

Таблица 1. Сравнение свойств ПСП

Тип ПСП	Длина сдвигового регистра	Период ПСП	Число различных ПСП заданного периода	Максимальный уровень побочных пиков АКФ и ВКФ	Максимальная длина ЛЭГ	Баланс нулей и единиц на периоде
M-последовательность	n	$2^n - 1$	$\frac{\varphi(2^n - 1)}{n}$	$2^{n/2}$	n	1
Касами	n – четно	$2^n - 1$	$2^{n/2}$	$2^{n/2} + 1$	$\frac{3n}{2}$	$2^{n/2} - 1$
Голд	n – нечетно	$2^n - 1$	$2^n + 1$	$2^{\frac{n+1}{2}} + 1$	$2n$	$1 \ldots 2^{\frac{n+1}{2}} + 1$
bent	n – кратно 4	$2^n - 1$	$2^{n/2}$	$2^{n/2} + 1$	$\sum_{k=1}^{n/4} C_{n/4}^k$	1

4. СРАВНИТЕЛЬНЫЙ АНАЛИЗ СВОЙСТВ *B*-ПОСЛЕДОВАТЕЛЬНОСТЕЙ И ЛИНЕЙНЫХ ПСП

Для сравнения в таблице 1 приведены основные характеристики *B*-последовательностей, а также последовательностей Голда и Касами, которые наиболее часто используются в радиосистемах различного назначения. Как известно, последовательности Голда и Касами получаются на основе *M*-последовательностей. Непосредственно сами *M*-последовательности исключены из сравнения, т.к. хорошо известно, что они существенно уступают двум последним по показателю уровня их взаимной корреляции, но вполне сравнимы с ними по другим показателям.

Из таблицы видно, что по длине периода и максимальному уровню боковых пиков АКФ и ВКФ все сравниваемые ПСП практически эквиваленты. По числу всех различных последовательностей заданного периода класс *B*-последовательностей (при фиксированной нелинейной функции $G(\cdot)$) не уступает последовательностям Касами и значительно превосходят *M*-последовательности (в таблице $\varphi(x)$ – функция Эйлера). По показателю баланса нулей и единиц на периоде *B*-последовательности эквивалентны *M*-последовательностям. Но главное преимущество *B*-последовательностей заключается в их существенно более высокой структурной сложности, что исключительно важно, например, для проектирования криптостойких систем.

Так при $n = 12$ для *B*-последовательностей максимальная длина линейного эквивалентного генератора составляет 298, в то время как для последовательностей Голда – 24, а для последовательностей Касами – только 18. При этом за счет возможности произвольного (в пределах соответствующего класса функций) выбора вида нелинейной функции $G(\cdot)$ общее количество различных *B*-последовательностей той же длины может быть увеличено в восемь раз.

При $n = 16$ картина получается еще более впечатляющей. Для *B*-последовательностей максимальная длина линейного эквивалентного генератора составляет 2516, а для последовательностей Голда и Касами – 32 и 24, соответственно, при возможности увеличения общего числа *B*-последовательностей той же длины в 1024 раза за счет произвольного выбора того или иного вида нелинейной функции.

ЗАКЛЮЧЕНИЕ

В статье подробно изложен алгоритм построения генератора *B*-последовательностей, который заключается в вычислении, при заданном минимальном многочлене $M_n(x)$, матрицы $\mathbf{L}$ и вектора $\boldsymbol{\tau}$. Генератор способен генерировать, в общем случае, целый набор ансамблей (классов) *B*-последовательностей. Вид выбранной нелинейной функции $G\left(\left[z_1, \ldots, z_{n/4}\right]\right)$ определяет некоторый класс генерируемых *B*-последовательностей, при этом степени свободы генератора внутри выбранного класса определяются наличием произвольно устанавливаемых коэффициентов $\mathbf{c} = \left[c_1, \ldots, c_{n/2}\right]^T$. Наличие указанных параметров позволяет практически мгновенно переключать генератор на генерирование новой последовательности.

Сравнительный анализ свойств линейных и нелинейных ПСП показывает, что *B*-последовательности являются серьезной альтернативой линейным ПСП для использования в широкополосных и сверхширокополосных системах, например, в системах связи, основанных на технологии CDMA, и в системах с повышенными требованиями к криптостойкости.

СПИСОК ЛИТЕРАТУРЫ

1. *Olsen J.D., Scholtz R.A., Welch L.R.* // IEEE Trans. 1982. V. IT-28. № 6. P. 858.
2. *Токарева Н.Н.* Нелинейные булевы функции: бент-функции и их обобщения. Saarbrucken: LAP LAMBERT Academic Publishing, 2011.
3. *Cheng F., Hua J., Zhu J. et al.* // 2010 WASE Int. Conf. on Information Engineering. Beidaihe. 14–15 Aug. N.Y.: IEEE, 2010. V. 3. P. 328.
4. *Федоров В.Б., Стариковский А.И., Парамонов А.А., Куликов Г.В.* Библиотека функций для системы MATLAB для расчета параметров нелинейного генератора псевдослучайных последовательностей и генерации таких последовательностей. Свидетельство о гос. рег. программы для ЭВМ № 2012611440. Реестр программ для ЭВМ 07.02.2012 г.
5. *Мак-Вильямс Ф.Дж., Слоен Н.А.* Теория кодов, исправляющих ошибки. М.: Связь, 1977.
6. *Артамкин И.В., Стариковский А.И.* // Изв. вузов СССР. Радиоэлектроника. 1986. Т. 29. № 9. С. 46.