УДК 519.725

В. Г. СТАРОДУБЦЕВ

ПРОВЕРОЧНЫЕ ПОЛИНОМЫ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ГОРДОНА—МИЛЛСА—ВЕЛЧА

Представлен алгоритм синтеза проверочных полиномов последовательностей Гордона—Миллса—Велча, основанный на использовании структурных свойств конечных полей с двойным расширением.

Ключевые слова: *последовательности с составным периодом, проверочные полиномы, конечные поля, неприводимые и примитивные полиномы.*

Одним из перспективных направлений развития сетей мобильной связи является применение технологии многостанционного доступа с кодовым разделением каналов. Эта технология предполагает использование псевдослучайных последовательностей, обладающих требуемыми корреляционными и структурными свойствами.

В современных системах связи применяются М-последовательности (МП), последовательности Голда, малого и большого множеств Касами, последовательности Баркера, Гордона—Миллса—Велча (ГМВ) и др. [1].

Среди циклических последовательностей, обладающих одноуровневой периодической автокорреляционной функцией, можно выделить М-последовательности и ГМВ-последовательности (ГМВП). При этом последние обладают более высокой структурной скрытностью, которая численно характеризуется эквивалентной линейной сложностью (ЭЛС) [2—4]. Это свойство определяет преимущество применения ГМВП в системах связи, к которым предъявляются жесткие требования по конфиденциальности.

ГМВП формируются над конечными полями с двойным расширением вида $GF[(p^m)^n]$, вследствие чего период данных последовательностей является составным числом, т.е. $N = p^{mn} - 1$, где p — характеристика поля, m, n — натуральные числа [5]. Так как ГМВП относятся к классу циклических последовательностей, то они могут формироваться с помощью регистров сдвига с линейной обратной связью [5—7]. Для ГМВП с периодом $N = p^{mn} - 1$ положение сумматоров в цепи обратной связи определяется коэффициентами проверочных полиномов вида

$$h_{\text{ГМВ}}(x) = x^k + h_{k-1}x^{k-1} + h_{k-2}x^{k-2} + \ldots + h_1 x + h_0, \qquad (1)$$

где k — степень проверочного полинома, численно характеризующая ЭЛС ГМВП; коэффициенты h_{i}, являются элементами поля $GF(p)$.

Алгоритм синтеза проверочных полиномов ГМВП в литературе не приводится. Для каждой конкретной последовательности проверочный полином определяется итеративным путем, например, с помощью алгоритма Берлекемпа—Месси.

Целью настоящей статьи является разработка алгоритма синтеза проверочных полиномов ГМВ-последовательностей, основанного на использовании структурных свойств конечных полей с двойным расширением, а также составление исчерпывающих перечней проверочных полиномов двоичных ГМВП с периодами $N = 63$ и 255 и троичных — с $N = 80$.

Разработка алгоритма выполняется на примере двоичной ГМВП с периодом $N = 63$, сформированной на основе М-последовательности с проверочным полиномом $h_{\text{МП}}(x) = x^6 + x + 1$. Символы М-последовательности записываются построчно в матрицы размерности $[J \times S] = [7 \times 9]$, ненулевые столбцы которой соответствуют различным сдвигам „короткой“ (характеристической) М-последовательности с периодом $J = 7$. Параметр S характеризует число сдвигов:

$$\mathbf{F}_{\text{МП}} = \begin{vmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{vmatrix}. \quad (2)$$

С использованием алгоритма формирования ГМВП, основанного на матричном представлении М-последовательностей с составным периодом [1, 5], формируется ГМВП с $N = 63$, которая также представляется в виде матрицы размерности $[J \times S] = [7 \times 9]$:

$$\mathbf{F}_{\text{ГМВ}} = \begin{vmatrix} 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \end{vmatrix}. \quad (3)$$

С помощью алгоритма Берлекемпа [6, 7] для ГМВП вида (3) определяется проверочный полином

$$h_{\text{ГМВ}}(x) = x^{12} + x^{11} + x^{10} + x^9 + x^7 + x^2 + 1. \quad (4)$$

Этот полином является произведением неприводимых над полем $GF(2)$ полиномов меньшей степени. Для их определения используется полный перечень неприводимых над $GF(2)$ полиномов степени 6 и ниже, корнями которых являются элементы расширенного поля Галуа $GF(2^6)$. Данные полиномы, их корни, а также периоды корней представлены в табл. 1. Искомые неприводимые полиномы определяются путем последовательного деления $h_{\text{ГМВ}}(x)$ на $h_i(x)$. В результате получим, что $h_{\text{ГМВ}}(x)$ вида (4) может быть представлен в виде произведения двух полиномов $h_{ci}(x)$ шестой степени (здесь ci — i-й сомножитель):

$$h_{\text{ГМВ}}(x) = h_{c1}(x)h_{c2}(x) = h_2(x)h_3(x) = \\ = (x^6 + x^4 + x^2 + x + 1)\,(x^6 + x^5 + x^2 + x + 1) \quad (5)$$

Таблица 1

Полиномы $h_i(x)$	Корни полиномов (показатели степени)	Периоды корней ε
$h_1(x) = x^6 + x + 1$	$\alpha^1, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \alpha^{32}$	63
$h_2(x) = x^6 + x^4 + x^2 + x + 1$	$\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}, \alpha^{48}, \alpha^{33}$	21
$h_3(x) = x^6 + x^5 + x^2 + x + 1$	$\alpha^5, \alpha^{10}, \alpha^{20}, \alpha^{40}, \alpha^{17}, \alpha^{34}$	63
$h_4(x) = x^6 + x^5 + x^3 + x^2 + 1$	11, 22, 44, 25, 50, 37	63
$h_5(x) = x^6 + x^5 + 1$	31, 62, 61, 59, 55, 47	63
$h_6(x) = x^6 + x^5 + x^4 + x^2 + 1$	15, 30, 60, 57, 51, 39	21
$h_7(x) = x^6 + x^5 + x^4 + x + 1$	23, 46, 29, 58, 53, 43	63
$h_8(x) = x^6 + x^4 + x^3 + x + 1$	13, 26, 52, 41, 19, 38	63
$h_9(x) = x^6 + x^3 + 1$	7, 14, 28, 56, 49, 35	9
$h_{10}(x) = x^3 + x + 1$	9, 18, 36	7
$h_{11}(x) = x^3 + x^2 + 1$	27, 54, 45	7
$h_{12}(x) = x^2 + x + 1$	21, 42	3
$h_{13}(x) = x + 1$	α^0	1

Для поля $GF(2^6)$ можно показать, что корни полинома $h_{c1}(x) = h_2(x)$ являются третьими степенями корней полинома $h_{МП}(x)$, являющегося примитивным, а корни полинома $h_{c2}(x) = h_3(x)$ — пятыми.

Алгоритм синтеза полной совокупности проверочных полиномов ГМВ-последовательностей основан на предположении о повторяемости соотношений между корнями проверочного полинома $h_{МП}(x)$ исходной М-последовательности и корнями полиномов $h_{c1}(x)$ и $h_{c2}(x)$, являющихся сомножителями проверочного полинома $h_{ГМВ}(x)$.

Известно [6], что для поля $GF(2^6)$ существует шесть различных примитивных полиномов, которые могут выступать в качестве проверочных полиномов при формировании М-последовательностей. Таким образом, для шести М-последовательностей с периодом N=63 можно получить шесть ГМВП и соответственно шесть проверочных полиномов двенадцатой степени.

В качестве примера сформируем проверочный полином ГМВП, основанной на М-последовательности с $h_{МП}(x) = h_7(x) = x^6 + x^5 + x^4 + x + 1$, одним из корней которого является элемент α^{23} (см. табл. 1).

Полиномы-сомножители для $h_{ГМВ}(x) = h_{c1}(x)\, h_{c2}(x)$ определяются следующим образом. Исходный полином $h_{МП}(x)$ имеет корень α^{23}. Тогда одним из корней полинома $h_{c1}(x)$ должен быть элемент $(\alpha^{23})^3 = \alpha^{69 \bmod 63} = \alpha^6$, что соответствует $h_{c1}(x) = h_2(x) = x^6 + x^4 + x^2 + x + 1$.

Полином $h_{c2}(x)$ должен иметь корень $(\alpha^{23})^5 = \alpha^{115 \bmod 63} = \alpha^{52}$, что соответствует $h_{c2}(x) = h_8(x) = x^6 + x^4 + x^3 + x + 1$.

Искомый проверочный полином для ГМВ-последовательности

$$h_{ГМВ}(x) = h_2(x)h_8(x) = x^{12} + x^9 + x^7 + x^6 + x^5 + x^4 + 1. \qquad (6)$$

Аналогичные вычисления для остальных примитивных полиномов поля $GF(2^6)$, являющихся проверочными для М-последовательностей, позволяют сформировать полную совокупность проверочных полиномов для ГМВ-последовательностей с периодом N=63 (табл. 2).

Таблица 2

$h_{ГМВi}(x)$	Полиномы-сомножители ГМВП $h_{c1}(x)\, h_{c2}(x)$	Полиномы для исходных М-последовательностей
$h_{ГМВ1}(x)$	$h_2(x)\, h_3(x) = x^{12} + x^{11} + x^{10} + x^9 + x^7 + x^2 + 1$	$h_1(x) = x^6 + x + 1$
$h_{ГМВ2}(x)$	$h_6(x)h_4(x) = x^{12} + x^8 + x^7 + x^6 + x^5 + x^3 + 1$	$h_3(x) = x^6 + x^5 + x^2 + x + 1$
$h_{ГМВ3}(x)$	$h_2(x)h_5(x) = x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^6 + x^5 + x^4 + x^2 + x + 1$	$h_4(x) = x^6 + x^5 + x^3 + x^2 + 1$
$h_{ГМВ4}(x)$	$h_6(x)h_7(x) = x^{12} + x^{10} + x^5 + x^3 + x^2 + x + 1$	$h_5(x) = x^6 + x^5 + 1$
$h_{ГМВ5}(x)$	$h_2(x)h_8(x) = x^{12} + x^9 + x^7 + x^6 + x^5 + x^4 + 1$	$h_7(x) = x^6 + x^5 + x^4 + x + 1$
$h_{ГМВ6}(x)$	$h_6(x)h_1(x) = x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + x + 1$	$h_8(x) = x^6 + x^4 + x^3 + x + 1$

Представленный алгоритм может быть использован для формирования совокупности проверочных полиномов ГМВП в виде произведения неприводимых полиномов для произвольного поля $GF[(p^m)^n]$. Для полей с характеристикой $p = 2$ число сомножителей в $h_{ГМВ}(x)$ может быть равно двум и более. Для полей с $p > 2$ число сомножителей больше двух.

Применимость представленного алгоритма для определения полной совокупности проверочных полиномов двоичных ГМВ-последовательностей с периодом N=255 проиллюстрируем на примере ГМВП, сформированной на основе М-последовательности с проверочным полиномом $h_{МП}(x) = x^8 + x^4 + x^3 + x^2 + 1$. Этот полином является примитивным, т.е. его корни суть примитивные элементы поля $GF(2^8)$: α, α^2, α^4, α^8, α^{16}, α^{32}, α^{64}, α^{128}.

Символы М-последовательности записываются построчно в виде матрицы размерности $[J \times S] = [15 \times 17]$, ненулевые столбцы которой соответствуют различным сдвигам „короткой“ М-последовательности с периодом $J = 15$. В соответствии с алгоритмом, представленным в работе [5], ГМВП с периодом $N = 255$ также представляется в виде матрицы размерности $[J \times S] = [15 \times 17]$:

$$\mathbf{F}_{\text{ГМВ}} = \begin{vmatrix} 0&0&0&0&1&0&0&1&1&1&0&1&1&0&0&1&1 \\ 0&0&0&0&1&0&1&0&1&0&0&0&0&1&1&1&0 \\ 1&0&0&1&1&1&0&0&1&0&0&1&1&0&0&1&0 \\ 1&1&0&1&1&1&1&1&1&0&1&1&1&0&1&0&0 \\ 1&1&0&1&0&1&1&0&0&1&1&0&0&0&1&1&1 \\ 1&1&0&1&1&1&0&0&1&1&1&0&0&1&0&0&1 \\ 0&1&0&0&0&0&0&0&0&1&1&1&1&1&0&1&1 \\ 1&0&0&1&1&1&1&1&1&1&0&0&0&1&1&1&1 \\ 0&1&0&0&1&0&0&1&1&0&1&0&0&1&0&0&0 \\ 1&0&0&1&0&1&0&1&0&1&0&0&0&0&0&0&1 \\ 1&1&0&1&0&1&0&1&0&0&1&1&1&1&0&1&0 \\ 0&1&0&0&1&0&1&0&1&1&1&1&1&0&1&0&1 \\ 0&0&0&0&0&0&1&1&0&1&0&1&1&1&1&0&1 \\ 1&0&0&1&0&1&1&0&0&0&0&1&1&1&1&0&0 \\ 0&1&0&0&0&0&1&1&0&0&1&0&0&0&1&1&0 \end{vmatrix}. \quad (7)$$

С помощью алгоритма Берлекемпа [6, 7] для ГМВ-последовательности вида (7) определяется проверочный полином

$$h_{\text{ГМВ}}(x) = x^{32} + x^{31} + x^{30} + x^{29} + x^{25} + x^{22} + x^{21} + x^{20} + x^{18} + x^{17} + x^{15} + x^{14} + x^{13} + x^{12} + x^{6} + x^{4} + x^{2} + x + 1, \quad (8)$$

являющийся произведением неприводимых над полем $GF(2)$ полиномов степени 8 и менее (табл. 3).

В результате разложения на множители полином $h_{\text{ГМВ}}(x)$ вида (8) может быть представлен произведением четырех полиномов восьмой степени:

$$h_{\text{ГМВ}}(x) = h_{\text{с1}}(x)\, h_{\text{с2}}(x)\, h_{\text{с3}}(x)\, h_{\text{с4}}(x) = h_4(x)\, h_6(x)\, h_7(x)\, h_{15}(x) = (x^8 + x^6 + x^5 + x^3 + 1)(x^8 + x^7 + x^6 + x^5 + x^2 + x + 1)\times \times (x^8 + x^5 + x^3 + x + 1)(x^8 + x^6 + x^4 + x^3 + x^2 + x + 1). \quad (9)$$

Таблица 3

№ прямого/ сопряженного полинома	Полиномы $h_i(x)$	Корни полиномов (показатели степени)	Периоды корней
1/20	$h_1(x) = x^8 + x^4 + x^3 + x^2 + 1$	$\alpha^1, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \alpha^{32}, \alpha^{64}, \alpha^{128}$	255
2/21	$h_2(x) = x^8 + x^6 + x^5 + x^4 + x^2 + x + 1$	$\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}, \alpha^{48}, \alpha^{96}, \alpha^{192}, \alpha^{129}$	85
3/22	$h_3(x) = x^8 + x^7 + x^6 + x^5 + x^4 + x + 1$	$\alpha^5, \alpha^{10}, \alpha^{20}, \alpha^{40}, \alpha^{80}, \alpha^{160}, \alpha^{65}, \alpha^{130}$	51
4/23	$h_4(x) = x^8 + x^6 + x^5 + x^3 + 1$	7,14,28,56,112,224,193,131	255
5/24	$h_5(x) = x^8 + x^7 + x^5 + x^4 + x^3 + x^2 + 1$	9,18,36,72,144,33,66,132	85
6/25	$h_6(x) = x^8 + x^7 + x^6 + x^5 + x^2 + x + 1$	11,22,44,88,176,97,194,133	255
7/26	$h_7(x) = x^8 + x^5 + x^3 + x + 1$	13,26,52,104,208,161,67,134	255
8/8	$h_8(x) = x^8 + x^7 + x^6 + x^4 + x^2 + x + 1$	15,30,60,120,240,225,195,135	17
9/27	$h_9(x) = x^4 + x + 1$	17,34,68,136	15
10/28	$h_{10}(x) = x^8 + x^6 + x^5 + x^2 + 1$	19,38,76,152,49,98,196,137	255
11/29	$h_{11}(x) = x^8 + x^7 + x^3 + x + 1$	21,42,84,168,81,162,69,138	85
12/30	$h_{12}(x) = x^8 + x^6 + x^5 + x + 1$	23,46,92,184,113,226,197,139	255
13/31	$h_{13}(x) = x^8 + x^4 + x^3 + x + 1$	25,50,100,200,145,35,70,140	51
14/32	$h_{14}(x) = x^8 + x^5 + x^4 + x^3 + x^2 + x + 1$	27,54,108,216,177,99,198,141	85
15/33	$h_{15}(x) = x^8 + x^6 + x^4 + x^3 + x^2 + x + 1$	37,74,148,41,82,164,73,146	255
16/34	$h_{16}(x) = x^8 + x^7 + x^6 + x + 1$	43,86,172,89,178,101,202,149	255
17/17	$h_{17}(x) = x^8 + x^5 + x^4 + x^3 + 1$	45,90,180,105,210,165,75,150	17

Продолжение таблицы 3

№ прямого/ сопряженного полинома	Полиномы $h_i(x)$	Корни полиномов (показатели степени)	Периоды корней
18/18	$h_{18}(x) = x^4 + x^3 + x^2 + x + 1$	51,102,204,153	5
19/19	$h_{19}(x) = x^2 + x + 1$	85,170	3
20/1	$h_{20}(x) = x^8 + x^6 + x^5 + x^4 + 1$	127,254,253,251,247,239,223,191	255
21/2	$h_{21}(x) = x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + 1$	63,126,252,249,243,231,207,159	85
22/3	$h_{22}(x) = x^8 + x^7 + x^4 + x^3 + x^2 + x + 1$	95,190,125,250,245,235,215,175	51
23/4	$h_{23}(x) = x^8 + x^5 + x^3 + x^2 + 1$	31,62,124,248,241,227,199,143	255
24/5	$h_{24}(x) = x^8 + x^6 + x^5 + x^4 + x^3 + x + 1$	111,222,189,123,246,237,219,183	85
25/6	$h_{25}(x) = x^8 + x^7 + x^6 + x^3 + x^2 + x + 1$	61,122,244,233,211,167,79,158	255
26/7	$h_{26}(x) = x^8 + x^7 + x^5 + x^3 + 1$	47,94,188,121,242,229,203,151	255
27/9	$h_{27}(x) = x^4 + x^3 + 1$	119,238,221,187	15
28/10	$h_{28}(x) = x^8 + x^6 + x^3 + x^2 + 1$	59,118,236,217,179,103,206,157	255
29/11	$h_{29}(x) = x^8 + x^7 + x^5 + x + 1$	87,174,93,186,117,234,213,171	85
30/12	$h_{30}(x) = x^8 + x^7 + x^3 + x^2 + 1$	29,58,116,232,209,163,71,142	255
31/13	$h_{31}(x) = x^8 + x^7 + x^5 + x^4 + 1$	55,110,220,185,115,230,205,155	51
32/14	$h_{32}(x) = x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + 1$	39,78,156,57,114,228,201,147	85
33/15	$h_{33}(x) = x^8 + x^7 + x^6 + x^5 + x^4 + x^2 + 1$	91,182,109,218,181,107,214,173	255
34/16	$h_{34}(x) = x^8 + x^7 + x^2 + x + 1$	53,106,212,169,83,166,77,154	255
35/35	$h_{35}(x) = x + 1$	α^0	1

Корнями с наименьшими показателями степени полиномов-сомножителей являются элементы поля $GF(2^8)$: для $h_4(x)$ – элемент α^7, для $h_6(x)$ — элемент α^{11}, $h_7(x)$ — α^{13}, $h_{15}(x)$ — α^{37}.

Таким образом, корни полиномов-сомножителей проверочного полинома ГМВ-последовательности являются соответственно 7-й, 11-й, 13-й и 37-й степенью корней проверочного полинома исходной М-последовательности.

Для поля $GF(2^8)$ существует шестнадцать различных примитивных полиномов (см. табл. 3). С помощью разработанного алгоритма синтеза можно сформировать полную совокупность из шестнадцати проверочных полиномов для ГМВ-последовательностей с N=255. Проведем вычисления, используя данные табл. 3.

Полином $h_{\text{ГМВ1}}(x) = h_4(x)h_6(x)h_7(x)h_{15}(x)$ определяется в соответствии с (9). Полином $h_{\text{ГМВ2}}(x)$ определяется через $h_{\text{МП}}(x) = h_4(x)$, имеющий корень α^7. Тогда одним из корней полинома $h_{c1}(x)$ должен быть элемент $\alpha^{7\cdot7} = \alpha^{49}$, что соответствует $h_{10}(x)$. Полином $h_{c2}(x)$ должен иметь корень $\alpha^{7\cdot11} = \alpha^{77}$, что соответствует $h_{34}(x)$, полином $h_{c3}(x)$ должен иметь корень $\alpha^{7\cdot13} = \alpha^{91}$, что соответствует $h_{33}(x)$, полином $h_{c4}(x)$ должен иметь корень $\alpha^{7\cdot37 \bmod 255} = \alpha^4$, что соответствует $h_1(x)$.

Остальные полиномы вычисляются аналогичным образом. Искомые проверочные полиномы тридцать второй степени для шестнадцати ГМВП приведены в табл. 4, также приведены проверочные полиномы для исходных М-последовательностей.

Таблица 4

$h_{\text{ГМВi}}(x)$	Полиномы-сомножители ГМВП $h_{c1}(x)\ h_{c2}(x)\ h_{c3}(x)\ h_{c4}(x)$	Проверочные полиномы для исходных М-последовательностей
$h_{\text{ГМВ1}}(x)$	$h_4(x)\ h_6(x)\ h_7(x)\ h_{15}(x)$	$h_1(x) = x^8 + x^4 + x^3 + x^2 + 1$
$h_{\text{ГМВ2}}(x)$	$h_{10}(x)\ h_{34}(x)\ h_{33}(x)\ h_1(x)$	$h_4(x) = x^8 + x^6 + x^5 + x^3 + 1$
$h_{\text{ГМВ3}}(x)$	$h_{34}(x)\ h_{26}(x)\ h_{23}(x)\ h_{10}(x)$	$h_6(x) = x^8 + x^7 + x^6 + x^5 + x^2 + x + 1$
$h_{\text{ГМВ4}}(x)$	$h_{33}(x)\ h_{23}(x)\ h_{34}(x)\ h_{12}(x)$	$h_7(x) = x^8 + x^5 + x^3 + x + 1$
$h_{\text{ГМВ5}}(x)$	$h_6(x)\ h_{30}(x)\ h_{20}(x)\ h_4(x)$	$h_{10}(x) = x^8 + x^6 + x^5 + x^2 + 1$
$h_{\text{ГМВ6}}(x)$	$h_7(x)\ h_{20}(x)\ h_6(x)\ h_{16}(x)$	$h_{12}(x) = x^8 + x^6 + x^5 + x + 1$
$h_{\text{ГМВ7}}(x)$	$h_1(x)\ h_{10}(x)\ h_{12}(x)\ h_{26}(x)$	$h_{15}(x) = x^8 + x^6 + x^4 + x^3 + x^2 + x + 1$
$h_{\text{ГМВ8}}(x)$	$h_{12}(x)\ h_{33}(x)\ h_{10}(x)\ h_{25}(x)$	$h_{16}(x) = x^8 + x^7 + x^6 + x + 1$
$h_{\text{ГМВ9}}(x)$	$h_{23}(x)\ h_{25}(x)\ h_{26}(x)\ h_{33}(x)$	$h_{20}(x) = x^8 + x^6 + x^5 + x^4 + 1$
$h_{\text{ГМВ10}}(x)$	$h_{28}(x)\ h_{16}(x)\ h_{15}(x)\ h_{20}(x)$	$h_{23}(x) = x^8 + x^5 + x^3 + x^2 + 1$
$h_{\text{ГМВ11}}(x)$	$h_{16}(x)\ h_7(x)\ h_4(x)\ h_{28}(x)$	$h_{25}(x) = x^8 + x^7 + x^6 + x^3 + x^2 + x + 1$

Продолжение таблицы 4

$h_{ГМВi}(x)$	Полиномы-сомножители ГМВП $h_{c1}(x)\ h_{c2}(x)\ h_{c3}(x)\ h_{c4}(x)$	Проверочные полиномы для исходных М-последовательностей
$h_{ГМВ12}(x)$	$h_{15}(x)\ h_4(x)\ h_{16}(x)\ h_{30}(x)$	$h_{26}(x) = x^8 + x^7 + x^5 + x^3 + 1$
$h_{ГМВ13}(x)$	$h_{25}(x)\ h_{12}(x)\ h_1(x)\ h_{23}(x)$	$h_{28}(x) = x^8 + x^6 + x^3 + x^2 + 1$
$h_{ГМВ14}(x)$	$h_{26}(x)\ h_1(x)\ h_{25}(x)\ h_{34}(x)$	$h_{30}(x) = x^8 + x^7 + x^3 + x^2 + 1$
$h_{ГМВ15}(x)$	$h_{20}(x)\ h_{28}(x)\ h_{30}(x)\ h_7(x)$	$h_{33}(x) = x^8 + x^7 + x^6 + x^5 + x^4 + x^2 + 1$
$h_{ГМВ16}(x)$	$h_{30}(x)\ h_{15}(x)\ h_{28}(x)\ h_6(x)$	$h_{34}(x) = x^8 + x^7 + x^2 + x + 1$

Разработанный алгоритм может быть использован для определения совокупности проверочных полиномов не только двоичных, но и „*p*“-ичных ГМВ-последовательностей. Для троичных последовательностей с периодом N=80 вычисления проведем на примере ГМВП, сформированной на основе М-последовательности с полиномом $h_{МП}(x) = x^4 + 2x^3 + 2$, корни которого – суть примитивные элементы поля $GF(3^4)$: α, α^3, α^9, α^{27}.

Троичная ГМВП с N=80 представляется в виде матрицы

$$\mathbf{F}_{ГМВ} = \begin{vmatrix} 0 & 0 & 0 & 2 & 1 & 2 & 1 & 2 & 0 & 2 \\ 2 & 1 & 1 & 2 & 2 & 2 & 0 & 1 & 0 & 2 \\ 1 & 2 & 2 & 0 & 2 & 0 & 1 & 1 & 0 & 0 \\ 1 & 2 & 2 & 2 & 0 & 2 & 2 & 0 & 0 & 2 \\ 0 & 0 & 0 & 1 & 2 & 1 & 2 & 1 & 0 & 1 \\ 1 & 2 & 2 & 1 & 1 & 1 & 0 & 2 & 0 & 1 \\ 2 & 1 & 1 & 0 & 1 & 0 & 2 & 2 & 0 & 0 \\ 2 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{vmatrix}. \qquad (10)$$

Проверочный полином определяется по алгоритму Берлекемпа

$$h_{ГМВ}(x) = x^{12} + x^{11} + x^8 + 2x^7 + 2x^6 + x^4 + 2x^2 + x + 2. \qquad (11)$$

Полином (11) является произведением неприводимых над полем $GF(3)$ полиномов степени 4 и менее (табл. 5).

Таблица 5

№ прямого/ сопряженного полинома	Полиномы $h_i(x)$	Корни полиномов (показатели степени)	Периоды корней
1/5	$h_1(x) = x^4 + 2x^3 + 2$	$\alpha^1, \alpha^3, \alpha^9, \alpha^{27}$	80
2/6	$h_2(x) = x^4 + x^3 + x^2 + 2x + 2$	$\alpha^7, \alpha^{21}, \alpha^{63}, \alpha^{29}$	80
3/7	$h_3(x) = x^4 + 2x^3 + 2x^2 + x + 2$	$\alpha^{11}, \alpha^{33}, \alpha^{19}, \alpha^{57}$	80
4/8	$h_4(x) = x^4 + 2x + 2$	13, 39, 37, 31	80
5/1	$h_5(x) = x^4 + x + 2$	53, 79, 77, 71	80
6/2	$h_6(x) = x^4 + x^3 + 2x^2 + 2x + 2$	17, 51, 73, 59	80
7/3	$h_7(x) = x^4 + 2x^3 + x^2 + x + 2$	23, 69, 47, 61	80
8/4	$h_8(x) = x^4 + x^3 + 2$	41, 43, 49, 67	80
9/10	$h_9(x) = x^4 + 2x^2 + 2$	5, 15, 45, 55	16
10/9	$h_{10}(x) = x^4 + x^2 + 2$	25, 75, 65, 35	16
11/12	$h_{11}(x) = x^4 + 2x^3 + x^2 + 1$	2, 6, 18, 54	40
12/11	$h_{12}(x) = x^4 + x^2 + 2x + 1$	26, 78, 74, 62	40
13/14	$h_{13}(x) = x^4 + x^3 + x^2 + 1$	14, 42, 46, 58	40
14/13	$h_{14}(x) = x^4 + x^2 + x + 1$	22, 66, 38, 34	40
15/16	$h_{15}(x) = x^4 + x^3 + 2x + 1$	4, 12, 36, 28	20
16/15	$h_{16}(x) = x^4 + 2x^3 + x + 1$	44, 52, 68, 76	20
17/17	$h_{17}(x) = x^4 + 2x^3 + x^2 + 2x + 1$	8, 24, 72, 56	10
18/19	$h_{18}(x) = x^2 + 2x + 2$	10, 30	8

Продолжение таблицы 5

№ прямого/ сопряженного полинома	Полиномы $h_i(x)$	Корни полиномов (показатели степени)	Периоды корней
19/18	$h_{19}(x) = x^2 + x + 2$	50, 70	8
20/20	$h_{20}(x) = x^4 + x^3 + x^2 + x + 1$	16, 48, 64, 32	5
21/21	$h_{21}(x) = x^2 + 1$	α^{20}, α^{60}	4
22/23	$h_{22}(x) = x + 1$	$\alpha^{40} = 2$	2
23/22	$h_{23}(x) = x + 2$	$\alpha^{80} = \alpha^0 = 1$	1

В результате разложения на множители полином $h_{\text{ГМВ}}(x)$ вида (11) может быть представлен в виде

$$h_{\text{ГМВ}}(x) = h_{\text{с1}}(x)\, h_{\text{с2}}(x)\, h_{\text{с3}}(x) = h_2(x)\, h_4(x)\, h_9(x) = \\ = (x^4 + x^3 + x^2 + 2x + 2)(x^4 + 2x + 2)(x^4 + 2x^2 + 2). \qquad (12)$$

Корнями с наименьшими показателями степени полиномов-сомножителей являются элементы поля $GF(3^4)$: для $h_2(x)$ — элемент α^7, $h_4(x)$ — α^{13}, $h_9(x)$ — α^5.

Таким образом, корни полиномов-сомножителей проверочного полинома ГМВП являются соответственно 7-й, 13-й и 5-й степенью корней проверочного полинома исходной М-последовательности.

Определим проверочный полином $h_{\text{ГМВ}}(x)$ для троичной ГМВП, формируемой на основе МП с полиномом $h_{\text{МП}}(x) = h_8(x) = x^4 + x^3 + 2$, одним из корней которого является элемент α^{41}.

Полиномы-сомножители для $h_{\text{ГМВ}}(x) = h_{\text{с1}}(x)\, h_{\text{с2}}(x)\, h_{\text{с3}}(x)$ определяются следующим образом. Исходный полином $h_{\text{МП}}(x)$ имеет корень α^{41}. Одним из корней полинома $h_{\text{с1}}(x)$ должен быть элемент $\alpha^{41\cdot 7} = \alpha^{287 \bmod 80} = \alpha^{47}$, что соответствует $h_7(x) = x^4 + 2x^3 + x^2 + x + 2$. Полином $h_{\text{с2}}(x)$ должен иметь корень $\alpha^{41\cdot 13} = \alpha^{533 \bmod 80} = \alpha^{53}$, что соответствует $h_5(x) = x^4 + x + 2$.

Полином $h_{\text{с3}}(x)$ должен иметь корень $\alpha^{41\cdot 5} = \alpha^{205 \bmod 80} = \alpha^{45}$, что соответствует $h_9(x) = x^4 + 2x^2 + 2$.

Полином $h_{\text{ГМВ}}(x)$, являющийся произведением трех полиномов, имеет следующий вид:

$$h_{\text{ГМВ}}(x) = h_{\text{с1}}(x)\, h_{\text{с2}}(x)\, h_{\text{с3}}(x) = h_7(x)\, h_5(x)\, h_9(x) = \\ = x^{12} + 2x^{11} + x^8 + x^7 + 2x^6 + x^4 + 2x^2 + 2x + 2. \qquad (13)$$

Выбрав в табл. 5 в качестве проверочных для исходных М-последовательностей восемь примитивных полиномов в поле $GF(3^4)$, можно сформировать восемь проверочных полиномов для ГМВ-последовательностей. Результаты вычислений представлены в табл. 6.

Таблица 6

$h_{\text{ГМВi}}(x)$	Полиномы-сомножители ГМВП $h_{\text{с1}}(x)\, h_{\text{с2}}(x)\, h_{\text{с3}}(x)$	Проверочные полиномы для исходной МП
$h_{\text{ГМВ1}}(x)$	$h_2(x)\, h_4(x)\, h_9(x)$	$h_1(x) = x^4 + 2x^3 + 2$
$h_{\text{ГМВ2}}(x)$	$h_8(x)\, h_3(x)\, h_{10}(x)$	$h_2(x) = x^4 + x^3 + x^2 + 2x + 2$
$h_{\text{ГМВ3}}(x)$	$h_5(x)\, h_2(x)\, h_9(x)$	$h_3(x) = x^4 + 2x^3 + 2x^2 + x + 2$
$h_{\text{ГМВ4}}(x)$	$h_3(x)\, h_1(x)\, h_{10}(x)$	$h_4(x) = x^4 + 2x + 2$
$h_{\text{ГМВ5}}(x)$	$h_6(x)\, h_8(x)\, h_{10}(x)$	$h_5(x) = x^4 + x + 2$
$h_{\text{ГМВ6}}(x)$	$h_4(x)\, h_7(x)\, h_9(x)$	$h_6(x) = x^4 + x^3 + 2x^2 + 2x + 2$
$h_{\text{ГМВ7}}(x)$	$h_1(x)\, h_6(x)\, h_{10}(x)$	$h_7(x) = x^4 + 2x^3 + x^2 + x + 2$
$h_{\text{ГМВ8}}(x)$	$h_7(x)\, h_5(x)\, h_9(x)$	$h_8(x) = x^4 + x^3 + 2$

Таким образом, в статье разработан алгоритм формирования проверочных полиномов как двоичных, так и недвоичных ГМВ-последовательностей. Представлены полные совокупности проверочных полиномов для двоичных ГМВ-последовательностей с периодами N=63 и 255 и для троичных ГМВП с N=80.

Данные проверочные полиномы могут быть использованы при разработке устройств формирования ГМВП, основанных на регистрах сдвига с линейными обратными связями.

Также представленный алгоритм может найти применение при разработке методов формирования псевдослучайных последовательностей, допускающих аналитическое представление в конечных полях.

СПИСОК ЛИТЕРАТУРЫ

1. *Юдачев С. С., Калмыков В. В.* Ансамбли последовательностей GMW для систем с кодовым разделением каналов // „Наука и образование: электронное научно-техническое издание“. 2012. № 1. <http://technomag.edu.ru/issue/264798.html>.

2. *Варакин Л. Е.* Системы связи с шумоподобными сигналами. М.: Радио и связь, 1985. 384 с.

3. *Ипатов В. П.* Периодические дискретные сигналы с оптимальными корреляционными свойствами. М.: Радио и связь, 1992. 152 с.

4. *Свердлик М. Б.* Оптимальные дискретные сигналы. М.: Сов. радио, 1975. 200 с.

5. *Стародубцев В. Г.* Алгоритм формирования последовательностей Гордона-Миллса-Велча // Изв. вузов. Приборостроение. 2012. Т. 55, № 7. С. 5—9.

6. *Питерсон У., Уэлдон Э.* Коды, исправляющие ошибки / Под ред. *Р. Л. Добрушина и С. И. Самойленко.* М.: Мир, 1976. 596 с.

7. *Стародубцев В. Г., Павлов О. А.* Помехоустойчивые коды в телекоммуникационных и информационных системах. Вып. 1. Конечные поля Галуа: элементы теории и практики: Учеб. пособие. СПб: ВКА им. А. Ф. Можайского, 2003. 252 с.

Сведения об авторе

Виктор Геннадьевич Стародубцев — канд. техн. наук, доцент; ООО „Мультисервисные сети и Телекоммуникации“, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, кафедра беспроводных телекоммуникаций; E-mail: vgstarod@mail.ru

Рекомендована кафедрой беспроводных телекоммуникаций НИУ ИТМО

Поступила в редакцию 20.12.12 г.

УДК 620.178

А. А. Виноградова, А. О. Казначеева, В. М. Мусалимов

ФРАКТАЛЬНЫЙ АНАЛИЗ ТОМОГРАММ ГОЛОВНОГО МОЗГА

Исследованы возможности применения фрактального анализа для оценки структуры объектов. Представлены результаты расчета показателя Херста для магнитно-резонансных томограмм головного мозга, вычислены параметры распределений, выполнена оценка вероятности попадания в доверительные интервалы. Проведено стохастическое моделирование для нормального и равномерного законов распределения, проанализированы особенности показателя Херста и возможность использования его в качестве диагностического показателя.

Ключевые слова: *показатель Херста, фрактальный анализ, томография, распределение, моделирование.*

Введение. Качество получаемых в клинической практике магнитно-резонансных томограмм и оценка диагностических признаков выполняются визуально на основе экспертной оценки. Субъективность восприятия изображений и сложность анализируемых структур