ОБРАБОТКА ШИРОКОПОЛОСНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ГОРДОНА–МИЛЛСА–ВЕЛЧА С ИСПОЛЬЗОВАНИЕМ ДВОЙСТВЕННОГО БАЗИСА НА ОСНОВЕ ДВУХ РЕГИСТРОВ

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: vladimirov.opds@gmail.com

Информация о статье
УДК 621.396
Язык статьи – русский

Ссылка для цитирования: Владимиров С.С., Когновицкий О.С. Обработка широкополосных последовательностей Гордона–Миллса–Велча с использованием двойственного базиса на основе двух регистров // Труды учебных заведений связи. 2019. Т. 5. № 2. С. 49–58. DOI:10.31854/1813-324X-2019-5-2-49-58

Аннотация: *Представлен алгоритм обработки и определения, с использованием двойственного базиса, начальных состояний регистров сдвига, формирующих широкополосные последовательности Гордона–Миллса–Велча (ГМВ), которые характеризуются большим их количеством и более высокой структурной скрытностью, чем широко используемые М-последовательности. Показано, что предложенный алгоритм, в отличие от известных, позволяет определять произвольные начальные состояния регистров сдвига, что расширяет возможности применения составных широкополосных последовательностей ГМВ для решения различных задач при передаче информации по каналам связи с шумами.*

Ключевые слова: *широкополосные последовательности, конечное поле, неприводимый и примитивный многочлен, регистр сдвига с линейной обратной связью, двойственный базис, функция след, децимация.*

Введение

Среди семейства псевдослучайных (шумоподобных) последовательностей, применяемых в системах связи, особое место занимают последовательности Гордона–Миллса–Велча (ГМВ), формируемые на основе регистров сдвига с обратной связью. ГМВ-последовательности обладают хорошими автокорреляционными свойствами, аналогичными корреляционным свойствам М-последовательностей, что позволяет успешно их применять для расширения спектра в широкополосных системах, для циклового фазирования, скремблирования, кодового разделения каналов и т. п. Отличительной особенностью ГМВ-последовательностей является их более высокая структурная скрытность.

Исследованиям свойств ГМВ-последовательностей, их синтезу и обработке посвящено значительное число работ отечественных и зарубежных авторов. К числу ранних работ отечественных авторов, посвященных исследованию ГМВ-последовательностей, относятся работы Е.И. Кренгеля [1, 2] и В.Г. Стародубцева [3, 4]. В частности, в трудах Е.И. Кренгеля подробно рассматриваются вопросы генерации ГМВ-последовательностей и их корреляционные свойства, а также применимость их в системах с кодовым разделением каналов. Научные труды В.Г. Стародубцева посвящены, главным образом, методам формирования ГМВ-последовательностей на основе регистров сдвига с линейной обратной связью, а также на основе матричного представления М-последовательностей составного периода над конечными полями с двойным расширением.

Очевидно, что ГМВ-последовательности, как псевдослучайные, могут найти применение в широкополосных системах связи не только для расширения спектра, но и как переносчики информации. При этом передаваемая информация может представляться определенными, например, начальными, состояниями ячеек регистра сдвига с обратной связью. Использование ГМВ-последовательностей обеспечивает большую структурную скрытность передачи информации, поэтому они в большей степени применимы для шифрования информации, закодированной, например, фазой М-последовательности. В [4] рассмотрена задача передачи информации в виде начальных фаз регистров сдвига с линейной обратной связью равной длины, формирующих ГМВ-последовательности.

Недостатком разработанного и представленного в работе [4] алгоритма является то, что начальные состояния обоих регистров выбираются одинаковыми. Из работы не ясно, насколько изменится и усложнится разработанный алгоритм, если начальные состояния ячеек регистров будут различными.

Кроме того, в указанной выше работе не рассматривается вопрос обработки и распознавания ГМВ-последовательностей на приеме. Наиболее часто применяемой является корреляционная обработка и распознавание ГМВ-последовательностей на приеме, особенно в системах с кодовым разделением CDMA. Однако, во многих случаях, например, для повышения безопасности передачи информации, надежности циклового фазирования и др., увеличивают структурную скрытность и, с этой целью, увеличивают длительность ГМВ-последовательностей, что, в случае корреляционной обработки, естественно приведет к усложнению реализации из-за установки на приеме большого количества корреляторов или согласованных фильтров. Поэтому актуальной является задача разработки, отличных от корреляционных, методов обработки и распознавания таких последовательностей на приеме.

В данной работе рассматривается применение для обработки и распознавания ГМВ-последовательностей двойственного базиса [5], расширяющего возможности применения ГМВ-последовательностей для решения различных задач. В частности, в отличие от рассмотренных в цитируемых источниках алгоритмов, при использовании двойственного базиса допускаются произвольные начальные состояния обоих регистров сдвига с линейными обратными связями.

Формирование ГМВ-последовательностей на основе регистров сдвига

Рассмотрим алгоритм формирования ГМВ-последовательностей на основе двух регистров сдвига. Во-первых, отметим, что псевдослучайные ГМВ-последовательности являются составными, наподобие последовательностей Голда или ЛРД-последовательностей [5]. При этом, в отличие от выше приведенных, основой ГМВ-последовательности является заданная исходная М-последовательность с периодом $N = 2^n - 1$, из которой путем децимаций формируются две другие последовательности – одна с периодом N, а вторая с меньшим периодом N_1, являющимся делителем N. Линейная сумма этих двух последовательностей и будет представлять собой формируемую ГМВ-последовательность с периодом N. Как показано в [4], эти две последовательности (рисунок 1) формируются с помощью двух n-элементных рекуррентных регистров сдвига с линейными обратными связями (РОС). Обе выходные последовательности поэлементно складываются по mod 2, образуя тем самым ГМВ-последовательности.

Для построения регистров сдвига с линейными обратными связями выбирают два неприводимых многочлена степени n – $h_1(x)$ и $h_2(x)$, корни которых являются p-сопряженными ($p = 2$) элементами расширенного поля GF(2^n) с первообразным элементом поля ε – корнем примитивного многочлена $g(x)$, по которому построены расширенное поле GF(2^n) и исходная М-последовательность. При этом степени корней многочлена $g(x)$ представляют собой циклокласс $\{1, 2, 4, 8, \ldots, 2^{n-1}\}$, а степени корней многочленов $h_1(x)$ и $h_2(x)$ – циклоклассы $\{q_1, 2q_1, 4q_1, \ldots, 2^{n-1}q_1\}$ и $\{q_2, 2q_2, 4q_2, \ldots, 2^{n-1}q_2\}$, соответственно, где q_1 и q_2 – индексы децимаций, выбранных для построения ГМВ-последовательности. Формируемая ГМВ-последовательность будет являться рекуррентной последовательностью с периодом $N = 2^n - 1$, удовлетворяющей характеристическому многочлену $h(x) = h_1(x) \cdot h_2(x)$ степени $2n$.

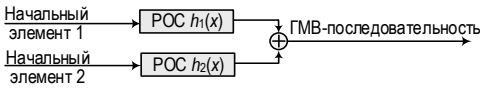

Рис. 1. Схема генератора ГМВ-последовательностей

Итак, как было заявлено ранее, задачей декодера на приеме будем считать определение переносчиков информации ГМВ-последовательностей, а именно – определение начальных фаз обеих составляющих последовательностей, которые обозначим как M_1 для многочлена $h_1(x)$ и M_2 для многочлена $h_2(x)$.

Обработка ГМВ-последовательностей с использованием двойственного базиса

Решение поставленной выше задачи зависит от того, с какой системой связи мы имеем дело, – синхронной или асинхронной. Наибольшее распространение среди широкополосных систем связи получили синхронные системы, в которых в качестве расширяющих могут использоваться также и ГМВ-последовательности, обладающие, к тому же повышенной структурной скрытностью по сравнению с широко применяемыми обычными М-последовательностями. При этом, как было отмечено, начальные фазы составных последовательностей могут представлять собой передаваемую информацию, в том числе это может быть адресная или другая специальная информация, известная только отправителю и получателю.

Кроме того, применение двойственного базиса за счет мажоритарного принятия решения обеспечивает, при более простой реализации, достоверность, сравнимую с корреляционной обработкой. Наконец, применение двойственного базиса позволяет избежать еще одного недостатка алгоритма, описанного в [4], который заключается в том, что формирование составляющих последовательностей M_1 и M_2 привязано к канонической исходной М-последовательности, образованной примитивным многочленом $g(x)$ степени n.

Рассмотрим на примере алгоритм обработки ГМВ-последовательностей, основанный на применении двойственного базиса, при условии, что формирование ГМВ-последовательностей происходит с помощью двух регистров сдвига по модулю многочленов $h_1(x)$ и $h_2(x)$ соответственно [6], включенных по схеме Галуа.

Проведем анализ алгоритмов формирования и обработки с использованием двойственного базиса ГМВ-последовательностей с периодом $N = 2^6 - 1$ над полем GF(2^6) на основе двух регистров сдвига с обратными связями. При этом исходные данные выберем те же, что и в работе [4], а именно, исходной М-последовательности $\{s\}$ соответствует характеристический примитивный многочлен $\varphi(x) = 1 + x + x^6$, корнями которого будут сопряженные первообразные элементы поля ε, ε^2, ε^4, ε^8, ε^{16}, ε^{32}. Составная двоичная ГМВ-последовательность $\{t\}$ представляет собой поэлементную сумму по mod 2 двух других последовательностей $\{u\}$ и $\{v\}$, которым соответствуют неприводимые характеристические многочлены $h_1(x)$ и $h_2(x)$. Условимся, что последовательность $\{u\}$ формируется из исходной М-последовательности $\{s\}$ путем децимаций с индексом $q_1 = 5$, а последовательность $\{v\}$ – с индексом децимации $q_2 = 3$. Тогда корнями многочлена $h_1(x)$ будут пятые степени корней многочлена $\varphi(x)$ [7], т. е. – $\{(\varepsilon)^5, (\varepsilon^2)^5, (\varepsilon^4)^5, (\varepsilon^8)^5, (\varepsilon^{16})^5, (\varepsilon^{32})^5\} = \{\varepsilon^5, \varepsilon^{10}, \varepsilon^{20}, \varepsilon^{40}, \varepsilon^{17}, \varepsilon^{34}\}$. Соответственно, корнями многочлена $h_2(x)$ будут третьи степени корней исходного многочлена $\varphi(x)$, т. е. – $\{\varepsilon^3, \varepsilon^6, \varepsilon^{12}, \varepsilon^{24}, \varepsilon^{48}, \varepsilon^{33}\}$. При этом из теории полей Галуа следует, что порядок корней многочленов $h_1(x)$ и $h_2(x)$ будет для $h_1(x)$: $\frac{63}{\text{НОД}(63,5)} = 63$ и для $h_2(x)$: $\frac{63}{\text{НОД}(63,3)} = 21$. Отсюда последовательность $\{u\}$ будет иметь максимальный период M_1, равный $N_1 = 63$, а последовательность $\{v\}$ будет состоять их трех периодов последовательности M_2 длиной $N_2 = 21$, формируемой многочленом $h_2(x)$.

Зная корни многочленов $h_1(x)$ и $h_2(x)$ по формулам Виета найдем и сами многочлены:

$$\begin{aligned} h_1(x) &= 1 + x + x^2 + x^5 + x^6, \\ h_2(x) &= 1 + x + x^2 + x^4 + x^6. \end{aligned} \qquad (1)$$

Так как последовательности $\{u\}$ и $\{v\}$ формируются из исходной М-последовательности $\{s\} = (s_0, s_1, s_2, s_3, s_4, \ldots s_i, \ldots\ldots s_{61}, s_{62})$ путем децимаций с индексами $q_1 = 5$ и $q_2 = 3$, то элементы последовательностей $\{u\}$ и $\{v\}$ будут определяться как $u_i = s_{q_1 i} = s_{5i\,(\text{mod}\,63)}$ и как $v_i = s_{q_2 i} = s_{3i\,(\text{mod}\,21)}$, соответственно, где $0 \le i \le 62$.

Из многочленов (1) следует, что элементы последовательностей $\{u\}$ и $\{v\}$ удовлетворяют рекуррентным уравнениям, соответственно:

$$\begin{aligned} u_{i\ge 6} &= u_{i-1} + u_{i-4} + u_{i-5} + u_{i-6}, (\text{mod}\ 2), \\ v_{i\ge 6} &= v_{i-1} + v_{i-4} + v_{i-5} + v_{i-6}, (\text{mod}\ 2). \end{aligned} \qquad (2)$$

Если произвольный элемент поля ε^i записать через левый степенной базис как $\varepsilon = c_0 + c_1\varepsilon + c_2\varepsilon^2 + c_3\varepsilon^3 + c_4\varepsilon^4 + c_5\varepsilon^5$, то, при заданном образующем многочлене $\varphi(x)$, функция след от этого элемента будет равна $T(\varepsilon^i) = c_5 = s_i$. Каноническая М-последовательность $\{s\}$ представляется как $\{s\} = \{T(1), T(\varepsilon), T(\varepsilon^2), T(\varepsilon^3), \ldots, T(\varepsilon^{61}), T(\varepsilon^{62})\}$. Двоичная $\{s\}$ и сформированные из нее последовательности $\{u\}$, $\{v\}$ и составная ГМВ-последовательность $\{t\}$ показаны в таблице 1.

Составной ГМВ-последовательности $\{t\}$ будет соответствовать характеристический многочлен:

$$\begin{aligned} h(x) = h_1(x) \cdot h_2(x) = p_0x^{12} + p_1x^{11} + +p_2x^{10} + \\ +p_3x^9 + p_4x^8 + p_5x^7 + p_6x^6 + p_7x^5 + p_8x^4 + \\ + p_9x^3 + p_{10}x^2 + p_{11}x + p_{12} = x^{12} + x^{11} + x^{10} + \\ +x^9 + x^7 + x^2 + 1. \end{aligned} \qquad (3)$$

Следовательно, ГМВ-последовательность $\{t\}$ будет удовлетворять рекуррентному уравнению:

$$\begin{aligned} t_{i\ge 12} = t_{i-1} + t_{i-2} + t_{i-3} + t_{i-5} + t_{i-10} + \\ + t_{i-12}, (\text{mod}\ 2). \end{aligned} \qquad (4)$$

Именно это свойство ГМВ-последовательности и позволяет применить для ее обработки двойственный базис. В соответствии с методикой, изложенной в [5], найдены коэффициенты двойственного базиса α_i относительно многочлена $h_1(x)$ и β_i относительно многочлена $h_2(x)$ (таблица 2), выраженные через элементы ε^i поля GF(2^6), построенного по исходному примитивному многочлену $\varphi(x)$.

Рассмотрим теперь нахождение начальных состояний ячеек регистров сдвига, формирующих последовательности $\{u\}$ и $\{v\}$, в процессе обработки на приемной стороне ГМВ-последовательности $\{t\}$.

Начальным элементам составных последовательностей $\{u\}$ и $\{v\}$ будут соответствовать элементы поля, представленные в степенной либо в векторной форме. Так, для последовательности $\{u\}$ начальный элемент регистра сдвига, соответствующего многочлену $h_1(x)$, будет иметь следующий общий вид:

$$\begin{aligned} C(\mu) = a_0 + a_1\mu + a_2\mu^2 + a_3\mu^3 + a_4\mu^4 + a_5\mu^5 \equiv \\ \equiv (a_0, a_1, a_2, a_3, a_4, a_5), \quad [\text{mod}\ 2, h_1(\mu)]; \end{aligned}$$

или выраженный через ε: (5)

$$\begin{aligned} C(\varepsilon) = c_0 + c_1\varepsilon + c_2\varepsilon^2 + c_3\varepsilon^3 + c_4\varepsilon^4 + c_5\varepsilon^5 \equiv \\ \equiv (c_0, c_1, c_2, c_3, c_4, c_5), \quad [\text{mod}\ 2, \varphi(\varepsilon)]. \end{aligned}$$

Аналогично для последовательности $\{v\}$:

$$\begin{aligned} D(\gamma) = b_0 + b_1\gamma + b_2\gamma^2 + b_3\gamma^3 + b_4\gamma^4 + b_5\gamma^5 \equiv \\ \equiv (b_0, b_1, b_2, b_3, b_4, b_5), \quad [\text{mod}\ 2, h_2(\gamma)]; \end{aligned}$$

или выраженный через ε: (6)

$$\begin{aligned} D(\varepsilon) = d_0 + d_1\varepsilon + d_2\varepsilon^2 + d_3\varepsilon^3 + d_4\varepsilon^4 + d_5\varepsilon^5 \equiv \\ \equiv (d_0, d_1, d_2, d_3, d_4, d_5), \quad [\text{mod}\ 2, \varphi(\varepsilon)]. \end{aligned}$$

ТАБЛИЦА 1. Формирование составной ГМВ-последовательности

{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}
	0	0	0	0	0	1	0	0	0	0	1	1	0	0	0	1	0	1	0	0	1
{u} q_1=5	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	1	1	1	1	1	1	0	1	0	1	1	1	0	0	0	1	1	0	0	1
{v} q_2=3	v_0	v_1	v_2	v_3	v_4	v_5	v_6	v_7	v_8	v_9	v_{10}	v_{11}	v_{12}	v_{13}	v_{14}	v_{15}	v_{16}	v_{17}	v_{18}	v_{19}	v_{20}
	0	0	0	0	0	1	0	1	0	0	1	0	0	1	1	0	0	1	0	1	1
{t}	t_0	t_1	t_2	t_3	t_4	t_5	t_6	t_7	t_8	t_9	t_{10}	t_{11}	t_{12}	t_{13}	t_{14}	t_{15}	t_{16}	t_{17}	t_{18}	t_{19}	t_{20}
	0	**1**	**1**	**1**	**1**	**0**	**1**	**1**	**1**	**0**	**0**	**1**	**1**	**1**	**1**	**0**	**1**	**0**	**0**	**1**	**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}
	1	1	1	0	1	0	0	0	1	1	1	0	0	1	0	0	1	0	1	1	0
{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	0	1	1	0	0	0	0	0	1	1	1	1	0	0	1	0	0	1	0
{v}	v_{21}	v_{22}	v_{23}	v_{24}	v_{25}	v_{26}	v_{27}	v_{28}	v_{29}	v_{30}	v_{31}	v_{32}	v_{33}	v_{34}	v_{35}	v_{36}	v_{37}	v_{38}	v_{39}	v_{40}	v_{41}
	0	0	0	0	0	1	0	1	0	0	1	0	0	1	1	0	0	1	0	1	1
{t}	t_{21}	t_{22}	t_{23}	t_{24}	t_{25}	t_{26}	t_{27}	t_{28}	t_{29}	t_{30}	t_{31}	t_{32}	t_{33}	t_{34}	t_{35}	t_{36}	t_{37}	t_{38}	t_{39}	t_{40}	t_{41}
	1	**1**	**0**	**1**	**1**	**1**	**0**	**1**	**0**	**0**	**0**	**1**	**1**	**0**	**1**	**0**	**1**	**1**	**0**	**0**	**1**
{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}
	1	1	1	0	1	1	0	0	1	1	0	1	0	1	0	1	1	1	1	1	1
{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	0	1	0	0	1	1	0	1	0	0	0	0	1	0	0	0	1	0	1	1
{v}	v_{42}	v_{43}	v_{44}	v_{45}	v_{46}	v_{47}	v_{48}	v_{49}	v_{50}	v_{51}	v_{52}	v_{53}	v_{54}	v_{55}	v_{56}	v_{57}	v_{58}	v_{59}	v_{60}	v_{61}	v_{62}
	0	0	0	0	0	1	0	1	0	0	1	0	0	1	1	0	0	1	0	1	1
{t}	t_{42}	t_{43}	t_{44}	t_{45}	t_{46}	t_{47}	t_{48}	t_{49}	t_{50}	t_{51}	t_{52}	t_{53}	t_{54}	t_{55}	t_{56}	t_{57}	t_{58}	t_{59}	t_{60}	t_{61}	t_{62}
	1	**0**	**1**	**0**	**0**	**0**	**1**	**1**	**1**	**0**	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**

ТАБЛИЦА 2. Коэффициенты двойственного базиса

$\alpha_i(\varepsilon)$	α_1	α_2	α_3	α_4	α_5	α_6	α_7	α_8	α_9	α_{10}	α_{11}	α_{12}
	ε^{43}	ε^{38}	ε^{31}	ε^{26}	ε^{21}	ε^{16}	ε^{11}	ε^{50}	ε^{45}	ε^{9}	ε^{47}	ε^{48}
$\beta_i(\varepsilon)$	β_1	β_2	β_3	β_4	β_5	β_6	β_7	β_8	β_9	β_{10}	β_{11}	β_{12}
	ε^{16}	ε^{13}	ε^{11}	ε^{8}	ε^{5}	ε^{2}	ε^{62}	ε^{55}	ε^{52}	ε^{32}	ε^{51}	ε^{19}

Более простая реализация будет в случае выражения начальных элементов через один элемент поля ε – корень исходного многочлена $\varphi(x)$, а не через различные элементы μ и γ – корни многочленов $h_1(x)$ и $h_2(x)$, где $\mu = \varepsilon^5$ и $\gamma = \varepsilon^3$.

Как показано в [5], начальные элементы последовательностей {u} и {v} могут быть определены по любому безошибочному 12-элементному участку принятой ГМВ-последовательности {t}. Предположим, что выделен 12-элементный участок канонической ГМВ-последовательности (см. таблицу 1) с начальным порядковым номером $i = 51$, т. е.:

t_{51}	t_{52}	t_{53}	t_{54}	t_{55}	t_{56}	t_{57}	t_{58}	t_{59}	t_{60}	t_{61}	t_{62}
0	1	0	0	0	1	0	0	0	0	0	0

Тогда, в соответствии с [5], найдем:

$$C(\varepsilon) = (\varepsilon^5)^{-i}\sum_{j=1}^{12}\alpha_j t_{i+j-1} = (\varepsilon^5)^{-51}(\alpha_2+\alpha_6) = \varepsilon^{-3}(\varepsilon^{38}+\varepsilon^{16}) = 1, \mod \varphi(\varepsilon);$$
$$D(\varepsilon) = (\varepsilon^3)^{-i}\sum_{j=1}^{8}\beta_j t_{i+j-1} = (\varepsilon^3)^{-51}(\beta_2+\beta_6) = \varepsilon^{-27}(\varepsilon^{13}+\varepsilon^{2}) = 1, \mod \varphi(\varepsilon). \quad (7)$$

Можно показать, что также выполняются равенства: $C(\mu) = 1 \pmod{h_1(\mu)}$; $D(\gamma) = 1 \pmod{h_2(\gamma)}$.

Таким образом, мы убеждаемся, что начальным элементам последовательностей {u} и {v} канонической ГМВ-последовательности {t} действительно соответствуют единичные элементы регистров сдвига, а передаваемая информация в векторном представлении будет: (C, D) = [(100000)(100000)].

Покажем, что алгоритм распознавания начальных состояний регистров остается таким же и при произвольных начальных элементах $C(\mu) \pmod{h_1(x)}$ и $D(\gamma) \pmod{h_2(x)}$ этих регистров.

Пусть начальные элементы регистров, формирующих последовательности {u} и {v}, будут равны, соответственно: $C(\mu) = \mu^{55} \equiv 1 + \mu^3 \rightarrow$ **[*a*]** = (a_0, a_1, a_2, a_3, a_4, a_5) = (100100) $\pmod{h_1(\mu)}$ и $D(\gamma) = 1 + \gamma + \gamma^2 \rightarrow$ **[*b*]** = (b_0, b_1, b_2, b_3, b_4, b_5) = (111000) $\pmod{h_2(\gamma)}$. Как видим, вектору **[*a*]** в десятичной системе счисления соответствует цифра 9 (младший разряд слева), а вектору **[*b*]** – цифра 7. Тогда первый элемент u_0 последовательности {u}, выраженный функцией след, будет равен $u_0 = T(\mu^{55}) = 1$, $\pmod{h_1(\mu)}$, а первый элемент v_0 последовательности {v} будет равен $v_0 = T(1+\gamma+\gamma^2) = 0$, $\pmod{h_2(\gamma)}$. Сумма этих элемен-

тов по mod 2 порождает первый элемент последовательности $\{t\}$ $t_0 = u_0 + v_0 = 1$. В таблице 3 представлены первые 15-элементные участки последовательностей $\{u\}$, $\{v\}$ и $\{t\}$, порождаемые указанными выше начальными элементами $C(\mu)$ и $D(\gamma)$.

ТАБЛИЦА 3. Первые 15 элементов последовательностей $\{u\}$, $\{v\}$ и $\{t\}$

$\{u\}$	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}
	1	0	0	0	1	0	1	1	0	1	1	1	1	1	1
$\{v\}$	v_0	v_1	v_2	v_3	v_4	v_5	v_6	v_7	v_8	v_9	v_{10}	v_{11}	v_{12}	v_{13}	v_{14}
	0	0	0	1	1	0	1	1	1	1	1	1	0	0	1
$\{t\}$	t_0	t_1	t_2	t_3	t_4	t_5	t_6	t_7	t_8	t_9	t_{10}	t_{11}	t_{12}	t_{13}	t_{14}
	1	0	0	1	0	0	0	0	1	0	0	0	1	1	0

Выделим первый 12-элементный участок ($i = 0$):

t_0	t_1	t_2	t_3	t_4	t_5	t_6	t_7	t_8	t_9	t_{10}	t_{11}
1	0	0	1	0	0	0	0	1	0	0	0

и обработаем его двойственным базисом:

$$C(\varepsilon) = \sum_{j=1}^{12} \alpha_j t_{i+j-1} = (\alpha_1 + \alpha_4 + \alpha_9) = (\varepsilon^{43} + \varepsilon^{26} + \varepsilon^{45}) = 1 + \varepsilon^3 + \varepsilon^5 = \varepsilon^{23}, \mod \varphi(\varepsilon);$$

$$D(\varepsilon) = \sum_{j=1}^{8} \beta_j t_{i+j-1} = (\beta_1 + \beta_4 + \beta_9) = (\varepsilon^{16} + \varepsilon^8 + \varepsilon^{52}) = \varepsilon + \varepsilon^3 = \varepsilon^{19}, \mod \varphi(\varepsilon).$$

Выделим теперь другой безошибочный 12-элементный участок (на расстоянии $i = 3$ от начала):

t_3	t_4	t_5	t_6	t_7	t_8	t_9	t_{10}	t_{11}	t_{12}	t_{13}	t_{14}
1	0	0	0	0	1	0	0	0	1	1	0

и также обработаем его двойственным базисом:

$$C(\varepsilon) = (\varepsilon^5)^{-3} \sum_{j=1}^{12} \alpha_j t_{i+j-1} = \varepsilon^{-15}(\alpha_1 + \alpha_6 + \alpha_{10} + \alpha_{11}) = \varepsilon^{48}(\varepsilon^{43} + \varepsilon^{16} + \varepsilon^9 + \varepsilon^{47}) = 1 + \varepsilon^3 + \varepsilon^5 = \varepsilon^{23}, \mathrm{mod}\varphi(\varepsilon);$$

$$D(\varepsilon) = (\varepsilon^3)^{-3} \sum_{j=1}^{8} \beta_j t_{i+j-1} = \varepsilon^{-9}(\beta_1 + \beta_6 + \beta_{10} + \beta_{11}) = \varepsilon^{-9}(\varepsilon^{16} + \varepsilon^2 + \varepsilon^{32} + \varepsilon^{51}) = \varepsilon + \varepsilon^3 = \varepsilon^{19}, \mathrm{mod}\varphi(\varepsilon).$$

Таким образом, после обработки и одного, и другого безошибочных участков получены одинаковые начальные элементы в векторном представлении:

$$C(\varepsilon) = (c_0, c_1, c_2, c_3, c_4, c_5) = (100101), [\mathrm{mod}2, \varphi(\varepsilon)];$$
$$D(\varepsilon) = (d_0, d_1, d_2, d_3, d_4, d_5) = (010100), [\mathrm{mod}2, \varphi(\varepsilon)]. \quad (8)$$

Это подтверждает возможность применения мажоритарного (по большинству) принятия решения с целью повышения достоверности декодирования информации, содержащейся в начальных элементах (векторах) регистров сдвига, соответствующих составным последовательностям $\{u\}$ и $\{v\}$.

Возможны два варианта кодирования информации ГМВ-последовательностей. Первый из вариантов состоит в том, что передаваемая информация представляется начальными элементами $C(\varepsilon)$ и $D(\varepsilon)$, которые на передающей стороне были, путем умножения на матрицы H и P вида (9), переведены в $C(\mu)$ и $D(\gamma)$ и в векторной форме были записаны в ячейки соответствующих регистров:

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}; \quad P = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}. \quad (9)$$

Блочная схема этого варианта представлена на рисунке 2. В этом первом варианте декодированная информация (при правильном декодировании) в виде элементов $C(\varepsilon)$ и $D(\varepsilon)$ будет после обработки ГМВ-последовательности непосредственно находиться в ячейках соответствующих регистров. Для обратного перевода (в случае необходимости) требуется умножить выделенные вектора (8) на матрицы (9), в результате чего получим:

$$[C(\varepsilon)] \cdot H = (c_0, c_1, c_2, c_3, c_4, c_5) \cdot H = (100101) \cdot H = (100100) \Rightarrow 1 + \mu^3 = C(\mu), \quad \mod h_1(\mu);$$
$$[D(\varepsilon)] \cdot P = (d_0, d_1, d_2, d_3, d_4, d_5) \cdot P = (010100) \cdot P = (111000) \Rightarrow 1 + \gamma + \gamma^2 = D(\gamma), \quad \mod h_2(\gamma).$$

Таким образом, после умножения на указанные матрицы мы получили те начальные элементы $C(\mu)$ и $D(\gamma)$, которые и были установлены на передающей стороне в ячейки регистров в качестве начальных.

Во втором варианте передаваемая информация представляется начальными элементами $C(\mu)$ и $D(\gamma)$, которые на передающей стороне в векторном виде будут непосредственно записаны в ячейки соответствующих регистров. В этом варианте полученные в результате декодирования (при правильном декодировании) элементы $C(\varepsilon)$ и $D(\varepsilon)$ могут быть в векторной форме переведены (в случае необходимости) в начальные элементы $C(\mu)$ и $D(\gamma)$ по тому же алгоритму, что и в первом варианте, т. е. путем умножения векторов $[c]$ и $[d]$ на соответствующие матрицы перевода H и P (9).

Выбор того или другого варианта дает возможность еще в большей степени повысить структурную скрытность передачи информации.

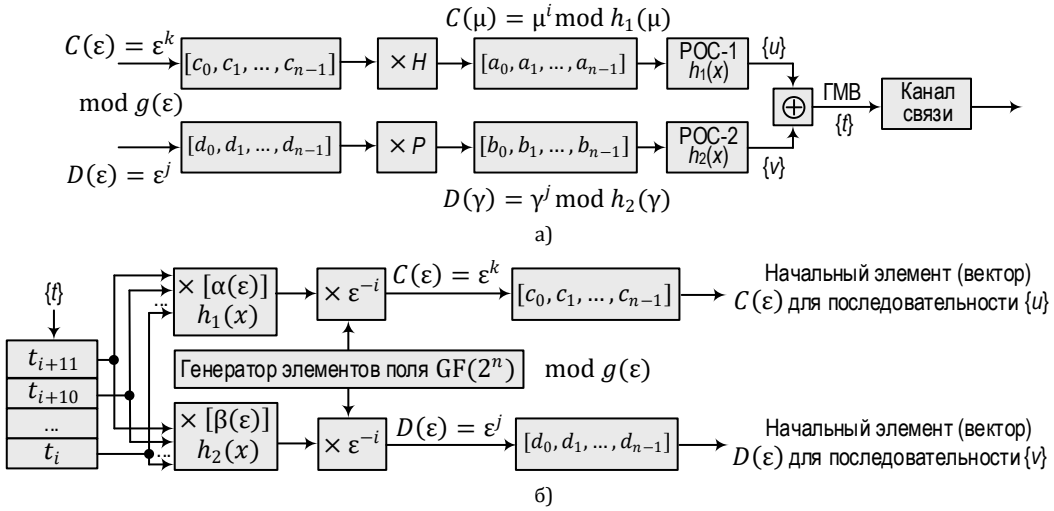

Рис. 2. Передающая (а) и приемная (б) части системы формирования и обработки ГМВ-последовательностей

Во втором варианте передаваемая информация представляется начальными элементами $C(\mu)$ и $D(\gamma)$, которые на передающей стороне в векторном виде будут непосредственно записаны в ячейки соответствующих регистров. В этом варианте полученные в результате декодирования (при правильном декодировании) элементы $C(\varepsilon)$ и $D(\varepsilon)$ могут быть в векторной форме переведены (в случае необходимости) в начальные элементы $C(\mu)$ и $D(\gamma)$ по тому же алгоритму, что и в первом варианте, т. е. путем умножения векторов $[c]$ и $[d]$ на соответствующие матрицы перевода H и P (9).

Выбор того или другого варианта дает возможность еще в большей степени повысить структурную скрытность передачи информации.

Для определения весового спектра рассмотренной ранее ГМВ-последовательности с периодом $N = 63$ над полем GF(2^6) был произведен полный перебор всех возможных начальных фаз, имеющих значения от 0 до 63 (в десятичном виде), и определены веса полученных ГМВ-последовательностей. Весовой спектр рассмотренной ГМВ-последовательности приведен в таблице 4.

ТАБЛИЦА 4. Весовой спектр ГМВ-последовательностей с периодом $N = 63$ над полем GF(2^6)

Количество ГМВ-последовательностей	0	24	28	32	36
Вес	1	588	504	1827	1176

Корреляционные свойства ГМВ-последовательности

На примере рассмотренной последовательности ГМВ-последовательность с периодом $N = 63$ над полем GF(2^6) оценим корреляционные свойства последовательностей разных весов. При расчете автокорреляционной функции (АКФ) и взаимокорреляционной (ВКФ) функции последовательности ГМВ-последовательности преобразуются от униполярного вида [1, 0] к биполярному [–1, 1].

Для оценки корреляционных свойств были выбраны по две ГМВ-последовательности каждого веса. На графиках (рисунки 3, 4, 5 и 6) начальные элементы каждой из ГМВ-последовательности обозначены в десятичном виде, соответствующем двоичному (векторному) представлению их элементов μ^i для $C(\mu)$ и γ^i для $D(\gamma)$, соответственно. Так, ГМВ-последовательности $G\{35; 9\}$ соответствует $G\{1 + \mu + \mu^5; 1 + \gamma^3\}$, а ГМВ-последовательности $G\{20; 23\}$ соответствует $G\{\mu^2 + \mu^4; 1 + \gamma + \gamma^2 + \gamma^4\}$.

Вначале определим автокорреляционные свойства выбранных ГМВ-последовательности. Апериодическая автокорреляционная функция (АпАКФ) последовательности $\{t\}$ вычисляется по формуле:

$$\text{АпАКФ}_k(\{t\}) = \sum_{i=0}^{N-1-k} t_i t_{i+k},$$

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

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

$$\text{ПАКФ}_k(\{t\}) = \sum_{i=0}^{N-1} t_i t_{(i+k) \bmod N}.$$

Значения апериодической и периодической ВКФ рассчитываются по аналогичным формулам, в которых рассматривается смещение одной последовательности относительно другой. Графики этих функций для ГМВ-последовательностей различных весов приведены на рисунках 5 и 6. На графике ВКФ для ГМВ-последовательностей веса 24 (см. рисунок 6), можно видеть, что выбранные последовательности циклически смещены друг относительно друга на 9 разрядов. Таким образом, при использовании ГМВ-последовательностей для задач синхронизации необходимо правильно подбирать начальные элементы последовательностей, так как они, образуя циклическую группу, при асинхронном детектировании могут определяться некорректно.

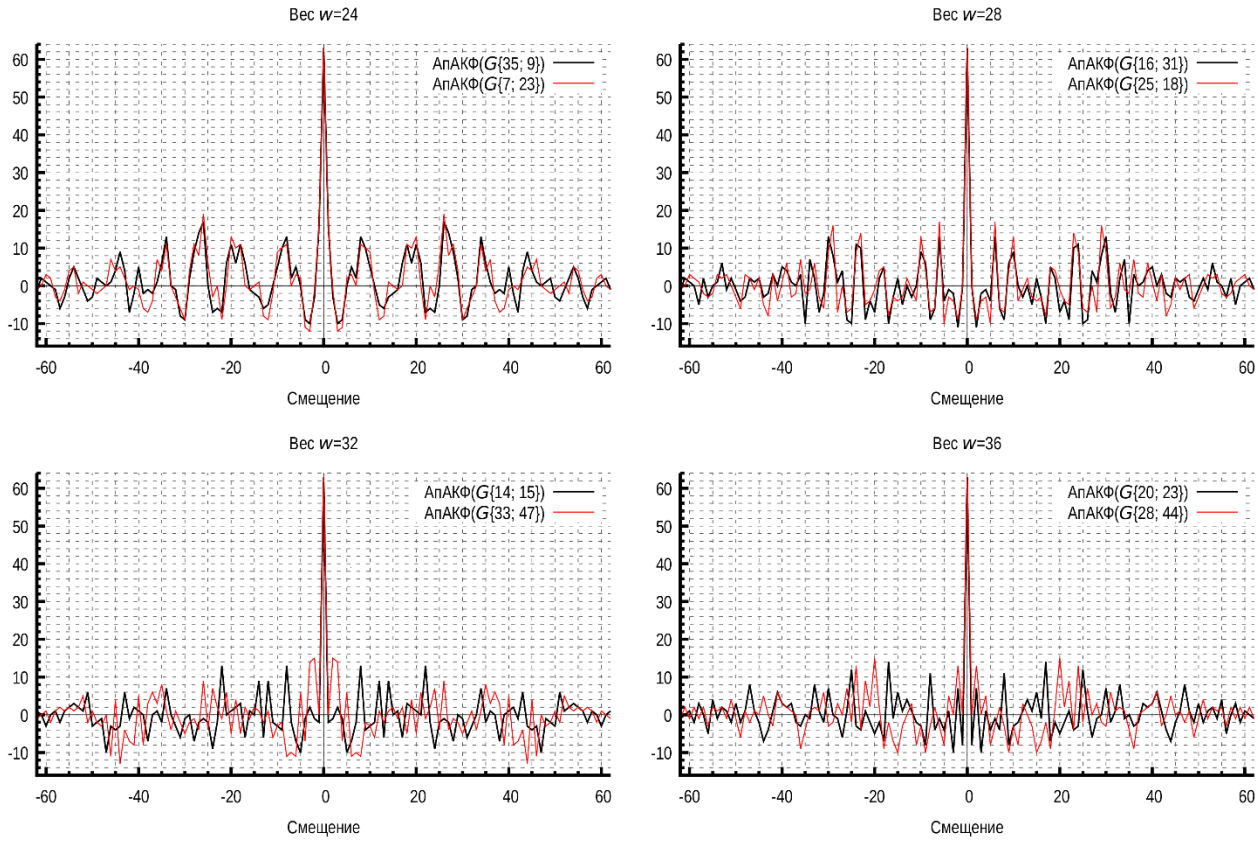

Рис. 3. Значения АпАКФ ГМВ-последовательностей различных весов

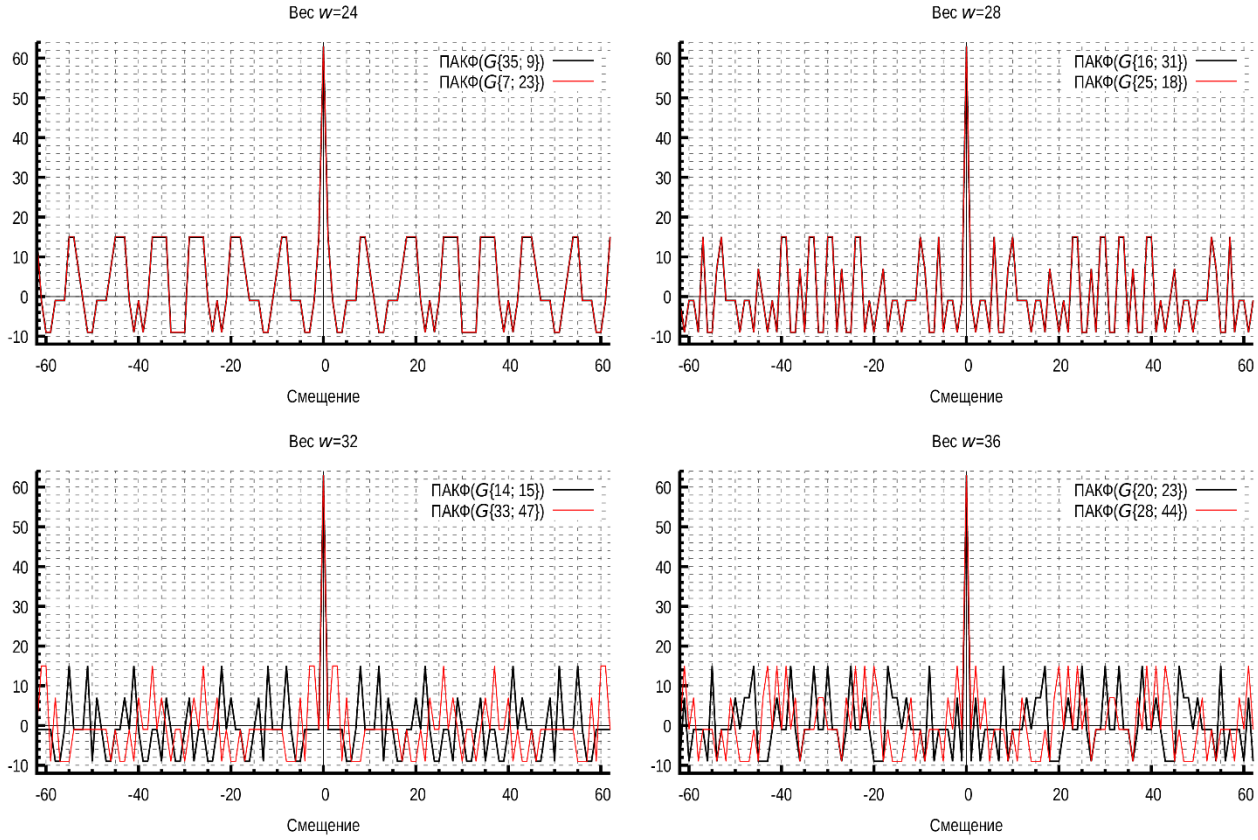

Рис. 4. Значения ПАКФ ГМВ-последовательностей различных весов

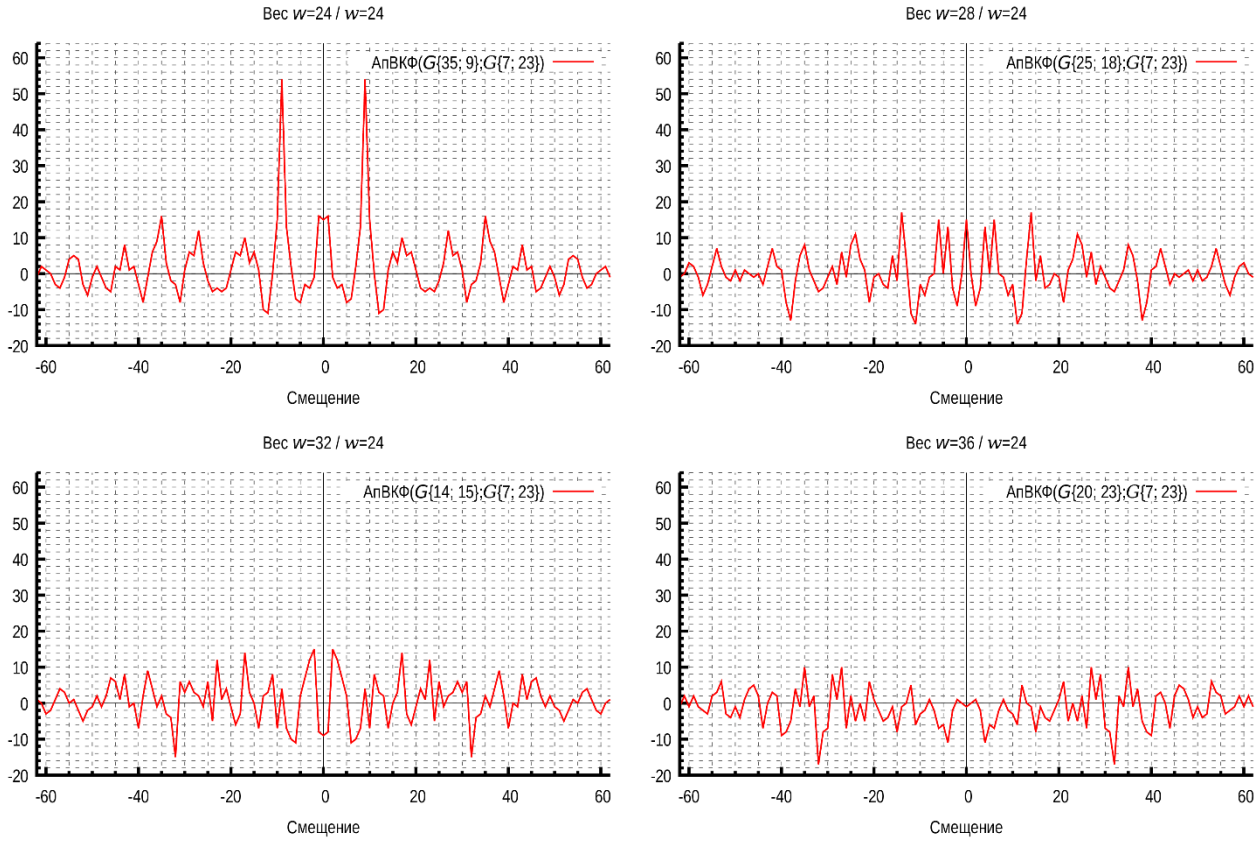

Рис. 5. Значения АпВКФ ГМВ-последовательностей различных весов

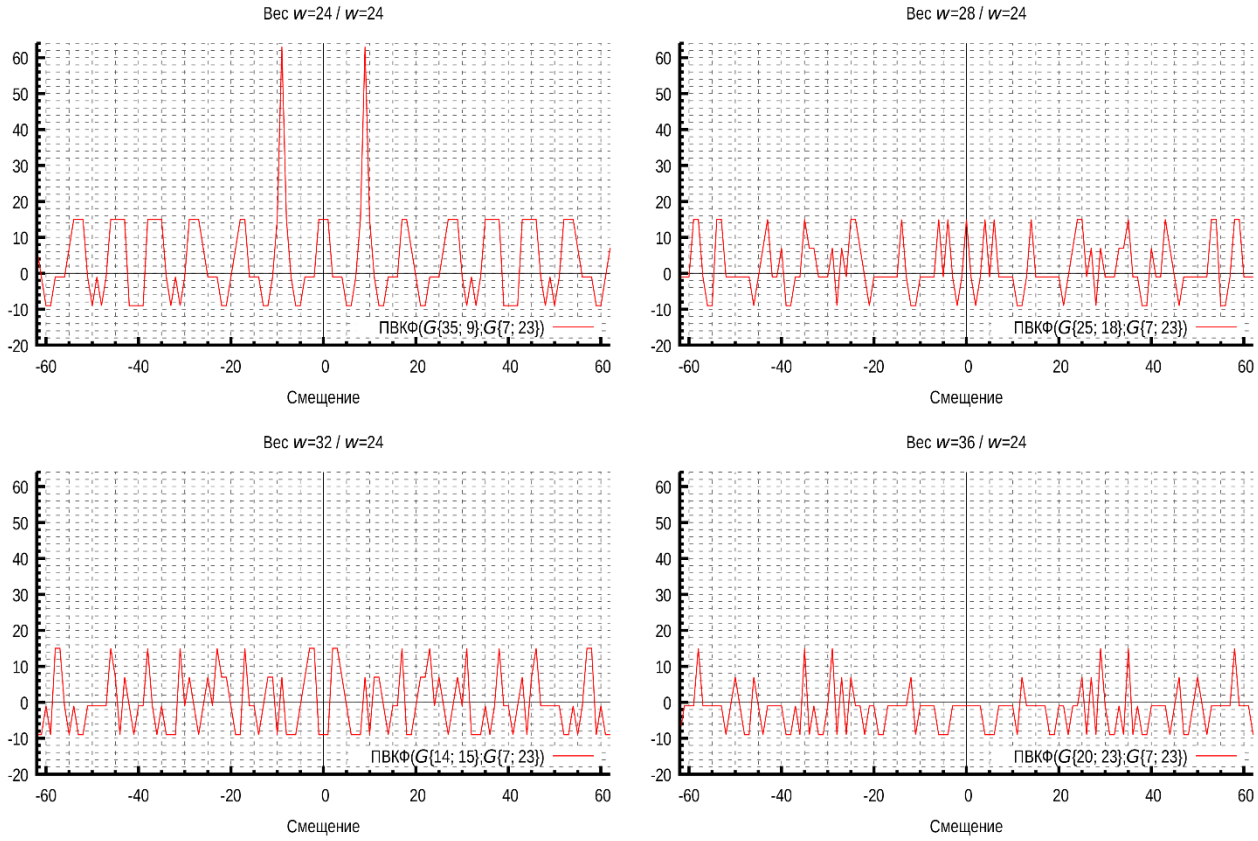

Рис. 6. Значения ПВКФ ГМВ-последовательностей различных весов

Вероятностные характеристики декодера ГМВ-последовательностей

Для оценки вероятностных характеристик синхронного декодера ГМВ-последовательностей с использованием двойственного базиса была написана модель системы передачи данных (СПД) для пакета математических вычислений GNU/Octave, схема которой представлена на рисунке 7. Моделирование производилось по методу Монте-Карло для двух моделей каналов: цифрового двоично-симметричного канала (ДСК) без памяти и канала с абсолютно-белым гауссовским шумом (АБГШ) совместно с двоичной фазовой манипуляцией (ФМн-2).

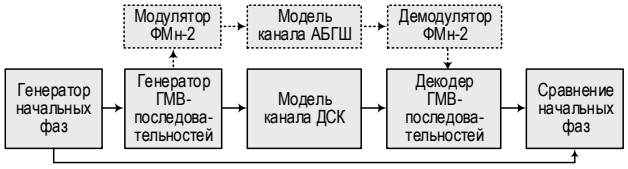

Рис. 7. Схема модели СПД для оценки вероятностных характеристик синхронного декодера ГМВ-последовательностей

При моделировании генератор начальных фаз случайным образом формирует начальные элементы $C(\mu)$ и $D(\gamma)$ и передает их в генератор ГМВ-последовательностей. Сформированная последовательность отправляется в канал передачи данных, откуда подается на вход декодера, реализующего мажоритарный алгоритм декодирования с использованием двойственного базиса. Затем вычисленные элементы сравниваются с начальными и производится накопление статистики.

Всего в результате декодирования возможны три исхода: правильное декодирование, когда его результат совпадает с начальными элементами, неправильное декодирование в случае несовпадения хотя бы одного из начальных элементов, и отказ от декодирования (обнаруженная неисправляемая ошибка), возникающий при невозможности определить только одну пару начальных элементов. Соответствующие этим исходам оценочные значения вероятностей обозначаются $P_{пд}$, $P_{нд}$ и $P_{од}$.

Графики вероятностных характеристик декодера ГМВ-последовательностей в линейном и логарифмическом масштабах для случая канала ДСК представлены на рисунках 8а, 8б, а для случая канала АБГШ – на рисунках 8в, 8г. Согласно полученным графикам вероятностных характеристик вероятность правильного приема кодовой комбинации на уровне 0,9999 достигается уже при нормированном соотношении сигнал/шум около 4 Дб. При отношении сигнал/шум, равном 0 Дб, вероятность правильного приема комбинации составляет уже 0,9. В канале ДСК эти точки соответствуют вероятностям битовой ошибки 0,015 и 0,08.

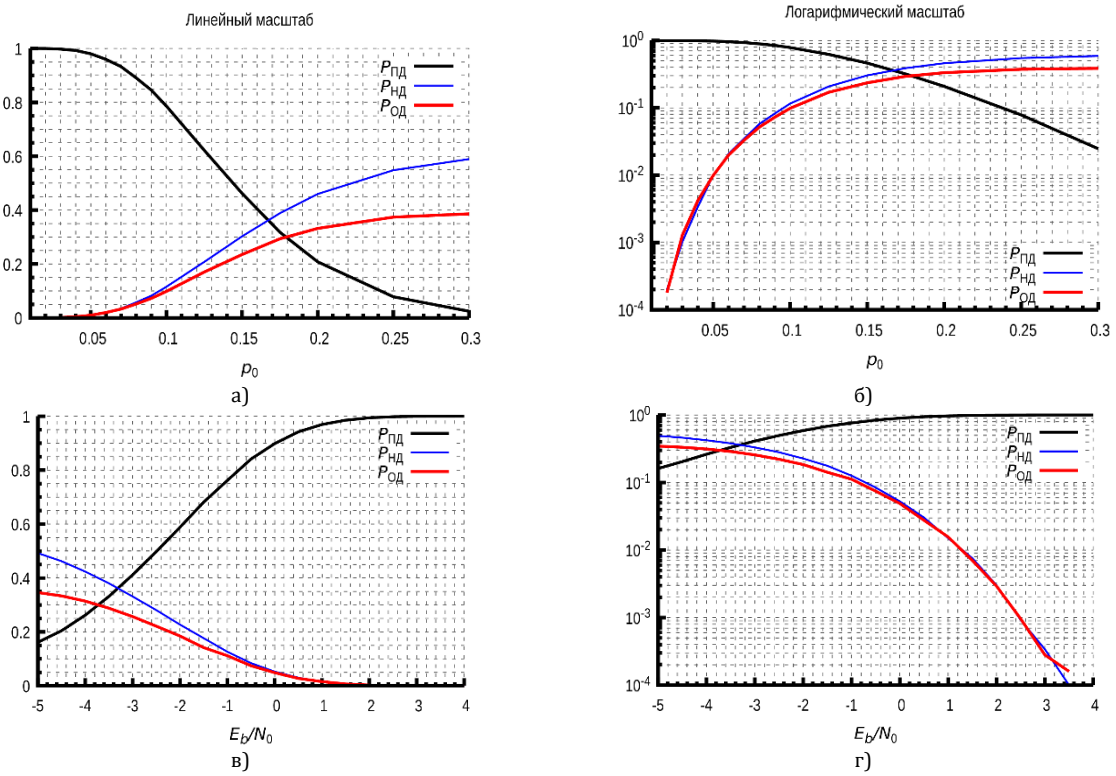

Рис. 8. Вероятностные характеристики декодера ГМВ-последовательностей для канала ДСК (а, б) и АБГШ с ФМн-2 (в, г)

Заключение

В работе был рассмотрен метод мажоритарного декодирования последовательностей Гордона–Милса–Велча и определены его вероятностные характеристики для каналов ДСК и АБГШ с манипуляцией ФМн-2. Определено, что часть ГМВ-последовательностей образует циклические группы, что приводит к необходимости тщательно выбирать их начальные элементы, в чтобы избежать ложных срабатываний системах с асинхронным детектированием.

Список используемых источников

1. Кренгель Е.И., Мешковский К.А. М-подобные последовательности над GF(2m) и их применение в широкополосных системах связи // Цифровая обработка сигналов. 2000. № 2. С. 14–19.
2. Кренгель Е.И., Мешковский К.А. Классификация двоичных последовательностей Гордона, Милза, Велча // Радиотехника. 2001. № 12. С. 13–15.
3. Стародубцев В.Г. Алгоритм формирования последовательностей Гордона–Миллса–Велча // Известия высших учебных заведений. Приборостроение. 2012. Т. 55. № 7. С. 5–9.
4. Стародубцев В.Г. Формирование последовательностей Гордона–Миллса–Велча на основе регистров сдвига // Известия высших учебных заведений. Приборостроение. 2015. Т. 53. № 6. С. 451–457.
5. Когновицкий О.С. Двойственный базис и его применение в телекоммуникациях. СПб.: Линк, 2009. 424 с.
6. Диксон Р.К. Широкополосные системы: Пер. с англ. / Под ред. В.И. Журавлева. М.: Связь, 1979. 304 с.
7. Сарвате Д.В., Персли М.Б. Взаимнокорреляционные свойства псевдослучайных и родственных последовательностей // Труды института инженеров по электротехнике и радиоэлектронике. 1980. Т. 68. № 5. С. 59–90.

* * *

DUAL BASIS BASED PROCESSING OF WIDEBAND GORDON–MILLS–WELCH SEQUENCES BASED ON TWO LINEAR REGISTERS

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

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

Article info
Article in Russian

For citation: Vladimirov S., Kognovitsky O. Dual Basis Based Processing of Wideband Gordon–Mills–Welch Sequences Based on Two Linear Registers. *Proceedings of Telecommunication Universities*. 2019;5(2):49–58. (in Russ.) Available from: https://doi.org/10.31854/1813-324X-2019-5-2-49-58

Abstract: *The paper presents a dual basis based algorithm for processing and determining the initial states of the shift registers that form the Gordon–Mills–Welch (GMW) wideband sequences, which are characterized by their greater number and higher structural secrecy than the widely used M sequences. It is shown that the proposed algorithm, in contrast to the known ones, allows one to determine arbitrary initial states of shift registers, which expands the possibilities of using composite wideband GMW sequences for solving various problems when transmitting information via communication channels with noise.*

Keywords: *wideband sequences, finite field, irreducible and primitive polynomial, linear feedback shift register, dual basis, trace function, decimation.*

References

1. Krengel E.I., Meshkovskii K.A. M-podobnye posledovatelnosti nad GF 2m i ikh primenenie v shirokopo-losnykh sistemakh sviazi [M-Like Sequences Over GF (2m) and Their Application in Wideband Communication Systems]. *Digital Signal Processing.* 2000;2:14–19. (in Russ.)
2. Krengel E.I., Meshkovskii K.A. Klassifikatsiia dvoichnykh posledovatelnostei Gordona, Milza, Velcha [Classification of Binary Sequences of Gordon, Mills, Welch]. *Radioengineering.* 2001;12:13–15. (in Russ.)
3. Starodubtsev V.G. An Algorithm of Gordon–Mills–Welch Sequence Formation. *Journal of Instrument Engineering*. 2012; 55(7):5–9. (in Russ.)
4. Starodubtsev V.G. Generation of Gordon–Mills–Welch Sequences on the Base of Shift Registers. *Journal of Instrument Engineering*. 2015;53(6):451–457. (in Russ.)
5. Kognovitsky O.S. Dvoistvennyi bazis i ego primenenie v telekommunikatsiiakh [Dual Basis and Its Application in Telecommunications]. St. Petersburg: Link Publ.; 2009. 424 p. (in Russ.)
6. Dikson R.K. Shirokopolosnye sistemy [Broadband Systems]. Trans. with English. Ed. V.I. Zhuravlev. Moscow: Sviaz Publ., 1979. 304 p. (in Russ.)
7. Sarvate D.V., Persli M.B. Vzaimnokorreliatsionnye svoistva psevdosluchainykh i rodstvennykh posledova-telnostei [Mutually Correlated Properties of Pseudorandom and Related Sequences]. *Trudy instituta inzhenerov po elektrotekhnike i radioelektronike*. 1980;68(5):59–90. (in Russ.)