УДК: 621.391

Теоретико-числовая модель аналитического оценивания и выбора ансамблей сигналов в асинхронно-адресных телекоммуникационных системах

В.Ю.Михайлов

Предложена теоретико-числовая модель представления функции взаимной корреляции (ФВК) кодов максимальной длины, позволяющая выполнить аналитическое оценивание характеристик ФВК путем анализа числовых сравнений. Предложена методика и примеры аналитического оценивания максимальных уровней ФВК. Использование методики не связано с компьютерными вычислительными процессами. Результаты носят общий характер и полезны для оперативной оценки возможностей построения квазиортогональных ансамблей сложных кодированных сигналов требуемого качества при проектировании асинхронно-адресных и командных авиационно-космических телекоммуникационных системах.

Ключевые слова: аналитическое оценивание; ансамбли сигналов; асинхронно-адресные системы; телекоммуникации, функции взаимной корреляции.

Введение

В [1, 2] показано, что периодическая функция взаимной корреляции (в дальнейшем ФВК) двух последовательностей $a(i+\tau)=S(\alpha^{i+\tau})$ и $b(i)=S(\alpha^{ik})$ длины $N=2^{2p}-1$ может быть определена по формуле

$$\theta_k(\tau)=\sum_{i=0}^{N-1}S(\alpha^{i+\tau})S(\alpha^{ik})=2^p(M-1)-1, \qquad (1)$$

где k – число, определяющее структуру последовательности $b(i)$, причем $(k,N)=1$ и

$$k\equiv 1(\mathrm{mod}\,(2^p-1)); \qquad (2)$$

τ – параметр задержки последовательности $b(i)$ - аргумент ФВК;

M – число решений алгебраического уравнения

$$\alpha^{\nu+\tau}+\alpha^{\nu k}=\gamma \qquad (3)$$

относительно неизвестной $\nu=\{0,1,...,2^p\}$;

$\alpha \in GF(2^{2p})$ – примитивный элемент поля $GF(2^{2p})$;

$\gamma \in GF(2^{p})$ – произвольный элемент подполя $GF(2^{p})$;

$$S(\alpha^i) = \varphi(T(\alpha^i));\ \varphi(x) = \begin{cases} +1\ при\ T(x) = 0; \\ -1\ при\ T(x) = 1. \end{cases},$$

а $T(x) = \sum_{i=0}^{n-1} x^{2^i}$ – двоичный след элемента x поля Галуа порядка 2^n [3, с. 194].

Работа [1], в основном, посвящена поиску и исключению из ансамбля заведомо «плохих» пар кодовых последовательностей, соответствующих максимально возможным значениям параметра M. Там же найдены условия существования пар последовательностей с уровнями ФВК приблизительно $N/3$.

В [2] сформулирован общий принцип синтеза квазиортогональных ансамблей указанного типа.

Цель дальнейшего анализа – уточнение ФВК (1) как функции параметра $M = f(k, \tau)$, поэтому основное внимание будет уделено решению алгебраического уравнения (3). Выполненный анализ этого уравнения показал, что все его решения соответствуют трем вариантам, в каждом из которых существуют от 2 до 3 подвариантов, в конечном итоге исчерпывающих все возможные решения уравнения (3). Полная схема вариантов решений представлена на рис. 1.

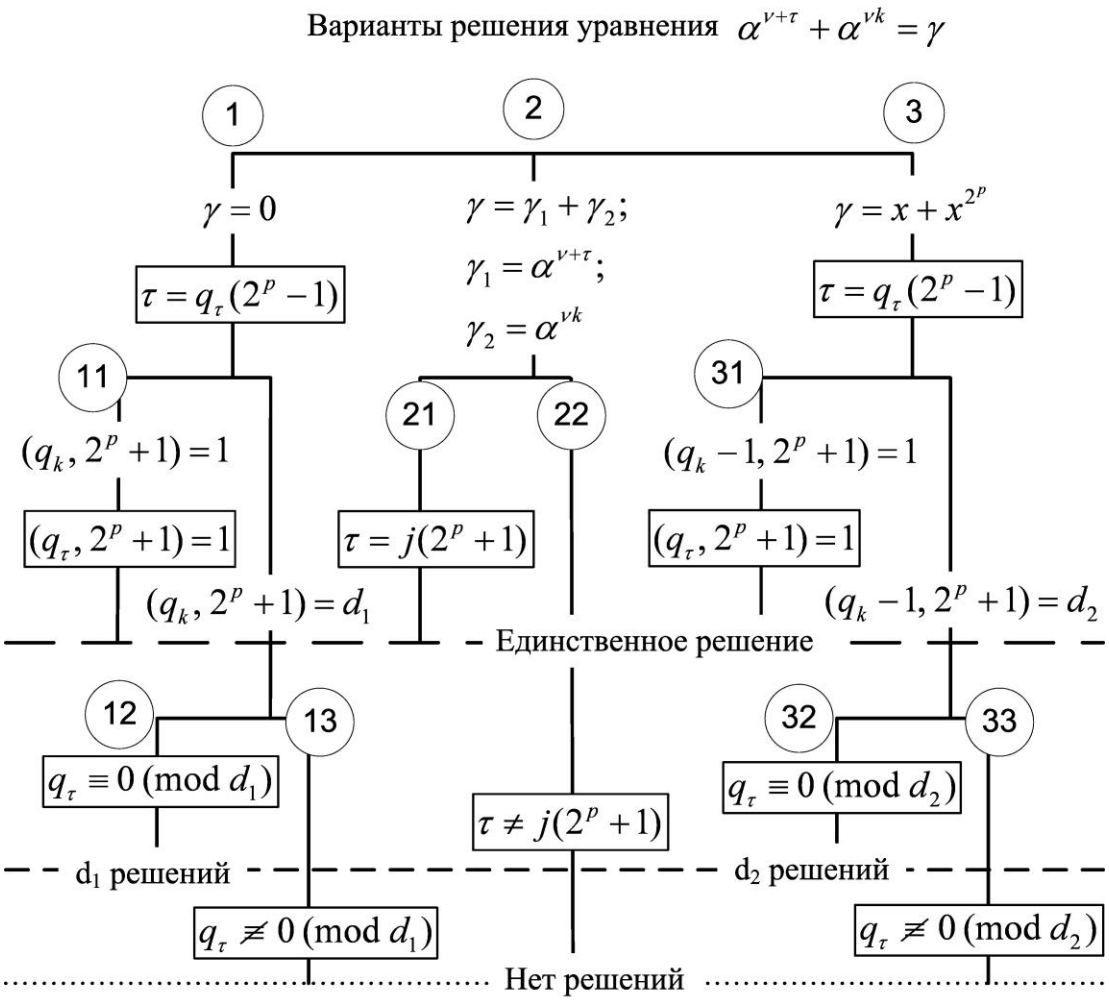

Рис. 1. Схема вариантов решений уравнения (3)

Вариант 1

$\gamma=0$ (ветвь 1 на рис.1).

В этом случае параметр ν должен удовлетворять сравнению

$$\nu+\tau\equiv\nu k\ (\mathrm{mod}\ \mathrm{N}). \qquad (4)$$

Для определения числа решений (4) представим k с учетом (2) в виде

$$k=q_k(2^p-1)+1. \qquad (5)$$

Тогда сравнение (4) приобретает вид

$$\tau\equiv\nu q_k(2^p-1)\ (\mathrm{mod}\ (2^{2p}-1)). \qquad (6)$$

Из теории сравнений [3, с. 66] следует, что решения сравнения (6) существуют только при условии делимости его левой части на 2^p-1, а следовательно значения τ должны иметь вид

$$\tau=q_\tau(2^p-1),\ q_\tau=0,1,...,2^p. \qquad (7)$$

После подстановки (7) в (6) и сокращения общего делителя получим

$$q_\tau \equiv \nu q_k \pmod{(2^p+1)}. \qquad (8)$$

Поскольку максимальное значение ν равно 2^p, то (8), очевидно, описывает все возможные решения сравнения (4).

Количество решений (8) зависит от величины наибольшего общего делителя (НОД) чисел q_τ, q_k и 2^p+1. НОД чисел a, b принято обозначается в виде (a, b). Если числа a, b – взаимно простые, т.е. не имеют общих делителей, то используется следующее обозначение $(a, b)=1$. Итак, возможны следующие три варианта решений сравнения (8):

1) сравнение имеет единственное решение при условиях $(q_k, 2^p+1)=1; (q_\tau, 2^p+1)=1$ (ветвь 11 на рис. 1);

2) сравнение имеет $(q_k, 2^p+1)=d_1>1$ решений при условии $q_\tau \equiv 0 \pmod{d_1}$ (ветвь 12 на рис. 1);

3) сравнение не имеет ни одного решения, если $(q_k, 2^p+1)=d_1$, но при этом $q_\tau \not\equiv 0 \pmod{d_1}$ (ветвь 13 на рис. 1).

Вариант 2

Этот вариант ограничивает область значений слагаемых рассматриваемого уравнения подмножеством элементов, принадлежащих подполю $GF(2^p)$ (ветвь 2 на рис. 1):

$$\begin{cases} \alpha^{\nu+\tau} = \gamma_1 \in GF(2^p); \\ \alpha^{\nu k} = \gamma_2 \in GF(2^p). \end{cases}.$$

Очевидно, что эта система эквивалентна следующей системе сравнений

$$\begin{cases} \nu+\tau \equiv 0 \pmod{(2^p+1)}; \\ \nu k \equiv 0 \pmod{(2^p+1)}. \end{cases} \qquad (9)$$

Анализ системы (9) показывает, что при $\nu \le 2^p$ она имеет единственное решение $\nu=0$ (ветвь 21 на рис.5.4), но только при условии $\tau \equiv 0 \pmod{(2^p+1)}$.

Следовательно, и уравнение (3) будет иметь два решения при следующих значениях аргумента ФВК:

$$\tau = (2^p+1)j;\ j=1, 2, ..., 2^p-2.$$

Здесь значение $\tau=0$ исключено, чтобы не допустить пересечения с рассмотренным ранее условием (4), соответствующим варианту 1.

Вариант 3

Этот вариант (ветвь 3 на рис. 1) задает представление (3) в виде функции отображения элемента поля $GF(2^{2p})$ в элемент подполя $GF(2^p)$ в виде

$$\gamma = x + x^{2^p}, \qquad (10)$$

где x – произвольный элемент поля $GF(2^{2p})$.

На основе определения двоичного следа [3, с. 194] несложно убедиться в результативности преобразования (10), поскольку двоичный след γ как элемента подполя $GF(2^p)$ в точности равен двоичному следу γ как элемента поля $GF(2^{2p})$.

Строго говоря, два первых варианта являются частными случаями третьего и выделяются с целью оперативной оценки снизу количества решений M.

Рассмотрим двоичный след элемента $\alpha^{\nu+\tau} + \alpha^{\nu k}$, определенного в (3), как элемента подполя $GF(2^p)$:

$$T_{2^p}(\alpha^{\nu+\tau} + \alpha^{\nu k}) = \alpha^{\nu+\tau} + \alpha^{2(\nu+\tau)} + \ldots + \alpha^{(\nu+\tau)2^{p-1}} +$$
$$+ \alpha^{\nu k} + \alpha^{2\nu k} + \ldots + \alpha^{\nu k 2^{p-1}}.$$

Отсюда следует, что $\alpha^{\nu+\tau} + \alpha^{\nu k} \in GF(2^p)$, если справедливо одно из двух представлений

$$\nu k \equiv (\nu + \tau)2^p \pmod N, \qquad (11)$$

или

$$\nu + \tau \equiv \nu k 2^p \pmod N, \qquad (12)$$

поскольку только при этих условиях указанное выражение является двоичным следом.

Более детальное рассмотрение показывает, что представление (12) полностью эквивалентно (11). Действительно, помножая левую и правую части (12) на 2^p, получим

$$(\nu + \tau)2^p \equiv \nu k 2^{2p} \pmod N \equiv \nu k \pmod N.$$

Таким образом, множество решений (3) в рассматриваемой ситуации совпадает с множеством решений (11).

Сравнение (11) эквивалентно сравнению

$\tau 2^p \equiv \nu(k - 2^p) \pmod{2^{2p} - 1}$, которое с учетом (2) приводится к виду

$$\tau 2^p \equiv \nu(q_k - 1)(2^p - 1) \pmod{2^{2p} - 1}.$$

Последнее сравнение имеет решения только для аргументов τ, определенных равенством (7), вследствие чего имеем:

$$q_\tau 2^p \equiv \nu(q_k - 1) \pmod{2^p + 1}. \qquad (13)$$

Поскольку по условию $\nu \le 2^p$, то (13) описывает все возможные решения (11). Количество решений сравнения (13) зависит от величины НОД чисел $q_\tau, q_k - 1$ и $2^p + 1$. При этом возможны следующие три варианта:

1) сравнение (13) имеет единственное решение при $(q_k - 1, 2^p + 1) = 1$ (ветвь 31 на рис.1);

2) сравнение (13) имеет $(q_k - 1, 2^p + 1) = d_2 > 1$ решений при условии $q_\tau \equiv 0 \pmod{d_2}$, так как $(d_2, 2^p) = 1$ (ветвь 32 на рис. 1);

3) сравнение (13) не имеет ни одного решения, если $(q_k - 1, 2^p + 1) = d_2$, но при этом $q_\tau \not\equiv 0 \pmod{d_2}$ (ветвь 33 на рис. 1).

Полученные результаты анализа соотношений (4), (9) и (11) необходимы для оценки количества решений M исходного уравнения (3).

Ожидаемые оценки, по крайней мере, при некоторых условиях будут носить характер нижней границы. В частности, это является следствием того, что рассмотренный выше вариант 3 оценивает принадлежность элемента $\alpha^{\nu+\tau} + \alpha^{\nu k}$ только к подполю порядка 2^p. Однако само это подполе $GP(2^p)$ может содержать подполя, порождающие дополнительные решения. Очевидно, что предложенный метод анализа никак не ограничивает рассмотрение и таких ситуаций, но в данной статье с целью достижения простоты изложения они не анализируются. В любом случае минимальное значение $M = 0$ и минимальный (с учетом знака) уровень ФВК всегда равен

$$\min_\tau \theta_k(\tau) = -(2^p + 1).$$

Из полученных выше результатов следует, что все множество значений k вида (5) разбивается на три подмножества, которые представлены схемами *a, b, c* на рис. 2.

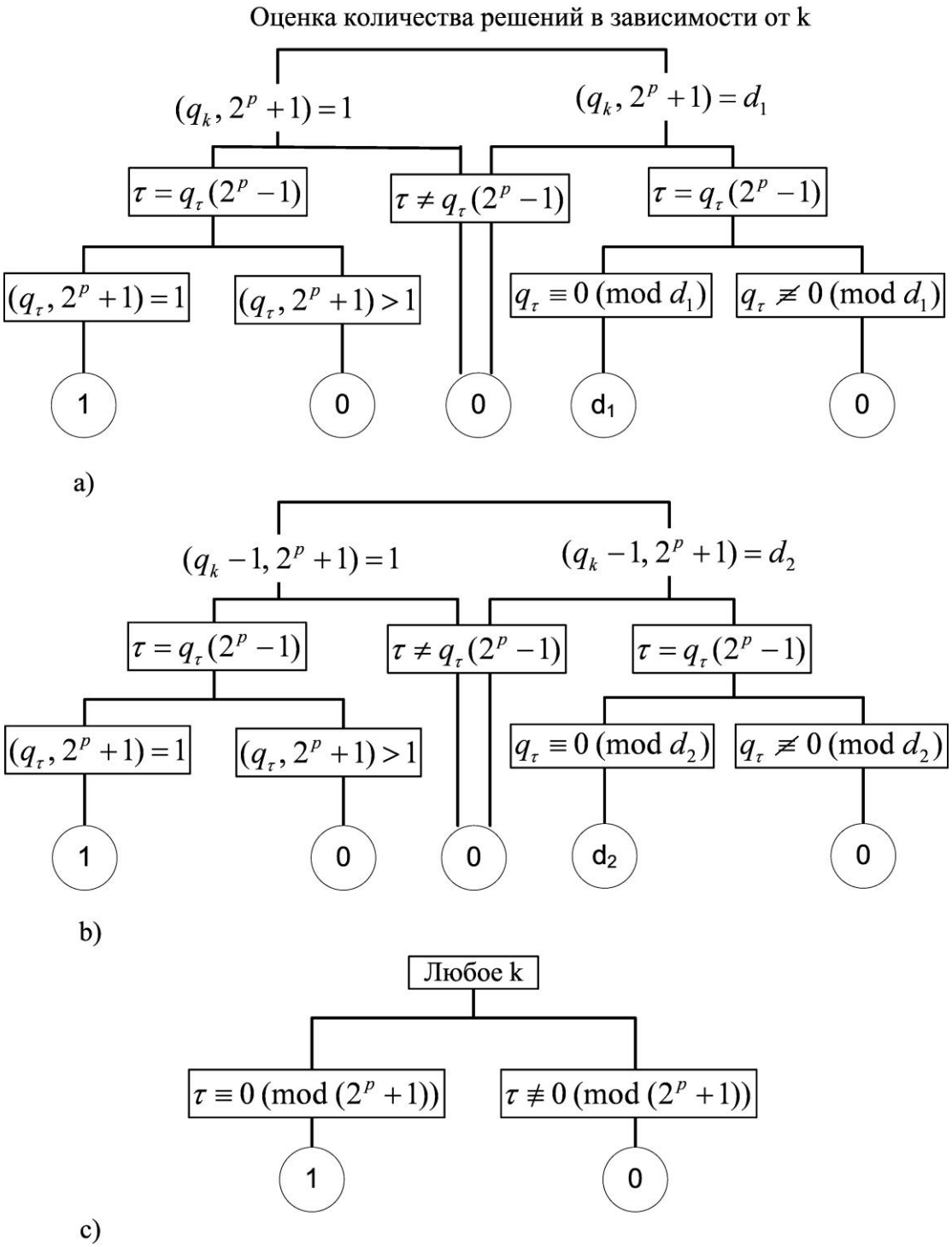

Рис. 2. Оценка количества решений *M*

Анализ вариантов решений на рис. 2 показывает, что лучшие с точки зрения минимального значения максимального уровня ФВК результаты получаются при выборе значений k, удовлетворяющих следующей системе уравнений:

$$\begin{cases}(q_k, 2^p+1)=1\\(q_k-1, 2^p+1)=1.\end{cases} \qquad (14)$$

Оценим возможности решения системы (14). Для этого перепишем условие (5) для k ,представленного в следующей эквивалентной форме

$$k = q_k(2^p + 1) - (2q_k - 1),$$

откуда вытекает ограничение для выбора числа q_k :

$$(2q_k - 1, 2^p + 1) = 1.$$

Таким образом, система (14) с учетом всех ограничений должна быть представлена в виде

$$\begin{cases} (q_k, 2^p + 1) = 1; \\ (q_k - 1, 2^p + 1) = 1; \\ (2q_k - 1, 2^p + 1) = 1. \end{cases} \qquad (15)$$

Каждое из условий можно представить в виде системы условий

$$(2q_k - 1, e_i) = 1; i = 1, 2, ..., m_p,$$

где e_i – i-й делитель числа $2^p + 1$;

m_p – количество делителей числа $2^p + 1$.

Таким образом, система (15) приобретает вид

$$\begin{cases} (q_k, e_i) = 1; \\ (q_k - 1, e_i) = 1; \quad \text{при } i = 1, 2, ..., m_p. \\ (2q_k - 1, e_i) = 1. \end{cases} \qquad (16)$$

Из (16) следует, что самые жесткие ограничения на выбор значений q_k накладывает минимальный делитель e_1 числа $2^p + 1$, значение которого зависит от свойств чисел p и $2^p + 1$. Одни из вариантов оценивания состоит в представлении минимального делителя в форме $e_1 = 2^e + 1$. Найдем далее условия, при которых $2^p + 1$ делит $e_1 = 2^l + 1$. Нетрудно установить, что таким условием является $p = (2t + 1)l$, где $t \geq 1$ - целое число. Отсюда, в частности, следует, что минимальный делитель $e_1 = 3$ соответствует значению $l = 1$ и любому нечетному числу $p = 2t + 1$, а минимальный делитель $e_1 = 5$ - значению $l = 2$ и любому четному числу вида $p = 2(2t + 1)$.

Кроме того, анализ показывает, что для некоторых четных значений p числа $2^p + 1$ могут быть простыми. В частности, скорее всего, многие (но не все) из чисел Ферма вида $2^p + 1; p = 2^s$ являются простыми. В этой ситуации система (15) имеет решение для любых

значений q_k. Однако для чисел p вида $p = 2^j(2q_p + 1);\ j > 0;\ q_p > 0$ числа $2^p + 1$ имеют минимальный делитель $e_1 = 2^{2^j} + 1$. Итак, при поиске наилучших кодовых последовательностей рассматриваемого подкласса система (16) может быть заменена системой

$$\begin{cases} (q_k, e_1) = 1; \\ (q_k - 1, e_1) = 1; \\ (2q_k - 1, e_1) = 1. \end{cases} \qquad (17)$$

и все возможные ее решения соответствуют четырем вариантам представления чисел p:

нечетные p вида $p = 2t + 1$, для которых $e_1 = 3$;

четные p вида $p = 2(2t + 1)$, для которых $e_1 = 5$;

четные p вида $p = 2^s$ такие, что числа Ферма вида $2^p + 1$ - простые;

четные p вида $p = 2^j(2q_p + 1);\ j > 1;\ q_p > 0$, для которых $e_1 = 2^{2^j} + 1$.

Вариант 1: $p = 2t + 1;\ e_1 = 3$

Для этого варианта система (17) решения не имеет, а следовательно этот вариант соответствует либо условию $(q_k, 2^p + 1) = d_1$, либо условию $(q_k - 1, 2^p + 1) = d_2$, где $d_1 = d_2 = e_1 = 3$. В частности, если $t = 2;\ p = 5$, то минимальное значение q_k по условию $(q_k, 2^p + 1) = d_1$ равно 3, что соответствует $k = 47$ (см. рис. 3b). При этом $(q_k - 1, 2^p + 1) = 1$, полное число решений $M = 5$ и максимальный уровень ФВК в соответствии с (1) равен

$$\theta_k(\tau) = 2^p(M - 1) - 1 = 2^{p+2} - 1.$$

Вариант 2: $p = 2(2t + 1);\ e_1 = 5$

Для этого варианта система (17) имеет два решения, а следовательно этот вариант соответствует условиям $(q_k, 2^p + 1) = 1$, $(q_k - 1, 2^p + 1) = 1$. В частности, если $t = 1;\ p = 6$, то минимальное значение q_k, удовлетворяющее (17), равно 2, что соответствует $k = 127$ (см. рис. 3c). При этом полное число решений $M = 3$ и максимальный уровень ФВК в соответствии с (1) равен

$$\theta_k(\tau) = 2^p(M - 1) - 1 = 2^{p+1} - 1.$$

Вариант 3: $p = 2^s$**,** число $2^p + 1$ **-** простое

Для этого варианта система (17) имеет также два решения, а следовательно этот вариант соответствует условиям $(q_k, 2^p + 1) = 1$, $(q_k - 1, 2^p + 1) = 1$. В частности, если $s = 1;\ p = 4$, то минимальное значение q_k, удовлетворяющее (17), равно 2, что соответствует $k = 31$ (см. рис. 3а). При этом полное число решений $M = 3$ и нижняя граница максимального уровня ФВК в соответствии с (1) равна

$$\theta_k(\tau) = 2^p(M-1) - 1 = 2^{p+1} - 1.$$

Отметим, что при существовании дополнительных подполей могут появляться не рассмотренные в данном анализе дополнительные решения. Рассматриваемый вариант как раз обладает указанным свойством. Поэтому, скорее всего, будут существовать значения k**,** при которых уровень ФВК величиной $2^{p+1} - 1$ будет превышен. Действительно, при $k = 47\,(q_k = 3), 61\,(q_k = 4)$ количество решений $M = 5$, что соответствует уровню $\theta_k(\tau) = 2^{p+2} - 1$, а при $k = 19\,(q_k = 5)$ $M = 4$**,** что соответствует уровню $\theta_k(\tau) = 3 \times 2^p - 1$.

Вариант 4. $p = 2^j(2q_p + 1);\ j > 1;\ q_p > 0$**,** $e_1 = 2^{2^j} + 1$**.**

Для этого варианта возможен выбор q_k таких, что система (17) имеет два решения, вследствие чего полное число решений $M = 3$ и максимальный уровень ФВК в соответствии с (1) равен

$$\theta_k(\tau) = 2^p(M-1) - 1 = 2^{p+1} - 1.$$

Таким образом, полученные результаты могут быть использованы как для построения квазиортогональных составных последовательностей типа кодов Голда, так и для предварительной отбраковки заведомо «плохих» комбинаций, например при алгоритмическом формировании ансамблей.

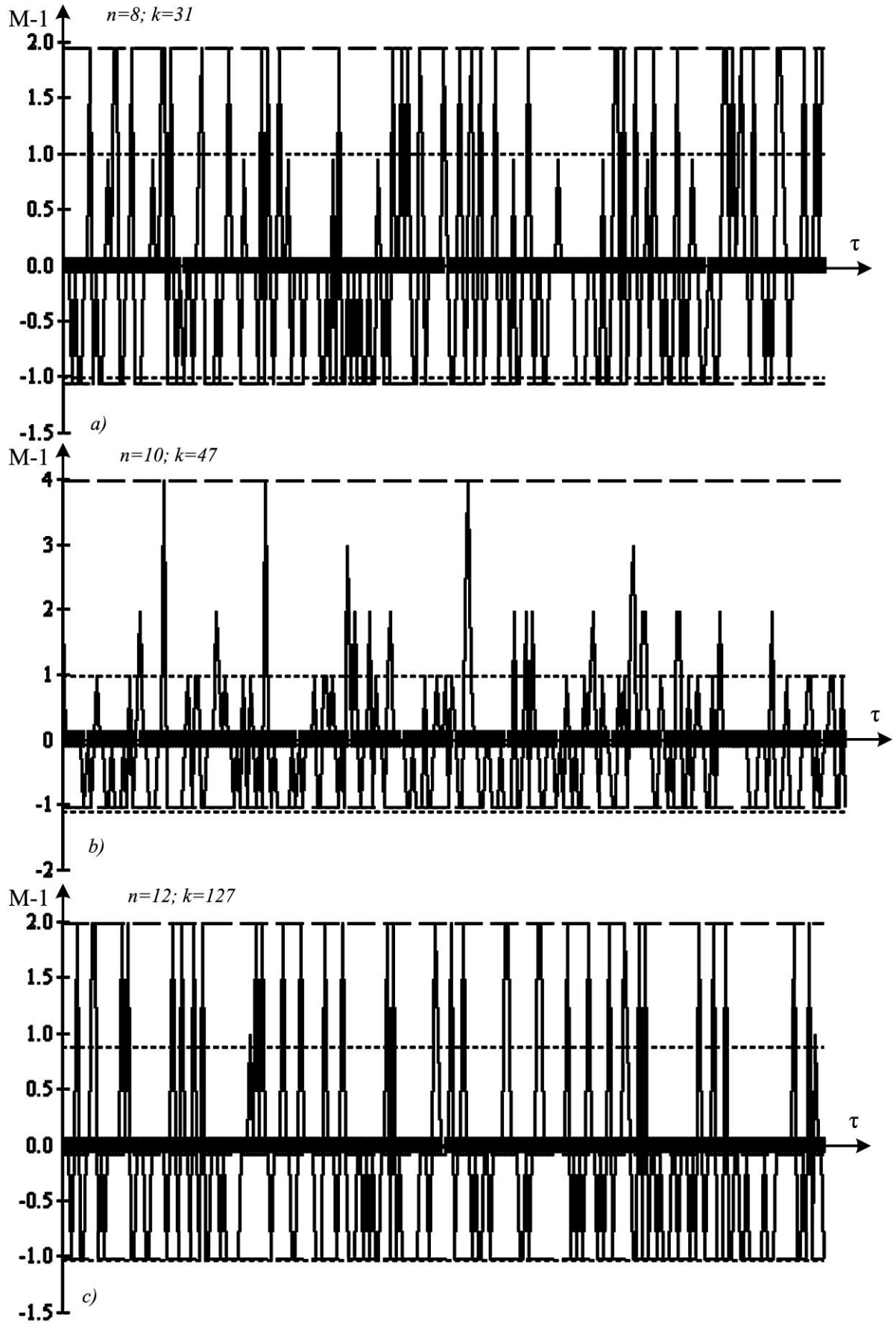

Рис. 3. Фрагменты ФВК

Заключение

Взаимнокорреляционные свойства ансамблей М-последовательностей полностью определяются структурой поля Галуа, из которого они отображаются на пространство двоичных символов. Эта зависимость очень сложная. В случае непростых значений длин М-последовательностей $N = 2^n - 1$ и, особенно, степеней порождающих многочленов n некоторые важные свойства ФВК удается вскрыть теоретико-числовыми методами. Один из таких методов при четных значениях степеней порождающих многочленов $n = 2p$ предложен в данной статье. Особенностью метода и построенной на его основе методики оценки характеристик ФВК является их аналитический характер, что несомненно расширяет границы знаний о свойствах этих широко используемых на практике кодовых последовательностей. Рассмотренные в статье примеры применения методики оценивания демонстрируют высокую точность аналитических результатов оценивания. Полученные результаты могут также рассматриваться как стартовая точка для дальнейшего развития метода и дальнейшей детализации свойств ФВК М-последовательностей рассматриваемого подкласса. Кроме того предложенный метод может быть успешно применен и для оценивания корреляционных свойств составных кодовых последовательностей, алгебраически связанных с М-последовательностями, в частности, кодов Голда.

Предложенный метод и методика оценивания ФВК может быть полезна при выборе ансамблей сложных кодированных сигналов в асинхронно-адресных и командных авиационно-космических телекоммуникационных системах.

Библиографический список

1. Михайлов В.Ю. Регулярный метод синтеза квазиортогональных ансамблей М-последовательностей // Радиотехника и электроника. – 1984. – №9. – С.1838-1840.

2. Михайлов В.Ю. О расчете максимальных значений функции взаимной корреляции М-последовательностей // Радиотехника и электроника. – 1982. – №6. – С.1219-1221.

3. Михайлов В.Ю., Мазепа Р.Б. Основы теории кодирования. – М.: МАИ-ПРИНТ, 2009. – 458 с.

Сведения об авторах

Владимир Юрьевич Михайлов, доцент Московского авиационного института (национального исследовательского университета), к.т.н., e-mail: mihvj@yandex.ru