

Последовательности на основе бент-функций для широкополосных систем с кодовым разделением каналов

77-48211/529235

01, январь 2013

Юдачев С. С.

УДК 621.396.4

Россия, МГТУ им. Н.Э. Баумана

judachev@gmail.com

Одной из важнейших тенденций современной техники является внедрение технологий широкополосной передачи и множественного доступа с кодовым разделением каналов в беспроводные системы и сети. Эти технологии позволяют значительно повысить скорости обмена и обработки информационных потоков, обеспечивают высокую помехоустойчивость и конфиденциальность, обладают высокой спектральной эффективностью, расширяют возможности работы в частотных диапазонах, перегруженных радиосредствами.

Так, для использования в сетях мобильной связи, наиболее перспективным признан метод многостанционного доступа с кодовым разделением каналов (CDMA). Этот метод основан на расширении спектра за счет использования псевдослучайных последовательностей (ПСП), обладающих необходимыми корреляционными свойствами, причем наиболее приоритетными в смысле технологической привлекательности признаны ансамбли бинарных последовательностей [1].

Известно достаточно много ансамблей бинарных ПСП, которые могут быть полезны при проектировании широкополосных систем связи – М-последовательности, последовательности Голда, Касами, Лежандра, Гордона-Милза-Уэлча и др. [2].

Однако большая часть ПСП, нашедших практическое применение в широкополосных системах, не свободна от ряда недостатков, в частности, структурная сложность их невелика. Эти и другие факторы побуждают не только искать пути оптимизации ансамблей последовательностей с приемлемыми корреляционными свойствами, но и исследовать новые классы ПСП, особенно обладающие повышенной структурной сложностью, в частности, нелинейные последовательности [3].

В последние годы был предложен целый ряд новых классов последовательностей в частности, последовательности на основе максимально нелинейных или бент-функций [2, 4]. При этом математическим аспектам теории синтеза ПСП зачастую уделяется намного больше внимания, чем разработке алгоритмов практического формирования и

исследованию свойств, что затрудняет оценку возможности их использования и те преимущества, которые они могут обеспечить при проектировании новых широкополосных систем.

Данная работа посвящена одному из перспективных классов нелинейных последовательностей – двоичным последовательностям на основе бент-функций. К их несомненным достоинствам кроме приемлемых свойств относят то, что они могут быть полезны как непосредственно, так и для расширения ансамблей последовательностей Касами.

В работе предложен алгоритм, на основе которого разработана программа, позволяющая формировать ансамбли бинарных бент-последовательностей различной длины и исследовать их основные свойства.

В дальнейшем используем следующие основные обозначения

$\bar{U} = (u_1, u_2, \dots, u_m)$, $\bar{V} = (v_1, v_2, \dots, v_m)$ – двоичные векторы длины m ,
 $\langle \bar{U}, \bar{V} \rangle$ - скалярное произведение этих векторов по модулю 2.

Булева функция от m переменных - произвольная функция отображающая множество двоичных векторов размерностью $m\mathbb{Z}_2^m$ на множество $\mathbb{Z}_2\{0,1\}$.

Аффинная булева функция f от переменных $v_1, v_2, \dots, v_m$

$$f(\bar{V}) = \langle \bar{U}, \bar{V} \rangle \oplus a$$

для некоторого вектора $\bar{U} \in \mathbb{Z}_2^m$ и константы $a \in \mathbb{Z}_2$.

Под расстоянием между двумя булевыми функциями от m переменных понимают расстояние Хэмминга (число координат, в которых вектора различаются) между их векторами длины 2^m .

Максимально нелинейной называют такую булеву функцию от m переменных (m – любое натуральное число), у которой расстояние Хэмминга от данной функции до множества всех аффинных функций является максимально возможным. В случае четного m это максимально возможное расстояние равно $2^{m-1} - 2^{(m/2)-1}$. В случае нечетного m точное значение максимального расстояния неизвестно.

В последнее время используют термины «максимально-нелинейные» функции и «бент-функции», хотя аналогия неполная. При четном числе переменных m эти функции совпадают, а при нечетном m бент-функции, в отличие от максимально-нелинейных не существуют [5].

Для определения бент-функций используют коэффициенты преобразования Уолша-Адамара. Преобразование Уолша-Адамара булевой функции f от m переменных это целочисленная функция W_f , заданная на множестве $\mathbb{Z}_2^m$ двоичных векторов длины m равенством:

$$W_f(\bar{V}) = \sum_{\bar{U} \in \mathbb{Z}_2^m} (-1)^{\langle \bar{U}, \bar{V} \rangle \oplus f(\bar{U})} .$$

Для коэффициентов Уолша-Адамара $W_f(\bar{V})$, $V \in \mathbb{Z}_2^m$, функции f справедливо равенство Парсеваля:

$$\sum_{\bar{V} \in \mathbb{Z}_2^m} (W_f(\bar{V}))^2 = 2^{2m} . \quad (1)$$

Поскольку число всех коэффициентов равно 2^m , из равенства следует, что максимум модуля коэффициента Уолша-Адамара не может быть меньше величины $2^{\frac{m}{2}}$.

Расстояние Хэмминга от произвольной булевой функции f до множества всех аффинных функций тесно связано с коэффициентами Уолша-Адамара этой функции. Это расстояние равно:

$$2^{m-1} - \frac{1}{2} \max_{V \in \mathbb{Z}_2^m} |W_f(\bar{V})| .$$

Очевидно, что чем меньше максимум модуля коэффициента Уолша-Адамара функции f , тем больше это расстояние.

Бент-функцией называют булеву функцию от m переменных (m чётно) такую, что модуль каждого коэффициента Уолша-Адамара этой функции равен $2^{\frac{m}{2}}$. Другими словами, булеву функцию f считают бент-функцией, если максимум модуля $W_f(\bar{V})$ достигает своего минимально возможного значения. В силу равенства Парсеваля (1) это имеет место, только если модули всех коэффициентов Уолша-Адамара этой функции совпадают и равны $2^{\frac{m}{2}}$.

Используя эти определения можно записать алгоритм формирования бент-последовательностей.

Бент-последовательность можно представить согласно [6]:

$$B_z(t) = f_z \left(tr_1^n(a^t), tr_1^n(a^{t+T}), \dots, tr_1^n(a^{t+(m-1)T}) \right) + tr_1^n(a \cdot a^t), \quad (2)$$

Где a – примитивный элемент поля $GF(2^n)$; $n = 2m = 4k$, k – положительное целое; $T = 2^m + 1$, T – положительное целое; tr_1^n – след, представляющий в данном случае М-последовательность длины $2^n - 1$. Здесь:

$$\begin{aligned} f_z(\bar{x}) &= f(\bar{x}) + \langle \bar{z}^T \bar{x} \rangle, \\ a_t &= tr_1^n(a^t). \end{aligned} \quad (3)$$

Функция $f(\bar{x})$ в уравнении (3) представляет собой бент-функцию, $\bar{x}$ – вектор-аргумент размерностью m ; а $\bar{z}^T$ – транспонированный вектор, состоящий из элементов «0» и «1» и имеющий длину m ; выражение $\langle \bar{z}^T \bar{x} \rangle$ обозначает скалярное произведение и означает перебор всех возможных комбинаций координат вектора-аргумента $\bar{x}$. Так как длина векторов $\bar{z}^T$ и $\bar{x}$ равна m , то число комбинаций $\bar{z}^T \bar{x}$ равно 2^m . Отсюда следует, что объем ансамбля бент-последовательностей равен 2^m или, $2^{\frac{n}{2}}$. След $tr_1^n(a^{t+T})$ является циклическим сдвигом М-последовательности на T элементов, $tr_1^n(a \cdot a^t) = tr_1^n(a^{t+T})$ – единичный циклический сдвиг этой М-последовательности.

Бент-функция $f(\bar{x})$ имеет в качестве аргумента вектор $\bar{x} = (x_1, x_2, \dots, x_m)$, где $x_1 = a_t, x_2 = a_{t+T}$ и $x_m = a_{t+(m-1)T}$. Примитивный полином для формирования М-последовательности может быть выбран в соответствии с [7].

Аналитическое выражение для $f(\bar{x})$ имеет вид:

$$f(\bar{x}) = x_1 \cdot x_2 \oplus x_3 \cdot x_4 \oplus \dots \oplus x_{m-1} \cdot x_m .$$

Здесь $x_{m-1} \cdot x_m$ - поэлементное перемножение соответствующих М-последовательностей.

В правиле формирования бент-последовательностей (2) используются М-последовательности длины $2^n - 1$. Поэтому длина бент- последовательностей также равна $2^n - 1$. Так как бент-функции существуют только при четном m , а $n = 2m$, то очевидно, что $n = 0 \pmod{4}$.

Алгоритм формирования ансамбля бент-последовательностей длины $2^n - 1$, может быть записан в следующем виде:

1. Выбор положительного целого $n = 0 \pmod{4}$.
2. Формирование М-последовательности a_t длины $2^n - 1$ в соответствии с выбранным примитивным полиномом степени n .
3. Формирование $m - 1$ циклического сдвига последовательности a_t на величину $T = 2^m + 1$, а также циклического сдвига a_t на 1 элемент.
4. Нахождение первой бент-последовательности из выражения (2) при условии $\bar{z}^T = (0, 0, \dots, 0)$, так что в уравнении (3) $f_z(\bar{x}) = f(\bar{x})$. Аргументами f_z являются найденные в п. 3 сдвиги М-последовательностей.
5. Остальные бент-последовательности ансамбля получаются путем суммирования по модулю 2 бент-последовательности, полученной в п. 4, и различных комбинаций сдвигов М-последовательностей. Эти комбинации вычисляются скалярным произведением $\langle z^T x \rangle$.

Рассмотрим формирование двух бент-последовательностей при $n = 4$. Последовательности столь малой длины практически бесполезны и выбраны здесь только для иллюстрации алгоритма. Очевидно, длина последовательностей равна $N = 2^4 - 1 = 15$. Выберем примитивный полином $p(x) = x^4 + x + 1$ [7] . Данному полиному соответствует М-последовательность:

$$a_t = \{1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0\}.$$

Далее запишем необходимые для генерации циклические сдвиги a_t :

$$a_{t+1} = \{0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1\},$$

$$a_{t+B} = \{1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0\}.$$

В соответствии с (2) первая бент-последовательность равна $B_1 = a_t \cdot a_{t+B} \oplus a_{t+1}$. Тогда:

$$a_t \cdot a_{t+B} = \{1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0\},$$

$$B_1 = \{1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1\}.$$

Вторую бент -последовательность находят при равенстве вектора $\bar{z}^T = \{0, 1\}$. Так

как $\langle \bar{z}^T \bar{z} \rangle = a_{t+B}$ (учитывая, что $\bar{x} = \{a_t, a_{t+B}\}$), то вторая бент-последовательность ансамбля вычисляется по формуле $B_2 = B_1 + a_{t+B}$:

$$B_2 = \{0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1\}$$

Аналогичным образом можно вычислить B_3 и B_4 .

Используя приведенный алгоритм и программу были сформированы ансамбли бент-последовательностей и исследованы их свойства до длины $2^{12} = 4095$ ($n=12$). В таблице 1 приводятся параметры для ансамблей бент-последовательностей трех различных длин: 15, 255 и 4095, в таблице 2- пример последовательностей длины 255.

Таблица 1

Параметры ансамблей бент-последовательностей

N	n	T	V	Порождающий полином $p(x)$ исходной М-последовательности
15	4	5	4	$x^4 + x + 1$
255	8	17	16	$x^8 + x^4 + x^3 + x^2 + 1$
4095	12	65	64	$x^{12} + x^6 + x^4 + x + 1$

Таблица 2

Последовательности длины 255

Ансамбль Бент-последовательностей при $N=255$
11000110010100111100010101100000111110110101001000110001110001001001101100110000 11001111010101100100000010100111110001110111110011000011000100110101100000111001 01110111011110101101000110001011000011110101101011001011011010010001010100011010 111101001101010
00111111000100011011101011100101000110000001001001110110110101100111101101010100 0101010011000110000101100111000110011111000000010111110011001110001101101011010 10111001000110000000001110100010010111001110000111110110100100110111001110111001 111100111000000
0011100101011000000000111110000001110101011101111110001000011011010110000010000 01100010111110101111000001011100101111011001010001000101110101001100010011111100 1101001100101000011101101111110101110100101011100000011000101111000110110110001 000100011101110

В работе проводится исследование бент-последовательностей для широкополосных систем с кодовым разделением каналов. Такие системы могут работать как в синхронном, так и в асинхронном режиме. Поскольку разделение каналов основано на корреляционной обработке, очевидно, что одним из основных направлений исследований должны быть расчеты корреляционных функций и характеристик.

Представляют интерес следующие разновидности корреляционных функций. Последовательности $a = \{a_1, a_2, \dots, a_N\}$ и $b = \{b_1, b_2, \dots, b_N\}$ являются бинарными и принимают значения «+1» или «-1». Тогда сумма вида:

$$R(k) = \sum_{i=1}^N a_i \cdot b_{i-k} \quad (4)$$

где N – длина последовательности, k – значение текущего сдвига между последовательностями, называется корреляционной функций (КФ) двух последовательностей.

1. Периодическая автокорреляционная функция (ПАКФ), определяемая выражением $R_{\text{ПАКФ}}(k) = \sum_{i=1}^N a_i \cdot a_{i-k}$. Сдвиг k является *циклическим*.
2. Аperiodическая автокорреляционная функция (ААКФ), определяется так же, как ПАКФ, за исключением того, что сдвиг k – *ациклический*. То есть элементы сдвигаемой последовательности не перемещаются в начало, а исключаются при вычислении КФ.
3. Периодическая взаимокорреляционная функция (ПВКФ), определяемая выражением (4). Сдвиг k – *циклический*.
4. Аperiodическая взаимокорреляционная функция (АВКФ), определяемая выражением (4). Сдвиг k – *ациклический*.
- 5.

Одной из основных задач при синтезе последовательностей для широкополосных систем является поиск ансамблей с наименьшим значением максимального бокового выброса u_{max} ААКФ, а также наименьшим их количеством.

Удобным инструментом для оценки корреляционных свойств является вычисление статистических характеристик корреляционных функций. К таким характеристикам относят:

- 1) Значение максимального положительного бокового выброса КФ $u_{\text{б max}}$;
- 2) Количество максимальных положительных боковых выбросов $N_{\text{б max}}$;
- 3) Значение максимального отрицательного бокового выброса КФ $u_{\text{б min}}$;
- 4) Количество максимальных отрицательных боковых выбросов $N_{\text{б min}}$;
- 5) Математическое ожидание модуля боковых выбросов $m(|u_{\text{б}}|)$;
- 6) Математическое ожидание боковых выбросов $m(u_{\text{б}})$;
- 7) Среднеквадратическое отклонение модуля боковых выбросов $\sigma(|u_{\text{б}}|)$;
- 8) Среднеквадратическое отклонение боковых выбросов $\sigma(u_{\text{б}})$;
- 9) Максимальный нормированный уровень выбросов (боковых для АКФ):

$$\chi_{\max} = \frac{(|u_{\delta \max}|, |u_{\delta \min}|)_{\max}}{N} \cdot 100\% ,$$

где запись $(x, y)_{\max}$ означает выбор наибольшего значения из x и y ;

10) Средний нормированный уровень выбросов (боковых для АКФ):

$$\chi_{\text{ср}} = \frac{m(|u_{\delta}|)}{N} \cdot 100\% ;$$

11) Количество нулей и единиц в последовательности.

Поскольку для расчета КФ и статистических характеристик требуется большой объем вычислений, на основе приведенного алгоритма была разработана специальная программа. В качестве среды разработки был выбран Microsoft Visual Studio 2010 Professional, предоставляющий широкие функциональные возможности. Данный программный продукт является одним из лидеров на рынке сред разработки и может служить универсальным инструментом для программиста. Выбор языка программирования C# в качестве базисного обусловлен необходимостью разработки не только программного алгоритма, но и пользовательского графического интерфейса для работы с программой «Windows Forms», в котором наиболее удобно работать с языком C#. В программном проекте можно выделить следующие основные компоненты:

- 1) «Program.cs»;
- 2) «Form1.cs»;
- 3) «Form3.cs»;
- 4) «Form5.cs».

Файл «Program.cs» содержит два основных класса: *Bent* и *Program*. В классе *Bent* определена функция «calcBentSeq», вычисляющая ансамбль Бент-последовательностей, а также процедуры для вычисления КФ Бент-последовательностей: CalcPAKF_B», «CalcPVKF_B», «CalcAAKF_B» и «CalcAVKF_B». В классе *Program* написан код функции «Ber_Mas», реализующей алгоритм вычисления линейной сложности исследуемых последовательностей. Разумеется, здесь описывается только часть используемых в программе функций и процедур. Остальные компоненты программы предназначены для ввода исходных данных и наглядного вывода результатов.

Используя приведенные алгоритм и программу на его основе были сформированы ансамбли бент-последовательностей и рассчитаны их характеристики. Из исследованных наибольший практический интерес представляют характеристики бент-последовательностей длины $N=4095$, часть из которых приведена ниже.

Периодические корреляционные функции этого ансамбля могут принимать три следующих значения: -65 , -1 и 63 . Примечательно, что и ПАКФ и ПВКФ имеют одинаковые статистические характеристики за исключением одного параметра: математическое ожидание выбросов для ПАКФ равно $m(u_{\delta}) = -1.0$, а для ПВКФ $m(u_{\delta}) = 0$. Среднеквадратическое отклонение (СКО) выбросов составляет $\sigma(u_{\delta}) = 63.5$.

Математическое ожидание модуля выбросов $m(|u_6|) = 63$, СКО модуля выбросов $\sigma(|u_6|) = 7.8$. Что касается максимального и среднего уровней выбросов периодических КФ ансамбля, то они равны $\chi_{max} = 1.6\%$ и $\chi_{cp} = 1.5\%$ от величины главного пика АКФ соответственно.

Апериодические автокорреляционные функции имеют границы упаковки от -187 до 165. Каждая ААКФ имеет 2÷4 максимальных положительных боковых выброса и столько же максимальных отрицательных выбросов. Математическое ожидание модуля выбросов находится в пределах $m(|u_6|) = (36.2 \div 37.4)$, а СКО модулям выбросов – $\sigma(|u_6|) = (25.4 \div 26.8)$. Значения неосновных выбросов характеризуются величинами: $m(u_6) = -0.5$, $\sigma(u_6) = (44.2 \div 45.9)$. Параметр χ_{max} в пределах (3.0÷4.6), а средний нормированный уровень боковых лепестков для всех последовательностей равен $\chi_{cp} = 0.9$

Выбросы апериодических ВКФ ансамбля бент-последовательностей при $N = 4095$ имеют значения от -201 до 185. АВКФ имеют 1÷3 максимальных положительных выброса, а также 1÷4 максимальных отрицательных. Остальные статистические характеристики ААКФ и АВКФ практически совпадают, за исключением границ значений математического ожидания выбросов и максимального уровня боковых выбросов, которые для АВКФ составляют $m(u_6) = (-0.5 \div 0)$ и $\chi_{max} = (3.1 \div 4.9)$.

В таблице 3 приводится сводка характеристик исследованных ансамблей бент-последовательностей длины 4095 элементов.

Таблица 3

Статистические характеристики бент-последовательностей

Характеристики бент-последовательностей $N=4095$									
Для периодических автокорреляционных функций									
$u_6 \max$	$u_6 \min$	$m(u_6)$	$m(u_6)$	$\sigma(u_6)$	$\sigma(u_6)$	$\chi_{\max},\%$	$\chi_{cp},\%$		
63	-65	63	-1.0	7.8	63.5	1.6	1.5		
Для аperiodических автокорреляционных функций									
$u_6 \max$	$N_6 \max$	$u_6 \min$	$N_6 \min$	$m(u_6)$	$m(u_6)$	$\sigma(u_6)$	$\sigma(u_6)$	$\chi_{\max},\%$	$\chi_{cp},\%$
119÷ 165	2÷4	(- 187) ÷ (-118)	2÷ 4	36.2÷ 37.4	-0.5	25.4÷ 26.8	44.2÷ 45.9	3.0÷ 4.6	0.9
Для периодических взаимокорреляционных функций									
$u_6 \max$	$u_6 \min$	$m(u_6)$	$m(u_6)$	$\sigma(u_6)$	$\sigma(u_6)$	$\chi_{\max},\%$	$\chi_{cp},\%$		
63	-65	63	0	7.8	63.5	1.6	1.5		
Для аperiodических взаимокорреляционных функций									
$u_6 \max$	$N_6 \max$	$u_6 \min$	$N_6 \min$	$m(u_6)$	$m(u_6)$	$\sigma(u_6)$	$\sigma(u_6)$	$\chi_{\max},\%$	$\chi_{cp},\%$
118÷ 185	1÷ 3	(- 201)÷ (-118)	1÷ 4	36.2÷ 37.4	(- 0.5)÷ 0	25.4÷ 26.8	44.2÷ 45.9	3.1÷ 4.9	0.9

Результаты исследования бент-последовательностей:

- 1) Все бент-последовательности являются сбалансированными.
- 2) Периодические автокорреляционные функции Бент-последовательностей имеют трехуровневую структуру. Среднеквадратическое отклонение модуля боковых выбросов у всех ПАКФ стремится к значению $\sigma(|u_6|) \rightarrow \sqrt{N}$. Математическое ожидание неосновных выбросов для исследуемых семейств составляет $m(u_6) = -1.0$.
- 3) Максимальный и средний уровни боковых лепестков при увеличении N значительно уменьшаются. Для бент-последовательностей длины 4095 элементов они не превышают 1.6 % от величины главного пика.
- 4) Аperiodические автокорреляционные функции исследуемых семейств бент-последовательностей имеют не менее 2 максимальных положительных боковых выбросов, а также не менее двух максимальных отрицательных боковых выбросов. Математическое ожидание боковых выбросов составляет $m(u_6) = -0.5$ для данных ансамблей. С увеличением длины последовательностей максимальный и средний уровень боковых выбросов уменьшается. Для последовательностей при $N=4095$ χ_{cp} составляет 0.9 % от величины основного выброса.
- 5) Периодические взаимокорреляционные функции бент-последовательностей имеют трехуровневую структуру, причем значения выбросов соответствуют значениям выбросов ПАКФ. Характеристики ПАКФ и ПВКФ практически совпадают.
- 6) Аperiodические взаимокорреляционные функции исследуемых ансамблей имеют от 1 до 4 максимальных положительных выбросов, а также от 1 до 4 максимальных отрицательных выбросов. Математическое ожидание выбросов для подавляющего большинства АВКФ составляет $m(u_6) = 0$. Максимальный и средний уровни боковых лепестков при увеличении N значительно уменьшаются. Для бент-последовательностей длины 4095 элементов они не превышают значений 4.9 % и 0.9 % от длины последовательности N .

Полученные результаты хорошо согласуются с теоретическими оценками свойств бент-последовательностей [2].

Заключение

Предложенные алгоритм и программа на его основе позволяют достаточно быстро и наглядно сформировать образцы бент-последовательностей различной длины и исследовать их основные свойства. Важно также, что этот метод основан на использовании различных копий М-последовательностей, широко используемых в настоящее время. На основе проведенных расчетов можно сделать вывод о перспективности применения бент-последовательностей для проектируемых широкополосных систем с кодовым разделением каналов.

Список литературы

1. Калмыков В.В., Федоров И.Б., Юдачев С.С. Системы сотовой и спутниковой связи. М.: Рудомино, 2010. 280 с.
2. Golomb S.W., Gong G. Signal design for good correlation for wireless communication, cryptography, and radar. New York: Cambridge University Press, 2005. 438 p.
3. CDMA: прошлое, настоящее, будущее / под ред. Л.Е. Варакина и Ю.С. Шинакова. М.: МАС, 2003. 608 с.
4. Ипатов В.П. Широкополосные системы и кодовое разделение сигналов. Принципы и приложения: пер. с англ./ под ред. В.П. Ипатова. М.: Техносфера, 2007. 488 с.
[Valery P.Ipatov. Spread Spectrum and CDMA. Principles and Applications. New York: John Wiley and Sons Ltd, 2005.].
5. Токарева Н.Н. Сильно нелинейные булевы функции: Бент-функции и их обобщения: дисс. ... канд. ф.-м. наук. Новосибирск, 2008. 120 с.
6. Cheng J. Hua, J. Zhu, L. Tong, L. Meng. Fast generation method of bent sequences and its application in ADS simulation. // WASE International Conference on Information Engineering, China, Beidaihe, 2010. С. 328-331.
7. Шумоподобные сигналы в системах передачи информации / В.Б. Пестряков, В.П. Афанасьев, В.Л. Гурвиц, Д.Л.Зайцев, Л.И.Зеликман, А.В.Пестряков, А.Л.Сенявский, Н.И.Смирнов; под ред. В.Б. Пестрякова. М.: Советское радио, 1973. 424 с.