УДК 621.391

АНАЛИЗ ЧАСТОТЫ ПОВТОРЕНИЙ RLE-БЛОКОВ В СЕМЕЙСТВАХ БИНАРНЫХ КОДОВ, НАИЛУЧШИХ ПО МИНИМАКСНОМУ КРИТЕРИЮ АВТОКОРРЕЛЯЦИОННОЙ ФУНКЦИИ

А.А. Ковылин, Д.В. Злобин, А.Ю. Родионов

Рассматриваются вопросы отыскания двоичных псевдослучайных последовательностей с автокорреляционной функцией, близкой к идеальной, предназначенных для использования в современных системах передачи информации, в том числе в мобильной связи и интерфейсах беспроводной передачи данных. При синтезе наборов двоичных последовательностей поставлена задача комплектования их на основе минимаксного критерия, по которому последовательность считается оптимальной в соответствии с предполагаемой областью применения. Получены оптимальные последовательности размерностью до 52, для них проведен анализ кодирования длин серий. Выявлены закономерности в распределении количества серий различной длины в кодах, оптимальных по выбранному критерию, что в дальнейшем позволит оптимизировать процесс поиска таких кодов.

Ключевые слова: псевдослучайные последовательности, хаотические сигналы, коды Баркера, минимаксный критерий, автокорреляционная функция, кодирование длин серий.

Введение

В связи с ростом популярности систем, использующих хаотические сигналы, актуально изучение функций, имеющих с ними интегральное соответствие, на основе псевдослучайных последовательностей

с наилучшими автокорреляционными свойствами. В соответствии с теоремой Винера–Хинчина сигналы с идеальной автокорреляционной функцией (АКФ) имеют наилучшие стохастические свойства. Подобные последовательности имеют широкое применение в системах радиолокации, синхронизации, расширения спектра и т.п. Отмечено использование шумоподобных последовательностей при анализе цепочек дезоксирибонуклеиновой кислоты (ДНК).

Учитывая большой интерес к представленной научной теме, встает вопрос о синтезе более длинных последовательностей, нежели те, что используются на сегодняшний день. Поиск оптимальных кодов большой длины методом простого перебора является весьма ресурсозатратной задачей. Все это подталкивает к созданию других методов поиска, обеспечивающих заданный критерий оптимальности, но при этом содержащих меньшее количество вычислительных операций, а следовательно, обладающих меньшим временем расчета. В работе авторами рассматривается один из способов оптимизации такого поиска.

Оптимальные дискретные сигналы

Для количественного определения степени отличия сигнала $u(t)$ и его смещенной во времени копии $u(t-\tau)$ принято вводить АКФ сигнала $u(t)$:

$$B_u(\tau) = \int_{-\infty}^{\infty} u(t)\, u(t-\tau)\, dt .$$

Для дискретного сигнала $u = \{u_0, u_1, \ldots, u_{M-1}\}$ АКФ имеет следующий вид:

$$B_u(n) = \sum_{j=-\infty}^{\infty} u_j\, u_{j-n} .$$

При синтезе оптимальных дискретных сигналов принято использовать минимаксный критерий: оптимальным считается сигнал с наименьшим уровнем наибольшего из боковых лепестков АКФ. Такой критерий отвечает существу проблемы [1].

Дискретные сигналы с наилучшей структурой АКФ являются объектом интенсивных исследований. Среди них большую известность получили сигналы Баркера. Эти сигналы обладают уникальным свойством: при всех $n \neq 0$ значения их АКФ не превышают единицы. Установлено, что не существует сигналов Баркера с числом элементов, большим 13. Однако в [2] говорится о том, что если последовательность Баркера длиной более 13 существует, то $n = 189\,260\,468\,001\,034\,441\,522\,766\,781\,604$ (т.е. более $2 \cdot 10^{30}$).

Свойства полученных кодов

В результате поиска всех существующих последовательностей по заданным критериям посредством разработанного алгоритма было обнаружено семейство кодов, с учетом зеркальных и обратных последовательностей. В табл. 1 приведено сравнение рассчитанных значений максимального уровня бокового лепестка (УБЛ) АКФ и значений, приведенных в [3]. Следует отметить, что параметры некоторых обнаруженных последовательностей превосходят результаты, приведенные в [3]. Такие параметры отмечены в табл. 1 символом ($^+$).

Длина кода	Максимальный УБЛ АКФ		Количество кодов	Длина кода	Максимальный УБЛ АКФ		Количество кодов
	расчет	литература [3]			расчет	литература [3]	
14	2	2	72	33	3	–	1132
15	2	2	104	34	3	–	408
16	2	2	80	35	**3**$^+$	4	888
17	2	2	32	36	**3**$^+$	4	1288
18	2	2	16	37	**3**$^+$	4	440
19	2	2	8	38	3	–	136
20	2	2	24	39	3	–	240
21	2	2	24	40	**3**$^+$	4	456
22	3	3	3024	41	**3**$^+$	4	120
23	3	3	4084	42	**3**$^+$	5	32
24	3	3	6864	43	**3**$^+$	4	96
25	**2**$^+$	3	8	44	**3**$^+$	4	120

Длина кода	Максимальный УБЛ АКФ		Количество кодов
	расчет	литература [3]	
26	3	3	1936
27	3	3	3096
28	2	2	16
29	3	3	2244
30	3	3	688
31	3	3	2008
32	3	–	3376

Длина кода	Максимальный УБЛ АКФ		Количество кодов
	расчет	литература [3]	
45	3	–	32
46	$\mathbf{3}^{+}$	5	8
47	$\mathbf{3}^{+}$	4	8
48	$\mathbf{3}^{+}$	5	32
49	4	–	392704
50	4	–	201352
51	3	–	8
52	4	–	264464

Таблица 1. Сводная таблица кодов

К примеру, один из кодов длиной 52 будет иметь вид (0100101001000001011101000001001100111110011111001110).

Можно отметить, что отношение главного пика АКФ к максимальному УБЛ для кодов длиной 51 и 28 элементов больше, чем у 13-элементного кода Баркера (рис. 1). Это говорит о существовании последовательностей длиной, превосходящей коды Баркера, обладающих лучшим отношением максимума АКФ к боковому лепестку.

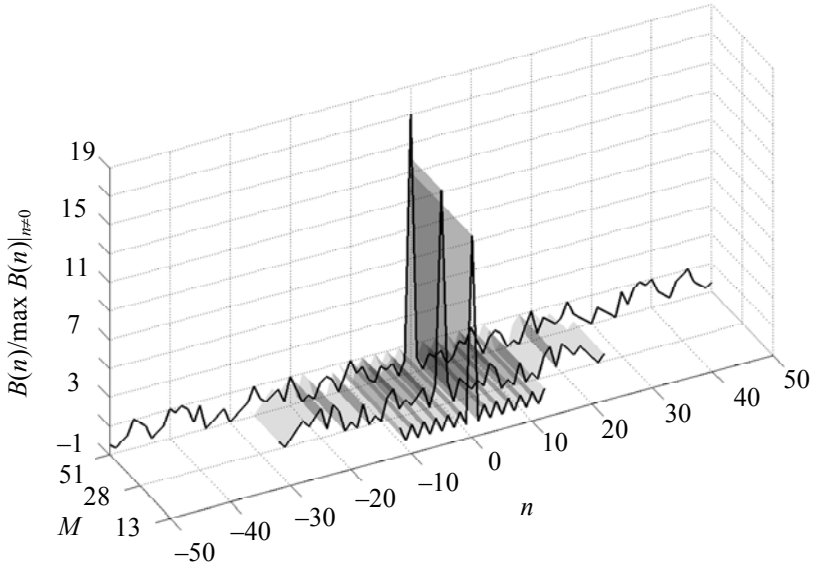

Рис. 1. АКФ оптимальных кодов длиной 13, 28 и 51 соответственно с нормой на максимальный уровень бокового лепестка

В современных системах радиоэлектроники широко применяются псевдослучайные последовательности, сформированные по определенным правилам, например, М-последовательности, последовательности Де Брейна, последовательности Гордона–Милса–Велча (GMW) [4]. Однако их длина кратна степени 2 ± 1, что существенно ограничивает выбор длины кода. При этом значения УБЛ АКФ с ростом длины последовательности уступают аналогичным показателям предложенных кодов (табл. 2).

Последовательности	Максимальное значение УБЛ АКФ при длине последовательности					
	15	16	17	31	32	33
М-последовательности	3	–	–	4	–	–
Последовательности Де Брейна	–	3	–	–	4	–
GMW-последовательности	–	–	3	–	–	6
Найденные коды	2	2	2	3	3	3

Таблица 2. Выборочное сравнение последовательностей по максимальному УБЛ АКФ

Анализ кодирования длин серий

Поиск кодов большой длины методом простого перебора вариантов оказывается весьма громоздким и является проблемой даже для современных вычислительных мощностей: время поиска всех бинарных последовательностей (по заданным критериям) длиной 52 элемента составляло около 180 дней на вычислительном сервере (4×4 ядра с тактовой частотой 3,2 ГГц) [5]. Между тем имеется явная тенденция применять сигналы с все большей размерностью, и это оправдывает поиск других методов синтеза, не связанных с подобными трудностями.

В настоящей работе проводится исследование частоты повторений RLE-блоков (Run-Length Encoding, кодирование длин серий) бинарных последовательностей, полученных с помощью разработанного программного приложения. При кодировании длин серий кодовая последовательность разбивается на блоки, состоящие из идущих подряд одинаковых элементов кода. Код при этом записывается как последовательность длин этих блоков. Таким образом, если рассмотреть известную бинарную последовательность Баркера длиной 13 – (1111100110101), то запись ее в формате RLE выглядит как (5221111), количество анализируемых RLE-блоков составит 7, а число уникальных блоков – 3.

Анализ сигнатур кодов показал характерное количество RLE-блоков, из которых были рассчитаны доли от общей длины кода (рис. 2). Это хорошо согласуется с теоремой Винера–Хинчина, так как конкретные RLE-блоки отвечают за нахождение определенных частот внутри кода, а неравномерность количества элементов в разных блоках показывает равномерность спектральной плотности кода.

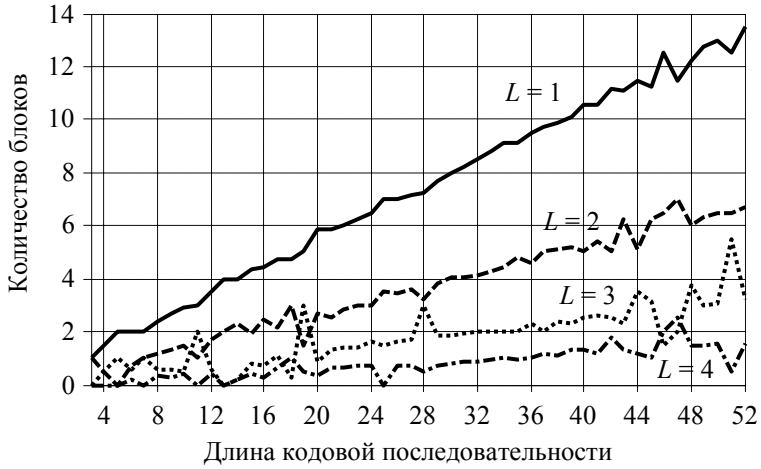

Рис. 2. Количество RLE-блоков длиной 1, 2, 3 и 4 элемента в зависимости от длины кода

Существуют три основных свойства любой двоичной псевдослучайной последовательности, которые могут быть использованы в качестве проверки на случайность. Это сбалансированность, цикличность и корреляция. Циклом (группой) называется непрерывная последовательность одинаковых двоичных чисел. Появление одной двоичной цифры автоматически начинает новый цикл. Длина группы равна количеству цифр в нем. Желательно, чтобы в каждом фрагменте последовательности приблизительно половину составляли циклы обоих типов длиной 1, приблизительно одну четверть – длиной 2, приблизительно одну восьмую – длиной 3 и т.д. [6]. Таким образом, доля содержания конкретной группы в рассматриваемом коде определяется выражением

$$p_i = 2^{-i},$$

где i – длина группы. В результате проведенного авторами в рамках данной работы исследования синтезированных сигнатур кодов вышеупомянутое распределение оказалось несколько иным:

$$p_i = 2^{-i-1}. \quad (1)$$

Варианты такого распределения представлены на рис. 3 (утолщенная линия). Распределение долей RLE-блоков в коде имеет медианный характер, так как сумма RLE-блоков в заданной пропорции не равна длине кода. Необходимую длину кода дополняют отклоненные от медианного значения RLE-блоки большой длины. В действительности эти отклонения незначительно будут влиять на время расчета кода необходимой длины. Алгоритм расчета подобных кодов предполагает рекуррентный анализ вновь найденных кодов для обновления значений распределения RLE-элементов в кодах. Количество RLE-элементов большой длины для найденных кодов имеет хаотический характер в пределах определенных чисел, в то время как число RLE-блоков малой длины имеют характерную линейную зависимость от длины кода, с распределением (1). С увеличением длины кода RLE-элементы большой длины также начинают подчиняться распределению (1).

Это предполагает сокращение времени расчета кодов, в отличие от метода простого перебора, в котором время расчета имеет степенную зависимость от длины кода.

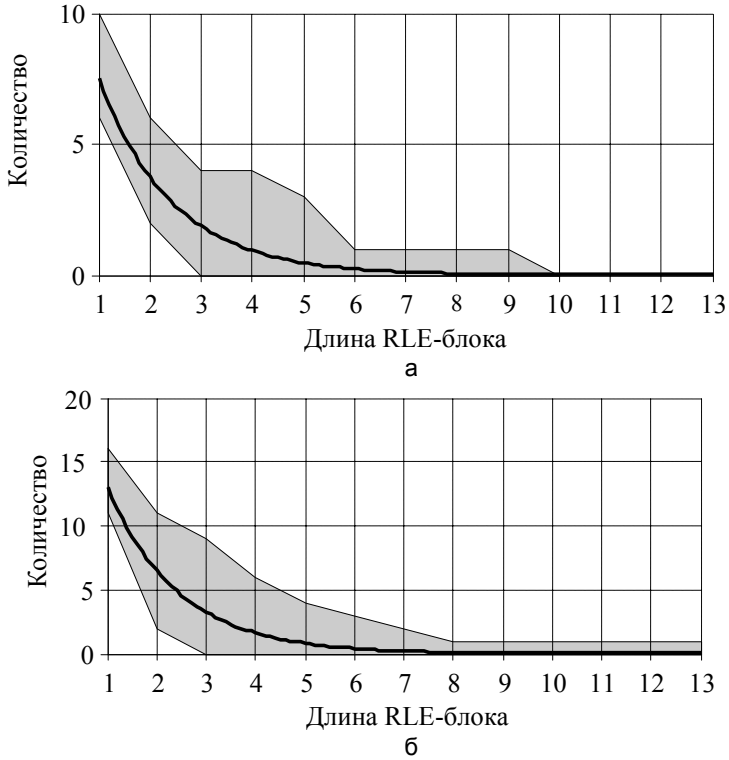

Рис. 3. Диапазон значений количества RLE-блоков в кодах длиной 30 (а) и 52 (б) (утолщенная линия – аппроксимирующая кривая)

Равномерность спектральной плотности кода – главное условие для получения минимального значения УБЛ его АКФ. График зависимости доли блока в коде от длины блока (рис. 3) хорошо апроксимируется экспоненциальной функцией.

Заключение

В результате поиска оптимальных двоичных последовательностей с размерностью, большей 13, было обнаружено существование кодов, превосходящих по своим автокорреляционным свойствам все известные. Выявлена тенденция к периодическому повышению «качества» кода с увеличением его длины, что говорит об актуальности дальнейшего поиска более длинных кодов.

Анализ частоты повторений RLE-блоков в найденных семействах бинарных кодов позволил выявить закономерности распределения количества блоков в зависимости от длины кода (1). Данные закономерности в дальнейшем позволят сузить область поиска оптимальных кодов при решении задач по синтезу и оптимизации структуры сложных сигналов.

Литература

1. Гантмахер В.Е., Быстров Н.Е., Чеботарев Д.В. Шумоподобные сигналы. Анализ, синтез, обработка. – СПб: Наука и техника, 2005. – 400 с.
2. Mossinghoff M.J. Wieferich pairs and Barker sequences // Designs, Codes and Cryptography. – 2009. – V. 53. – № 3. – P. 149–163.
3. Свердлик М.Б. Оптимальные дискретные сигналы. – М.: Советское радио, 1975. – 200 с.
4. Golomb S.W., Gong G. Signal design for good correlation for wireless communication, cryptography and radar. – US: Cambridge University Press, 2005. – 438 p.
5. Чусов А.А., Ковылин А.А., Стаценко Л.Г., Миргородская Ю.В. Параллельный поиск сигналов с заданными взаимно и автокорреляционными свойствами на многопроцессорных платформах // Известия вузов. Радиоэлектроника. – 2010. – Т. 54. – № 8. – С. 29–35.
6. Скляр Б. Теоретические основы и практическое применение: Пер. с англ. – 2-е изд., испр. – М.: Вильямс, 2004. – 1104 с.

Ковылин Александр Александрович – Дальневосточный федеральный университет, инженер, kalexer@hotmail.com

Злобин Дмитрий Владимирович – Дальневосточный федеральный университет, инженер, memrbomel@mail.ru

Родионов Александр Юрьевич – Дальневосточный федеральный университет, кандидат физ.-мат. наук, доцент, deodar1618@mail.ru