

Радиотехническая аппаратура и ее применение

УДК 621.391

Формирование нелинейных бинарных последовательностей с расширенным ансамблем

С.В. Мальцев, Р.П. Богуш

Предложен метод формирования нелинейных бинарных последовательностей с расширенным ансамблем; представлены результаты исследований и дано сравнение основных характеристик полученных последовательностей с известными сигналами.

The method of formation of non-linear binary sequences with an enlarged ensemble is proposed. The results of researches are presented and the comparison of the main characteristics of the obtained sequences with known signals is given.

Традиционными сигналами для систем передачи информации считаются коды, построенные на базе M -последовательностей [1, 2]. Однако малая структурная сложность, обусловленная линейностью и групповыми свойствами этих сигналов, затрудняет обеспечение секретности передачи информации, а относительно небольшой размер формируемого ансамбля накладывает ограничения на число абонентов в физически существующем канале связи. Повышение имито- и криптостойкости систем передачи информации возможно при использовании нелинейных сигналов.

Ц е л ь р а б о т ы – *представить метод формирования нелинейных бинарных последовательностей с расширенным ансамблем и определить качественные характеристики полученных последовательностей.*

Одним из путей формирования таких сигналов является использование нелинейных математических структур и их свойств. Вариант подобного подхода предложен в [3]. Полученные последовательности, названные авторами АВ кодами, отвечают требованиям, предъявляемым к автокорреляционной (АКФ) и взаимокорреляционной (ВКФ) функциям сигналов для использования в системах передачи информации. Нелинейность этих сигналов позволяет

предположить наличие высокой структурной сложности, хотя в [3] этот вопрос не рассматривался.

Для формирования нелинейных бинарных последовательностей представляют интерес математические структуры типа:

$$F(n_i) = \alpha n_i^\sigma (\ln n_i)^\tau,$$

где α, σ, τ – константы, удовлетворяющие условиям

$$\alpha \in \{R\}, \quad 0 < \sigma < 1, \quad \tau \in \{R\}, \quad n_i \in [1, N];$$

R – множество действительных чисел; N – длина формируемой последовательности.

Известно, что в функциях подобного типа в первом разряде после запятой значащие цифры десятичного представления результата вычислений распределены по равномерному закону. Следовательно, можно формировать бинарные последовательности с элементами a_i по правилу

$$a_i = x_i \bmod 2,$$

где x_i – значащая цифра десятичного представления результата вычислений в первом разряде после запятой.

Формирование бинарной последовательности длиной N осуществляется путем перебора i в диапазоне $1, 2, \dots, N$ при фиксированных значениях α, σ, τ . Для получения каждого символа последова-

тельности определяется лишь цифра в первом разряде после запятой десятичного представления результата вычислений.

Тип сигнала	Максимальное значение боковых пиков корреляционной функции			Эквивалентная линейная сложность			Разбаланс		
	1024	2048	4096	1024	2048	4096	1024	2048	4096
Голда	2,03	2,02	2,02	20	22	24	4,41	3,13	2,21
Касами	2,03	2,02	2,02	25	27,5	30	3,03	2,17	1,53
Бент-функции	1,03	1,02	1,02	64	128	256	0,09	0,04	0,02
Последовательности де Брейна	8,00	11,31	16,0	1022	2046	4094	-	-	-
Формируемые последовательности	2,74	3,24	3,03	1015	2037	4085	2,6	1,69	0,91

Формирование новой последовательности выполняется путем изменения параметров α , σ , τ . При этом величина размера ансамбля определяется количеством вариантов изменений значений α , σ , τ и практически неограниченна.

В результате эксперимента был сформирован массив последовательностей для проведения анализа свойств полученных сигналов. Сравнение АКФ и ВКФ сформированных последовательностей и АВ кодов, предлагаемых в [3], приводится на рисунке. Результаты эксперимента показывают, что представленные последовательности имеют улучшенную АКФ, а ВКФ обоих видов кодов с уве-

ансамбля, приведены в таблице. Анализ таблицы показал, что представленные последовательности характеризуются гораздо более высокой эквива-

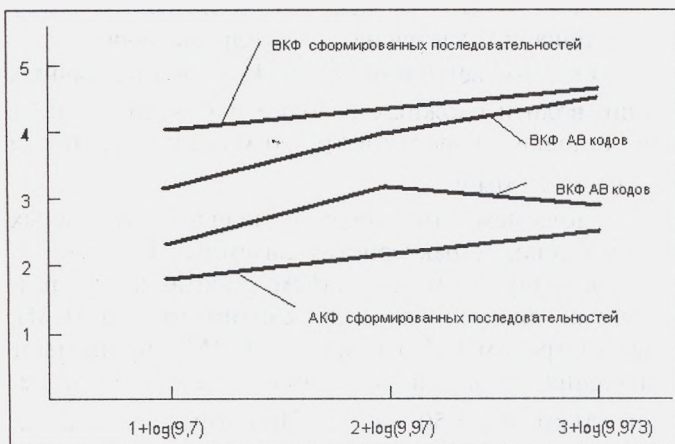
лентной линейной сложностью по сравнению с традиционными сигналами, и в то же время АКФ и ВКФ полученных последовательностей и сигналов на основе M -последовательностей достаточно близки. Несомненным достоинством предложенного метода является возможность получения последовательностей произвольной длины с практически неограниченным размером ансамбля.

- Нелинейные последовательности, полученные с использованием предлагаемого метода, благодаря свойствам АКФ и ВКФ могут применяться в системах связи множественного доступа с кодовым разделением каналов. Кроме того, высокая эквивалентная линейная сложность таких последовательностей делает их привлекательными для применения в современных комплексах закрытия информации, а также в помехозащищенных системах связи со скачкообразной перестройкой частоты.

Литература

1. Варакин Л.Е. Системы связи с шумоподобными сигналами. – М.: Радио и связь, 1985.
2. Gold R. Optimal binary sequences for spread spectrum multiplexing. – IEEE Trans. Inform. Theory IT-13, 1967, N 4.
3. Auslander L., Barbano P., Communication Codes and Bernoulli Transformation. – Appl. and Comp. Harm. Analysis, 1998, v. 5.
4. Стельмашенко Б.Г., Тараненко П.Г. Нелинейные псевдослучайные последовательности в широкополосных системах передачи информации. – Зарубежная радиоэлектроника, 1988, № 9.

Поступила после доработки 28 апреля 2000 г.



личением длины последовательностей асимптотически стремятся к одной и той же величине.

Сравнения параметров сигналов, полученных на основе предложенного метода и наиболее распространенных линейных и нелинейных последовательностей [4], имеющих значительный размер