УДК 621.396:621.391.26

КОРРЕЛЯЦИОННЫЕ ХАРАКТЕРИСТИКИ НЕКОТОРЫХ БИНАРНЫХ R4-КОДОВ И АНСАМБЛЕЙ СИГНАЛОВ НА ИХ ОСНОВЕ

Ю. В. Чепруков[а], *канд. техн. наук*
М. А. Соколов[б], *доктор техн. наук, профессор*
[а]*Российский государственный университет туризма и сервиса, филиал в г. Сочи, РФ*
[б]*Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, РФ*

Введение: *постоянное повышение эффективности различных систем управления и связи возможно при использовании более совершенных бинарных кодов и систем сигналов на их основе. Известные N элементные бинарные коды, используемые в упомянутых системах, не позволяют получить достаточно низкий уровень боковых пиков автокорреляционной и взаимной корреляционной функций совокупности кодов при вариации N в широких пределах. Целью работы является исследование вопросов синтеза N элементных бинарных кодов с заданными уровнями R и W боковых пиков автокорреляционной и взаимной корреляционной функций.* ***Результаты:*** *приведена таблица результатов синтеза кодов с R = 4 при N ≤ 32. Изложена в общем виде методика и особенности синтеза ансамблей бинарных кодов с заданным уровнем W боковых пиков взаимной корреляционной функции. Выдвинуты гипотезы и составлены модели, позволившие получить аналитические оценки количественных характеристик таких наборов кодов, приведен пример.* ***Практическая значимость:*** *возможно использование в системах управления и связи. Выдвинута идея шифрования с помощью этих кодов. Указана потенциальная возможность создания «тихих» компьютеров и компьютерных сетей, что может позже привести к разработке «тихого» Интернета.*

Ключевые слова *— ансамбли, системы сигналов, бинарные коды, автокорреляционная функция, уровень боковых пиков.*

Введение

В современных системах управления, связи и радиолокации широко используются шумоподобные сигналы (ШПС). Разновидностью ШПС являются фазоманипулированные сигналы [1], которые характеризуются бинарными кодовыми последовательностями, или просто кодами. Примером систем, в которых используются указанные сигналы, являются системы связи с кодовым разделением абонентов. Главным вопросом является выбор сигналов. Под системой понимается множество сигналов, определяемых единым правилом их построения [1]. Обозначим базу ШПС B^*. Число сигналов в системе L называют объемом системы сигналов. Система считается малой, когда $L = \sqrt{B^*} << B^*$, нормальной при $L \approx B^*$ и большой при $L >> B^*$. Существует нерешенная проблема разработки алгоритмов построения систем фазоманипулированных сигналов [1]. Примером малой системы являются функции Уолша, используемые в CDMA (Code Division Multiple Access — системы с кодовым разделением каналов) [2]. Представлены требования к системам сигналов для CDMA, которые сформулированы в виде минимаксного критерия качества. Системы сигналов, удовлетворяющие таким условиям, названы оптимальными. К ним отнесены, например, ансамбли Голда, Касами, Камалетдинова. В работе [3] отмечен недостаток упомянутых систем, заключающийся в сильной разреженности значений длин кодов ($N = 2^n - 1 = 3, 7, 15, 31, 63, 127...$; $n = 2, 3, ...$), что ограничивает их применение. Указанные системы основаны на M-последовательностях, характеристики которых изложены в работах [1, 3]. Из них следует, что минимальное значение уровня боковых пиков (УБП) автокорреляционной функции (АКФ) $B_1 \approx (0{,}7...1{,}25)/\sqrt{N}$, а УБП взаимной корреляционной функции (ВКФ) $B_2 \approx (1{,}4...5)/\sqrt{N}$. Используемый для исследований математический аппарат — поля Галуа. В монографии [4] дана классификация ансамблей и методов синтеза, указаны проблемы применения известных методов. Например, при синтезе ансамблей кодов на основе полей Галуа сейчас применяются таблицы полиномов первой половины прошлого века.

Вопросы синтеза кодовых последовательностей при наличии требований к периодической АКФ и ВКФ изложены в работе [5]. Однако предложенные варианты решения не предназначены для синтеза одиночных бинарных кодов и ансамблей.

Таким образом, вопросы синтеза ансамблей сигналов актуальны для широкого класса коммуникационных систем, но недостаточно исследованы.

В работе [6] сформулирована задача, предложен метод решения, представлены результаты синтеза для $R = 2{,}3$; $N \le 25$. Показаны существенные преимущества синтезированных кодов по сравнению с M-последовательностями.

Коды с $R = 1$ (коды Баркера) и коды с $R = 2;3$ ($R2$- и $R3$-коды) составляют подмножества $R4$-кодов

(согласно данному ниже определению), для них $R = 4$.

Краткий обзор литературы, проведенный в работе [7], показал, что сейчас в различных системах используются в основном давно предложенные и подробно изученные сигналы. Там же представлены результаты синтеза $R2$-кодов. Они эффективнее лучших кодов Баркера по относительному УБП в 14/13 раза, позволяют получить разнообразные коэффициенты сжатия (22 варианта) и количество кодов 480 достаточно велико. Составлена таблица $R2$-кодов. Обосновано предположение, что $N = 28$ соответствует максимальному порядку $R2$-кодов.

В данной работе получены $R4$-коды для $N \le 32$. Выполнен анализ их корреляционных характеристик, показаны возможности синтеза множества ансамблей сигналов.

Назовем бинарные коды, АКФ которых в области боковых пиков может изменяться в пределах $\pm R$ ($0 \le R \le N - 1$, R — целое), R-кодами. Они составляют множество $G_{R,N}$. Пусть $B_3 = R/N$ — относительная величина УБП АКФ кодов, а T — длительность каждого из N импульсов. Тогда можно обозначить

$$\left\{G^i_{R,N}\right\} = \left\{P^i_j,\ j = \overline{1,N}\right\},\ P^i_j = \pm 1,\ i = \overline{1, g_{R,N}} \qquad (1)$$

множество бинарных последовательностей условных значений начальных фаз $P^i_j = \pm 1$ импульсов, которые соответствуют R-кодам [6, 7], количество которых равно $g_{R,N}$. Здесь P^i_j — коэффициенты последовательностей, причем индексы i, j определяют, соответственно, порядковый номер последовательностей и различные элементы каждой из них. Совокупности R-кодов будем называть W-ансамблями, если значения ВКФ всевозможных пар кодов изменяются в пределах $\pm W (1 \le W \le N - 1$, W — целое). Эти совокупности составляют системы сигналов, если обладают свойствами, упоминавшимися выше. Цель работы — получить $R4$-коды (найти $G_{4,N}$ и $g_{4,N}$) для $N \le 32$, построить W-ансамбли, провести анализ их характеристик, высказать предложения по применению.

Задача и методика синтеза, особенности решения

Введем для R-кодов функции $S^*(t)$ и $S(t)$, которые определяют, соответственно, АКФ и его модуль. В моменты $t_k = kT$, отсчитываемые от начала АКФ, эти функции принимают экстремальные или нулевые значения, причем $S(t_N) = N$. Аналогично введем $V_{x,y}(t)$ для модуля ВКФ $R4$-кодов с индексами «x» и «y» (пояснения даны ниже). Эти функции также будем рассматривать в моменты $t_k = kT$, отсчитываемые от начала ВКФ. Тогда задача синтеза заключается в определении коэффициентов кодов, для которых выполняются неравенства [6, 7]

$$S(t_k) = \left|\sum_{j=1}^{k} P^i_j \cdot P^i_{N+j-k}\right| \le R;$$

$$k = \overline{1, N-1},\ i = \overline{1, g_{4,N}}. \qquad (2)$$

После решения получим $R4$-коды, которые можно пронумеровать (1, ..., $g_{4,N}$) и составить множество $G_{4,N}$. Коды из этого множества включаются в W-ансамбль, если для совокупности пар кодов выполняются условия

$$V_{x,y}(t_k) = \left|\sum_{j=1}^{k} P^x_j \cdot P^y_{N+j-k}\right| \le W;\ k = \overline{1, 2 \cdot N - 1}, \qquad (3)$$

где x, y ($x \ne y$) — номера (индексы) $R4$-кодов из множества $G_{4,N}$. Обозначим $H(N, R, W)$ количество W-ансамблей, но объем кодов в них может быть различным, поэтому введем величину $H(N, R, W, J)$, где J — численность каждой из систем сигналов, $J = 2$, ..., $g_{R,N}$. Следовательно, общее количество W-ансамблей равно сумме количества ансамблей численностью ($J1$, $J2$ ...): $H(N, R, W) = (H(N, R, W, J1) + H(N, R, W, J2) + ...)$. Примеры использования этих параметров даны ниже. Итак, задача синтеза (2), (3) решается в два этапа.

Этап 1: рассматривается система неравенств (2) и в соответствии с работами [6, 7] определяются $R4$-коды в количестве $g_{4,N}$, составляющие множество $G_{4,N}$. Перейдем к полученным результатам этапа 1.

Результаты синтеза $R4$-кодов

Некоторые результаты синтеза $R4$-кодов для $6 \le N \le 32$ представлены в табл. 1. Использован метод упорядоченного перебора [7]. Указаны коды с первым коэффициентом (+1) (прямые коды). Имеются в том же количестве коды с противоположными знаками всех коэффициентов, но их АКФ одинаковы. Прочерки во второй колонке означают, что для $N = 25$, ..., 30 общее количество кодов $g_{4,N}$ не определялось, но даны примеры. В первой и второй колонках указаны значения N и количество $R4$-кодов, а в третьей колонке — кодовые последовательности и половины их АКФ (в круглых скобках), так как они симметричны относительно максимума. Вычисления выполнены на общедоступном персональном компьютере, программы составлены на языке QBasic.

■ *Таблица 1*

N	$g_{4,N}$	$\{P_{i,j}\}$; ($S^*(t_k)$, $k = 1, \ldots, N$)
6	30	1,1,–1,–1,1,1; (1,2,–1,–4,1,6). 1,–1,–1,1,1,–1; (–1,2,1,–4,–1,6)
7	65	1,1,–1,–1,–1,1,1; (1,2,–1,–4,–3,2,7). 1,1,1,–1,–1,–1,1; (1,0,–1,–4,–1,2,7)
8	104	1,1,–1,–1,–1,–1,1,1; (1,2,–1,–4,–3,–2,3,8). 1,1,1,1,1,1,–1,1; (1,0,1,2,3,4,3,8)
9	194	1,1,1,1,–1,1,1,1,1; (1,2,3,4,1,2,3,4,9)
10	334	1,1,1,1,–1,1,–1,1,1,1; (1,2,3,2,1,0,–1,4,1,10)
11	616	1,1,1,1,–1,1,1,–1,1,1,1; (1,2,3,2,1,2,1,4,1,2,11)
12	936	1,1,1,1,–1,1,–1,–1,1,1,1,1; (1,2,3,4,1,0,–1,–4,1,2,3,12)
13	1672	1,1,1,1,1,–1,–1,1,–1,1,1,1,1; (1,2,3,4,3,2,–1,–2,–3,2,3,4,13)
14	2582	1,–1,1,1,1,–1,–1,1,–1,1,1,1,1,1; (1,0,1,2,3,0,3,–2,–1,0,1,2,1,14)
15	4130	1,1,–1,1,1,1,–1,–1,1,–1,1,1,1,1,1; (1,2,1,2,3,2,1,2,–3,0,1,2,1,2,15)
16	6170	1,1,1,1,1,1,–1,1,–1,–1,1,1,1,–1,1,1; (1,2,1,2,3,4,1,0,3,–4,1,2,3,2,3,16)
17	10202	1,1,1,–1,1,1,1,–1,–1,1,–1,1,1,1,1,1,1; (1,2,3,2,3,4,3,2,–1,2,–3,2,3,2,3,4,17)
18	13458	1,1,1,–1,1,1,1,1,–1,1,–1,–1,1,1,–1,–1,1,1; (1,2,1,–2,–1,4,3,–2,–3,0,3,–2,3,4,1,–4,1,18)
19	20316	1,1,1,1,1,–1,1,–1,1,1,–1,–1,1,1,–1,1,1,1,1; (1,2,3,4,3,2,3,0,–1,4,–1,0,1,0,3,4,1,2,19)
20	27490	1,1,1,1,1,1,–1,–1,1,1,–1,–1,1,–1,1,–1,1,1,1,1; (1,2,3,4,3,4,1,0,–1,–2,1,0,–1,–4,1,4,1,2,3,20)
21	41320	1,1,1,1,1,1,–1,1,–1,–1,1,1,–1,–1,–1,1,–1,1,1,1,1; (1,2,3,4,3,4,1,0,–3,–4,1,–4,1,0,–3,–2,1,2,3,4,21)
22	48870	1,1,1,1,1,1,–1,1,–1,1,–1,–1,1,–1,1,1,–1,–1,1,1,1,1; (1,2,3,4,3,2,1,2,–1,0,1,–2,–1,–4,1,0,3,–2,3,4,1,22)
23	68172	1,1,1,1,–1,–1,–1,1,1,–1,1,–1,1,–1,–1,1,1,–1,–1,1,1,1,1; (1,2,3,4,1,–2,–3,–2,1,2,3,–4,–3,2,1,2,–3,2,–1,–4,–3,2,23)
24	86124	1,1,1,1,1,1,–1,–1,–1,1,1,–1,1,–1,1,–1,–1,1,1,–1,1,1,1,1; (1,2,3,4,3,4,3,0,–3,–2,1,0,–1,–2,3,4,–3,–4,1,0,1,2,3,24)
25	–	1,1,1,1,1,–1,1,1,–1,1,–1,–1,1,1,1,–1,1,–1,–1,–1,1,1,1,–1,1; (1,0,1,2,3,0,3,–2,–3,0,–1,2,3,–2,1,0,3,2,1,–2,–1,0,1,0,25)
26	–	1,1,1,1,1,1,–1,–1,1,1,–1,–1,1,–1,1,–1,1,1,–1,1,–1,–1,–1,1,1,1,1; (1,2,3,4,3,2,1,–2,–1,0,1,4,–1,–2,1,–2,–1,4,1,–4,3,–2,3,0,1,26)
27	–	1,1,1,1,1,1,1,–1,–1,1,1,–1,–1,1,–1,1,–1,1,1,–1,1,–1,–1,–1,1,1,1,1; (1,2,3,4,3,2,3,0,–1,0,–1,2,3,0,–3,0,–1,0,3,0,–3,4,–1,4,1,2,27)
28	–	1,1,1,1,1,1,–1,–1,–1,1,1,1,1,–1,1,–1,1,–1,1,1,1,–1,–1,1,1,–1,1,1,1,1,1; (1,2,3,4,3,4,3,0,–3,–2,3,2,1,0,3,2,1,–2,3,4,1,0,–3,4,–3,2,3,28)
29	–	1,1,1,1,1,1,–1,–1,–1,1,1,1,1,–1,1,–1,1,1,1,–1,1,1,1,–1,–1,1,1,–1,1,1,1,1,1; (1,2,3,4,3,4,3,0,–3,–2,3,2,1,2,3,4,3,–2,3,4,1,2,1,–2,1,2,–1,4,29)
30	–	1,1,–1,1,1,1,1,1,1,–1,1,1,1,–1,1,–1,–1,–1,1,1,1,1,–1,1,–1,–1,1,–1,1,–1,1,1; (1,2,–1,0,3,0,3,–2,1,0,1,2,1,–4,1,–2,1,0,1,2,–3,4,3,2,–1,2,–1,4,–3,30)
31	286977	1,1,1,1,1,–1,1,1,1,–1,–1,1,1,–1,1,–1,1,–1,1,1,–1,1,–1,–1,1,1,–1,1,1,1,1,1; (1,2,3,4,3,2,3,2,1,4,–3,–2,3,4,1,–2,–1,4,1,2,3,–2,1,0,1,4,3,4,1,–2,31)
32	358464	1,–1,–1,1,1,1,1,1,1,1,–1,1,1,1,–1,–1,1,1,–1,1,–1,1,–1,–1,–1,1,1,1,1,1,–1,1,1,–1; (–1,2,1,–4,1,2,–1,0,–1,4,3,4,3,2,–1,–4,1,2,–3,4,–3,0,1,4,–3,–2,3,4,–1,–2,1,32)

Синтез *W*-ансамблей *R*-кодов

Перейдем к следующему этапу.

Этап 2: исследуется система неравенств (3), определяются *W*-ансамбли, находятся $H(N, R, W)$, $H(N, R, W, J)$. На этом этапе используется способ, применимый для произвольных значений (R, N, W). Он состоит в том, что берется множество $G_{R,N}$ и среди всех пар находятся такие коды, для которых УБП ВКФ превышает допустимое заданное значение. Возможно существование нескольких таких пар, они последовательно «разрываются» путем перемещения в разные вновь создаваемые подмножества. Это позволяет собрать в этих подмножествах лишь коды, для которых УБП ВКФ не более допустимой величины. Употребим этот способ и рассмотрим синтез *W*-ансамблей, используя все имеющиеся

$g_{4,N}$-коды. Обозначим $\mathbf{V}_{i,j}$ матрицу наибольших значений УБП модулей ВКФ всех пар (i, j) кодов из $G_{R,N}$ (учитывается корреляция каждого кода с номером i с произвольным другим кодом j). Эти значения матрицы ВКФ $\mathbf{V}_{i,j}$ потенциально могут принимать значения (1, ..., (N − 1)), причем наибольшая величина соответствует случаю, когда в $G_{R,N}$ имеются коды, различающиеся лишь одним символом. Очевидно, что $\mathbf{V}_{i,j} = \mathbf{V}_{j,i}$ и размер матрицы равен $g_{4,N} \times g_{4,N}$. Пример матрицы имеется ниже. Обозначим V_m и V_n наибольшее и наименьшее значения всех элементов $\mathbf{V}_{i,j}$. Введем набор $G0$ натуральных чисел (1, ..., $g_{4,N}$), позволяющий пронумеровать все коды, и назовем его исходным множеством номеров кодов. Рассмотрим следующие операции.

Шаг 0. В первую по счету строку табл. 2 записываются номера элементов $G0$. Это множество соответствует единственному $W = V_m$-ансамблю (здесь $H(N, R, V_m) = H(N, R, V_m, J) = 1$, $J = g_{4,N}$). В последней колонке даны значения УБП ВКФ и количество ансамблей, равное числу колонок со списками кодов.

Шаг 1. Из матрицы $\mathbf{V}_{i,j}$ выбираются пары индексов (s, u) ($s \neq u$) (s, u — индексы, порядковые номера R-кодов из $G0$), для которых ее значения равны V_m. Например, это пары ((s_1, u_1), ..., (s_{p1}, u_{p1})). Их необходимо «развести» путем перемещения в разные множества. Возможно появление разных типов пар индексов, существенно влияющих на результат. Ниже рассмотрены некоторые из них. Роль таких множеств выполняют колонки табл. 2. Для упрощения чтения цифровая часть индексов в строках таблиц поднята в строку (s_1 записано $s1$). Перед рассмотрением методики синтеза в общем виде, переходом к анализу и заполнению таблиц разберем несколько возможных вариаций образования пар номеров кодов, обоснуем для приложения выбор типичных версий.

Отвлечемся от действий 1-го шага и сформулируем способ пересмотра всех пар (s, u) номеров кодов из $G0$. Это возможно при изменении индексов по следующему правилу: для каждого s = 1, ..., ($g_{4,N}$ − 1) проводится вариация значений $u = s + 1$, ..., $g_{4,N}$, при этом всегда будет справедливо $s < u$. Перейдем к рассмотрению некоторых вариантов образования пар индексов. Это позволит позже дать оценку количества ансамблей, получаемых в результате удалений. На нее существенное влияние оказывает соотношение между номерами кодов разделяемых пар.

Вариант 1: все p_1 пар состоят из различных индексов, т. е. (s_1, u_1), (s_2, u_2), ..., (s_{p1}, u_{p1}). Это означает, что имеются ансамбли из двух кодов, удаления не требуются и надо перейти к следующему шагу методики.

Вариант 2: имеется множество пар с одинаковым первым номером пары (s_1, u_1; s_1, u_2; s_1, u_3; ...). Учитывая, что пары требуется разделить, целесообразно их объединить в обобщенную пару номеров (s_1, (u_1, u_2, u_3, ...)), тогда при разрыве пар удаляется s_1 либо все индексы в скобке. Синтез ансамблей начинается с анализа пар, имеющих наибольшее значение ВКФ. Целесообразно обратиться к парам, относящимся к случаю варианта 2, например (s_1, (u_1, u_2, u_3)). Укажем на другие модификации пар.

Вариант 3: простые пары (s, u) с индексом s, близким к своему наибольшему значению ($g_{4,N}$ − 1). Так как $u > s$ и $u \leq g_{4,N}$, то количество вариантов значений для u будет мало, что и определяет образование небольшого количества таких простых пар, а не обобщенных.

Вариант 4: имеется набор номеров кодов, в котором часть индексов удалена при выполнении предыдущих действий. Далее в соответствии с методикой удаляются оставшиеся не удаленными индексы либо никакие действия не осуществляются, если один из индексов простой пары или они оба оказались в числе ранее удаленных. То же касается обобщенных пар. Количество колонок в таблице не увеличивается (примеры ниже).

Вернемся к 1-му шагу. В 1-й колонке табл. 2 используется двойной индекс: первое число — номер шага; второе число — номер операции разделения пар кодов. Поэтому п. 1.2 означает, что рассматривается 2-я операция 1-го шага для УБП ВКФ V_m. Во 2-й строке табл. 2 показано разделение кодов в разные колонки. Начиная со 2-й по счету строки, в колонках приводятся индексы удаляемых кодов. Поэтому во 2-й строке 2-й и 3-й колонок удалены коды с индексами s_1 и (u_1, u_2, u_3) соответственно, а коды со всеми другими индексами сохраняются (номера удаленных кодов отмечаются знаком (^)). В результате колонка разделяется надвое и образуется два новых списка номеров индексов. Будем называть такие совокупности текущими множествами номеров кодов.

■ ***Таблица 2***

№ п. п.	Группы индексов						V_{ij}
0	(1,2, ..., $g_{4,N}$)						$V_m/1$
1.1	($\hat{s}1$)			($\hat{u}1$, $\hat{u}2$, $\hat{u}3$)			$V_m/2$
1.2	($\hat{s}1$; $\hat{s}2$)		($\hat{s}1$; $\hat{u}4$, $\hat{u}5$, $\hat{u}6$)	($\hat{u}1$, $\hat{u}2$, $\hat{u}3$; $\hat{s}2$)		($\hat{u}1$, $\hat{u}2$, $\hat{u}3$; $\hat{u}4$, $\hat{u}5$, $\hat{u}6$)	$V_m/4$
1.3	($\hat{s}1$; $\hat{s}2$; $\hat{s}3$)	($\hat{s}1$; $\hat{s}2$; $\hat{u}5$)	($\hat{s}1$; $\hat{u}4$, $\hat{u}5$, $\hat{u}6$)	($\hat{u}1$, $\hat{u}2$, $\hat{u}3$; $\hat{s}2$; $\hat{s}3$)	($\hat{u}1$, $\hat{u}2$, $\hat{u}3$; $\hat{s}2$; $\hat{u}5$)	($\hat{u}1$, $\hat{u}2$, $\hat{u}3$; $\hat{u}4$, $\hat{u}5$, $\hat{u}6$)	$V_{m-1}/6$

Их количество фиксируется в последней колонке, и после рассмотренного разделения обобщенной пары оно равно двум. Процедура аналогично проводится и для других пар. Например, для (s_2, (u_4, u_5, u_6)) проведено разделение, результаты занесены в 3-ю строку табл. 2, количество колонок (текущих множеств номеров кодов) равно четырем.

Ниже понадобится следующее по порядку убывания значение УБП ВКФ, обозначим его V_{m-1}. Оно может отличаться от V_m более чем на единицу. Допустим, $V_m = N - 1$, тогда последующее в таком ряду значение $\mathbf{V}_{i,j}$ может быть, к примеру, $V_{m-1} = N - 3$. Также заметим, что символ «V» относится к матрице, а родственная величина «W» — к ансамблям. Полученные в результате проведения операций на выбранном шаге текущие множества номеров соответствуют W-ансамблям.

При рассмотрении методики количество операций разделения обобщенных пар может быть велико. Индекс s непременно будет приближаться к своему наибольшему значению ($g_{4,N} - 1$), поэтому в соответствии с данными ранее объяснениями вероятно появление простых пар (вариант 3), например (s_3, u_5).

Для наборов в 3-й строке 2-й колонки разделение есть (получим 4-ю строку, 2-ю и 3-ю колонки), а 3-я строка, 3-я колонка не делится, дадим пояснения. Показан один из вариантов последствий, связанных с повторным появлением одного из номеров индексов в паре (здесь это u_5). Такой номер появлялся ранее в другой паре (возможность указана в варианте 4). Следовательно, в текущем множестве (3-я строка, 3-я колонка) ничего удалять не требуется, так как пара (s_3, u_5) разорвана путем удаления u_5 в предыдущей строке и указанная колонка не разделяется. То же относится и к набору номеров из 3-й строки 5-й колонки. В результате количество кодов не удваивается, а становится равным шести (последняя колонка 4-й строки). Иначе говоря, часть ансамблей может состоять из кодов, для которых все пары имеют УБП ВКФ меньше V_m, поэтому для них на этом шаге удаления не производятся, они не делятся (содержат коды с достаточно хорошими корреляционными свойствами).

По итогам операций 1-го шага получены текущие множества, представленные в 4-й строке, у которых УБП ВКФ меньше, чем был ранее. Обозначим их $G1(i)$, $i = (1, ..., 6)$. Они составляют $W = V_{m-1}$ -ансамбли в количестве $H(N,R,V_{m-1}) = 6$. С учетом проведенных удалений два ансамбля имеют численность $J1 = g_{4,N} - 3$ (это следует из 2-й, 3-й колонок), один — $J2 = g_{4,N} - 4$ (4-я колонка), два — $J3 = g_{4,N} - 5$ (5-я, 6-я колонки), один — $J4 = g_{4,N} - 6$ (7-я колонка). Следовательно, $H(N, R, V_{m-1}, J1) = 2$, $H(N, R, V_{m-1}, J2) = 1$, $H(N, R, V_{m-1}, J3) = 2$, $H(N, R, V_{m-1}, J4) = 1$, а всего 6.

Шаг 2. Выполняются операции, изложенные для шага 1, с учетом значений матрицы ВКФ, равных $\mathbf{V}_{i,j} = V_{m-1}$, формируются новые пары. Например, рассмотрим набор (s_1, (u_k, u_m, u_n)), где индексы во внутренних скобках примем (s_2, s_3, u_6). Количество колонок стремительно увеличивается. Перенесем первые четыре колонки табл. 2 в новую табл. 3, добавив еще одну для значения УБП ВКФ и количества текущих множеств (ансамблей кодов здесь три). Остальные колонки транспортируем в табл. 4. В созданных таблицах повторена последняя строка, так как конец одного шага удобно считать началом другого.

В табл. 3 индекс s_1 удален ранее, поэтому пары для разрыва отсутствуют, колонки не меняются. В табл. 4 пары «разъединяются» путем удаления s_1 либо (s_2, s_3, u_6), причем какие-то из этих индексов оказываются удаленными ранее. Для удобства последующей проверки удаляемые номера отделяются в строках таблиц знаком (;) и записываются в порядке их удаления, а не по порядку

■ ***Таблица 3***

№ п. п.	Группы индексов				V_{ij}
2.1	($\hat{s}1$; $\hat{s}2$; $\hat{s}3$)		($\hat{s}1$; $\hat{s}2$; $\hat{u}5$)	($\hat{s}1$; $\hat{u}4$, $\hat{u}5$, $\hat{u}6$)	$V_{m-1}/3$
2.2	($\hat{s}1$; $\hat{s}2$; $\hat{s}3$)		($\hat{s}1$; $\hat{s}2$; $\hat{u}5$)	($\hat{s}1$; $\hat{u}4$, $\hat{u}5$, $\hat{u}6$)	$V_{m-1}/3$
2.3	($\hat{s}1$; $\hat{s}2$; $\hat{s}3$; $\hat{u}5$)	($\hat{s}1$; $\hat{s}2$; $\hat{s}3$; $\hat{u}6$)	($\hat{s}1$; $\hat{s}2$; $\hat{u}5$)	($\hat{s}1$; $\hat{u}4$, $\hat{u}5$, $\hat{u}6$)	$V_{m-2}/4$

■ ***Таблица 4***

№ п. п.	Группы индексов							V_{ij}
2.1	($\hat{u}1$, $\hat{u}2$, $\hat{u}3$;$\hat{s}2$; $\hat{s}3$)			($\hat{u}1$, $\hat{u}2$, $\hat{u}3$; $\hat{s}2$; $\hat{u}5$)		($\hat{u}1$, $\hat{u}2$, $\hat{u}3$; $\hat{u}4$, $\hat{u}5$, $\hat{u}6$)		$V_{m-1}/3$
2.2	($\hat{u}1$, $\hat{u}2$, $\hat{u}3$; $\hat{s}2$; $\hat{s}3$; $\hat{s}1$)		($\hat{u}1$, $\hat{u}2$, $\hat{u}3$; $\hat{s}2$, $\hat{s}3$, $\hat{u}6$)	($\hat{u}1$, $\hat{u}2$, $\hat{u}3$; $\hat{s}2$; $\hat{u}5$; $\hat{s}1$)	($\hat{u}1$, $\hat{u}2$, $\hat{u}3$; $\hat{s}2$; $\hat{u}5$; $\hat{s}3$, $\hat{u}6$)	($\hat{u}1$, $\hat{u}2$, $\hat{u}3$; $\hat{u}4$, $\hat{u}5$, $\hat{u}6$; $\hat{s}1$)	($\hat{u}1$, $\hat{u}2$, $\hat{u}3$; $\hat{u}4$, $\hat{u}5$, $\hat{u}6$; $\hat{s}2$, $\hat{s}3$)	$V_{m-1}/6$
2.3	($\hat{u}1$, $\hat{u}2$, $\hat{u}3$; $\hat{s}2$; $\hat{s}3$; $\hat{s}1$; $\hat{u}5$)	($\hat{u}1$, $\hat{u}2$, $\hat{u}3$; $\hat{s}2$; $\hat{s}3$; $\hat{s}1$; $\hat{u}6$)	($\hat{u}1$, $\hat{u}2$, $\hat{u}3$; $\hat{s}2$, $\hat{s}3$, $\hat{u}6$)	($\hat{u}1$, $\hat{u}2$, $\hat{u}3$; $\hat{s}2$; $\hat{u}5$; $\hat{s}1$)	($\hat{u}1$, $\hat{u}2$, $\hat{u}3$; $\hat{s}2$; $\hat{u}5$; $\hat{s}3$, $\hat{u}6$)	($\hat{u}1$, $\hat{u}2$, $\hat{u}3$; $\hat{u}4$, $\hat{u}5$, $\hat{u}6$; $\hat{s}1$)	($\hat{u}1$, $\hat{u}2$, $\hat{u}3$; $\hat{u}4$, $\hat{u}5$, $\hat{u}6$; $\hat{s}2$, $\hat{s}3$)	$V_{m-2}/7$

из первоначального следования в 1-й строке табл. 2 (если удаляется, например, s_1, то записываем его в конце строки удаления, а не в начале). В конце этого шага, как и предыдущего, в соответствии с изложенными ранее причинами, рассмотрим простую пару (по варианту 3). Допустим, это (s, u), где $s = u_5$, $u = u_6$. В табл. 3 набор номеров (2-я колонка, 2-я строка) делится, а 3-я и 4-я колонки — нет, так как там u_5, а (u_5, u_6) уже удалены. В табл. 4 по тем же причинам разделяется лишь совокупность номеров (2-я колонка, 2-я строка), а все другие — нет. В конце 2-го шага получим текущие множества $G2(i)$, $i = (1, ..., 11)$, составляющие $W = V_{m-2}$-ансамбли (3-я строка табл. 3, 4). Здесь $H(N, R, V_{m-2}) = 11$ (общее количество последних колонок указанных таблиц) и $J1 = g_{4,N} - 3$, $J2 = g_{4,N} - 4$, $J3 = g_{4,N} - 6$, $J4 = g_{4,N} - 7$, $J5 = g_{4,N} - 8$, т. е. $H(N, R, V_{m-1}, J1) = 1$, $H(N, R, V_{m-1}, J2) = 3$, $H(N, R, V_{m-1}, J3) = 4$, $H(N, R, V_{m-1}, J4) = 2$, $H(N, R, V_{m-1}, J5) = 1$ (всего 11). Эти наборы параметров интересны для исследования дифференциации по численности.

Шаг 3. Процедура повторяется до получения W-ансамблей с требуемым объемом кодов, необходимым значением УБП ВКФ либо при достижении V_n. Если в ансамблях остается лишь два кода либо значения УБП ВКФ для всех пар кодов равны, то операции с ними далее не производятся. Введем $\hat{G}_{R,N,W}$ — множество номеров кодов, удаленных при реализации методики. Тогда, если интерпретировать W как искомое множество номеров кодов, эти индексы ансамблей можно представить в виде разности множеств $W = G_{R,N} / \hat{G}_{R,N,W}$ (исходное множество без удаленных индексов). Окончательные результаты получаются, если в исходной последовательности (1-я строка табл. 2) удалить индексы, записанные в последних строках табл. 3, 4. После нахождения $H(N,R,V_n)$, $H(N,R,V_n,J)$ и нужных кодов рассмотрение задачи завершается.

Заметим, что параметр J (численность наборов кодов) по существу соответствует использованной ранее величине L — количеству сигналов, а $B^* = N$ (для бинарных кодов). Сравнивая все J с N, можно делать выводы о соответствии полученных W-ансамблей введенным понятиям о системе сигналов и ее объеме. Так как количество ансамблей равно $H(N, R, W, J)$, то допустимо говорить о синтезе комплекта или совокупности систем бинарных сигналов.

В первой строке табл. 2 даны номера исходного множества кодов, а в последней колонке — УБП ВКФ и количество наборов (колонок с номерами).

Уделим внимание матрице $\mathbf{V}_{i,j}$, конкретизация которой в начале методики синтеза при рассмотрении задачи в общем виде, возможно, отвлекла бы внимание от сути задачи. Теперь целесообразно представить ее с учетом проведенных операций. Матрица изображена в виде табл. 5, где даны две системы обозначений индексов i, j: по порядку номеров (условно до $g_{4,N} = 9$) и в соответствии с обозначениями индексов в рассмотренной выше методике (в скобках). Значения в ячейках заданы согласно проведенным операциям (V_m и V_{m-1}), а все прочие заданы символически величинами V_{m-2}. Элементы главной диагонали не относятся по смыслу к $\mathbf{V}_{i,j}$ и вычеркнуты.

Данная матрица позволяет полнее изложить сущность методики синтеза.

Количество ансамблей $H(N,R,W)$ можно получить, проведя все указанные операции методики, но их трудоемкость велика, и желательно иметь аналитическое выражение для приближенной оценки. Получим такое соотношение.

Общее количество всевозможных пар (s, u) равно $Po = g_{R,N}(g_{R,N} - 1)/2$. Предположим, что для любого значения матрицы ВКФ в образовании пар участвуют почти все коды. То есть коды в $G0$ не разделяются на совокупности, в которых для некоторых значений $\mathbf{V}_{i,j}$ пары образуются

■ ***Таблица 5***

i / *j*	1 (*s*1)	2 (*s*2)	3 (*s*3)	4 (*u*1)	5 (*u*2)	6 (*u*3)	7 (*u*4)	8 (*u*5)	9 (*u*6)
1 (*s*1)		V_{m-1}	V_{m-1}	V_m	V_m	V_m	V_{m-2}	V_{m-2}	V_{m-1}
2 (*s*2)	V_{m-1}		V_{m-2}	V_{m-2}	V_{m-2}	V_{m-2}	V_m	V_m	V_m
3 (*s*3)	V_{m-1}	V_{m-2}		V_{m-2}	V_{m-2}	V_{m-2}	V_{m-2}	V_m	V_{m-2}
4 (*u*1)	V_m	V_{m-2}	V_{m-2}		V_{m-2}	V_{m-2}	V_{m-2}	V_{m-2}	V_{m-2}
5 (*u*2)	V_m	V_{m-2}	V_{m-2}	V_{m-2}		V_{m-2}	V_{m-2}	V_{m-2}	V_{m-2}
6 (*u*3)	V_m	V_{m-2}	V_{m-2}	V_{m-2}	V_{m-2}		V_{m-2}	V_{m-2}	V_{m-2}
7 (*u*4)	V_{m-2}	V_m	V_{m-2}	V_{m-2}	V_{m-2}	V_{m-2}		V_{m-2}	V_{m-2}
8 (*u*5)	V_{m-2}	V_m	V_m	V_{m-2}	V_{m-2}	V_{m-2}	V_{m-2}		V_{m-1}
9 (*u*6)	V_{m-1}	V_m	V_{m-2}	V_{m-2}	V_{m-2}	V_{m-2}	V_{m-2}	V_{m-1}	

из кодов одного списка номеров, а для других $\mathbf{V}_{i,j}$ — иного комплекта кодов. Иначе говоря, отсутствует группировка кодов, и в парах участвуют примерно одинаково часто все коды. Это приводит к тому, что когда для пар (s, u) индексы s и u изменяются пропорционально соответственно от 1 до ($g_{R,N} - 1$) и от $s + 1$ до $g_{R,N}$, то и количество пар в целом, можно ожидать, будет изменяться с такой же закономерностью. Поэтому, пока s мало, то количество версий составления обобщенных пар со всеми другими кодам велико.

При разделении таких пар происходит раздвоение текущих множеств и колонок таблиц, в которые они входили. Общее количество множеств, а потом и ансамблей увеличивается. Поэтому можно сделать два предположения:

1) если имеется Pr обобщенных пар, то из исходного набора кодов при последовательном делении этих пар можно получить новые множества, количество которых будет равно $N_W \sim 2^{Pr}$, и это справедливо для любой первоначальной совокупности кодов любого текущего множества. Иначе говоря, для любой операции и на всех шагах каждое множество номеров кодов непременно должно содержать также номера кодов, входящих в рассматриваемую обобщенную пару, и поэтому обязательно осуществляется деление надвое;

2) весь комплект простых пар всегда разделяется на предыдущих операциях с обобщенными парами. Когда доходит очередь до операций с простыми парами (вариант 4), то деления не происходит.

Практически эти условия могут не всегда выполняться, что приведет к погрешностям оценок. Однако условия 1 и 2 являются разнохарактерными (невыполнение 1-го приводит к уменьшению, а 2-го — к росту количества множеств), поэтому их одновременное невыполнение может привести к компенсации и результату, близкому к истинному. Учтя указанную неопределенность путем расширения значений ξ, введем искомую оценку в виде

$$N_W = 2^{\xi},\ \xi = Pr \pm 1. \qquad (4)$$

Положения 1, 2 возьмем за основу создания *модели 1* вычисления количества ансамблей. В дальнейших работах она может быть уточнена на основании более подробного анализа матрицы $\mathbf{V}_{i,j}$.

Заметим, что количество обобщенных пар зависит от параметров сигналов, что можно в общем виде представить функцией $Pr = f(N, R, W)$. Для ее нахождения используется матрица ВКФ (см. табл. 5). Например, для $W = V_{m-1}$ нужно принять во внимание и все индексы, соответствующие большим значениям ВКФ (не только для V_{m-1}, но и для V_m). Начнем с уровня V_m и выберем s_1 во 2-й колонке. Движемся вниз по строчкам, находящимся ниже главной диагонали матрицы (т. е., начиная со 2-й строчки). Определяем для выбранного значения ВКФ величины 2-го индекса обобщенной пары. Это позволяет найти такую пару, состоящую из индексов (s_1, (u_1, u_2, u_3)). Потом отметим s_2 в 3-й колонке, спускаемся ниже диагонали до 3-й строчки и для V_m определяем вторые индексы и всю пару (s_2, (u_4, u_5, u_6)). Действуя сходно для s_3, получим набор (s_3, u_5) (это не обобщенная пара). Видно, что других вариантов нет, для этого шага $Pr = 2$. Того же достигнем, если двигаться по колонкам. Далее задаем V_{m-1}, действуем аналогично, находим обобщенную пару (s_1, (s_2, s_3, u_6)), а (u_5, u_6) таковой не является. Всего получим $Pr = 3$ и для $\xi = Pr$ справедливо $N_W = 8$, что меньше $H(N, R, V_{m-2}) = 11$. Различия связаны с условностью выбора обобщенных пар для наглядной иллюстрации разнообразных случаев. Имеются ограничения на применение модели 1 для W, близких к V_n, когда по указанным ранее причинам множества не разделяются и операции с ними не осуществляются. Итак, в результате анализа количество ансамблей можно оценить величиной $H(N,R,W) \approx N_W = 2^{\xi}$ ($\xi = Pr \pm 1$).

Далее исследуем изменение числа кодов J в ансамблях в зависимости от W при фиксированных N, R. Ранее отмечалось, что после разрыва пар количество кодов быстро растет, поэтому рассмотрим указанную зависимость для случая, когда после разделения пар сохраняются не два, а один набор кодов. Удобно оставлять для дальнейшего анализа исключительно наборы с удаленным первым индексом пары. Это означает, что в табл. 2–4 сохраняется лишь крайняя левая колонка с номерами кодов. Так, при «разделе» простой пары (s, u) из двух текущих множеств ($G_1(\hat{s})$ и $G_1(\hat{u})$) оставляется единственно первый, а при операции с двумя парами (s_1, u_1), (s_2, u_2) из четырех возможных оставляется только $G_2(\hat{s}1, \hat{s}2)$. В итоге можно быстрее получить хотя бы не полный, а частичный результат для предварительного анализа (ценой потери общности решения). Это важно при больших N. Теперь требуется наблюдать за изменениями одного множества кодов после каждого «обрыва» пар и можно получать для разных W хотя бы по одному ансамблю из всех. Применим такой подход («быстрый синтез») для поиска зависимости количества кодов в ансамбле от уровня W.

Приведем соображения для обоснования требуемого аналитического соотношения. Выберем один из R-кодов с $W = V_n$. В бинарных кодах коэффициенты принимают значения (±1). Будем рассматривать, для конкретности, коды с $P_1 = 1$, а все другие P_j пусть могут соответствовать любому из этих двух вариантов. Поэтому будем последовательно, начиная с P_2, варьировать знаки коэффициентов, получая наборы разнообразных

кодов. Если осуществить это с P_2, то вместе с исходным кодом получим всего $n = 2$ кода; если изменить P_2 и P_3, то всего будет $n = 4$ кода, т. е. при последовательном изменении знаков t коэффициентов получим $n = 2^t$ вариантов кодов. Обоснуем связь t и W. Пусть t мало, тогда лишь небольшое количество кодов может удовлетворять жестким корреляционным требованиям и составлять ансамбли с W, близким к V_n (это могут быть наборы из двух, трех кодов). При увеличении t количество вариантов комбинаций будет расти, и для получения больших по численности ансамблей непременно необходимо увеличивать W. Однако при этом не все коды могут удовлетворять требованиям (2), и функциональная связь t и W существенно изменится (пример ниже). Вместе с ростом W и приближением его к V_m количество R-кодов, различающихся лишь одним символом, невелико. С другой стороны, известно, что ВКФ есть сумма произведений коэффициентов двух сдвигаемых друг относительно друга последовательностей. Следовательно, ориентируясь на наихудший случай, вместе с изменениями знаков кодов и повышением их количества найдутся такие пары, что для них пропорционально увеличится максимальное значение УБП ВКФ, поэтому создание больших по объему ансамблей возможно лишь при росте W. С учетом всех приведенных обстоятельств логично предположить, что $W \sim t$, и тогда $n \approx 2^W$. Дополнительно подчеркивая зависимость n от W, запишем $n_W \approx 2^W$. Ранее численность ансамблей обозначалась символом J. Поэтому $J_W \approx 2^W$ — оценка объема W-ансамблей R-кодов при вариации W.

Из проведенных рассуждений сформулируем два положения:

1) численность W-ансамблей пропорциональна показательной функции от W ($J_W \approx 2^W$);

2) указанная закономерность справедлива для всех W-ансамблей.

Эти высказывания примем как гипотезы и возьмем за основу *модели 2* вычисления количества кодов в W-ансамблях. Она применима, как было обосновано, лишь для W, которые заметно меньше V_m. Степень корректности моделей 1, 2 можно будет оценить впоследствии на основании разбора результатов синтеза. Совместное применение обеих моделей позволяет найти объем и численность ансамблей R-кодов, при этом считается, что число J_W кодов во всех наборах одинаковое.

Назовем зависимость характерной численности от уровня W ансамблей ($J_W \approx 2^W$) калибровочной характеристикой. Пусть $J_W = \alpha 2^{W(1-Vn/N)}$, где α — неопределенный коэффициент, подлежащий выбору. Для построения графика удобно провести переобозначение

$$Q(W) = \alpha 2^{W(1-Vn/N)}. \qquad (5)$$

Уровень α выбирается из условия нормировки: при $W = V_n$ имеем минимально возможную численность $J_{W\ \min} = 2$. Подставив $J_W = Q = 2$ в левую часть (5), получим α, которую обозначим $\alpha 1$ (1-й вариант):

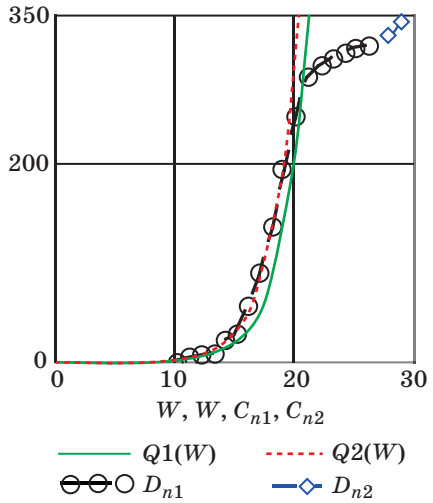
$$\alpha = \alpha 1 = 2^{1-\delta}, \text{ где } \delta = (1 - V_n/N)V_n. \qquad (6)$$

Для $N = 30$, $V_n = 10$ вычислим по (6) $\alpha 1 \approx 0{,}02$ и получим калибровочную характеристику $Q1(W) = 0{,}02 \cdot 2^{W \cdot 2/3}$.

Это соотношение, установленное на основании модели 2, сопоставим с имеющимися результатами синтеза $R3$-кодов (они входят в множество $R4$-кодов) с $N = 30$, для которых $g_{3,30} = 344$. Использован «быстрый синтез», найдена функция $J = D_n(W)$ — зависимость численности ансамблей J от уровня W (это дискретная функция с дискретным аргументом), а также $V_n = 10$, $V_m = 29$ (при $W = 27$ ансамбли отсутствуют). Результаты синтеза представлены ниже графически.

Согласно модели 2, объем всех ансамблей одинаков и равен характерной численности $J_W = Q(W)$ (расчетная характеристика). Вместе с тем для одного из ансамблей по результатам синтеза получена $J = D_n(W)$ (фактическая зависимость), следовательно, имеются основания для сравнения $Q(W)$ и $D_n(W)$. Введем для дальнейшего применения нормированную величину $C = W/N$, которая определяет «долю» W относительно N.

Графики дискретной функции $D_n(W)$, данной в форме отсчетов, и калибровочной характеристики $Q1(W)$, представленной в виде непрерывной линии, приведены на рисунке. По оси абсцисс отложены уровни W, которые могут изменяться в пределах [1, ..., 29], а по оси ординат — значения указанных функций, способные варьироваться в интервале [2, 344]. Знаком ○ отмечены дискретные величины для W из интервала [10, ..., 26], а ◇ — на промежутке [28, 29].



■ Калибровочные характеристики

Такая калибровочная характеристика является универсальной и может быть применена в интервале $[W_н, W_в]$, где $W_н = V_n$, а $W_в = N/\sqrt{2}$, однако при этом максимальная погрешность составляет около 42 % (для центральных значений аргумента). Вместе с тем возможно увеличение точности. Если W принадлежит интервалам [10; 14] или [20; 21] (для C это [0,33; 0,47] и [0,67; 0,7]), то погрешность менее 10 %. Когда W принимает значения между (14; 20) (C в пределах (0,47; 0,67)), то необходимо определять коэффициент α по формуле (2-й вариант)

$$\alpha = \alpha 2 = (1 + V_n/N)2^{1-\delta},$$
$$\delta = (1 - V_n/N)V_n. \qquad (7)$$

Тогда округленно $\alpha = \alpha 2 = 0{,}03$, а график $Q2(W)$ пунктирно дан на рисунке, причем точность значительно увеличилась. Итак, модель 2 качественно совпадает с результатами синтеза в широком диапазоне вариаций аргумента.

Если задать параметры N, R, W, определить $g_{R,N}$, найти уровень V_n, то, используя (5)–(7) и варьируя W от 1 до N–1, возможно получить искомую оценку $J_W = Q(W)$ численности W-ансамблей. Она может изменяться от двух до $g_{R,N}$. Для $R4$-кодов $g_{R,N}$ велико, поэтому могут быть получены W-ансамбли большой численности, а также составлены комплекты ансамблей (системы сигналов).

Анализ позволил оценить характерную численность ансамблей, но актуальной задачей является и определение диапазона отклонений σ_W от уровня J_W. Если J_W — характерная численность большинства ансамблей из общего их количества, то интересно оценить, какие значения объемов ансамблей еще возможны.

В рамках методики синтеза во всех множествах проводятся удаления. При наименьшем количестве удаленных индексов численность ансамблей будет наибольшей (левые колонки табл. 2–4). Если удаляется много номеров, то объем ансамблей мал (крайние правые столбцы таблиц). Максимальную численность $J_{W\max}$ будут иметь ансамбли, в которых каждый из Pr раз будет удаляться по одному индексу кодов, поэтому $J_{W\max} = g_{R,N} - Pr$. Введем уровни, по которым будут определяться отклонения σ_W. Обозначим $J_{W в} = (J_{W\max} + J_W)/2$ и $J_{W н} = (J_{W\min} + J_W)/2$ верхнюю и нижнюю граничные численности W-ансамблей. Теперь определим отклонение соотношением $\sigma_W = J_{W в} - J_{W н}$, тогда получим

$$\sigma_W = (g_{R,N} - Pr)/2 - 1. \qquad (8)$$

Численность основного объема ансамблей изменяется в интервале $[J_W - 0{,}5\sigma_W; J_W + 0{,}5\sigma_W]$, в котором средним значением является J_W — численность большинства ансамблей основного объема.

Для удобства и компактного анализа рассмотрим простейший **пример**.

Дано: $N = 5$, $R = 3$, $g_{3,N} = 14$, $Pr = 7$, $V_n = 2$. *Найти*: все расчетные характеристики W-ансамблей (N_W, J_W, σ_W).

Решение:

1) исходные коды составляют один ансамбль с $W = 4$, и можно синтезировать ансамбли с $W = 2{,}3$. Как отмечалось, модель 1 не применима для малых W, поэтому Pr задано лишь для $W = 3$. Используем (4) для $\xi = Pr$ и получим $N_3 = 128$;

2) так как $C = 0{,}6$ для $W = 3$, то, применив (7), найдем $\alpha 2 = 1{,}22$ и с помощью (5) вычислим $J_3 = Q(3) = 4{,}0$. При $W = 2$ всегда имеется наименьшая численность $J_2 = 2$;

3) из (8) найдем $\sigma_3 = 2{,}5$, а σ_2 не может быть найдена из-за несуществования, как было сказано, Pr для $W = 2$. Поэтому большинство ансамблей с $W = 3$ имеют численность $J_3 = 4$, но имеются также ансамбли с численностью $J_3 \pm \sigma_3/2$, т. е. $J = 3$ и $J = 5$.

Ответ: количество ансамблей предположительно равно 128; среди них большинство для $W = 3$ имеет численность по четыре кода, а при $W = 2$ — по два кода; в общем количестве ансамблей с $W = 3$ присутствуют ансамбли с тремя и пятью кодами. (Использованы оценочные параметры, поэтому ответ сформулирован в предположительной форме).

Полученные величины сравним с итогами полного синтеза. Всего для данных, приведенных в примере, в случае $W = 3$ существует $H(5,3,3) = 99$ кодов, т. е. погрешность сделанной оценки 29 %. Распределение по численностям набора кодов: пар — $H(5,3,3,2) = 4$; троек — $H(5,3,3,3) = 23$; четверок — $H(5,3,3,4) = 46$; пятерок — $H(5,3,3,5) = 24$; шестерок — $H(5,3,3,6) = 2$. Распределение практически симметрично относительно наибольшего количества четверок. Основной объем ансамблей, состоящих из троек, четверок и пятерок, составляет почти 94 % от общего числа. Если $W = 2$, то $H(5,3,2) = 18$. Сравнивая с ответом примера, видим, что оценки численности вполне удовлетворительны. Вот вариант ансамбля кодов с характерной численностью: 1, –1, 1, –1, –1; 1, 1, –1, 1, 1; 1, –1, –1, 1, 1; 1, –1, –1, –1, 1. Согласно классификации, приведенной выше, этот ансамбль можно отнести, вероятно, к нормальной системе сигналов.

Заключение

Известна система кодирования ASCII (American Standard Code for Information Interchange — стандартный код информационного обмена). Каждый из 256 символов характеризуется комбинацией из восьми двоичных символов или

импульсов (байт). Каждому байту можно сопоставить один из $R4$-кодов в соответствии с алфавитом. Количество кодов $g_{4,N}$ велико, и можно получить большой объем вариантов алфавитов системы ASCII. Это позволяет пользователям средств вычислительной техники выбирать алфавит представления своих рабочих данных, что совместно с известными достоинствами ШПС [1] затруднит несанкционированный доступ к ним, повысит информационную безопасность. Эти возможности могут использоваться в системах управления, передачи данных и вычислительных системах, в том числе в компьютерах. По аналогии с радиолокационными системами на ШПС [4] их разумно назвать «тихими» компьютерами, они будут обладать всеми достоинствами ШПС. Эти возможности могут быть распространены на локальные и глобальные компьютерные сети с перспективой создания «тихого» Интернета, в котором повышена защищенность от несанкционированного доступа к электронной персональной информации.

Обширный набор алфавитов позволяет решать задачи шифрования путем выбора кодов, привлекаемых для их создания, независимо от известных методов шифрования. Появляется новая, дополнительная ступень защиты.

Литература

1. **Варакин Л. Е.** Системы связи с шумоподобными сигналами. — М.: Радио и связь, 1985. — 384 с.
2. **Ипатов В. П., Орлов В. К., Самойлов И. М., Смирнов В. Н.** Системы мобильной связи: учеб. пособие для вузов/ под ред. В. П. Ипатова. — М.: Горячая линия – Телеком, 2003. — 272 с.
3. **Ipatov V. P.** Spread Spectrum and CDMA. Principles and Applications. — N. Y.: John Wiley and Sons Ltd., 2004. — 373 p.
4. **Гантмахер В. Е., Быстров Н. Е., Чеботарев Д. В.** Шумоподобные сигналы. Анализ, синтез, обработка. — СПб.: Наука и техника, 2005. — 400 с.
5. **Tang X., Ding C.** New Classes of Balanced Quaternary and Almost Balanced Binary Sequences With Optimal Autocorrelation Value// IEEE Transactions on Information Theory. 2010. Vol. 56. N 12. P. 6398–6405.
6. **Чепруков Ю. В., Соколов М. А.** Синтез фазоманипулированных сигналов с требуемым уровнем боковых пиков АКФ // Радиотехника. 1991. № 5. С. 68–70.
7. **Чепруков Ю. В., Соколов М. А.** Бинарные R2-коды, их характеристики и применение // Информационно-управляющие системы. 2014. № 1. С. 76–83.

UDC 621.396:621.391.26

Correlation Characteristics of Some Binary R-4 Codes and Ensembles of Signals on Their Basis

Cheprukov Yu. V.[a], PhD., Tech., chuv52@mail.ru
Socolov M. A.[b], Dr. Sc., Tech., Professor, guap22@mail.ru
[a]Russian State University of Tourism and Service in Sochi, 24/a, Kirpichnaia St.,354340, Sochi, Russian Federation
[b]Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation

Purpose: Continuous increase in the efficiency of various control & communication systems is possible when using more advanced binary codes and signaling systems on their basis. Known N-element binary codes used in these systems do not allow us to obtain a sufficiently low level of the lateral peaks of the autocorrelation and mutual correlation functions of a set of codes when N varies over a wide range. The purpose of this work is studying the synthesis of N-element binary codes with given R and W levels of lateral peaks of the autocorrelation and mutual correlation functions. **Results:** A table of code synthesis results is given for $R = 4$ and $N \le 32$. A general account is given of the technique and features of binary code ensemble synthesis with a given level W of lateral peaks of mutual correlation function. To obtain analytical estimates of quantitative characteristics of such code sets, certain hypotheses are proposed, models built and an example given. **Practical relevance:** The results can be used in control & communication systems. The idea of encipherement with these codes has been formulated. There is a potential way to create «quiet» computers and computer networks, leading to the development of «quiet» Internet.

Keywords — Group, Binary Code, Autocorrelation Function, Side Level.

References

1. Varakin L. E. *Sistemy sviazi s shumopodobnymi signalami* [Communication Systems with Noise Signals]. Moscow, Radio i sviaz' Publ., 1985. 384 p. (In Russian).
2. Ipatov V. P., Orlov V. K., Samoilov I. M., Smirnov V. N. *Sistemy mobil'noi sviazi* [Mobile Communication Systems]. Ed. V. P. Ipatov. Moscow, Goriachaia liniia – Telekom Publ., 2003, 272 p. (In Russian).
3. Ipatov V. P. *Spread Spectrum and CDMA. Principles and Applications*. New York, John Wiley and Sons Ltd., 2004. 373 p.
4. Gantmaher V. E., Bystrov N. E., Chebotarev D. V. *Shumopodobnye signaly. Analiz, sintez, obrabotka* [Pseudo-noise Signals. Analysis, Synthesis, and Processing]. Saint-Petersburg, Nauka i tehnika Publ., 2005. 400 p. (In Russian).
5. Tang X., Ding C. New Classes of Balanced Quaternary and Almost Balanced Binary Sequences with Optimal Autocorrelation Value. *IEEE Transactions on Information Theory*, 2010, vol. 56, no. 12, pp. 6398–6405.
6. Cheprukov Ju. V., Socolov M. A. Synthesis of Phasemanipulated Signals with Required Level of Side Peaks ACF. *Radiotehnika*, 1991, no. 5, pp. 68–70 (In Russian).
7. Cheprukov Yu. V., Socolov M. A. Binary R2-Codes, Their Features and Application. *Informatsionno-upravliaiushchie sistemy*, 2014, no. 1, pp. 76–83 (In Russian).