УДК 621.396.43

Псевдослучайные двоичные последовательности с нулевой зоной автокорреляции и боковыми выбросами ±(p+1)

Е.И. Кренгель

Рассматриваются сбалансированные двоичные псевдослучайные последовательности длины p×(p+1) большой линейной сложности, построенные на основе матрицы декомпозиции m-последовательности длины $N=p^2-1$ над GF(p) и последовательностей длины p с идеальной автокорреляцией. Показывается, что для всех p>3 они имеют четырехуровневую периодическую автокорреляционную функцию (ПАКФ) с боковыми выбросами ± (p+1) и регулируемой нулевой зоной автокорреляции (ZACZ). Найдены выражения для общего числа полученных последовательностей и их линейной сложности. Приведена блок-схема генератора этих последовательностей.

Введение

Двоичные псевдослучайные последовательности с идеальной автокорреляцией длины 2^n-1 [1,2,3] и почти идеальные двоичные последовательности длины $2(p^m+1)$, где $p>2$ – простое число, [4,5,6] широко применяются во многих областях связи, радиолокации и навигации. Двоичная последовательность называется почти идеальной, если ее периодическая автокорреляционная функция при всех ненулевых сдвигах, кроме одного, равна нулю [5]. В мобильных системах широкополосной связи, подвергающихся воздействию многолучевости, такие последовательности используются для синхронизации, оценки канала и измерения дальности. Наряду с ними большой интерес представляют последовательности, обладающие нулевой зоной корреляции (ZCZ) при ненулевых сдвигах [3]. Однако большинство известных ZCZ-последовательностей имеют достаточно большие боковые выбросы автокорреляции вне нулевой зоны [7,8], сопоставимые со значением основного пика, что ухудшает характеристики поиска и обнаружения сигналов.

Целью настоящей работы является построение ансамблей сбалансированных двоичных последовательностей с относительно широкой нулевой зоной автокорреляции (ZACZ) и малыми значениями боковых выбросов за ее пределами.

Конструирование

Пусть $p=4t-1>2$ – простое число, α и β – примитивные элементы полей $GF(p^2)$ и $GF(p)$ соответственно и $\mathbf{a}=\{a_i\}$ – p-ичная m-последовательность длины $N=p^2-1$ с элементами $a_i = Tr_1^2(\alpha^i) = \sum_{j=0}^{1} \alpha^{ip^j}$, $0\leqslant i<p^2-1$.

Рассмотрим матрицу декомпозиции $\mathbf{A}$ последовательности $\mathbf{a}$ по столбцам, состоящую из $T=(p^2-1)/(p-1)=p+1$ строк и $p-1$ столбцов [1]. Эта матрица содержит единственную строку с номером $T/2$, состоящую из всех нулей, тогда как остальные являются циклическими сдвигами некоторой короткой p-ичной m-последовательности (последовательности степеней некоторого первообразного корня g по модулю p) длины $p-1$. Обобщая результаты [9] для $p>2$, находим, что последовательность

$$\boldsymbol{e}=\{\boldsymbol{e}_i\}=\begin{cases}\infty, & (\mathrm{Tr}_1^2(\alpha^{T/2}))=0\\ \mathrm{ind}_\beta(\mathrm{Tr}_1^2(\alpha^j)), & (\mathrm{Tr}_1^2(\alpha^j))\neq 0\end{cases}, \qquad (1)$$

где $0\leqslant j<p^2-1$, $ind_\beta x$ – индекс (логарифм) x по основанию β, есть последовательность сдвигов, первые p целочисленных элементов которой определяют значения циклических сдвигов строк матрицы декомпозиции относительно некоторой исходной m-последовательности длины $p-1$, а символ ∞ указывает на последовательность из всех нулей. Из определения (1) следует, что для всех $0\leqslant i=k+j(p+1)<N$ имеет место $e_{k+j(p+1)}=(ek+j) \bmod p-1$, $k=0,2,\ldots p$, $j=0,1,\ldots p-2$. Подобно теореме 2 [9], основное свойство последовательности сдвигов для случая $p>2$ может быть сформулировано следующим образом. Для любых фиксированных $l\in \boldsymbol{Z}\ (p^2-1)$ каждый

элемент из $Z(p-1)$ появляется в разностях $(\mathbf{e}_k - e_{k+l}) \bmod (p-1)$, $k=0,1,2,...p$, точно один раз. В дальнейшем под последовательностью сдвигов мы будем подразумевать первые $T=p+1$ ее членов, т.е. $\mathbf{e}=\{ek\}$. Обозначим через $e(i)=\{e_{i+k}\}$, $0\leqslant i<p^2-1$, $0\leqslant k\leqslant p$, последовательность сдвигов, соответствующую i-му сдвигу исходной p-ичной m-последовательности, при этом положим $\mathbf{e}=e(0)$. Очевидно, все элементы такой последовательности, за исключением одного, могут принимать значения от 0 до $p-2$. Заменим в матрице $\mathbf{A}$ все ненулевые строковые последовательности соответствующими сдвигами некоторой двоичной псевдослучайной последовательности $\boldsymbol{c}$ длины p с идеальной автокорреляцией (двухуровневой ПАКФ со значениями p и -1), а строку из $p-1$ нулей заменим соответственно строкой из p нулей. При этом образуется новая матрица $\mathbf{A}^*$ порядка $(p+1)\times p$. Далее производим над матрицей $\mathbf{A}^*$ операцию, обратную декомпозиции последовательности. В результате получаем новую сбалансированную двоичную последовательность $\mathbf{b}$ длины $p(p+1)$ с общим членом:

$$b_i = c_{(ind_\beta(Tr_1^2(\alpha^k))+j) \bmod p}, \qquad (2)$$

где $0\leqslant i=k+j(p+1)<N$, $0\leqslant k\leqslant p$, $0\leqslant j\leqslant p-1$.

Пример 1. Пусть $p=7$ и $p(x)=x^2+x+3$ – примитивный полином над GF(7). Тогда матрица декомпозиции $\mathbf{A}$ m-последовательности а длины 48 над GF(7) имеет вид, представленный в *табл. 1*. Из *табл. 1* находим $\mathbf{e}=\{3,4,3,1,\infty,5,2,4\}$. Пусть последовательность $\mathbf{c}$ есть m-последовательность 1001110. После замещения получаем следующую матрицу (*табл. 2*), из которой восстанавливаем искомую последовательность $b=\{111001011110001110110110010100111011000000000011001010101\}$.

Таблица 1.

i/j	0	1	2	3	4	5	e_i
0	4	6	4	5	1	3	3
1	4	5	1	3	2	6	4
2	4	6	4	5	1	3	3
3	3	2	6	4	5	1	1
4	0	0	0	0	0	0	∞
5	5	1	3	2	6	4	5
6	2	6	4	5	1	3	2
7	4	5	1	3	2	6	4

Таблица 2.

i/j	0	1	2	3	4	5	6
0	1	1	1	0	1	0	0
1	1	1	0	1	0	0	1
2	1	1	1	0	1	0	0
3	0	0	1	1	1	0	1
4	0	0	0	0	0	0	0
5	1	0	1	0	0	1	1
6	0	1	1	1	0	1	0
1	1	1	0	1	0	0	1

Автокорреляция

При рассмотрении автокорреляции полученных последовательностей воспользуемся свойствами последовательностей сдвига. Пусть A*(i), 0Ji<p(p+1), есть декомпозиционная матрица i-го сдвига последовательности b. Покажем, что число совпадающих строк в матрицах A* и A*(i) при iA0 и pA3 может быть равно 0, 1, 2. Действительно, при сдвигах i=j(p+1) совпадает только одна строка из нулей. При остальных сдвигах может иметь место «совпадение» или «отставание» фаз ненулевых строковых последовательностей относительно соответствующих строк матрицы A(i). Это может приводить к следующему:

- отсутствию совпадения в тех позициях, в которых оно имело место для $\mathbf{A}$ и $\mathbf{A}(i)$;
- появлению дополнительных совпадений.

Очевидно, что число дополнительных совпадений не может быть более одного, т.к. в противном случае это противоречило бы свойству последовательности сдвигов. Таким образом, число совпадений может принимать три значения: 0, 1, 2. Соответствующие им значения ПАКФ будут равны $-(p+1)$, 0 и $p+1$. В результате ПАКФ будет 4-уровневой, со значениями $-(p+1)$, 0, $p+1$ и $p(p+1)$. Исключение составляет случай $p=3$, при котором число совпадений при ненулевых сдвигах принимает два значения: 0 и 1, и ПАКФ оказывается 3-уровневой.

Из свойств последовательности сдвига следует, что если значения ее первых $p+1$ элементов $e_i\leqslant p-3$, то длина нулевой зоны автокорреляции $ZACZ\geqslant p+1$. Соответственно, если значения элементов $e_i\leqslant p-4$, то $ZACZ\geqslant 2(p+1)$ и т.д. Поэтому, выбирая различные фазы сдвиговой последовательности, можно менять величину этой зоны. Для получения максимально возможной величины нулевой зоны автокорреляции предлагается воспользоваться следующей процедурой.

1. Находим все фазы последовательностей сдвигов $\boldsymbol{e}(i)$, для которых разность t между наименьшим и наибольшим значениями элементов этой последовательности, взятая по модулю $p-1$, является максимальной.

2. Среди найденных на шаге 1 последовательностей сдвигов выбираем такую, у которой расстояние Δ, измеряемое числом сдвигов влево между первым максимальным и последним минимальным элементами, максимально. Назовем эту последовательность сдвигов оптимальной (в общем случае таких последовательностей может быть несколько).

3. На основе этой оптимальной последовательности сдвигов и последовательности $\mathbf{c}$ длины p с идеальной

автокорреляцией строим новую последовательность **b** с максимально возможным значением ZACZ.

Можно показать, что в этом случае длительность ZACZ нулевой зоны автокорреляции около главного лепестка равна

$$ZACZ= (t-1)(p+1)+(\Delta-1). \qquad (3)$$

Формула (3) справедлива для всех p, за исключением p=3. В этом случае **e**={1,1,u,1} и t=1. Однако последовательность b=110111010000, построенная на основе e(0), имеет ПАКФ={12 0 0 0 0 -4 -4 -4 0 0 0 0} с ZACZ=4. Поэтому для общности положим здесь t=2 и D=1. Вместе с тем необходимо отметить, что любая последовательность сдвигов **e**(i) содержит информацию, по которой можно оценить величину параметра t. Расположим для этого все целочисленные элементы некоторой сдвиговой последовательности **e**(i) в порядке возрастания. Обозначим полученную последовательность через $\varepsilon(i)=\{\varepsilon_{ik}\}$, где $\varepsilon_{ik}\leqslant\varepsilon_{ik+1}$, $0\leqslant k<p$. Пусть $d_i=\max\{(\varepsilon_{ik+1}-\varepsilon_{ik}),\ 0\leqslant k<p;\ (\varepsilon_{i0}-\varepsilon_{ip-1}) \bmod (p-1)\}$, т.е. d_i есть максимум разностей (по модулю p–1) соседних элементов последовательности $\varepsilon(i)$, выбираемых по циклу в порядке убывания их номеров. Тогда, в силу свойств последовательности сдвигов, будет справедливо следующее неравенство: $d_i\leqslant t\leqslant d_i+1$. Последнее означает, что t всегда равно d_i или d_i+1, $|d_i-d_l|$ = 0 либо 1, $0\leqslant i<N$, $0\leqslant l<N$.

Пример 2. В случае примера 1 оптимальная последовательность сдвигов равна **e**(37)={3,0,2,2,3,2,0,∞} и имеет параметры t=3 и Δ=2. На основе **e**(37) строим последовательность b=11001010101111001011110001110110110010100111011000000000 со следующей ПАКФ:(56 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 -8 0 0 0 -8 -8 0 0 8 -8 -8 -8 8 0 0 -8 -8 0 0 0 -8 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0). Отсюда находим ZACZ=17. Такой же результат получаем, используя формулу (3): ZACZ=8×(3–1)+2–1=17. Результаты расчета оптимальных значений ZACZ для других семи примитивных полиномов степени 2 над GF(7) приведены в *табл. 3*.

Таблица 3.

№	Примитивный полином	ZACZ
1	x^2+2x+5	19
2	x^2+6x+3	
3	x^2+4x+5	18
4	x^2+5x+3	
5	x^2+x+3	17
6	x^2+5x+5	
7	x^2+2x+3	10
8	x^2+3x+5	

Пример 3. Пусть p=11 и x^2+2x+6 – примитивный полином над GF(11). Соответствующая этому полиному сдвиговая последовательность **e**={1,6,4, 3,4,1,∞,7,1,1,3,6}.С помощью описанной выше процедуры находим оптимальную последовательность сдвигов {6,0,0,2,5,1,6,4, 3,4,1,∞} с параметрами t=4 и Δ=10. Выберем в качестве короткой последовательности с нулевым сдвигом последовательность Лежандра вида 11011100010. Тогда сконструированная на их основе последовательность b={0110110111100111000111000001010101011110110001001101100001011100011010010001010100000011001010010000111111011110101000100111110110} имеет ПАКФ: (132 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 -12 -12 0 0 -12 0 -12 -12 0 -12 -12 0 12 12 0 -12 0 -12 12 12 -12 12 12 -12 0 -12 0 12 12 0 -12 -12 0 -12 -12 0 -12 0 0 -12 -12 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0) с ZACZ=45. Такой же результат получается из формулы (3): ZACZ=12×(4–1)+10–1=45.

Пример 4. Пусть p=31 и x^2+x+12 – примитивный полином над GF(31). Соответствующая этому полиному последовательность сдвигов имеет вид: **e**={3,12,15,9,4,8,27,2,4,17,10,21,1,1,15,1,∞,17,2,19, 20,11,1,9,27,26,22,4,1,7,14,12}. Отсюда находим оптимальную последовательность **e**(122)={25,7,4,10, 17,15,7,16,19,13,8,12,1,6,8,21,14,25,5,5,19,5,∞,21, 6,23,24,15,5,13,1,0} с параметрами t=5 и Δ=1. Пусть **c** есть последовательность Лежандра длины 31 вида 1001001000011101010001111011011. В этом случае компьютерный расчет ПАКФ последовательности **b**={000011000101010100000001111101011001000100 0 1 0 0 0 1 1 1 1 1 0 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 0 1 0 0 1 1 0 0
100101001001001101100001000010110011100010010110000111001010111000100100100001000100110110111011111101001001101000101100111100000101011101011111100100111101101001101011110011111000011001111110000011011110101011100101011000111011111100000110010100010010111101100110111101001011100011010111011100000010001101011110011100100110001111111000000110110011100101100011100000001001001010101111110111101000000000101011001000111101101101000100010010001010101100110111111011010110011110111110100101010011110100100011011010000111110110011111001010110011110110001100100111010001111000011110100000011001000000011100010100100010110111101110101110011110110011000111011001101010011101111100010101011111100100111000011010100101100010000111100101011010010100

0100111010011110111001010001010010010101000
1101000000101111111111110000001010010010001
0011000010100001100110000001011001010001100
1110101011111100011111111110001101011000110
0000001100111} длины 992 дает значение ZACZ=128. Это совпадает со значением ZACZ, вычисленным по формуле (3). Ниже, в *табл. 4,* приведены результаты расчета ZACZ для всех $p \leqslant 31$, а также для p=43 и p=127.

Таблица 4.

p	Многочлен	L	t	Δ	ZACZ
3	x^2+x+2	12	2	1	4
7	x^2+2x+5	56	3	4	19
11	x^2+2x+6	132	4	10	45
19	x^2+x+2	380	5	4	83
23	x^2+x+7	552	3	19	66
31	x^2+x+12	992	5	1	128
43	x^2+x+3	1892	6	5	224
127	x^2+x+3	16256	4	107	490

Уникальность

При конструировании последовательностей длины $p(p+1)$ правомерен вопрос: насколько их длина уникальна по отношению к другим известным двоичным последовательностям с нулевой зоной автокорреляции. Поскольку многие ZCZ-последовательности имеют длину, равную степени числа 2, ограничимся рассмотрением почти идеальных двоичных последовательностей длины $2(p^m+1)$. Расчеты показали, что для всех $p \leqslant 443$, исключая 7, полученные последовательности имеют длину, отличную от последовательностей с почти идеальной автокорреляцией. Более того, было обнаружено, что для всех оканчивающихся на 1 или 3 значений $p=4t+1$ число $p(p+1)/2-1$ всегда кратно 5 и в то же время не является степенью числа 5. Для доказательства положим $p=10u+1$. Тогда число $p(p+1)/2-1=50u^2+15u$ кратно 5. Далее, замечаем, что в выражении $(50u^2+15u)/5=u(10u+3)$ второй сомножитель $10u+3$ не кратен 5. Поэтому $p(p+1)/2-1$ не может являться степенью числа 5. Аналогичными рассуждениями это утверждение доказывается для всех p, оканчивающихся на 3.

Число последовательностей

Количество различных 4-уровневых последовательностей длины $p(p+1)$ при оптимальной сдвиговой последовательности вычисляется по формуле:

$$V=\varphi(p^2-1)U/2, \qquad (4)$$

где φ – функция Эйлера, а U – число различных двоичных последовательностей длины p с идеальной функцией автокорреляции. В качестве таких последовательностей могут быть использованы m-последовательности, последовательности Лежандра, Холла, а также последовательности No-Golomb-Gong-Lee-Gaal [1,2]. Ниже, в *табл. 5,* приведены результаты расчета значений V для всех $p \leqslant 31$, а также p=43 и 127.

Таблица 5.

p	L	U	$\varphi(p^2-1)/2$	V	*Тип c*	LC(c)	LC
3	12	1	2	2	Z	2	8
7	56	2	8	16	Z	3	24
11	132	2	16	32	L	10	120
19	380	2	48	96	L	18	360
23	552	2	80	160	L	11	264
31	992	8	128	1024	Z/L	5/15	160/480
43	1892	8	240	1920	H	43	1892
127	16256	80	2304	184320	L	63	8064

Линейная сложность

Результаты компьютерного расчета линейной сложности LC(b) последовательностей **b** для $p \leqslant 31$ методом Берлекэмпа-Месси приведены в *табл. 5*. Буквами *Z*, *H* и *L* здесь обозначены последовательности **c**, принадлежащие соответственно к семействам Зингера (m-последовательности), Холла и Лежандра. При этом предполагалось, что линейная сложность m-последовательностей и последовательностей Холла равна соответственно n и p [10], а линейная сложность последовательностей Лежандра в зависимости от p может принимать следующие значения: $(p-1)/2$, если $p=8k-1$ и $p-1$, если $p=8k+3$ [11]. Полученные расчетные данные дают основание сделать вывод, что в общем случае линейная сложность последовательности **b** выражается следующей формулой:

$$LC(\mathbf{b})=(p+1)\,LC(\mathbf{c}), \qquad (5)$$

где $LC(\mathbf{c})$ – линейная сложность короткой последовательности **c**.

Реализация

В зависимости от значений p i-й элемент последовательности **b** может быть вычислен двумя способами. При небольших p предварительно вычисляется последовательность сдвигов $\{e_k\}$, значения которой записываются в устройство памяти (например, ПЗУ) и затем циклически (с периодом p) используются для формирования адреса $(e_k + j)$ *mod* p элементов ко-

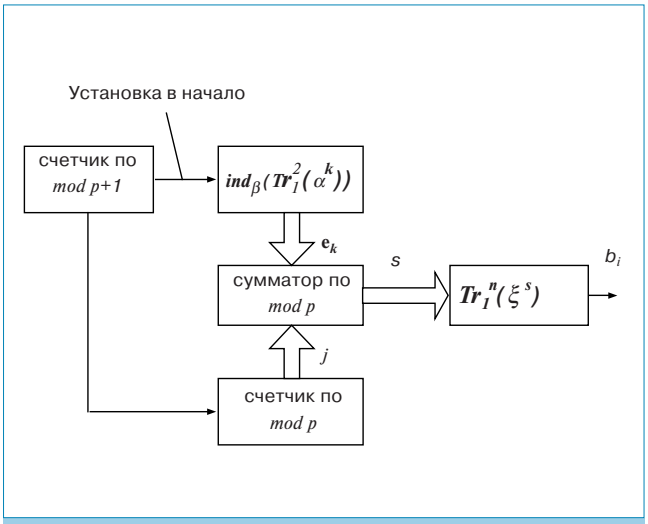

Рис. 1. Блок-схема генератора последовательности с нулевой зоной автокорреляции на основе короткой m-последовательности длины p

роткой последовательности **c**, также находящейся в памяти. Подобная идея использовалась и для генерации последовательностей Гордона-Милза-Велча [12]. В случае же больших p на каждом такте более целесообразно вычислять текущее значение $e_k = ind_\beta(Tr_1^2(\alpha^k))$. В результате объем необходимой памяти, которая теперь в основном расходуется на хранение последовательности **c**, сокращается в два и более число раз. Существенное упрощение получается sпри $p=2^n-1$, когда в качестве последовательности **c** выбирается m-последовательность. В этом случае формула (2) преобразуется к виду:

$$b_i = Tr_1^n(\xi^{(ind_\beta(Tr_1^2(\alpha^k))+j) \bmod p}), \qquad (6)$$

где ξ – примитивный элемент поля Галуа GF(2^n). Блок-схема генератора по формуле (6) представлена на *рис. 1*.

Заключение

Построены новые ансамбли сбалансированных двоичных псевдослучайных последовательностей длины $p\times(p+1)$ со сравнительно широкой регулируемой зоной нулевой автокорреляции и значениями боковых выбросов 0, $\pm(p+1)$ за ее пределами. Эти последовательности обладают большой линейной сложностью, которая в некоторых случаях достигает предельно возможного значения, равного длине последовательности. Полученные последовательности могут быть использованы в системах мобильной широкополосной связи для синхронизации, оценки канала и измерения дальности.

Литература

1. L.D. Baumert. Cyclic difference sets. – Berlin, Springer-Verlag, 1971.

2. J.S. No, S. Golomb, G. Gong, H. K. Lee, P. Gaal. Binary pseudorandom sequences of period 2n-1 with ideal autocorrelation. – IEEE. Trans. Inform. Theory, vol.44, No.2, March, 1998.

3. P. Fan and M. Darnell. Sequence Design for Communications Applications. – Research Studies Press Ltd., London, 1996.

4. Ипатов В.И. Периодические дискретные сигналы с оптимальными корреляционными свойствами. – М.: Радио и связь, 1992.

5. A. Pott and S. Bradley. Existance and nonexistence of almost perfect autocorrelation sequences. IEEE Transaction on Information Theory, vol. IT-41, No. 1, pp. 301–304, 1995.

6. H.D. Lüke. Binary Alexis sequences with perfect correlation. – IEEE Transactions on Communications, Vol. 49, No. 6, June, pp.966–968, 2001.

7. Naoki Suehiro, Naoki Suehiro, Noriyoshi Kuroyanagi, Kenji Takatsukasa. A Binary Sequence Pair with Zero Correlation Zone Derived from Complementary Pairs.-Coding, Communications and Broadcasting, Research Studies Press, ISBN 0-86380-259-1.

8. J-sang Cha. Even-phase ZCD codes for MAI Cancelled DS-CDMA Systems. – ITC-CSCC, July, 2002.

9. Games A.R. Cross-correlation of m-sequences and GMW-sequences with the same primitive polynomial. – Journal Discrete applied mathematics, 12, 1985.

10. Kim J-H and Song H-Y. On the linear complexity of Hall's sextic Residue sequences. – IEEE Transaction on Information Theory, vol. 47, No.5, 2001, pp.2094–2096.

11. Ding C., Helleseth T. On the linear complexity of Legendre sequences.– IEEE Transaction on Information Theory, vol. 44, No.3, 1998, 1276–1278.

12. А. с. N 674204, кл.H03 K/84 с приоритетом от 05.07.1977. Генератор псевдослучайных последовательностей двоичных сигналов. // Мешковский К.А., Кренгель Е.И.