МАЛОЕ МНОЖЕСТВО ПОСЛЕДОВАТЕЛЬНОСТЕЙ КАСАМИ И ИХ ДЕКОДИРОВАНИЕ НА ОСНОВЕ ДВОЙСТВЕННОГО БАЗИСА

С.С. Владимиров[1], **О.С. Когновицкий**[1*]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация
*Адрес для переписки: kogn@yandex.ru

Информация о статье
УДК 621.396
Язык статьи – русский

Ссылка для цитирования: Владимиров С.С., Когновицкий О.С. Малое множество последовательностей Касами и их декодирование на основе двойственного базиса // Труды учебных заведений связи. 2018. Т. 4. № 1. С. 22–31.

Аннотация: *Современное развитие систем цифровой передачи сообщений все в большей степени ориентируется на применение широкополосных методов передачи, основанных, в частности, на расширении спектра прямой последовательностью. Применение широкополосных сигналов обеспечивает повышение эффективности систем по таким показателям, как помехоустойчивость, снижение энергии передаваемых сигналов, повышение уровня скрытности самого процесса передачи информации по каналу с помехами, повышение эффективности работы системы фазирования и др. Наиболее часто для расширения спектра прямой последовательностью выбирают М-последовательности и последовательности Голда, характеристики и методы обработки которых достаточно подробно изучены и представлены во многих публикациях. Статья посвящена последовательностям малого семейства Касами, которые имеют ряд преимуществ по сравнению с М-последовательностями и последовательностями Голда. Рассматривается новый подход к обработке последовательностей малого семейства Касами на основе двойственного базиса.*

Ключевые слова: *последовательности Касами, малое множество последовательностей Касами, двойственный базис, вероятность ошибки.*

Введение

Во многих радиотехнических системах применяются специальные последовательности, к которым относятся следующие: М-последовательности, составные последовательности Голда, ЛРД-последовательности, а также малое и большое семейства последовательностей Касами. Их используют для расширения спектра прямой последовательностью, адресации в многоадресатных системах, скремблировании потоков цифровых данных, синхронизации приемо-передатчика, измерения дальности до объекта. Общей характерной особенностью указанных выше последовательностей является их рекуррентность.

В процессе декодирования последовательности необходимо, как правило, после ее обнаружения, определить фазу последовательности. Для этого используют различные структурные свойства применяемых последовательностей, в частности свойство рекуррентности. В качестве критериев оценки эффективности методов обнаружения и обработки рекуррентных последовательностей чаще всего используют вероятности правильного и неправильного декодирования, временные задержки анализа, а также сложность аппаратно-программной реализации.

Наиболее простыми методами обнаружения и обработки рекуррентных последовательностей являются метод приема по безошибочному участку рекуррентной последовательности [1] и метод последовательной оценки Уорда [2]. Но эти методы неприменимы в случае асинхронно-адресных систем, где каждому адресату соответствует своя начальная фаза последовательности. В то же время методы имеют широкое применение как в асинхронных системах для фазового запуска приемника, так и в синхронных системах для контроля за синфазным состоянием приемника. Однако в этих случаях указанные методы не обеспечивают высокой надежности выделения рекуррентной последовательности при наличии ошибок в канале связи.

С целью повышения надежности декодирования таких последовательностей часто применяют корреляционные методы обработки [3]. Эти методы практически применяют на уровне звена данных. В случае же многоадресатной передачи они могут быть применены только в строго синхронной сети. При этом последовательности должны обладать хорошими ортогональными или квазиортогональными свойствами.

Актуальной задачей поэтому является разработка новых, более эффективных, методов обнаружения и декодирования рекуррентных, главным образом составных, последовательностей, в том числе и последовательностей малого семейства Касами [4, 5]. К числу таких методов относятся методы декодирования составных последовательностей на основе теории полей Галуа с использованием сопровождающей матрицы и мажоритарной оценкой значений элементов декодируемой составной последовательности [6]. Рассмотрим далее метод декодирования последовательностей малого семейства Касами на основе двойственного базиса над расширенным полем Галуа GF(2^n) [7].

Свойства и формирование последовательностей малого семейства Касами

Прежде всего приведем характерные свойства последовательностей малого семейства Касами {К$_м$} над полем GF(2^n), где степень n должна быть четным числом. Сама последовательность Касами {К$_м$} является составной с периодом $N_1 = 2^n - 1$ и представляет собой поэлементную сумму двух последовательностей максимального периода, одна из которых $\{u\}$ является М$_1$-последовательностью, порождаемой примитивным многочленом $h_1(x)$ степени n, а другая $\{v\}$ – М$_2$-последовательностью, порождаемой неприводимым многочленом $h_2(x)$ степени $n/2$ [4, 5]. При этом, если считать ε первообразным элементом поля GF(2^n) и одним из корней многочлена $h_1(x)$, то всеми nкорнями этого многочлена будут p-сопряженные ($p = 2$) элементы поля:

$$\{\varepsilon, \varepsilon^p, \varepsilon^{p^2}, \dots, \varepsilon^{p^{n-1}}\} = \{\varepsilon, \varepsilon^2, \varepsilon^4, \dots, \varepsilon^{2^{n-1}}\} = \\ = \{\varepsilon_1, \varepsilon_2, \varepsilon_3, \dots, \varepsilon_n\},$$

где $\varepsilon_i = \varepsilon^{2^{i-1}}$, $i = 1, 2, \dots, n$.

Тогда для построения последовательности Касами {К$_м$} второй многочлен $h_2(x)$ степени $n/2$ должен быть таким, чтобы его корнями были q-ые степени корней многочлена $h_1(x)$, т.е.:

$$\{\varepsilon^q, (\varepsilon^2)^q, (\varepsilon^4)^q, \dots, \left(\varepsilon^{2^{\frac{n}{2}-1}}\right)^q\} = \left\{\mu, \mu^2, \mu^4, \dots, \mu^{2^{\frac{n}{2}-1}}\right\},$$

где $\mu = \varepsilon^q$, а $q = 2^{\frac{n}{2}} + 1$.

В этом случае, как следует из теории полей Галуа [8], порядок корней многочлена $h_2(x)$ будет равен периоду N_2 последовательности $\{v\}$:

$$N_2 = \frac{N_1}{\text{НОД}(q, N_1)} = \frac{2^n - 1}{\text{НОД}(2^{\frac{n}{2}} + 1, 2^n - 1)},$$

где НОД(a,$в$) – наибольший общий делитель чисел a и $в$.

При этом элементы u_i канонической последовательности $\{u\}$ представляют собой функции-след от элементов ε^i, т.е.:

$$u_i = T(\varepsilon^i) = \varepsilon^i + (\varepsilon^i)^2 + \dots + (\varepsilon^i)^{2^{n-1}} \in \text{GF}(2), \quad (1)$$

где $i = 0, 1, 2, \dots, (2^n - 2)$.

Зная корни $\mu, \mu^2, \mu^4, \dots, \mu^{2^{n/2-1}}$ многочлена $h_2(x) = x^{n/2} + p_1 x^{n/2-1} + \dots + p_{\frac{n}{2}-1} x + p_{\frac{n}{2}}$, легко по формулам Виета найти его коэффициенты $p_i \in$ GF(2) и, тем самым, вид самого многочлена $h_2(x)$.

По заданному многочлену $h_1(x)$ и найденному многочлену $h_2(x)$ получим составную последовательность $\{s\}$ малого семейства Касами как поэлементную сумму по mod2 последовательностей $\{u\}$ и $\{v\}$, формируемых как функции-след двумя генераторами с обратными связями по модулям$h_1(x)$ и $h_2(x)$ соответственно.

Рассмотрим теперь метод декодирования последовательностей малого семейства Касами на основе двойственного базиса. При этом целью декодирования будет определение начальной фазы такой последовательности, составленной из начальных фаз последовательностей $\{u\}$ и $\{v\}$.

В [7] рассмотрен метод декодирования на основе двойственного базиса составных последовательностей Голда и ЛРД-последовательностей. Аналогичным образом могут быть декодированы и составные последовательности малого семейства Касами.

Выберем в качестве исходных данных поле GF(2^6) ($n = 6$) с первообразным элементом ε и примитивный многочлен $h_1(x) = 1 + x + x^6$с сопряженными корнями ε, ε^2, ε^4, ε^8, ε^{16}, ε^{32}. Будем считать, что поле GF(2^6) образовано тем же многочленом $h_1(x)$, а его элементы ε^i представляют собой вычеты по двойному модулю относительно левого степенного базиса $(1, \varepsilon, \varepsilon^2, \varepsilon^3, \varepsilon^4, \varepsilon^5)$, т. е.:

$$\varepsilon^i = a_0 + a_1\varepsilon + a_2\varepsilon^2 + a_3\varepsilon^3 + a_4\varepsilon^4 + a_5\varepsilon^5; \\ \text{modd}(2, h_1(x)). \quad (2)$$

Исходя из этих исходных данных, последовательности максимальной длины $\{u\}$ с периодом $N_1 = 2^6 - 1 = 63$ будет соответствовать характеристический многочлен $h_1(x)$, а последовательности $\{v\}$ – многочлен $h_2(x)$ степени $n/2 = 3$, корнями которого будут q-ые степени ($q = 2^3 + 1 = 9$) корней многочлена $h_1(x)$, т. е.:

$$\mu = (\varepsilon)^9, \mu^2 = (\varepsilon^2)^9 = \varepsilon^{18}, \mu^4 = (\varepsilon^4)^9 = \varepsilon^{36}. \quad (3)$$

Тогда порядок N_2 корней многочлена $h_2(x)$ будет равен:

$$N_2 = \frac{N_1}{\text{НОД}(9, N_1)} = \frac{63}{\text{НОД}(9,63)} = 7.$$

Запишем многочлен $h_2(x)$ в общем виде как $h_2(x) = x^3 + p_1x^2 + p_2x + p_3$ и, используя формулы Виета, по известным корням $\theta_1 = \mu, \theta_2 = \mu^2, \theta_3 = \mu^4$ находим: $p_1 = 1, p_2 = 0, p_3 = 1$. Следовательно, $h_2(x) = x^3 + x^2 + 1$.

Представив элемент ε^i в полиномиальной форме (2), запишем последовательность $\{u\}$ через функцию-след как:

$$\{u\} = (u_0, u_1, u_2, \dots, u_i, \dots, u_{62}) = \\ = [T(c), T(c\varepsilon), T(c\varepsilon^2), \dots, T(c\varepsilon^i), \dots, T(c\varepsilon^{62})], \\ \text{modd}(2, h_1(x)). \quad (4)$$

Аналогично, элементы v_i, $i = 0, 1, \dots, 6$, последовательности $\{v\}$ с периодом $N_2 = 7$ могут быть представлены через функцию-след как:

$$\{v\} = (v_0, v_1, v_2, \dots, v_6) = \\ = [T(d), T(d\mu), T(d\mu^2), \dots, T(d\mu^6)], \\ \text{modd}(2, h_2(x)). \quad (5)$$

где $d \in \text{GF}(2^3)$ – начальный элемент последовательности $\{v\}$.

Если учесть, что функция-след от элемента (2) в поле $\text{GF}(2^6)$ равна $T(\varepsilon^i) = a_5$, то при $c = 1$ последовательность (4) будет являться канонической и иметь вид, приведенный в таблице 1.

ТАБЛИЦА 1. Каноническая М-последовательность, образованная полиномом $h_1(x)$

u_0	u_1	u_2	u_3	u_4	u_5	u_6	u_7	u_8
0	0	0	0	0	1	0	0	0
u_9	u_{10}	u_{11}	u_{12}	u_{13}	u_{14}	u_{15}	u_{16}	u_{17}
0	1	1	0	0	0	1	0	1
u_{18}	u_{19}	u_{20}	u_{21}	u_{22}	u_{23}	u_{24}	u_{25}	u_{26}
0	0	1	1	1	1	0	1	0
u_{27}	u_{28}	u_{29}	u_{30}	u_{31}	u_{32}	u_{33}	u_{34}	u_{35}
0	0	1	1	1	0	0	1	0
u_{36}	u_{37}	u_{38}	u_{39}	u_{40}	u_{41}	u_{42}	u_{43}	u_{44}
0	1	0	1	1	0	1	1	1
u_{45}	u_{46}	u_{47}	u_{48}	u_{49}	u_{50}	u_{51}	u_{52}	u_{53}
0	1	1	0	0	1	1	0	1
u_{54}	u_{55}	u_{56}	u_{57}	u_{58}	u_{59}	u_{60}	u_{61}	u_{62}
0	1	0	1	1	1	1	1	1

Аналогично, если элемент $\mu_i \in \text{GF}(2^3)$ представить в полиномиальной форме записи $\mu^j = b_0 + b_1\mu + b_2\mu^2$, $\text{modd}(2, h_2(x))$, где коэффициенты $b_i \in \text{GF}(2)$, то функция-след от такого элемента будет равна $T(\mu^i) = (b_0 + b_1 + b_2)$, mod2.

Тогда каноническая последовательность $\{v\}$ при $d = 1$ будет следующей:

$$\{v\} = (v_0, v_1, v_2, \dots, v_6) = \\ = [T(1), T(\mu), T(\mu^2), \dots, T(\mu^6)] = (1110100). \quad (6)$$

В случае не канонической последовательности $\{u\}$, у которой $c \neq 1$, ее элементы u_i будут определяться через функцию-след так, как следует из (4).

Также, если начальный элемент последовательности $\{v\}$ равен произвольному элементу $d \neq 1$, то элементы v_i этой последовательности будут определяться через функцию-след, как следует из (5):

$$v_{i \bmod 7} = T(d\mu^i)\text{modd}(2, h_2(x)). \quad (7)$$

Как указывалось ранее, составная последовательность $\{s\}$ малого семейства Касами формируется как поэлементная сумма по mod2 последовательностей $\{u\}$ и $\{v\}$. Очевидно, что в одном периоде последовательности максимальной длины $\{u\}$ будет содержаться 9 периодов последовательности $\{v\}$. В качестве примера будем рассматривать варианты формирования последовательности Касами $\{s\}$ при условии различных начальных элементов c и d последовательностей $\{u\}$ и $\{v\}$.

Отметим, что рассматриваемой составной последовательности $\{s\}$ малого семейства Касами соответствует характеристический многочлен:

$$P(x) = h_1(x) \cdot h_2(x) = \\ = (1 + x + x^6)(1 + x^2 + x^3) = \\ = 1 + x + x^2 + x^4 + x^6 + x^8 + x^9. \quad (8)$$

Тогда последовательность $\{s\}$ будет удовлетворять рекуррентному уравнению:

$$s_i + s_{i+1} + s_{i+2} + s_{i+4} + s_{i+6} + s_{i+8} + s_{i+9} = 0, \\ \text{mod2}; \ i \geq 0. \quad (9)$$

Как известно, наиболее простыми методами определения фазы рекуррентной последовательности являются метод обнаружения и декодирования фазы по «скользящему» безошибочному m-элементному участку и метод Уорда, где m – степень многочлена $P(x)$, равная в данном примере (9).

Для декодирования последовательности $\{s\}$ малого семейства Касами, т.е. определения начальных фаз c- и d-последовательностей $\{u\}$ и $\{v\}$ соответственно, с использованием двойственного базиса и с учетом корней многочленов $h_1(x)$ и $h_2(x)$, найдем по методике, изложенной в [7], коэффициенты двойственного базиса α_i – для $h_1(x)$ и β_i – для $h_2(x)$, $i = 1,2,3,\dots,9$, (таблица 2).

ТАБЛИЦА 2. Коэффициенты двойственного базиса

α_i для $h_1(x)$	α_1	α_2	α_3	α_4	α_5	α_6	α_7	α_8	α_9
	ε^{14}	ε^{19}	ε^{38}	ε^{37}	ε	1	ε^{22}	ε^{21}	ε^{15}
β_i для $h_2(x)$	β_1	β_2	β_3	β_4	β_5	β_6	β_7	β_8	β_9
	μ	μ^5	μ^3	μ^2	0	0	μ	1	μ^2

Выберем составные последовательности $\{u\}$ и $\{v\}$ каноническими. Тогда в результате суммирования по mod2 последовательности $\{u\}$ (см. таблицу 1) и 9-кратной последовательности $\{v\}$ в виде (6), будет получена каноническая составная последовательность $\{s_1\}$ малого семейства Касами (таблица 3).

ТАБЛИЦА 3. Вычисление канонической составной последовательности $\{s_1\}$ малого семейства Касами

$\{u\}$	u_0	u_1	u_2	u_3	u_4	u_5	u_6	u_7	u_8	u_9	u_{10}	u_{11}	u_{12}	u_{13}	u_{14}	u_{15}	u_{16}	u_{17}	u_{18}	u_{19}	u_{20}
	0	0	0	0	0	1	0	0	0	0	1	1	0	0	0	1	0	1	0	0	1
$\{v\}$	v_0	v_1	v_2	v_3	v_4	v_5	v_6	v_0	v_1	v_2	v_3	v_4	v_5	v_6	v_0	v_1	v_2	v_3	v_4	v_5	v_6
	1	1	1	0	1	0	0	1	1	1	0	1	0	0	1	1	1	0	1	0	0
$\{s\}$	s_0	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8	s_9	s_{10}	s_{11}	s_{12}	s_{13}	s_{14}	s_{15}	s_{16}	s_{17}	s_{18}	s_{19}	s_{20}
	1	1	1	0	1	1	0	1	1	1	1	0	0	0	1	0	1	1	1	0	1
$\{u\}$	u_{21}	u_{22}	u_{23}	u_{24}	u_{25}	u_{26}	u_{27}	u_{28}	u_{29}	u_{30}	u_{31}	u_{32}	u_{33}	u_{34}	u_{35}	u_{36}	u_{37}	u_{38}	u_{39}	u_{40}	u_{41}
	1	1	1	0	1	0	0	0	1	1	1	0	0	1	0	0	1	0	1	1	0
$\{v\}$	v_0	v_1	v_2	v_3	v_4	v_5	v_6	v_0	v_1	v_2	v_3	v_4	v_5	v_6	v_0	v_1	v_2	v_3	v_4	v_5	v_6
	1	1	1	0	1	0	0	1	1	1	0	1	0	0	1	1	1	0	1	0	0
$\{s\}$	s_{21}	s_{22}	s_{23}	s_{24}	s_{25}	s_{26}	s_{27}	s_{28}	s_{29}	s_{30}	s_{31}	s_{32}	s_{33}	s_{34}	s_{35}	s_{36}	s_{37}	s_{38}	s_{39}	s_{40}	s_{41}
	0	0	0	0	0	0	0	1	0	0	1	1	0	1	1	1	0	0	0	1	0
$\{u\}$	u_{42}	u_{43}	u_{44}	u_{45}	u_{46}	u_{47}	u_{48}	u_{49}	u_{50}	u_{51}	u_{52}	u_{53}	u_{54}	u_{55}	u_{56}	u_{57}	u_{58}	u_{59}	u_{60}	u_{61}	u_{62}
	1	1	1	0	1	1	0	0	1	1	0	1	0	1	0	1	1	1	1	1	1
$\{v\}$	v_0	v_1	v_2	v_3	v_4	v_5	v_6	v_0	v_1	v_2	v_3	v_4	v_5	v_6	v_0	v_1	v_2	v_3	v_4	v_5	v_6
	1	1	1	0	1	0	0	1	1	1	0	1	0	0	1	1	1	0	1	0	0
$\{s\}$	s_{42}	s_{43}	s_{44}	s_{45}	s_{46}	s_{47}	s_{48}	s_{49}	s_{50}	s_{51}	s_{52}	s_{53}	s_{54}	s_{55}	s_{56}	s_{57}	s_{58}	s_{59}	s_{60}	s_{61}	s_{62}
	0	0	0	0	0	1	0	1	0	0	0	0	0	1	1	0	0	1	0	1	1

Аналогично рассчитываются и неканонические последовательности Касами, складывающиеся из М-последовательностей $\{u\}$ и $\{v\}$, начальные фазы которых не равны 1. Например, в таблице 4 приведена последовательность Касами $\{s_2\}$, образованная сложением M_1-последовательности $\{u_2\}$ с начальной фазой $c_2 = \varepsilon^5$ и M_2-последовательности $\{v_2\}$ с начальной фазой $d_2 = \mu^2$.

ТАБЛИЦА 4. Пример неканонической последовательности Касами $\{s_2\}$

s_0	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8
0	0	1	0	0	0	0	1	0
s_9	s_{10}	s_{11}	s_{12}	s_{13}	s_{14}	s_{15}	s_{16}	s_{17}
1	1	0	0	1	1	1	0	1
s_{18}	s_{19}	s_{20}	s_{21}	s_{22}	s_{23}	s_{24}	s_{25}	s_{26}
1	1	0	1	0	1	1	1	0
s_{27}	s_{28}	s_{29}	s_{30}	s_{31}	s_{32}	s_{33}	s_{34}	s_{35}
1	1	1	1	0	1	1	0	0
s_{36}	s_{37}	s_{38}	s_{39}	s_{40}	s_{41}	s_{42}	s_{43}	s_{44}
0	0	1	1	1	0	0	0	1
s_{45}	s_{46}	s_{47}	s_{48}	s_{49}	s_{50}	s_{51}	s_{52}	s_{53}
1	1	1	0	1	1	1	1	1
s_{54}	s_{55}	s_{56}	s_{57}	s_{58}	s_{59}	s_{60}	s_{61}	s_{62}
0	0	0	1	1	0	0	1	1

Корреляционные свойства последовательностей малого семейства Касами

Рассмотрим корреляционные свойства последовательностей малого семейства Касами на примере вычисленных ранее канонической последовательности $\{s_1\}$ и неканонической последовательности $\{s_2\}$. Необходимо отметить, что при расчете автокорреляционной (АКФ) и взаимокорреляционной (ВКФ) функций необходимо преобразовать последовательности от униполярного вида [1, 0] к биполярному виду [–1, 1].

Вначале определим автокорреляционные свойства последовательностей $\{s_1\}$ и $\{s_2\}$. Апериодическая автокорреляционная функция (АпАКФ) вычисляется по формуле:

$$\text{АпАКФ}_k(\{s\}) = \sum_{i=0}^{N-1-k} s_i s_{i+k},$$

где k – сдвиг относительно исходной последовательности $\{s\}$.

Значения АпАКФ последовательностей $\{s_1\}$ и $\{s_2\}$ приведены на графике (рисунок 1).

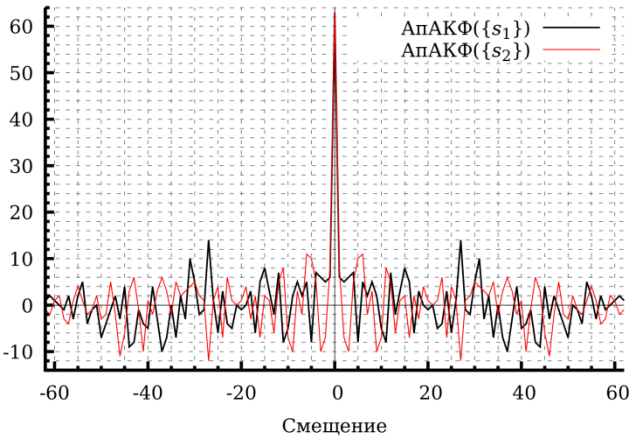


Рис. 1. Значения АпАКФ последовательностей $\{s_1\}$ и $\{s_2\}$

Периодическая автокорреляционная функция (ПАКФ) вычисляется для замкнутой в кольцо последовательности {s} по формуле:

$$\text{ПАКФ}_k(\{s\}) = \sum_{i=0}^{N-1} s_i s_{(i+k) \bmod N}.$$

Значения ПАКФ последовательностей $\{s_1\}$ и $\{s_2\}$ приведены на графике (рисунок 2).

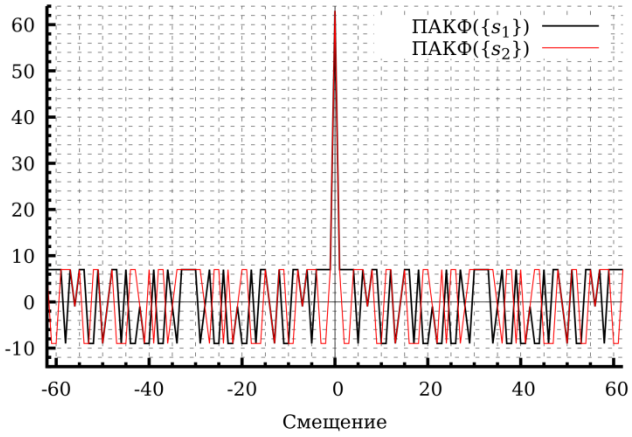


Рис. 2. Значения ПАКФ последовательностей {s_1} и {s_2}

Значения апериодической и периодической ВКФ рассчитываются по аналогичным формулам, в которых рассматривается смещение одной последовательности относительно другой. Графики этих функций для последовательностей {s_1} и {s_2} приведены на рисунке 3.

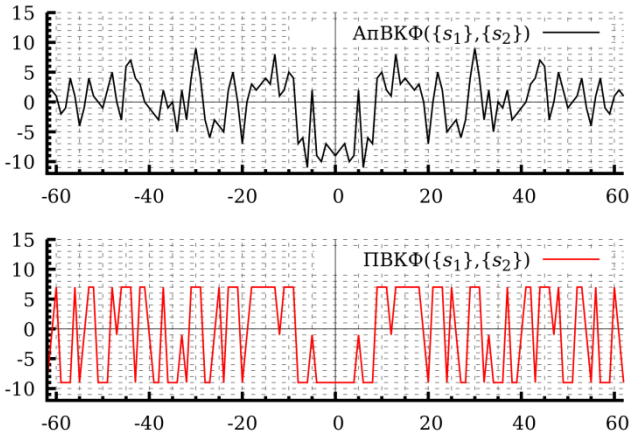


Рис. 3. Значения АпВКФ и ПВКФ последовательностей {s_1} и {s_2}

Рассмотрим декодирование последовательностей малого семейства Касами для двух вариантов систем – синхронной и асинхронной, с использованием двойственного базиса [7].

Декодирование последовательности Касами в синхронной системе

В синхронной системе известны начала принимаемых последовательностей {s}, следовательно при выделении безошибочного 9-элементного участка $(s_i, s_{i+1}, s_{i+2}, s_{i+3}, s_{i+4}, s_{i+5}, s_{i+6}, s_{i+7}, s_{i+8})$ декодеру известно значение индекса i, определяющему месторасположение символа s_i от начала последовательности {s}. Таким образом, зная значение индекса i и коэффициенты двойственного базиса, по принятому безошибочному m-элемент-ному участку, в соответствии с методикой [7], будут определены начальные фазы c и d последовательностей {u} и {v}.

Например, первый же 9-элементный участок канонической последовательности {s_1}, приведенной в таблице 3, принят без ошибок, следовательно $(s_0, s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8) = (111011011)$. Тогда начальные фазы будут следующие:

$$c = \alpha_1 + \alpha_2 + \alpha_3 + \alpha_5 + \alpha_6 + \alpha_8 + \alpha_9 =$$
$$= \varepsilon^{14} + \varepsilon^{19} + \varepsilon^{38} + \varepsilon + 1 + \varepsilon^{21} + \varepsilon^{15} = 1 \mod h_1(x);$$

$$d = \beta_1 + \beta_2 + \beta_3 + \beta_5 + \beta_6 + \beta_8 + \beta_9 =$$
$$= \mu + \mu^5 + \mu^3 + 0 + 0 + 1 + \mu^2 = 1 \mod h_2(x).$$

Таким образом, составные последовательности {u} и {v} являются каноническими с начальными фазами $c = 1$ и $d = 1$. Из этого можно сделать очевидный вывод, что только по одному безошибочному m-элементному участку последовательности {s} могут быть определены фазы составных последовательностей, тогда как простые методы обработки по «зачетному» участку и метод Уорда не позволяют это сделать.

Для повышения надежности декодирования последовательностей Касами {s} метод на основы двойственного базиса позволяет применить мажоритарный принцип обработки различных m-элементных участков, в том числе и перекрывающихся. Пусть в принимаемой последовательности из таблицы 2 выделенm-элементный участок $(s_{24}, s_{25}, s_{26}, s_{27}, s_{28}, s_{29}, s_{30}, s_{31}, s_{32}) = (000010011)$,в котором $i = 24$. Поэтому, также безошибочному, участку вычислим начальные фазы последовательностей {u} и {v}:

$$c = \varepsilon^{-24}(\alpha_5 + \alpha_8 + \alpha_9) = \varepsilon^{-24}(\varepsilon + \varepsilon^{21} + \varepsilon^{15}) =$$
$$= 1 \mod h_1(x);$$
$$d = \mu^{-24}(\beta_5 + \beta_8 + \beta_9) = \mu^{-3}(0 + 1 + \mu^2) =$$
$$= 1 \mod h_2(x).$$

То есть, получен тот же результат, что и подтверждает возможность мажоритарного декодирования в канале с ошибками по большинству одинаковых значений c и d.

Пусть теперь принимаемая в синхронной системе последовательность {s} не является канонической, т. е. начальные элементы c и d отличны от 1, и задача декодера состоит в определении их с использованием двойственного базиса.

Для примера выберем неканоническую последовательность {s_2}, приведенную в таблице 4.Выберем в этой последовательности безошибочный участок: $(s_0, s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8) = (001000010)$ при $i = 0$. Тогда начальные фазы последовательностей {u_2} и {v_2}, формирующих неканоническую последовательность Касами {s_2} (см. таблицу 4), в синхронной системе будут равны:

$$c_2 = \alpha_3 + \alpha_8 = \varepsilon^{38} + \varepsilon^{21} = \varepsilon^5 \mod h_1(x);$$

$$d_2 = \beta_3 + \beta_8 = \mu^3 + 1 = \mu^2 \mod h_2(x).$$

Для проверки мажоритарности метода выберем другой безошибочный участок, например с $i = 53$: $(s_{53}, s_{54}, s_{55}, s_{56}, s_{57}, s_{58}, s_{59}, s_{60}, s_{61}) = (100011001)$.

Расчетные значения начальных фаз c_2 и d_2 для такого участка будут следующие:

$$c = \varepsilon^{-53}(\alpha_1 + \alpha_5 + \alpha_6 + \alpha_9) =$$
$$= \varepsilon^{-53}(\varepsilon^{14} + \varepsilon + 1 + \varepsilon^{15}) = \varepsilon^{-53} \cdot \varepsilon^{58} =$$
$$= \varepsilon^5 \mod h_1(x);$$
$$d = \mu^{-53}(\beta_1 + \beta_5 + \beta_6 + \beta_9) = \mu^{-4}(\mu + 0 + 0 + \mu^2) =$$
$$= \mu^{-4} \cdot \mu^6 = \mu^2 \mod h_2(x).$$

Таким образом, как и было указано ранее, начальными фазами составных последовательностей $\{u_2\}$ и $\{v_2\}$ в синхронной системе будут элементы $c_2 = \varepsilon^5$ и $d_2 = \mu^2$, или двоичные комбинации $(a_0, a_1, a_2, a_3, a_4, a_5) = (000001)$ и $(b_0, b_1, b_2) = (001)$, которые были установлены на передающей стороне как начальные состояния ячеек модульных регистров, соответствующих многочленам $h_1(x)$ и $h_2(x)$ соответственно.

Декодирование укороченных последовательностей Касами

Использование мажоритарного принципа декодирования последовательностей Касами позволяет использовать укороченные последовательности, которые представляют собой первые K символов исходной последовательности.

При использовании укороченных последовательностей значительно сокращается количество m-элементных участков, по которым вычисляются начальные фазы и производится мажоритарное декодирование. В частности, для них недоступно закольцовывание последовательности. Например, для укороченной последовательности Касами длиной $K = 21$ доступно всего 13 таких участков. В общем случае, для укороченной последовательности длины K можно использовать $K - m + 1$ m-элементных участков. В остальном, принцип декодирования остается тем же самым.

Вероятностные характеристики декодера последовательностей Касами на основе двойственного базиса при синхронном декодировании

Для оценки вероятностных характеристик синхронного декодирования по методу двойственного базиса использовалось моделирование по методу Монте-Карло. В системе математических вычислений GNU/Octave была построена модель системы передачи с моделью канала связи, через которую передавались последовательности Касами, сформированные по случайным образом сгенерированным начальным фазам. На приемной стороне последовательности декодировались и полученные в результате начальные фазы сверялись с исходными и накапливалась статистика.

Моделирование проводилось для двух моделей каналов:

1) Модель двоично-симметричного канала (ДСК).

2) Модель канала АБГШ совместно с двоичной фазовой манипуляцией.

Схемы моделей систем передачи приведены на рисунках 4 и 5 соответственно.

Рис. 4. Модель системы передачи с каналом ДСК

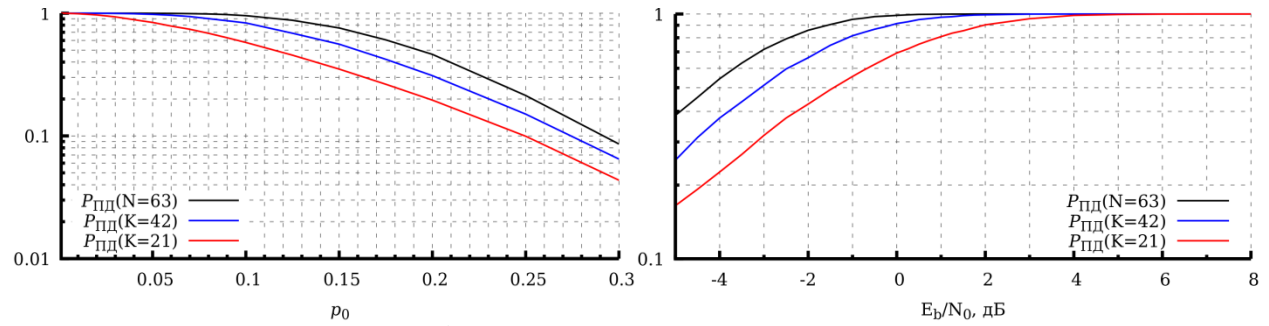
Рис. 5. Модель системы передачи с каналом АБГШ и манипуляцией ФМ-2

При моделировании в той и другой моделях было передано по 20000 последовательностей Касами на каждое значение битовой ошибки в канале ДСК и каждое значение отношения сигнал/шум в канале АБГШ. В результате были получены оценочные значения (т. н. «доли») вероятностей правильного декодирования $P_{ПД}$, неправильного декодирования $P_{НД}$ и отказа в декодировании $P_{ОД}$. Под отказом в декодировании понимается ситуация, при которой в результате мажоритарного декодирования не представляется возможным однозначно определить значение начальной фазы.

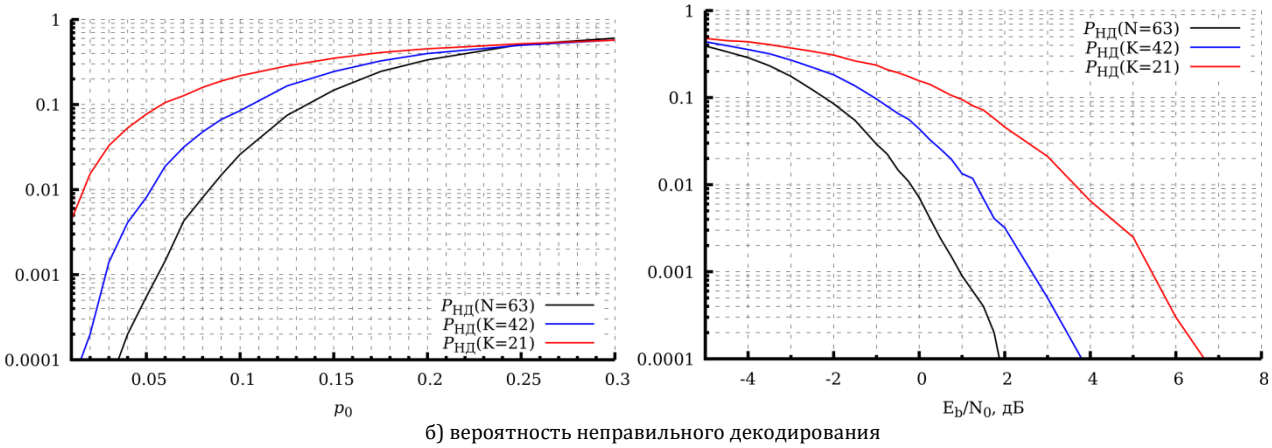
Вероятностные характеристики были определены для полной последовательности Касами длины $N = 63$ и для укороченных последовательностей длиной $K = 21$ и $K = 42$.

На рисунке 6приведены графики вероятностных характеристик (вероятности правильного декодирования, вероятности неправильного декодирования и вероятности отказа от декодирования) декодера последовательностей Касами на основе двойственного баланса при синхронном детектировании для случая канала ДСК и для случая канала АБГШ с манипуляцией ФМ-2.

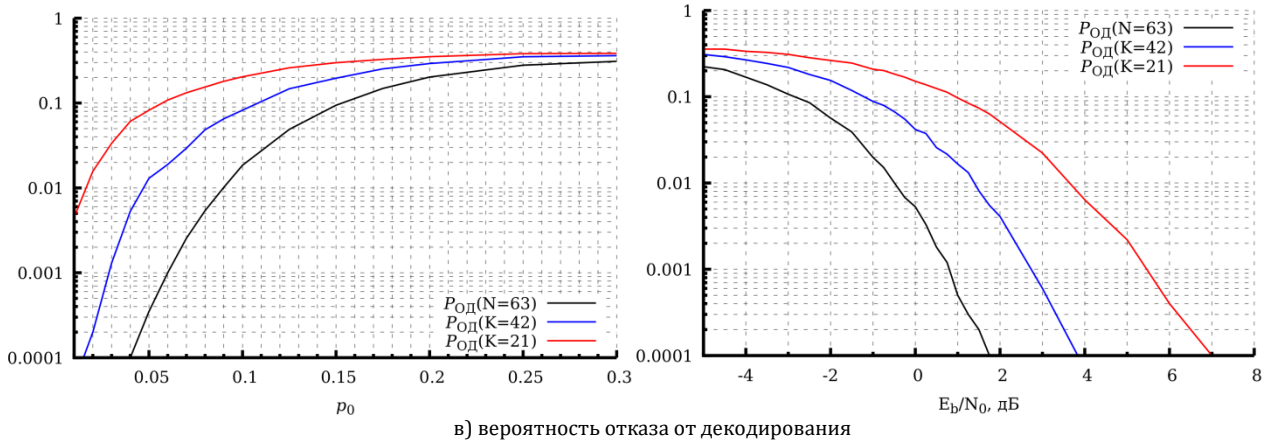
Из приведенных графиков видно, что с укорочением последовательности ухудшаются вероятностные характеристики декодера. Однако в каналах с низкой вероятностью битовой ошибки (с высоким отношением сигнал/шум) использование укороченных комбинаций оправдано.



а) вероятность правильного декодирования



б) вероятность неправильного декодирования



в) вероятность отказа от декодирования

Рис. 6. Графики вероятностных характеристик для случая канала ДСК (слева) и для случая канала АБГШ с манипуляцией ФМ-2 (справа)

Декодирование последовательности Касами в асинхронной системе

Рассмотрим теперь вариант асинхронной системы, когда фаза последовательности $\{u\}$ является фазирующей, а фаза последовательности $\{v\}$ переносит в себе адрес получателя или некоторую другую конфиденциальную информацию, предназначенную только получателю.

Другим заманчивым вариантом может быть асинхронно-адресная система, в которой фаза c последовательности $\{u\}$ является одновременно и фазирующей комбинацией и адресом получателя. Рассмотрим именно такой вариант, при котором в результате декодирования последовательности $\{s\}$ будет определена фазапоследовательности $\{u\}$. Причем, обработка последовательности $\{s\}$ на приеме будет производиться получателями в соответствии с их собственными начальными фазами, т. е. их адресами. В таких асинхронно-адресных системах приемники находятся в режиме «ожидания» и все время пытаются обнаружить предназначенную для них информацию путем идентификации известной им фазы c последовательности $\{u\}$.

Суть декодирования последовательности Касами будет в том, чтобы, зная начальный элемент последовательности $\{u\}$, выделить на приеме L последовательных элементов поля $GF(2^6)$ $(\varepsilon^i, \varepsilon^{i+1}, \varepsilon^{i+2}, \ldots, \varepsilon^{i+L-1})$ и запустить в автономный режим работы модульный генератор элементов поля до окончания последовательности $\{u\}$, что

будет соответствовать вхождению системы в синхронизм с передающим концом. Одновременно будет определена фаза последовательности $\{v\}$, которая будет переносить в себе некоторую другую конфиденциальную информацию, предназначенную только получателю, например, фазу скремблирующей последовательности или фазу широкополосной последовательности, расширяющей спектр, и др.

Рассмотрим этот процесс обнаружения последовательности малого семейства Касами и вхождения приемника в синхронизм для нашего примера при отсутствии ошибок в канале.Пусть получатель пытается обнаружить последовательность Касами при пороге $L = 5$, зная ее начальную фазу $c = \varepsilon^5$. При этом к получателю последовательность поступает с некоторого случайного символа x_1.

Рассмотрим процесс обработки представленного в таблице 5 фрагмента последовательности $\{s\}$.

Проследим обработку с применением двойственного базиса 9-элементных участков, начиная с элемента x_1, с целью обнаружения последовательности $\{u\}$ с начальной фазой $c = \varepsilon^5$ и установления цикловой фазы (таблица 6).

ТАБЛИЦА 5. Фрагмент последовательности {s} для асинхронной обработки

x_1	x_2	x_3	s_0	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8	s_9	s_{10}	s_{11}	s_{12}	…
0	0	0	0	0	1	0	0	0	0	1	0	1	1	0	0	…

ТАБЛИЦА 6. Обнаружение последовательности {u} с применением двойственного базиса

№	9-элементные участки									Обработка с использованием двойственного базиса
	x_1	x_2	x_3	s_0	s_1	s_2	s_3	s_4	s_5	$\varepsilon_1 = \varepsilon^{-5} \cdot \alpha_6 = \varepsilon^{-5} = \varepsilon^{57}$
	0	0	0	0	0	1	0	0	0	
2	x_2	x_3	s_0	s_1	s_2	s_3	s_4	s_5	s_6	$\varepsilon_2 = \varepsilon^{-5} \cdot \alpha_5 = \varepsilon^{-5} \cdot \varepsilon = \varepsilon^{58}$
	0	0	0	0	1	0	0	0	0	
3	x_3	s_0	s_1	s_2	s_3	s_4	s_5	s_6	s_7	$\varepsilon_3 = \varepsilon^{-5}(\alpha_4 + \alpha_9) = \varepsilon^{-5}(\varepsilon^{37} + \varepsilon^{15}) = \varepsilon^{59}$
	0	0	0	1	0	0	0	0	1	
4	s_0	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8	$\varepsilon_4 = \varepsilon^{-5}(\alpha_3 + \alpha_8) = \varepsilon^{-5}(\varepsilon^{38} + \varepsilon^{21}) = 1$
	0	0	1	0	0	0	0	1	0	
5	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8	s_9	$\varepsilon_5 = \varepsilon^{-5}(\alpha_2 + \alpha_7 + \alpha_9) = \varepsilon^{-5}(\varepsilon^{19} + \varepsilon^{22} + \varepsilon^{15}) = \varepsilon$
	0	1	0	0	0	0	1	0	1	
6	s_2	s_3	s_4	s_5	s_6	s_7	s_8	s_9	s_{10}	$\varepsilon_6 = \varepsilon^{-5}(\alpha_1 + \alpha_6 + \alpha_8 + \alpha_9) = \varepsilon^{-5}(\varepsilon^{14} + 1 + \varepsilon^{21} + \varepsilon^{15}) = \varepsilon^2$
	1	0	0	0	0	1	0	1	1	
7	s_3	s_4	s_5	s_6	s_7	s_8	s_9	s_{10}	s_{11}	$\varepsilon_7 = \varepsilon^{-5}(\alpha_5 + \alpha_7 + \alpha_8) = \varepsilon^{-5}(\varepsilon + \varepsilon^{22} + \varepsilon^{21}) = \varepsilon^3$
	0	0	0	0	1	0	1	1	0	
8	s_4	s_5	s_6	s_7	s_8	s_9	s_{10}	s_{11}	s_{12}	$\varepsilon_8 = \varepsilon^{-5}(\alpha_4 + \alpha_6 + \alpha_7) = \varepsilon^{-5}(\varepsilon^{37} + 1 + \varepsilon^{22}) = \varepsilon^4$
	0	0	0	1	0	1	1	0	0	

Таким образом, после обработки восьмого 9-элементного участка будут выделены $L = 5$ последовательных элементов поля, а именно: $1, \varepsilon, \varepsilon^2, \varepsilon^3, \varepsilon^4$ – что свидетельствует об обнаружении ожидаемой последовательности $\{s\}$, в которой составная последовательность $\{u\}$ имеет начальную фазу $c = \varepsilon^5$. Далее, для вхождения в синхронизм, последний выделенный элемент поля $GF(2^6)$, равный ε^4, записывается в модульный регистр многочлена $h_1(x)$, после чего потактово происходит досчет до состояния ε^{54}, которому будет соответствовать прием из канала последнего 9-элементного участка $(s_{54}, s_{55}, s_{56}, s_{57}, s_{58}, s_{59}, s_{60}, s_{61}, s_{62})$. Этому состоянию и будет соответствовать окончание приема последовательности $\{s\}$ как фазирующей для пользователя с начальным элементом последовательности $\{u\}$, равным $c = \varepsilon^5$.

Поясним теперь, как будет определена информационная начальная фаза d второй составной последовательности $\{v\}$ в составе последовательности $\{s\}$ малого семейства Касами. По выделенному последнему безошибочному 9-элементному участку $(s_4, s_5, s_6, s_7, s_8, s_9, s_{10}, s_{11}, s_{12}) = (000101100)$ из таблицы 6, когда пороговый счетчик на $L = 5$ сработает, с помощью коэффициентов β_i двойственного базиса вычисляется соответствующий по времени элемент μ^i поля $GF(2^3)$, образованного многочленом $h_2(x)$. В результате вычисления получим:

$$\mu^i = \beta_4 + \beta_6 + \beta_7 = \mu^2 + 0 + \mu = \mu^6.$$

Запишем полученный элемент в генератор элементов поля $GF(2^3)$ на основе многочлена $h_2(x)$, который начнет потактово работать в автономном режиме до появления в первом регистре состояния ε^{54}. Во втором генераторе в это время окажется некоторый элемент μ^j, умножив его на $\mu^m = \mu^9$, получим искомую информацию, т. е. начальную фазу d последовательности $\{v\}$. В нашем примере $\mu^j = 1$, следовательно, начальная фаза d последовательности $\{v\}$ будет равна $d = \mu^j \cdot \mu^9 = \mu^2; \bmod h_2(x)$.

Таким же образом фазы c и d определяются и при наличии ошибок в последовательности $\{s\}$ с тем отличием, что принятие решения относитель-

но фазы *c* будет осуществляться мажоритарно по большинству одинаковых значений при обработке различных 9-элементных участков последовательности {*s*}.

Заключение

В заключение сравним множество последовательностей малого семейства Касами и их корреляционные функции с последовательностями Голда.

Общее количество последовательностей малого семейства Касами зависит от конкретных условий их применения. Если начальная фаза *c* для длинной исходной М$_1$-последовательности {*u*} является фиксированной, например фазирующей, а фаза последовательности {*v*} переносит в себе адрес получателя или некоторую другую конфиденциальную информацию, предназначенную только получателю, то количество различных последовательностей Касами {*s*}, с учетом нулевой последовательности {*v*}, будет равно $2^{\frac{n}{2}} = \sqrt{N_1 + 1}$. В рассматриваемом примере таких различных последовательностей будет 8. Для сравнения, при применении последовательностей Голда с таким же периодом и при тех же условиях количество различных последовательностей будет равно $N_1 + 2$, т. е. 65 для $n = 6$. В общем виде для данного случая количество различных последовательностей Голда превышает количество различных последовательностей малого семейства Касами в $\frac{N_1+2}{\sqrt{N_1+1}} \approx \sqrt{N_1 + 1} = \sqrt{2^n} = 2^{\frac{n}{2}}$ раза. Следовательно, количество информации, передаваемой одной последовательностью Голда по сравнению с последовательностью малого семейства Касами такого же периода N_1, увеличивается в $\frac{\log_2 2^n}{\log_2 2^{\frac{n}{2}}} = 2$ раза. Именно по критерию скорости передачи информации преимущество на стороне последовательностей Голда.

Второй случай относится к системам, в которых формируются последовательности с различными начальными фазами как для длинной исходной М$_1$-последовательности {*u*}, например, адресной в асинхронно-адресных системах, так и в последовательности {*v*}. Тогда при использовании последовательностей Касами количество различных таких последовательностей будет, учитывая и нулевую последовательность {*v*}, равно $N_1 \times (N_2 + 1) = (2^n - 1) \times 2^{\frac{n}{2}} \approx 2^{\frac{3n}{2}}$. Для рассматриваемого в данной статье примера последовательностей Касами это количество будет равно $63 \times 8 = 504$. В то же время, количество различных по фазе последовательностей Голда с таким же периодом (с учетом двух дополнительных, когда последовательность {*u*} или последовательность {*v*} в составной последовательности Голда будет нулевой) будет равно 2^{2n}. Таким образом, количество различных по фазе последовательностей Голда превышает количество различных по фазе последовательностей Касами, как и в первом случае, примерно в $2^{n/2}$ раз. Т. е. преимущество последовательностей Голда над последовательностями малого семейства Касами одинакового периода по информационному выигрышу остается неизменным.

Сравним теперь последовательности Касами и последовательности Голда с одинаковым периодом по *корреляционным* свойствам.

Выше (см. рисунки 2 и 3) представлены полученные путем моделирования, ненормированные периодические автокорреляционные и взаимно корреляционные функции рассматриваемых в статье последовательностей малого семейства Касами. Результаты моделирования подтвердили, что коэффициенты корреляции, как ПАКФ (кроме основного пика), так и ПВКФ, принимают лишь три значения, а именно {–1, – *q*, (*q* – 2)}, где индекс децимации $q = 2^{n/2} + 1$, т. е. для нашего примера {–1, – 9, 7}. В то же время, коэффициенты корреляции для последовательностей Голда такого же периода будут примерно в два раза больше. Так, при таком же периоде $N = 63$ коэффициенты корреляции последовательностей Голда будут {–1, – 17, 15}. Отсюда следует вывод, что корреляционные свойства последовательностей Голда примерно в 2 раза хуже по сравнению с последовательностями малого семейства Касами такого же периода, что обеспечивает более высокую помехоустойчивость последовательностей Касами при их передаче по каналам с ошибками. Таким образом, по критерию корреляции преимущество на стороне последовательностей малого семейства Касами.

Кроме того, помехоустойчивость последовательностей малого семейства Касами по сравнению с последовательностями Голда одинакового периода будет выше благодаря тому, что *m*-элементные участки в последовательностях Голда в 4/3 раза длиннее (в последовательности Касами $m = \frac{3n}{2}$, а в последовательности Голда $m = 2n$). Следовательно, это увеличивает вероятность приема *m*-элементных участков последовательности Голда с ошибками и, тем самым, уменьшает вероятность правильного распознавания последовательности Голда по сравнению с последовательностями Касами при мажоритарной обработке таких последовательностей.

С учетом вышеизложенного можно сделать вывод, что последовательности малого семейства Касами обладают более высокой помехоустойчивостью в сравнении с последовательностями Голда с одинаковым периодом.

Список используемых источников

1. Лосев В.Р., Бродская Е.Б., Коржик В.И. Поиск и декодирование сложных дискретных сигналов. М.: Связь, 1979. 302 с.
2. Диксон Р.К. Широкополосные системы. М.: Связь, 1979. 304 с.
3. Ипатов В.П. Широкополосные системы и кодовое разделение сигналов. Принципы и приложения. М.: Техносфера, 2007. 488 с.
4. Kasami T. Weight Distribution Formula for Some Class of Cyclic Codes. Technical Report R285. April 1966. Illinois: University of Illinois. 32 p.
5. Yefeng H.E., Wenping M.A. Generalized Kasami Sequences: The Small Set // Journal of Computational Information Systems. 2011. No. 7. PP. 4065–4070.
6. Косолапов А.С., Второв А.В. Координатный метод синхронизации и распознавания двоичных составных кодовых последовательностей // Инженерный журнал: наука и инновации. 2014.№ 6(30).17 с.
7. Когновицкий О.С. Двойственный базис и его применение в телекоммуникациях. СПб.: Линк, 2009. 424 с.
8. Sarwate D.V., Pursley M.B. Crosscorrelation Properties of Pseudorandom and Related Sequences // Proceedings IEEE. Vol. 68. No. 5. May 1980. PP. 583–619.

* * *

THE SMALL SET OF KASAMI SEQUENCES AND THEIR DECODING BASED ON THE DUAL BASIS

S. Vladimirov[1], O. Kognovitsky[1]

[1]The Bonch-Bruevich Saint-Petersburg State University of Telecommunication,
St. Petersburg, 193232, Russian Federation

Article info
Article in Russian

For citation: Vladimirov S., Kognovitsky O. The Small Set of Kasami Sequences and their Decoding Based on the Dual Basis // Proceedings of Telecommunication Universities. 2018. Vol. 4. Iss. 1. PP. 22–31.

Abstract: *The current development of digital transmission systems increasingly focuses on the use of wideband data transmission methods based, in particular, on the direct sequence spread spectrum (DSSS). The use of wideband signals provides an increase in the efficiency of systems in terms of such indicators as noise immunity, a decrease in the energy of transmitted signals, an increase in the level of stealth of the process of data transmission over a noisy channel, an increase in the efficiency of the phasing system, etc. The most often choice for DSSS are maximum length sequences and Gold sequences, the characteristics and processing methods of which have been studied in sufficient detail and presented in many publications. The article is devoted to the sequences of the small set of Kasami sequences, which have a number of advantages over Gold and maximum length sequences. A new Kasami sequences small set processing approach based on a dual basis is considered.*

Keywords:*Kasami sequence, Kasami sequence small set, dual basis, error probability.*