

# **СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ, ПРИМЕНЯЕМЫХ ДЛЯ ПОВЫШЕНИЯ НАДЕЖНОСТИ ПЕРЕДАЧИ ИНФОРМАЦИИ**

**В. О. Старостенко**

*Гомельский государственный технический университет  
имени П. О. Сухого, Беларусь*

Научный руководитель Е. А. Храбров

В последние годы значительный прогресс в телекоммуникационных технологиях достигнут благодаря переходу на цифровые виды связи, которые, в свою очередь, базируются на стремительном развитии микропроцессоров. Один из ярких примеров этого – появление и быстрое внедрение технологии связи с цифровыми шумоподобными сигналами.

Основные свойства цифровой связи с шумоподобными сигналами – защищенность канала связи от перехвата, помех и подслушивания. В качестве шумоподобных сигналов используют сложные сигналы, сформированные на основе псевдослучайных последовательностей (кодов). Очень часто необходимо большое число разных кодовых последовательностей с хорошими корреляционными свойствами, например для обеспечения конфиденциальности или в каналах связи с кодовым разделением при наличии большого числа абонентов. Наиболее известные и широко используемые псевдослучайные последовательности (ПСП) – это линейные рекуррентные последовательности максимальной длины или М-последовательности. Они обладают хорошими корреляционными свойствами и легко формируются на основе регистров сдвига. Имеется широкий ансамбль М-последовательностей различной длины, однако длина данных ПСП строго определена и равна  $N = 2^k - 1$ . При необходимости использования ПСП другой длины можно взять последовательности Лежандра (коды квадратичных вычетов), Зингеровы коды или коды Якоби.

Так же наиболее известными кодовыми последовательностями являются сигналы Баркера. Достоинство этих сигналов заключается в том, что боковые пики автокорреляционной функции (АКФ) минимальные и не превышают значения  $1/N$ . Кодовые последовательности, обладающие таким свойством, найдены только для  $N \leq 13$ . В табл. 1 приведены известные кодовые последовательности Баркера. В последнем столбце таблицы приведен уровень боковых пиков АКФ.

Таблица 1

Кодовые последовательности Баркера и АКФ

N	$a_i$ при $i$													$R_{21}$
	1	2	3	4	5	6	7	8	9	10	11	12	13	
3	0	0	1											-1/3
4	0	0	1	0										1/4
5	0	0	0	1	0									1/5
7	0	0	0	1	1	0	1							-1/7
11	0	0	0	1	1	1	0	1	1	0	1			-1/11
13	0	0	0	0	0	1	1	0	0	1	0	1	0	1/13

На рис. 1 изображены огибающие автокорреляционных функций сигналов Баркера для  $N = 11$  и  $N = 13$ .

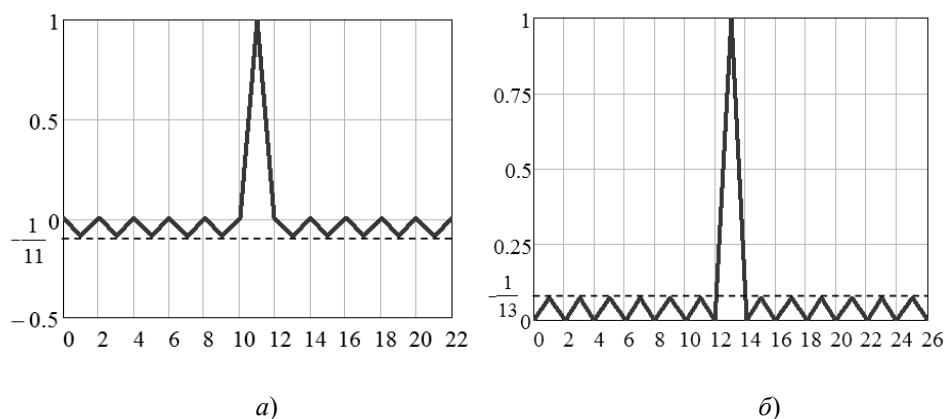


Рис. 1. АКФ сигналов Баркера (а) при  $N = 11$ ; (б) при  $N = 13$ 

Коды Баркера были получены им путем перебора, но существуют методы нахождения оптимальных кодовых последовательностей, не предполагающих слепой перебор. Такие методы основаны на отыскании кодов дающих одноуровневую периодическую функцию автокорреляции (ПФАК), после чего при помощи циклического сдвига полученной последовательности на  $l$  символов находят оптимальные. К таким последовательностям относятся коды упомянутые ранее: М-последовательности, коды квадратичных вычетов, Зингеровы коды и коды Якоби.

Построение кодов квадратичных вычетов базируется на использовании двухзначного характера мультипликативной группы простого поля  $GF(p)$  с числом позиций  $N = 4x + 3$ ,  $x = 0, 1, \dots$  В теории чисел для определения кодовой последовательности вводится понятие – символ Лежандра. Если есть символ Лежандра (символ  $n$  по отношению к  $N$ ), то символы последовательности Лежандра определяются как

$$a_i = \begin{cases} 1 & \text{при } n = 0 \pmod{N} \\ \left(\frac{n}{N}\right) & \text{при } n \neq 0 \pmod{N} \end{cases}$$

В табл. 2 приведены характеристики некоторых последовательностей квадратичных вычетов.

Таблица 2

#### Характеристики оптимальных кодов квадратичных вычетов

$N$	$l_{\text{опт}}$	$r_{\mu}$	$N$	$l_{\text{опт}}$	$r_{\mu}$
7	5	1	67	22	5
11	3	1	71	20	5
19	4 5 6 7 8 14 16 17	3	79	15 16 26 27 53 54 55 56	6
23	7 8 17	3	83	21 23 24 25	6
31	6 7 10 11 12 20 21 22 23 24	4	103	13 16 20 21 22 25 26 29 30 31 34 35 37 38 39 69 70 78 79 81 82	8
43	8 9 10 11 33 34 35 36	4	107	27 30 78 81 82 83	7
47	35	4	127	36 37	7
59	12 15 16 40 41 44 45 47	5	131	97 98 99	8

Зингеровы коды имеют длину  $N = (pn - 1) / (p - 1)$ , их построение основано на использовании свойств подобия и зависимости элементов поля  $GF(pn)$ . В табл. 3 приведены результаты расчетов оптимальных по минимаксному критерию импульсных кодов порождаемых Зингеровыми последовательностями.

Таблица 3

#### Характеристики оптимальных Зингеровых кодов

$N$	$l_{\text{опт}}$	$r_{\mu}$
4	0 1 2 3	1
6	2 3 4 5	2
8	3 4 5 6	3

13	12	1
40	9	5

Построение М-последовательностей базируется на свойствах поля  $GF(2n)$  при  $N = 2n - 1$ . Свойства М-последовательностей хорошо изучены. В табл. 4 приведены характеристики некоторых оптимальных кодов порождаемых М-последовательностями.

Таблица 4

**Характеристики оптимальных кодов  
порождаемых М-последовательностями.**

Из сравнения различных типов ПСП с одноуровневой ПФАК по минимаксному критерию оптимальности можно сделать вывод, что при использовании небольшого числа последовательностей нет разницы в выборе определенного типа ПСП. Более того при равной длине кодовые последовательности разных типов могут совпадать. Так, например, последовательность Лежандра длиной  $N = 11$  и код Зингера длиной  $N = 13$  совпадают с кодами Баркера; М – последовательность при  $N = 31$  совпадает с последовательностью Лежандра. Если же нужен широкий ансамбль последовательностей, то рационально применять М-последовательности.

Л и т е р а т у р а

82. Варакин, Л. Е. Системы связи с шумоподобными сигналами / Л. Е. Варакин – Москва : Радио и связь, 1985. – 384 с.
83. Свердлик, М. Б. Оптимальные дискретные сигналы / М. Б. Свердлик – Москва : Совет. радио, 1975. – 200 с.
84. Маковеева, М. М. Системы связи с подвижными объектами / М. М. Маковеева, Ю. С. Шинаков. – Москва : Радио и связь, 2002. – 440 с.