PACS 03.67.Dd; 03.67.Lx

Алгебраическое решение задачи синтеза кодовых последовательностей

А.Н.Леухин

Предлагается алгебраическое решение «сложной» задачи синтеза фазокодированных (ФК) последовательностей с нулевым уровнем боковых лепестков циклической автокорреляционной функции (АКФ). Показано, что решение задачи синтеза связано с существованием разностных множеств для заданной размерности кода. Решена задача оценки количества возможных кодовых комбинаций при заданной размерности кода. Отмечена связь между проблемой синтеза ФК последовательностей с фундаментальными математическими проблемами дискретной математики и, в первую очередь, с рядом комбинаторных задач, решение которых, как и решение задачи факторизации числа, сводится к алгебраическим методам с использованием теории полей и групп Галуа.

Ключевые слова: *фазокодированные последовательности, квазиравномерный энергетический спектр, группа Галуа системы уравнений, разностное множество.*

1. Введение

С самого начала развития теории квантовых вычислений возникла проблема разделения областей применения квантовых и классических вычислений [1]. Существующий ряд нерешенных проблем классической дискретной математики связан, в первую очередь, с трудностью решения алгебраических задач, основанных на теории конечных групп и полей. Выделим проблемы, решение которых представляет большой практический интерес: 1) задача факторизации числа; 2) задача существования разностных множеств с заданными параметрами; 3) задача разбиения множества коэффициентов, задающих автоморфные множества исходному разностному, на непересекающиеся классы коэффициентов без конкретизации метода кодирования; 4) синтез всех симметричных уравновешенных блок-схем, матрицы инцидентности которых представляют собой циркулянт; 5) синтез всех конечных проективных плоскостей и проективных геометрий заданной размерности; 6) аналитическое выражение для неприводимых полиномов над заданным полем Галуа $GF(q^s)$.

Отметим, что этот перечень является далеко не полным, а сами указанные проблемы имеют много общего и возникают в связи с практическими применениями: в криптографических системах, при синтезе кодов, исправляющих ошибки, при синтезе шумоподобных сигналов [2]. В некоторых частных случаях все указанные проблемы являются решенными, но в целом классическая сложность алгоритмов решения поставленных задач не доказана. Однако существуют квантовые алгоритмы, использование которых позволяет решать многие так называемые трудные задачи за полиномиальное число итераций. При этом главным аргументом в пользу их применения часто является отсутствие на сегодняшний день классического алгоритма решения той же трудной задачи.

В данной работе будет представлено решение одной из таких трудных задач – задачи синтеза фазокодированных (ФК) последовательностей с нулевым уровнем боковых лепестков циклической автокорреляционной функции (АКФ), и приведен классический алгоритм ее решения.

2. Постановка задачи синтеза фазокодированных последовательностей

В настоящее время широкое применение в радиотехнических системах нашли коды с нулевыми боковыми лепестками циклической АКФ, обладающие, так же как и белый шум, равномерным энергетическим спектром. Поэтому вопросы синтеза шумоподобных кодовых последовательностей, их практической реализации и обработки являются актуальными. При больших градациях фазы известен ряд последовательностей, обладающих одноуровневой АКФ с нулевым значением боковых лепестков [3]: коды Френка, коды класса р, коды, ассоциированные с линейным частотно-модулированным (ЛЧМ) сигналом. В [4] рассматривается код в виде композиционного контура, синтез которого основан на теоретических положениях контурного анализа, описанных в монографии [5].

На сегодняшний день задача синтеза всех возможных ФК последовательностей с нулевым уровнем боковых лепестков для заданной размерности N не является решенной. Разработано множество методов и подходов для синтеза кодов с хорошими корреляционными свойствами. В этой работе рассмотрен новый подход, позволяющий решить задачу синтеза ФК последовательностей с нулевым уровнем боковых лепестков циклической АКФ, основанный на теории Галуа. Отдельные аспекты реше-

А.Н.Леухин. Марийский государственный технический университет, Россия, 424000 Йошкар-Ола, пл. Ленина, 3;
e mail: inf@marstu.mari.ru; fun_man@list.ru

Поступила в редакцию 2 июня 2005 г.

ния задачи, связанные с так называемым базисным решением, ранее обсуждались в работе [6].

Дискретную ФК последовательность $\boldsymbol{\Gamma} = \{\gamma_n\}_{0,N-1}$ запишем как

$$\gamma_n = \exp(\mathrm{i}\varphi_n), \quad n = 0, ..., N-1, \tag{1}$$

где значение фазы на каждом n-м кодовом интервале определяется из диапазона $\varphi_n \in [0, 2\pi]$; N – число кодовых элементов в коде, а модуль каждого кодового элемента $|\gamma_n| = 1$.

Циклическую АКФ найдем из выражения

$$\eta_\tau = \sum_{n=0}^{N-1} \gamma_{n+\tau \ (\mathrm{mod}\, N)} \gamma_n^*, \quad \tau = 0, 1, ..., N-1. \tag{2}$$

Требуется определить вид кода $\boldsymbol{\Gamma} = \{\gamma_n\}_{0,N-1}$, чтобы выполнялось условие равенства нулю всех боковых отсчетов циклической АКФ, т. е.

$$\eta_0 = N, \quad \eta_1 = 0, \quad \eta_2 = 0, ..., \eta_{N-1} = 0. \tag{3}$$

При этом необходимо выяснить, для любых ли целых положительных значений N существуют кодовые последовательности, удовлетворяющие условию (3), а также определить общее число P решений в случае существования решений при заданной размерности и разработать алгоритм синтеза полного семейства кодов с нулевым уровнем боковых лепестков циклической АКФ при заданной размерности кода N.

Записывая выражение энергетического спектра для ФК последовательности $\boldsymbol{\Gamma} = \{\gamma_n\}_{0,N-1}$ как

$$|\rho_m|^2 = \left|\sum_{n=0}^{N-1} \gamma_n \exp\left(-\mathrm{i}\frac{2\pi}{N}mn\right)\right|^2, \ m = 0, ..., N-1,$$

и учитывая, что $|\rho_0|^2 = |\rho_1|^2 = ... = |\rho_{N-1}|^2 = N$, получаем систему уравнений

$$\sum_{n=1}^{N-1} \left\{\cos\left(\varphi_n - \frac{2\pi}{N}mn\right) + \sum_{l=n+1}^{N-1} \cos\left[\varphi_n - \varphi_l + \frac{2\pi}{N}m(l-n)\right]\right\} = 0, \tag{4}$$

на основании которой и будем искать углы $\varphi_1, \varphi_2, ..., \varphi_{N-1}$.

3. Решения задачи синтеза ФК последовательностей, полученных на основе базисных

Базисные решения. Анализируя систему уравнений (4), можно доказать, что хотя бы для одного решения должно выполняться условие

$$\varphi_1 = \varphi_{N-1}, \quad \varphi_2 = \varphi_{N-2}, ..., \quad \varphi_{]N/2[} = \varphi_{]N/2[}, \tag{5}$$

где]...[означает целую часть числа. Такое решение назовем *базисным*.

Исходные базисные решения можно определить на основании выражений

$$\varphi_{l,n} = \phi_l[n^2(\mathrm{mod}\, N_1)], \tag{6}$$

где

$$N_1 = \begin{cases} 2N & \text{при } N\,(\mathrm{mod}\,2) \equiv 0, \\ N & \text{при } N\,(\mathrm{mod}\,2) \equiv 1; \end{cases}$$

$n = 0, ..., N-1$; $\phi_l = 2\pi\lambda_l/N_1$; λ_l – число, взаимно-простое с числом N_1; $l = 1, 2, ..., \varphi(N_1)$; $\varphi(N_1)$ – функция Эйлера.

Если размерность ФК последовательности является квадратом некоторого целого числа k, т. е. $N = k^2$, то исходными базисными решениями системы уравнений (4) будут также являться решения вида

$$\varphi_{s,n} = \phi_s k \left\{\left[\begin{array}{c}\overbrace{0\cdot 1, 1\cdot 1, ..., (k-1)\cdot 1}^{k}; \overbrace{k\cdot 3, (k+1)\cdot 3, ..., (2k-1)\cdot 3}^{k}, ..., \\ \overbrace{(k^2-k)(2k-1), (k^2-k+1)(2k-1), ..., (k^2-1)(2k-1)}^{k}\end{array}\right](\mathrm{mod}\, M)\right\}, \tag{7}$$

где

$$M = \begin{cases} 2k & \text{при } k\,(\mathrm{mod}\,2) \equiv 0, \\ k & \text{при } k\,(\mathrm{mod}\,2) \equiv 1; \end{cases}$$

$\phi_s = 2\pi\lambda_s/N_1$; λ_s – число, взаимно-простое с числом M; $s = 1, 2, ..., \varphi(M)$; $\varphi(M)$ – функция Эйлера от числа M.

Кроме того, если k является четным числом, то кроме решений вида (6) и (7) существуют исходные базисные решения системы уравнений (4) вида

$$\varphi_{s,n} = \phi_s k \left\{\left[\begin{array}{c} 0, \overbrace{0, 0, ..., 0}^{k/2}; \overbrace{2\cdot 1, 2\cdot 2, ..., 2\cdot k}^{k}; \overbrace{4\cdot(k+1), 4\cdot(k+2), ..., 4\cdot 2k}^{k}, ..., \\ \overbrace{2\cdot(k-1)(k-1)^2, ..., 2\cdot(k-1)(k^2-k-1)}^{k}; \overbrace{0, 0, ..., 0}^{k/2}\end{array}\right](\mathrm{mod}\, 2k)\right\}, \tag{8}$$

где $\phi_s = 2\pi\lambda_s/N_1$; λ_s – число, взаимно-простое с числом k; $s = 1, 2, ..., \varphi(k)$.

Группа Галуа системы уравнений (4). Можно доказать, что корни системы уравнений (4) φ_1, $\varphi_2, ..., \varphi_{N-1}$ удовлетворяют операциям взаимной замены – подстановкам, не нарушающим соотношения между корнями системы уравнений. Если индексы корней системы уравнений (4) $1, 2, 3, ..., N-1$ умножить на число λ, взаимно-простое с числом N, то получим, что каждый n-й корень, где $n = 1, 2, 3, ..., N-1$, перейдет в новый корень с индексом $\lambda \cdot n(\mathrm{mod}\, N)$. Такую подстановку будем представлять в виде

$$T_{\lambda_l} = \{[1 \to \lambda_l \cdot 1\ (\mathrm{mod}\, N)],\ [2 \to \lambda_l \cdot 2\,(\mathrm{mod}\, N)], ...,$$
$$[N-1 \to \lambda_l \cdot (N-1)\,(\mathrm{mod}\, N)]\}, \quad (9)$$

где $l = 1, 2, ..., \varphi(N_1)$; $\varphi(N)$ – функция Эйлера. Совокупность подстановок вида

$$\mathrm{Gal}(\boldsymbol{T}) = \{\boldsymbol{T}_{\lambda_1}, \boldsymbol{T}_{\lambda_2}, ..., \boldsymbol{T}_{\lambda_{\varphi(N)}}\} \quad (10)$$

образует группу Галуа $\varphi(N)$-го порядка, где $l = 1, 2, ..., \varphi(N)$. Так как любая группа Галуа является абелевой, то система уравнений (4) имеет решение при любой размерности N.

Если размерность ФК последовательности $N = k^2$, то решение системы уравнений (4) можно рассматривать в виде квадратной матрицы $\boldsymbol{\Phi} = ||\Phi_{ij}||$, где $\Phi_{ij} = \varphi_n$, $n = 0, ..., k^2-1$, а значение индекса n инкрементируется при каждом изменении индексов $i = 0, ..., k-1$ и $j = 0, ..., k-1$. Допустимыми являются подстановки

$$S_{\lambda_l} = \{[1 \to \lambda_l \cdot 1(\mathrm{mod}\, k)],\ [2 \to \lambda_l \cdot 2\,(\mathrm{mod}\, k)], ...,$$
$$(k-1 \to \lambda_l \cdot (N-1)\,(\mathrm{mod}\, k)]\}, \quad (11)$$

где λ_l – число, взаимно-простое с числом k; $l = 1, 2, ..., \varphi(k)$; $\varphi(k)$ – функция Эйлера. Совокупность подстановок, меняющих местами столбцы матрицы $\boldsymbol{\Phi}$,

$$\mathrm{Gal}(\boldsymbol{S}) = \{\boldsymbol{S}_{\lambda_1}, \boldsymbol{S}_{\lambda_2}, ..., \boldsymbol{S}_{\lambda_{\varphi(k)}}\}, \quad (12)$$

образует группу Галуа $\varphi(k)$-го порядка дополнительных подстановок.

В случае четных значений числа k группу Галуа подстановок корней системы уравнений (4), образованную выражениями (10), (12), можно дополнить. Вспомогательный индекс s определим из выражения $n = s - k/2\,(\mathrm{mod}\, N)$. С учетом такого циклического сдвига из матрицы $\boldsymbol{\Phi}$ можно получить матрицу $\boldsymbol{\Psi} = ||\Psi_{ij}||$, где $i = 0, ..., k-1$, $j = 0, ..., k-1$, $\Psi_{ij} = \varphi_n$, $n = k^2 - k/2 + 1$, $k^2 - k/2 + 2$, ..., $k^2 - k/2$, а значение индекса n инкрементируется при каждом изменении индексов i, j. Допустимыми являются следующие подстановки:

$$V_{\lambda_1} = \{[1 \to \lambda_l \cdot 1(\mathrm{mod}\, k)],\ [2 \to \lambda_l \cdot 2\,(\mathrm{mod}\, k)], ...,$$
$$[k-1 \to \lambda_l \cdot (N-1)\,(\mathrm{mod}\, k)]\}, \quad (13)$$

где λ_l – число, взаимно-простое с числом k; $l = 1, 2, ..., \varphi(k)$; $\varphi(k)$ – функция Эйлера. Совокупность подстановок, меняющих местами строки матрицы $\boldsymbol{\Psi}$,

$$\mathrm{Gal}(\boldsymbol{V}) = \{\boldsymbol{V}_{\lambda_1}, \boldsymbol{V}_{\lambda_2}, ..., \boldsymbol{V}_{\lambda_{\varphi(k)}}\}, \quad (14)$$

образует группу Галуа $\varphi(k)$-го порядка дополнительных подстановок.

После применения подстановок вида (14) к решению системы уравнений (4), представленному в виде матрицы $\boldsymbol{\Psi}$, необходимо выполнить обратный переход от матрицы $\boldsymbol{\Psi}$ к матрице $\boldsymbol{\Phi}$, используя выражение $n = s - k/2\ (\mathrm{mod}\ N)$.

Решения системы уравнений (4), полученные на основе базисных. Применив допустимые подстановки корней системы уравнений (4) в виде (10), (12), (14) к исходным базисным решениям в виде (6)–(8), мы получим все возможные базисные решения. Общее число базисных решений системы уравнений (4) размерности N обозначим через L. Для каждого полученного базисного решения можно получить еще N не базисных решений:

$$\Psi_{n+l\cdot N, N-n+m\,(\mathrm{mod}\ N)}) = \varphi_{l,m} - \varphi_{l,n}\,(\mathrm{mod}\, 360°), \quad (15)$$

где $l = 0, ..., L-1$; $n = 0, ..., N-1$; $m = 0, ..., N-1$.

Общее число возможных решений системы уравнений (4) обозначим через P. Выше было показано, что следует различать три случая решений:

1. Для произвольного N, где $N \neq k^2$, k – целое положительное число, определим общее число возможных решений

$$P = \varphi(N)N, \quad (16)$$

причем для *нечетного* N число базисных решений $L = \varphi(N)$, а для *четного* N число $L = \varphi(2N)$.

2. Для $N^2 = k$, где k – нечетное число, количество возможных решений

$$P = [\varphi(N)\varphi(k) + \varphi(N)\varphi(k)/2]N$$
$$= \frac{3}{2}\varphi(N)\varphi(k)N, \quad (17)$$

причем в этом случае $L = \frac{3}{2}\varphi(N)\varphi(k)$.

3. Для $N = k^2$, где k – четное число, количество возможных решений таково:

в случае *четных* $k/2$

$$P = \left[\varphi(2N)\varphi(k) + \frac{\varphi(N)}{4}\varphi(2k)\varphi(k)\right.$$
$$\left. + \frac{\varphi(N)}{2}\varphi(k)\right]\frac{N}{2} = \frac{\varphi(N)\varphi(k)}{4}[5 + \varphi(k)]N, \quad (18а)$$

и при этом $L = \varphi(N)\varphi(k)[5 + \varphi(k)]/2$;

в случае *нечетных* $k/2$

$$P = \left[\varphi(2N)\varphi(k) + \frac{\varphi(N)}{4}\varphi(2k)\varphi(k)\right.$$
$$\left. + \frac{\varphi(N)}{2}\varphi(k)\right]\frac{N}{2} = \frac{\varphi(N)\varphi(k)}{8}[9 + 2\varphi(k)]N, \quad (18б)$$

и при этом $L = \{[\varphi(N)\varphi(k)]/4\}[9 + 2\varphi(k)]$.

Особый случай $N = 4$. Рассмотрим теперь особый случай, при котором длина кодовой последовательности $N = 4$. Система уравнений (4) с учетом существования базисного решения может быть представлена в виде

$$2\cos\varphi_1 + \cos\varphi_2 + 1 + 2\cos(\varphi_1 - \varphi_2) = 0,$$
$$\cos\varphi_2 + 1 = 0. \quad (19)$$

Отсюда следует, что $\varphi_2 = 180°$, а φ_1 и, следовательно, φ_3 могут принимать любое значение из диапазона $[0°, 360°]$, т. е. $\varphi_1 = \varphi_3 \in [0°, 360]°$. Поэтому существует бесконечно много базисных решений вида

$$0^\circ, \varphi_1, 180^\circ, \varphi_1, \tag{20а}$$

где φ_1 может принимать любое значение из диапазона $[0^\circ, 360^\circ]$. С учетом преобразований (17) решениями системы уравнений (21) будут также являться решения вида

$$0^\circ, \varphi_1, 0^\circ, \varphi_1 + 180^\circ. \tag{20б}$$

Подчеркнем, что только в особом случае, т. е. при $N = 4$, можно синтезировать сколь угодно много кодовых последовательностей с нулевыми боковыми лепестками циклической АКФ. В этом случае $P = \infty$, причем число базисных решений $L = \infty$. Во всех остальных случаях, с учетом ограничения $\varphi = 0^\circ$, число кодовых последовательностей будет конечным.

4. Решения, полученные на основе разностных множеств

Достаточное условие существования кода с одноуровневой АКФ состоит в существовании разностного множества $D(N, K^+, \lambda)$ (где $K^\pm$ – число элементов разностного множества размерности N, λ – число повторений разности элементов разностного множества), и наоборот, если существует разностное множество, то обязательно должен существовать код с одноуровневой АКФ [1]. На сегодняшний день задача синтеза всех возможных разностных множеств для заданной размерности N считается не решенной. В работе [7] приведена классификация известных разностных множеств. К ним относятся:

1. Разностное множество, полученное на основе квадратичных вычетов:

$$D(N = 4x + 3 = p, K^+ = 2x, \lambda = x),$$

$$x = 0, 1, 2, ..., \quad p \text{ – простое число.} \tag{21}$$

Такому разностному множеству соответствует код Лежандра. Мощность метода кодирования (количество неинверсно-изоморфных коэффициентов) определится как

$$M_\text{c} = 1. \tag{22}$$

2. Разностное множество Зингера:

$$D\left(N = \frac{q^s - 1}{q - 1},\ K^+ = \frac{q^{s-1} - 1}{q - 1},\ \lambda = \frac{q^{s-2} - 1}{q - 1}\right),$$

$$q = p^n. \tag{23}$$

Данному разностному множеству соответствует код Зингера. Мощность метода кодирования определим из выражения

$$M_\text{c} = \frac{\varphi(p^n - 1)}{(p - 1)n}. \tag{24}$$

Интерес представляет частный случай разностного множества Зингера $q = 2^n$, $s = 1$:

$$D(N = 2^n - 1,\ K^+ = 2^{n-1} - 1,\ \lambda = 2^{n-2} - 1). \tag{25}$$

Данному разностному множеству соответствует m-последовательность. Мощность метода кодирования

$$M_\text{c} = \frac{\varphi(2^n - 1)}{2n}. \tag{26}$$

3. Разностное множество Якоби:

$$D(N = 4x + 3 = p(p + 2),\ K^+ = 2x + 1,\ \lambda = x). \tag{27}$$

Данному разностному множеству соответствует код Якоби. Мощность метода кодирования, как и в случае кода Лежандра $M_\text{c} = 1$.

4. Разностное множество Холла:

$$D(N = 4x + 3 = 4y^2 + 27 = p,\ K^+ = 2x + 1,\ \lambda = x),$$

$$y = 1, ... \tag{28}$$

Данному разностному множеству соответствует код Холла. Мощность метода кодирования

$$M_\text{c} = 3. \tag{29}$$

Отметим, что в предыдущих работах, например в [1], разностные множества использовались только для синтеза фазоманипулированных последовательностей (на каждом кодовом интервале $\varphi_n = 0$ или $\varphi_n = \pi$) с одноуровневой АКФ. В настоящей работе показано, что разностные множества можно использовать для синтеза ФК последовательностей. На каждом кодовом интервале ФК последовательности значения фаз таковы:

$$\varphi = \{0, 0, \phi, 0, 0, \phi, ..., 0, \phi, 0\}, \tag{30}$$

где позиции ненулевых значений фаз определяются соответствующим разностным множеством. Для нулевого уровня боковых лепестков градация фазы ϕ определится из выражения

$$\phi = \pi - \arccos\left(\frac{N - 1}{N + 1}\right). \tag{31}$$

Кроме указанных решений, выполнив применительно к решению (30) преобразования в соответствии с выражением (15), можно получить в общем случае N решений. Для решений, полученных на основе разностных множеств, полная группа Галуа системы уравнений (4) будет приводить к решениям вида

$$\varphi_{l,n} = \psi_n - 2\pi l n / N, \quad l = 0, 1, ..., N - 1,$$

$$n = 0, 1, ..., N - 1. \tag{32}$$

С учетом сказанного общее число полученных на основе разностных множеств возможных решений

$$P = 2M_\text{c}N^2. \tag{33}$$

5. Пример синтеза ФК последовательностей

При размерности $N = 7$ имеем общее число решений P', полученных на основе базисных ($P' = 42$), из которых шесть решений – базисные:

$$\varphi = \left\{0, \frac{2\pi}{7}, 4\frac{2\pi}{7}, 2\frac{2\pi}{7}, 2\frac{2\pi}{7}, 4\frac{2\pi}{7}, \frac{2\pi}{7}\right\},$$

$$\varphi = \left\{0, 2\frac{2\pi}{7}, \frac{2\pi}{7}, 4\frac{2\pi}{7}, 4\frac{2\pi}{7}, \frac{2\pi}{7}, 2\frac{2\pi}{7}\right\},$$

$$\varphi = \left\{0,\ 3\frac{2\pi}{7},\ 5\frac{2\pi}{7},\ 6\frac{2\pi}{7},\ 6\frac{2\pi}{7}, 5\frac{2\pi}{7},\ 3\frac{2\pi}{7}\right\},$$

$$\varphi = \left\{0,\ 4\frac{2\pi}{7},\ 2\frac{2\pi}{7},\ \frac{2\pi}{7},\ \frac{2\pi}{7}, 2\frac{2\pi}{7},\ 4\frac{2\pi}{7}\right\},$$

$$\varphi = \left\{0,\ 5\frac{2\pi}{7},\ 6\frac{2\pi}{7},\ 3\frac{2\pi}{7},\ 3\frac{2\pi}{7}, 6\frac{2\pi}{7},\ 5\frac{2\pi}{7}\right\},$$

$$\varphi = \left\{0,\ 6\frac{2\pi}{7},\ 3\frac{2\pi}{7},\ 5\frac{2\pi}{7},\ 5\frac{2\pi}{7},\ 3\frac{2\pi}{7},\ 6\frac{2\pi}{7}\right\}.$$

На их основе, пользуясь преобразованиями вида (15), можно получить еще $6 \times 6 = 36$ решений.

При размерности $N = 7$ существует одно неинверсное изоморфное разностное множество – множество квадратичных вычетов, приводящее к решению вида

$$\varphi = \{0, 0, \phi, 0, \phi, \phi, 0\},$$

где $\phi = 138.59^\circ$.

С учетом преобразований (15) и (33) общее число решений, полученных на основе разностных множеств, определится как $P'' = 98$. Тогда в случае $N = 7$ общее число возможных решений системы уравнений (4) $P = P' + P'' = 42 + 98 = 140$.

6. Заключение

Таким образом, в результате исследований определено общее число возможных решений P и разработан алгебраический алгоритм синтеза ФК последовательностей с нулевым уровнем боковых лепестков циклической АКФ при заданной размерности кода. Показано, что разностные множества могут быть получены на основе решаемой задачи синтеза кодовых последовательностей.

Работа выполнена при финансовой поддержке грантов РФФИ № 03-02-17276 и 04-01-00243.

1. Klyshko D.N. *Phys. Lett. A*, **1**, 227 (1997).
2. Свердлик М.Б. *Оптимальные дискретные сигналы* (М.: Сов. радио, 1975).
3. Варакин Л.Е. *Системы связи с шумоподобными сигналами* (М.: Радио и связь, 1985).
4. Фурман Я.А., Роженцов А.А. *Радиотехника*, **8**, 5, (2000).
5. Леухин А.Н. и др. *Введение в контурный анализ; приложения к обработке изображений и сигналов* (М.: Физматлит, 2003).
6. Леухин А.Н. *Вестник КГТУ,* **5**, 3, (2004).
7. Холл М. *Комбинаторика* (М.: Мир, 1970).