КОДОВОЕ РАЗДЕЛЕНИЕ КАНАЛОВ НА ОСНОВЕ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ЗНАЧНОСТИ 127

Миллер Ф., Мешковский К.А., Кренгель Е.И., Архипкин В.Я., Соколов А.Г.

Государственный Центр Компьютерных Технологий, Силикон-Телеком-Софт
103498, Москва, МИЭТ, ЦКТ СТС
тел. (095) 530-4616, факс (095) 530-6236, E-mail bsd@access.orgland.ru

Реферат. Исследуются взаимно корреляционные свойства и линейная сложность классов двоичных псевдослучайных последовательностей значности 127 на основе совершенных разностных множеств. Дается оценка эффективности их использования в системах связи с CDMA.

Для систем связи с многостанционным доступом с кодовым разделением каналов (CDMA) требуется, чтобы используемые в них кодовые последовательности имели малые значения автокорреляционных и взаимно-корреляционных функций (АКФ и ВКФ). Среди двоичных псевдослучайных последовательностей (ПСП) значности 127 наиболее известны m-последовательности и ПСП Голда, корреляционные свойства которых достаточно подробно исследованы в [1]. Однако при данной значности N=127 существует много других классов ПСП, имеющих такие же близкие к идеальным периодические АКФ (ПАКФ), что и m-последовательности. К ним относятся ПСП на основе различных классов совершенных разностных множеств с параметрами v=127, k=63, λ=31 [2], для которых все неглавные значения ПАКФ равны $\theta = v - 4(k - \lambda) = -1$.

Компактная запись совершенных разностных множеств с параметрами v=127, k=63, λ=31 приведена в Таблице 1. Здесь буквами A, B, C обозначены разностные множества Бомера-Фридриксена [2], а буквами S, L, H соответственно разностные множества Зингера, Лежандра и Холла.

Таблица 1

Разностные множества (127,63,31)

	ВЫЧЕТЫ α_j														
	5	7	9	11	13	15	19	21	23	27	29	43	47	55	63
S		1			1	1	1	1	1				1	1	11
H	1		1	1				1		1	1	1		1	1
A			1	1	1		1	1		1	1		1		1
B				1	1	1	1	1	1		1			1	1
C			1		1	1		1	1		1	1		1	1

Единицами в соответствующей строке отмечены те вычеты α_j в первой строке таблицы, которые участвуют в образовании соответствующего данной строке множества по правилу α_j $\mathbf{2^i}$ **,** $0 \le i \le 6 \bmod 127$. Коэффициентов α_j всегда 9 для любого множества и они образуют $k = 9 \cdot 7 = 63$ вычета. Все 18 изоморфных множеств каждого эквивалентного класса образуются последовательным умножением на первообразный корень 3 mod 127 по правилу $\{\alpha_j\}3^k$, $1 \le k \le 18$, кроме множества Холла, которое имеет только 6 изоморфных множеств $\{\alpha_j\}3^k$, $1 \le k \le 6$. Множество Лежандра образуется по простому правилу $\alpha_j \equiv 9^i$, $0 \le i \le 62 \bmod 127$ и имеет только два изоморфных множества – прямое и обратное.

Таким образом, существуют 2 изоморфных разностных множеств Лежандра, 6 изоморфных разностных множеств Холла и по 18 изоморфных разностных множеств в классах Зингера, A, B и C, т.е. всего 80 множеств. Псевдослучайные последовательности двоичных символов “1” и “0” образуются записью символов “0” на позициях, соответствующих по номеру вычетам разностных множеств, и записью символов “1” на всех остальных (127-63)=64 позициях. Образованные таким способом ПСП классов A, B, C известны еще как последовательности Бомера-Фридриксена. При этом последовательности класса Зингера оказываются идентичными m-последовательностям значности 127.

Интересно, что в отличие от класса S ПСП классов L, H, A, B и C нелинейны и имеют линейную сложность, превышающую линейную сложность m-последовательностей значности 127, для которых она равна 7. Напомним, что параметр линейной сложности последовательности, введенный для оценки степени непредсказуемости символов последовательности, численно равен длине эквивалентного регистра сдвига с линейной обратной связью, посредством которого может быть сформирована данная последовательность [3]. Поэтому, довольно привлекательным может стать использование этих ПСП в качестве базисных для генерации ПСП GMW [4], так как линейная сложность у таких ПСП GMW, как показывают расчеты, в целом оказывается больше, чем у ПСП GMW на основе базисных m-последовательностей [5]. К тому же согласно [6] применение ПСП классов L, H, A, B, C в качестве базисных для генерации ПСП GMW 2^{7J}, где J=2, приводит к существенному увеличению общего числа ПСП GMW.

ПСП символов Лежандра – ПСП L.

ПСП L образуют самый маломощный класс ПСП с двухуровневой ПАКФ, состоящий из двух ПСП: прямой и обратной, символы которых обладают свойством зеркально-инверсной симметрии. На основании этого свойства получено следующее точное выражение для пикового значения ПВКФ ПСП L.

$$\theta_c = N - 2 \quad (1)$$

где N – значность ПСП.

Так, например, для N=127, θ_c=125. Отсюда приходим к выводу о невозможности совместного использования двух ПСП L в системах CDMA. С другой стороны, компьютерный анализ показал, что среди всех известных 80-ти ПСП с двухуровневыми ПАКФ ПСП L обладают наилучшими корреляционными параметрами автооптимальности (АО), введенными в [1].

Действительно, для них существует такой АО-сдвиг, при котором пиковое значение нечетной (меандро-инвертированной) АКФ равно $\hat{\theta}_{AO} = 13$, при этом энергия боковых лепестков S=1491. Другой не менее важной по значимости особенностью ПСП L является их ВКФ с ПСП S. На компьютере были получены результаты, по которым пиковые значения ПВКФ ПСП L с m-последовательностями (класс ПСП S) для одной половины ПСП S составляет 17, а для другой - соответственно 19. Это обстоятельство делает возможным сформировать множество из семи последовательностей, состоящее из 6-ти ПСП S максимального связного множества и одной ПСП L с пиковым значением θ_c=19, причем в 85% случаях это значение равно 17. Здесь уместно заметить, что произвольное множество ПСП S периода 127 из 7-ми и более ПСП характеризуется сравнительно большим пиковым значением взаимной корреляции θ_c=41.

ПСП классов A, B, C.

Внутри каждого класса ПСП введем нумерацию, при которой ПСП с номером k будет соответствовать изоморфный коэффициент $3^k \bmod 127$. Можно показать, что в этом случае матрица пиковых значений P_{ij} ПВКФ для каждого такого класса будет обладать следующим замечательным свойством. Каждая последующая строка корреляционной матрицы P_{ij} является циклическим сдвигом вправо ее предыдущей строки. Таким образом, все строки матрицы, начиная с первой, могут быть получены из нулевой, при этом достаточно вычислить только первые ее 9 элементов. В таблице 2 приведены нулевые строки матрицы P_{ij} для каждого класса A, B, C, а также для класса ПСП S, имеющего тот же самый набор изоморфных коэффициентов.

Таблица 2

Пиковые значения ПВКФ ПСП классов A, B, C, S.

j	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
P^A_{0j}	127	23	23	23	23	41	27	41	23	25	23	41	27	41	23	23	23	23
P^B_{0j}	127	23	29	21	25	25	41	31	27	27	27	31	41	25	25	21	29	23
P^C_{0j}	127	41	41	25	23	19	17	23	41	43	41	23	17	19	23	25	41	41
P^S_{0j}	127	17	17	17	17	17	41	41	41	21	41	41	41	17	17	17	17	17

Из анализа этой таблицы следует, что при выборе подмножеств из 9 ПСП класс A оказывается более предпочтительным, т.к. при этом параметр θ_c=27, тогда как для классов B, C и S θ_c=41. Проведенные на компьютере расчеты пиковых значений ПВКФ пар ПСП, взятых из различных классов, приводят к следующему выводу. Комбинации ПСП из различных классов A, B, C, S образуют множества ПСП с большими значениями θ_c, чем у ПСП исходных классов. При этом множество из 36-ти ПСП классов C и S имеет параметр θ_c=43, в то время как множества ПСП, составленные соответственно из классов $A \bigcap B$, $A \bigcap C$, $B \bigcap C$, $A \bigcap S$, $B \bigcap S$ обладают сравнительно более худшими параметрами θ_c, достигающими значений 69÷71. Интересно отметить, что взаимнокорреляционный параметр θ_c ПСП L с ПСП классов A, B, C составляет соответственно 43, 29 и 27.

Для более полного представления корреляционных свойств ПСП классов A, B, C целесообразно рассмотреть их нечетные ПВКФ. Известно, что нечетные ВКФ так же как и АКФ зависят от выбора сдвигов коррелируемых ПСП. Для нахождения оптимальных сдвигов, минимизирующих значение $\hat{\theta}_c$ была использована квазиоптимальная процедура поиска. В таблице 3 (верхняя часть от диагонали) приведены значения пиков нечетной ВКФ для последовательностей класса A при оптимальных сдвигах, минимизирующих эти значения. Соответственно, в таблице 3(нижняя часть от диагонали) приведены значения пиков нечетной ВКФ для автооптимальных сдвигах этих последовательностей. Из таблицы 3 видно, что существует подмножество из 14 последовательностей класса A со значением корреляционного параметра

$\hat{\theta}_c$=33. Для сравнения при АО сдвигах для этого же подмножества ПСП $\hat{\theta}_c$=43. В целом же для ПСП класса А этот параметр при оптимальных и автооптимальных сдвигах соответственно равен 35 и 47. Заметим, что ПСП классов B, C и S при АО-сдвигах обладают примерно такими же значениями ВКФ, что и класс А.

Таблица 3.

Пиковые значения нечетных ВКФ ПСП класса А при оптимальных и автооптимальных сдвигах

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
0	25/21	31	29	31	29	33	31	29	31	29	29	33	33	31	31	31	33	31
1	33	19/17	33	31	23	33	33	27	31	27	27	29	31	33	33	27	29	27
2	27	25	21/19	29	33	27	31	29	31	33	29	27	29	31	27	33	31	29
3	39	33	37	17/17	31	31	33	29	31	31	33	31	31	35	27	31	33	29
4	27	25	39	31	21/21	33	29	29	29	31	31	29	27	33	31	27	29	27
5	31	29	29	27	35	21/19	25	29	29	27	31	31	31	35	35	25	33	29
6	37	41	31	31	39	35	21/19	29	29	31	33	35	35	31	29	29	31	31
7	27	27	35	27	25	43	27	23/19	31	27	31	31	35	35	29	31	29	31
8	27	29	27	39	29	29	31	37	21/17	31	27	27	33	31	31	27	29	25
9	41	29	31	35	37	35	35	35	31	23/21	29	27	27	29	33	33	31	27
10	29	41	29	29	31	33	29	27	31	33	29/17	35	35	29	27	31	31	31
11	31	29	47	29	27	39	35	27	35	27	25	23/19	29	27	35	31	35	29
12	35	29	29	43	25	31	27	31	31	39	33	37	25/17	29	35	33	29	27
13	37	31	27	25	43	31	33	25	33	27	25	39	31	25/21	23	31	33	33
14	35	33	39	31	31	43	27	35	27	31	29	29	27	35	33/19	33	33	33
15	35	29	35	27	33	27	43	29	31	37	41	31	31	39	35	23/19	33	29
16	35	27	27	31	25	35	29	47	31	27	27	35	27	25	43	27	31/19	29
17	31	31	35	31	33	27	31	31	37	27	29	27	39	29	29	31	37	21/17

Последовательности Холла.

Аналогично предыдущему, при соответствующей нумерации ПСП H строки корреляционной матрицы P_{ij} ПВКФ могут быть получены из нулевой посредством ее циклических сдвигов вправо. Эта строка имеет вид:

0	1	2	3	4	5
127	41	41	43	41	41

Нами доказано аналитически, что наибольшая нижняя граница максимума ПВКФ ПСП Холла равна

$$\hat{e} = (N+2)/3 \tag{2}$$

что и подтвердил компьютерный расчет для N=127. Дополнительно к этому были также исследованы ПВКФ ПСП H с ПСП остальных классов. В результате было установлено, что наиболее предпочтительными являются сочетания ПСП H с ПСП классов B и S, для которых параметр θ_c не превышает значения 41, тогда как сочетание с классами A и C дают θ_c=69. Кроме того, для ПСП H были также исследованы нечетные ВКФ при АО и оптимальных сдвигах. Оказалось, что в первом случае $\hat{\theta}_c = 47$, а во втором - 29.

Линейная сложность ПСП классов S, L, H, A,B, C

В недавно опубликованной работе [7] было показано, что последовательности A, B, C являются частным случаем при n=7 трех новых семейств последовательностей, получивших соответственно условные названия: Предложение 3, Предложение 5 и Предложение1. Причем последовательности всех этих семейств выражаются в виде сумм следовых функций. В соответствии с этим для ПСП классов A, B, C имеем:

$$a(t) = tr_1^7(a^t) + tr_1^7(a^{5t}) + tr_1^7(a^{21t}) + tr_1^7(a^{13t}) + tr_1^7(a^{29t}) \tag{3}$$

$$b(t) = tr_1^7(a^t) + tr_1^7(a^{5t}) + tr_1^7(a^{21t}) + tr_1^7(a^{13t}) + tr_1^7(a^{29t}) \tag{4}$$

$$c(t) = tr_1^7(a^t) + tr_1^7(a^{9t}) + tr_1^7(a^{13t}) \tag{5}$$

Аналогичные представления также были найдены для ПСП H и L значности 127 [8]

$$: h(t) = tr_1^7(a^t) + tr_1^7(a^{25t}) + tr_1^7(a^{47t}) \tag{6}$$

$$l(t) = \sum_{i=0}^{8} tr_1^7(a^{3^{2i}t}) \tag{7}$$

Из выражений (3)-(7) легко вычисляется линейная сложность этих последовательностей, значения которой представлены в Таблице 4.

Таблице 4

Тип последовательности	Линейная сложность
m-последовательность	7
Лежандра (L)	63
Холла (H)	21
A	35
B	35
C	21

Дальнейшие исследования показали , что на основе нелинейных последовательностей классов L, H, A, B и C могут быть построены ПСП GMW с линейной сложностью, превышающей линейную сложность ПСП GMW на основе m-последовательностей 127. В частности, было установлено, что линейная сложность ПСП GMW 2^{14}-1 на основе одной из ПСП Лежандра равна 1232, когда как максимальная линейная сложность ПСП GMW на основе m-последовательностей составляет 448.

Выводы.

1. ПСП классов L, H, A, B и C значности 127, построенные на основе разностных множеств с параметрами v=127, k=63, λ=31, образуют в совокупности мощное множество из 62-х последовательностей с близкими к идеальным значениями ПАКФ. Использование этих ПСП наряду с m-последовательностями в системах связи с CDMA позволяет значительно расширить возможность выбора множеств ПСП с приемлемыми корреляционными параметрами. ПСП классов L, H, A, B и C целесообразно также использовать в тех случаях, когда требуются последовательности с более высокой, чем у m-последовательностей линейной сложностью.

2. Другой не менее важной областью приложения последовательностей классов L, H, A, B и C может стать их использование в качестве базисных для генерации новых классов ПСП GMW, что приводит к существенному увеличению общего числа этих последовательностей. Кроме того, в силу нелинейности последовательностей классов L, H, A, B и C линейная сложность таких ПСП GMW может быть достаточно высокой.

Литература.

1. M.B.Pursley and H.F.Roefs, “Numerical evaluation of correlation parameters for optimal phases of binary shift-register sequences”, IEEE Trans.Comm.,vol.COM-27,pp.1597-1604, 1979
2. L.D.Baumert, “Cyclic Difference Sets”, Springer-Verlag Berlin-Heidelberg-New-York, 1971.
3. L.Key, “Analysis of the structure and complexity of non-linear binary sequence generators”, IEEE Trans. on Information Theory, vol.IT-22, pp.732-736, 1976.
4. Мешковский К.А, Кренгель Е.И. Генератор псевдослучайных последовательностей Гордона, Милза, Велча. - Техника средств связи, сер.ТРС, вып.3, 1979.
5. R.A.Scholtz, L.R.Welch, “GMW sequences”, IEEE Trans. on Information Theory, vol.IT-30, N3, pp.548-553, 1984.
6. Кренгель Е.И. О числе псевдослучайных последовательностей Гордона, Милза, Велча. - Техника средств связи, сер.ТРС, вып.3, 1979.
7. J.S.,No, S.W. Golomb, G. Gong, H.K. Lee, P. Gaal. Binary pseudorandom sequences of period 2^n-1 with ideal correlation.- IEEE Transactions on Inform. Theory, vol.44, No. , 1998.
8. J.-S No, K.Yang, H.Chung and H.-Y. Song. On the construction of binary sequences with ideal autocorrelation property.- in Proc.1996 IEEE ISITA'96, Canada, Sept.,1996

CODE DIVISION MULTIPLE ACCESS BASED ON PSEUDORANDOM SEQUENCES OF PERIOD 127

Miller F.S., Meshkovsky K.A., Krengel E.I., Arkhipkin V.Ya., Sokolov A.G.

State Center of Computer Technologies, Silicon-Telecom-Soft
103498, Moscow, MIEE, CTC
tel.(095) 530-4616, fax (095) 530-6236, E-mail bsd@access.orgland.ru

Summary. The cross correlation properties and the linear complexity pseudorandom sequence classes of period 127 based on perfect difference sets are studied. The efficiency estimation of their application in CDMA communications systems is presented.

For the code division multiple access communications (CDMA) systems the code sequences used in them must have low values of the autocorrelation and the cross correlation functions (ACF and CCF). Among binary pseudorandom sequences (PRS) of period 127, the m-sequences and the Gold sequences, the correlation properties of which have been studied explicitly enough in [1], are the most known ones. However, with N=127 many other PRS classes having the same, close to ideal, periodic ACF (PACF) as the m-sequences, exist. They include PRS based on different classes of perfect difference sets with V =127, k =63, λ =31 parameters [2], for which all sidelobes PACF values are $\theta = V - 4(k-\lambda) = -1$. In all, there are 2 Legendre PRS (class L), 6 Hall PRS (class H), 18 m-sequences (class S) and 18 PRS in each class A, B and C of Baumert-Fredricksen family. Note, that in contrast to class S, PRS of L, H, A, B and C classes are non-linear and have the linear complexity higher than that of the m-sequences [3]. Therefore, the employment of these PRS as the basic ones for GMW PRS generation [4] would be rather attractive, because the linear complexity of such GMW PRS, as the calculations show, as a whole appears to be higher, than that one of GMW PRS based on the m-sequences [5]. Besides, according to [6], the application of PRS of L, H, A, B, C classes as the basic ones for GMW sequences 2^{7J}, where J≥2, results in a significant increase of the GMW PRS total number.

PRS of Legendre symbols – L PRS.

L PRS consist of two PRS: direct and inverse, the symbols of which have the mirror-inverse symmetry property. Besides, their periodic CCF (PCCF) is always three-level one with 3, –1 and –125 values. Obviously, the existence of a super-high peak is a significant restriction for a combined employment of these sequences. On the other hand, the computer analysis has demonstrated that of all known 80 PRS with two-level PACF, L PRS have the best correlation parameters of auto-optimality (AO) introduced in [1].

PRS of A, B, C classes.

In each PRS class the numbering will be introduced, where an isomorphic coefficient $3^k \bmod 127$ will correspond to PRS with k number. It can be shown that in this case the matrix of the peak values P_{ij} PCCF for each such class will have the following remarkable property. Each successive row of the correlation matrix P_{ij} is the cyclic shift to the right of its preceding row. In the Table 1, the first rows of P_{ij} matrix for each A, B, C classes as well as for class S having the same set of isomorphic coefficients are presented.

Table 1

PCCF peak values for PRS of A, B, C, S classes

j	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
P_{0j}^{A}	127	23	23	23	23	41	27	41	23	25	23	41	27	41	23	23	23	23
P_{oj}^{B}	127	23	29	21	25	25	41	31	27	27	27	31	41	25	25	21	29	23
P_{oj}^{C}	127	41	41	25	23	19	17	23	41	43	41	23	17	19	23	25	41	41
P_{oj}^{S}	127	17	17	17	17	17	41	41	41	21	41	41	41	17	17	17	17	17

Linear complexity of PRS of S, L, H, A, B, C classes

In the recently published paper [7] it has been shown that A, B, C sequences represent a special case with n=7 of three new sequence families conventionally named: Sentence 3, Sentence 5 and Sentence 1. Moreover, the sequences of all these families are expressed as a sum of trace functions. Similar expressions have been obtained in [8] for L and H PRS. Using them, the linear complexity of these sequences is easily calculated, and its values are presented in Table 2.

Table 2

sequence type	Linear complexity
m-sequences	7
Legendre (L)	63
Hall (H)	21
A	35
B	35
C	21

Further studies have shown that based on the non-linear sequences of L, H, B and C classes GMW PRS can be constructed with the linear complexity exceeding the linear complexity of GMW PRS on the basis of the m-sequences 127. In particular, it has been determined that the linear complexity of GMW PRS 2^{14}-1 based on one of Legendre PRS is 1232, while the maximum linear complexity of GMW PRS based on the m-sequences is 448.

Conclusions

PRS of L, H, A, B and C classes of period 127 built on the basis of the difference sets with v=127, k=63, λ=31 parameters form in total a powerful set of 62 sequences with the close to ideal PACF values. The employment of these PRS together with the m-sequences in CDMA systems allows to significantly increase the possibility of choosing the PRS sets with the acceptable correlation parameters. It is also advisable to use PRS of L, H, A, B and C classes in cases, when the sequences with the linear complexity higher than that one of m-sequences are required.

Another no less important application area for the sequences of L, H, A, B and C classes can be their employment as the basic ones for generation of GMW PRS new classes, which results in a considerable increase of the total number of these sequences. Moreover, due to the non-linear sequences of L, H, A, B and C classes the linear complexity of such GMW PRS can be high enough.

References

1. M.B.Pursley and H.F.Roefs, "Numerical evaluation of correlation parameters for optimal phases of binary shift-register sequences", IEEE Trans.Comm., vol.COM-27, pp.1597-1604, 1979.

2. L.D.Baumert, "Cyclic Difference Sets", Springer-Verlag Berlin-Heidelberg-New-York, 1971.

3. L.Key, "Analysis of the structure and complexity of non-linear binary sequence generators", IEEE Trans. On Information Theory, vol.IT-22, pp.732-736, 1976

4. Meshkovsky K.A., Krengel E.I. Gordon, Mills Welch pseudorandom sequence generator. – Tekhnika sredstv svyazi, ser. TRS, vyp.3, 1979.

5. .R.A.Scholtz, L.R.Welch, 'GMW sequences", IEEE Trans. On Information Theory, vol.IT-30, N3, pp.548-553, 1984.

6. Krengel E.I. On the number of Gordon, Mills, Welch pseudo-random sequences, Tekhnika sredstv svyazi, ser. TRS, vyp.3, 1979.

7. J. S.No, S.W.Golomb, G.Gong, H.K.Lee, P.Gaal. Binary pseudorandom sequences of period 2^n –1 with ideal correlation.- IEEE Transactions on Inform. Theory, vol.44, No.2, 1998.

8. J.S. No, K.Yang, H.Chung and H.-Y.Song. On the construction of binary sequences with ideal autocorrelation property.- in Proc.1996 IEEE ISITA'96, Canada, Sept., 1996.