УДК 621.391

А.А. Замула

Харьковский национальный университет имени В.Н. Каразина, Харьков

МОЩНОСТЬ МЕТОДА КОДИРОВАНИЯ ХАРАКТЕРИСТИЧЕСКИХ ДИСКРЕТНЫХ СИГНАЛОВ

Приводится математическая модель синтеза одного класса дискретных последовательностей. Анализируются свойства различных дискретных последовательностей, в частности, корреляционные и ансамблевые свойства. Приводятся исследования объема (мощности кодирования) характеристических дискретных последовательностей.

Ключевые слова: *дискретные последовательности, сигнал, объем системы сигналов, поле Галуа, правило кодирования, мощность метода кодирования, двузначный характер мультипликативной группы.*

Введение

Одним из путей повышения эффективности радиоканалов является создание частотной избыточности с применением фазоманипулированных широкополосных сигналов (ФМШПС). При этом к манипулирующим (расширяющим спектр) последовательностям предъявляется ряд требований: хорошие автокорреляционные свойства, относительно равномерный спектр, допустимый уровень максимальных пиков взаимно-корреляционных функций, большой объем, существование для большого числа значений длительностей. Подходя с этих позиций к различным системам сигналов, можно выделить, как наиболее отвечающие перечисленным требованиям, М-последовательности, последовательности с трехуровневой функцией взаимной корреляции, характеристические дискретные сигналы и др. [1 – 4].

М-последовательности обладают малым объемом, определяемым из соотношения:

$$M = \varphi(N)/m, \qquad (1)$$

где $\varphi(\cdot)$ – функция Эйлера; L – число элементов последовательности; m – степень примитивного полинома, в соответствии с которым построен линейный рекуррентный регистр сдвига – формирователь М-последовательности.

М-последовательности существуют для весьма разреженного числа значений L, определяемых из выражения:

$$L = 2^m - 1. \qquad (2)$$

При этом расширение спектра возможных значений L с целью увеличения ансамбля системы сигналов приводит к ухудшению корреляционных свойств данной системы сигналов.

В статье рассмотрены N-позиционные коды (характеристические дискретные сигналы) с двухуровневой периодической функцией автокорреляции (ПФАК), построение которых базируется на использовании характера мультипликативной группы поля $GF(p^n)$ для $N = 4x + 2 = p^n - 1$ и $N = 4x = p^n - 1$ [5].

Основные результаты исследований

Воспользуемся понятием двузначного характера ψ мультипликативной группы $GF(p^n)$ и сформулируем правила кодирования для данной системы сигналов:

$$\mu = \{\mu_i : i = 0, 1, \dots, p^n - 2\},$$

$$\left.\begin{aligned} &\mu_i = \psi(\Theta^i + 1), \text{ если } \Theta^i + 1 \equiv 0 (\text{mod } p);\\ &\mu_i = 1, \qquad\quad \text{если } \Theta^i + 1 \equiv 0 (\text{mod } p); \end{aligned}\right\} \qquad (3)$$

$$\left.\begin{aligned} &\mu_i = \psi(\Theta^i + 1), \text{ если } \Theta^i + 1 \equiv 0 (\text{mod } p);\\ &\mu_i = -1, \qquad\quad \text{если } \Theta^i + 1 \equiv 0 (\text{mod } p); \end{aligned}\right\} \qquad (4)$$

где θ – первообразный элемент поля $GF(p^n)$.

Воспользовавшись выражением для периодической функции автокорреляции (ПФА) бинарного фазоманипулированного сигнала, построенного на базе кода

$$R_\mu(m) = \sum_{i=0}^{N-1} \mu_i \mu_{i+m},$$

с учетом правила кодирования (3) и, учитывая, что $\psi(0) = 0$, найдем

$$R_\mu(m) = \begin{cases} N, \text{ если } m \equiv 0 (\text{mod } N);\\ \sum\limits_{i=1}^{p^n-2} \psi(\Theta^i + 1)\psi(\Theta^{i+m} + 1) +\\ +\psi(-\Theta^m + 1) + \psi(-\Theta^{-m} + 1) = \\ = A + \psi(-\Theta^m + 1) +\\ +\psi(-\Theta^- + 1) \text{если } m \equiv 0 (\text{mod } N). \end{cases} \qquad (5)$$

С учетом свойств характера ψ выражение для A из (5) можно записать в виде

$$A = \psi(\Theta^m) \sum_{i=0}^{p^n-2} \psi(\Theta^i + 1)\psi(\Theta^i + \Theta^{-m}) = \\ = \psi(\Theta^m) E. \qquad (6)$$

Когда i в (5) пробегает все значения от нуля до $p^n - 2$, степени первообразного элемента Θ побегают все ненулевые элементы расширенного поля $GF(p^n)$. Поэтому, обозначая нулевые элементы поля через $a_i, i = 0, 1, \dots, p^n - 2$, можно перейти от суммы по индексу i к сумме по всем нулевым элементам поля $GF(p^n)$:

$$E = \sum_{\substack{a_i \in GF(p^n),\\ a_i \neq 1 (\text{mod } p)}} \psi(a_i + 1)\psi(a_i + \Theta^{-m}).$$

Обозначим $b_i = a_i + 1$ и с учетом того, что a_i пробегают все ненулевые элементы поля $GF(p^n)$, то b_i пробегают все элементы поля $GF(p^n)$, за исключением 1, поэтому

$$E = \sum_{\substack{b_i \in GF(p^n),\\ b_i \neq 1 (\text{mod } p)}} \psi(b_i)\psi(b_i + \Theta^{-m} - 1). \qquad (7)$$

Далее, если $b_i = 1$, то $E = \psi(\Theta^{-m})$. Поэтому, добавляя и вычитая $\psi(\Theta^{-m})$ и учитывая, что $\psi(0) = 0$, можно преобразовать (7) к виду

$$E = \sum_{b_i \in GF(p^n),} \psi(b_i)\psi(b_i + \Theta^{-m} - 1) = \\ = \sum_{b_i \in GF(p^n),\, b_i \neq 0 (\text{mod } p)} \psi(b_i)\psi(b_i + \Theta^{-m} - 1) - \psi(\Theta^{-m}) =$$

$$= \sum_{\substack{b_i \in GF(p^n),\\ b_i \neq 0(\mathrm{mod}\, p)}} \psi(b_i^2)\psi[1+(\Theta^{-m}-1)b_i^{-1}] - \psi(\Theta^{-m}) =$$

$$= \sum_{b_i \in GF(p^n),\, b_i \neq 0(\mathrm{mod}\, p)} \psi[1+(\Theta^{-m}-1)b_i^{-1}] - \psi(\Theta^{-m}).$$

Но так как $b_i \in GF(p^n), b_{i\neq 0(\mathrm{mod}\, p)}$, то b_i^{-1} также побегает все ненулевые элементы поля $GF(p^n)$, т.е. обозначая $c_i = b_i^{-1}$, имеем

$$E = \sum_{\substack{c_i \in GF(p^n),\\ c_{i\neq 0(\mathrm{mod}\, p)}}} \psi[1+dc_i] - \psi(\Theta^{-m}), \qquad (8)$$

где $d = (\Theta^{-m}-1) \neq 0(\mathrm{mod}\, p)$, так как $m \neq 0(\mathrm{mod}\, N)$.

Известно, что для любого нетривиального характера справедливо:

$$\sum_{x \in GF(p)} \psi(ax+b) = 0, \quad a \neq 0(\mathrm{mod}\, P),\ a, b \in GF(p^n). \qquad (9)$$

Из соотношения (7) следует:

$$\sum_{x \in GF(p^n)} \psi(ax+b) = \sum_{x \in GF(p^n),\, x \neq 0(\mathrm{mod}\, P)} \psi(ax+b) + \psi(b) = 0, \qquad (10)$$

откуда

$$\sum_{x \in GF(p^n)} \psi(ax+b) = -\psi(b). \qquad (11)$$

С учетом (8) – (11) получим

$$E = -1 - \psi(\Theta^{-m}). \qquad (12)$$

Подставляя выражение (12) в (6) и (3), находим

$$R_\mu(m) = \psi(\Theta^m)[-1-\psi(\Theta^{-m})] + \psi(-\Theta^m+1) + \psi(-\Theta^{-m}+1). \qquad (13)$$

Заметим, что выражение (13) справедливо для любого $N = p^n - 1$.

Далее ограничимся случаем $N = 4x+2 \equiv 2(\mathrm{mod}\, 4)$.

Одним из свойств двухзначного характера является [5]:

$$\psi(-1) = \begin{cases} -1, & p^n - 1 \equiv 2(\mathrm{mod}\, 4), \\ 1, & p^n - 1 \equiv 0(\mathrm{mod}\, 4). \end{cases} \qquad (14)$$

Тогда, согласно (14):

$$\psi(-1) = -1. \qquad (15)$$

Учитывая (15) и то, что

$$\psi(a) = \psi(a^{-1}), \quad a \neq 0(\mathrm{mod}\, P), \qquad (16)$$

преобразуем (13) к виду

$$R_\mu(m) = -1 - \psi(\Theta^m) + \psi(\Theta^m - 1)\cdot[-1+\psi(\Theta^m)]. \qquad (17)$$

Из выражения (17) следует, что:

если $\psi(\Theta^m) = 1$ и $\psi(\Theta^m - 1) = 1$, то $R_\mu(m) = -2$,

если $\psi(\Theta^m) = 1$ и $\psi(\Theta^m - 1) = -1$, то $R_\mu(m) = -2$,

если $\psi(\Theta^m) = -1$ и $\psi(\Theta^m - 1) = 1$, то $R_\mu(m) = 2$,

если $\psi(\Theta^m) = -1$ и $\psi(\Theta^m - 1) = -1$, то $R_\mu(m) = -2$,

$m \neq 0(\mathrm{mod}\, N)$.

Так как Θ – первообразный элемент поля $GF(p^n)$, то степени $\Theta^i, i = 0, 1, \ldots, p^n - 2$ пробегают все $p^n - 1$ ненулевые элементы поля $GF(p^n)$, а элементы $\Theta^i + 1, i = 0, 1, \ldots, p^n - 2$, нулевой и все нулевые элементы поля $GF(p^n)$, кроме 1, поскольку для некоторого $i, \Theta^i + 1 \equiv 0(\mathrm{mod}\, p)$ и ни для какого $i, \Theta^i + 1 \neq 1(\mathrm{mod}\, p)$ так как $\Theta^i \neq 0(\mathrm{mod}\, p)$.

Учитывая изложенное и то, что $\psi(1) = 1$, легко заключить, что среди $p^n - 2$ ненулевых элементов $\Theta^i + 1$ поля $GF(p^n)$ имеется $[1/2(p^n - 1) - 1]$ элементов, для которых ψ равно –1 (т.е. квадратичных невычетов поля $GF(p^n)$). Поэтому для правила кодирования (3) число символов кода μ, принимающих значение +1, равно

$$K^+ = \frac{1}{2}(p^n - 1) - 1 + 1 = \frac{1}{2}(p^n - 1) = \frac{N}{2} = 2x + 1.$$

Таким образом, правило кодирования (3) приводит к коду с двухуровневой ПФА $R_\mu(m) = -2, 2$ с параметрами

$$N = 4x + 2,\ K^+ = 2x + 1,\ \lambda_1 = x. \qquad (18)$$

Для кодов, полученных согласно правилу кодирования (4), ПФА $R_\mu(m)$ равна N, если $m \equiv 0(\mathrm{mod}\, N)$;

$$\sum_{i=0}^{p^n-2} \psi(\Theta^i + 1)\psi(\Theta^{i+m} + 1) - \psi(-\Theta^m + 1) - \psi(\Theta^i + 1) - \psi(-\Theta^{-m} + 1) = A - \psi(-\Theta^{-m} + 1) - \psi(-\Theta^{-m} + 1), \qquad (19)$$

если $m \neq 0(\mathrm{mod}\, N)$.

После преобразований, аналогичных (6) – (7), получим

$$R_\mu(m) = \psi(\Theta^m)[-1-\psi(\Theta^m)] - \psi(-\Theta^m + 1) - \psi(-\Theta^{-m} + 1). \qquad (20)$$

Выражение (20) справедливо для любого $N = p^n - 1$. Для $N = 4x + 2 = 2(\mathrm{mod}\, 4)$, учитывая (15) и (16), преобразуем (20) к виду

$$R_\mu(m) = -1 - \psi(\Theta^m) - \psi(-\Theta^m - 1)[-1 + \psi(\Theta^m)]. \qquad (21)$$

Из выражения (21) следует, что:

если $\psi(\Theta^m) = 1$ и $\psi(\Theta^m - 1) = 1$, то $R_\mu(m) = -2$,

если $\psi(\Theta^m) = 1$ и $\psi(\Theta^m - 1) = -1$, то $R_\mu(m) = -2$,

если $\psi(\Theta^m) = -1$ и $\psi(\Theta^m - 1) = 1$, то $R_\mu(m) = 2$,

если $\psi(\Theta^m) = -1$ и $\psi(\Theta^m - 1) = -1$, то $R_\mu(m) = -2$, $m \neq 0(\mathrm{mod}\ N)$.

Для правила кодирования (4) рассуждения, аналогичные приведенным ранее, показывают, что число символов кода, принимающие значение 1, равно $2x$. Таким образом, правило кодирования (4) приводит к коду с двухуровневой ПФА $R_\mu(m) = -2, 2$, с параметрами

$$N = 4x + 2,\ K^+ = 2x,\ \lambda_1 = x - 1,\ \lambda_2 = x. \quad (22)$$

Для исследования мощности системы характеристических дискретных сигналов образуем множество из чисел, равных порядковым номерам символов кода μ, принимающих значения 1. Множество

$$B = \{i : \mu_i = 1, i = 0, 1, \ldots, p^n - 2\} \quad (23)$$

есть разностное множество, сбалансированное на два уровня, с параметрами (18), если μ определяется правилом кодирования (3), и с параметрами (21), если μ определяется правилом кодирования (4).

Мощность метода кодирования равна числу классов неинверсно-изоморфных коэффициентов, которые могут быть получены разложением мультипликативной группы $T = \{t\}$ $(t, N) = 1$ на смежные классы по классу автоморфных коэффициентов. Докажем, что числа $p^k (\mathrm{mod}\ N)$, $k = 0, 1, \ldots, n-1$ являются автоморфными коэффициентами множества B (23). Согласно (23):

$$B_{p^k}(N, K^+, \lambda_1, \lambda_2) \equiv p^k B(N, K^+, \lambda_1, \lambda_2)(\mathrm{mod}\ N) \equiv$$

$$\equiv p^k \{i : \mu_i = 1, i = 0, 1, \ldots, p^n - 2\}(\mathrm{mod}\ N) \equiv$$

$$\equiv \{i\, p^k : \mu_i = 1, i = 0, 1, \ldots, p^n - 2\}(\mathrm{mod}\ N).$$

Обозначим $n = i\, p^k$, тогда $i = n\, p^{-k}$ и

$$B_{p^k}(N, K^+, \lambda_1, \lambda_2) \equiv \{n : \mu_{np^{-k}} = 1,$$

$$n = 0, 1, \ldots, p^n - 2\}(\mathrm{mod}\ N),$$

где, по определению (3):

$$\mu_{np^{-k}} = \psi[\Theta^{np^{-k}} + 1] = \psi[(\Theta^n)^{p^{-k}} + 1].$$

В поле характеристики p:

$$\psi[(\Theta^n)^{p^{-k}} + 1] = \psi[(\Theta^n + 1)^{p^{-k}}] = [\psi(\Theta^n + 1)]^{p^{-k}}].$$

Так как для всякого нечетного p, $p > 2$,:

$$[\psi(\Theta^n + 1)]^{p^{-k}} = \psi(\Theta^n + 1), \quad (24)$$

то $\mu_{np^{-k}} = \mu_n$ и

$$B_{p^k}(N, K^+, \lambda_1, \lambda_2) = \{n : \mu_n = 1,$$

$$n = 0, 1, \ldots, p^n - 2\}(\mathrm{mod}\ N). \quad (25)$$

Сопоставляя (23) и (25), легко видеть, что $B = B_{p^k}$. Тем самым доказано, что числа p^k, $k = 0, 1, \ldots, n-1$ являются автоморфными коэффициентами множества $B(N, K^+, \lambda_1, \lambda_2)$ (23).

Множество коэффициентов $T = \{t\}$, $(t, N) = 1$ разбивается на $\varphi(N)/n$ непересекающихся классов. Действительно, так как множество $T = \{t\}$, содержащее $\varphi(N)$ коэффициентов, есть мультипликативная группа по модулю N, а класс автоморфных коэффициентов $T_1 = \{p^k, k = 0, 1, \ldots, n-1\}$, содержащий n коэффициентов, является подгруппой T, разбивая группу T на смежные классы по подгруппе T_1, получим $\varphi(N)/n$ смежных классов, каждый из которых содержит n коэффициентов. Таким образом, число изоморфных множеств (23) равно $\varphi(N)/n$.

Методика построения всех классов коэффициентов T_k, $k = 1, \ldots, \varphi(N)/n$, состоит в следующем. Класс автоморфных коэффициентов, как уже указывалось, содержит все степени числа p:

$$T_1 = \{t_{1,i} \equiv p^i (\mathrm{mod}\ N), i = 0, 1, \ldots, n-1\}. \quad (26)$$

Классы T_k состоят из элементов $t_{k,i}$, определяемых следующим образом:

$$T_k = \{t_{k,i} \equiv \tilde{t}_k t_{1,i} (\mathrm{mod}\ N), \tilde{t}_k \in T_k,$$

$$\tilde{t}_k \notin T_1, T_2, \ldots, T_{k-1}\}, \quad (27)$$

$$k = 2, 3, \ldots, \varphi(N)/n,\ i = 0, 1, \ldots, n-1.$$

Для каждого коэффициента $t_{k,i}$ можно найти такой коэффициент $t_{l,u}$, чтобы

$$t_{k,i} + t_{l,u} \equiv 0(\mathrm{mod}\ N).$$

Классы T_k и T_l являются инверсно-изоморфными. Взяв по одному коэффициенту из каждого инверсно-изоморфного класса, получим множество T неинверсно-изоморфных коэффициентов, приводящих к $\varphi(N)/2n$ неинверсно-изоморфным разностным множествам, сбалансированным на два уровня. Таким образом, мощность каждого из методов кодирования (3) и (3а) равна $\varphi(N)/2n$.

Заметим, что природа изоморфизма связана с использованием для построения множества $B(N, K^+, \lambda_1, \lambda_2)$ различных первообразных элементов поля $GF(p)$ (если $N = p - 1$) или различных первообразных неприводимых над полем $GF(p)$ полиномов степени n (если $N = p^n - 1$, $n > 1$).

Действительно, если θ_1 и θ_2 – различные первообразные элементы поля $GF(p)$, то $\theta_2 \equiv \theta_1^k$, $(k, p-1) = 1$ и, следовательно,

$$B_{\theta_1} = \{i : \phi(\theta_1^i + 1) = 1, i = 0, 1, \ldots, p^n - 2\},$$

$$B_{\theta_2} = \{i : \phi(\theta_1^{ki} + 1) = 1, i = 0, 1, \ldots, p^n - 2\} = \quad (28)$$

$$= \{uk^{-1} (\mathrm{mod}\ N) : \phi(\theta_1^u + 1) = 1, u = 0, 1, \ldots, p^n - 2\},$$

откуда видно, что B_{θ_1} и B_{θ_2} не автоморфны.

Аналогично доказывается, что если θ_1 и θ_2 – корни различных первообразных неприводимых над полем GF(p) полиномов степени n, то B_{θ_1} и B_{θ_2} не автоморфны.

С другой стороны, если использовать для построения разностного множества, сбалансированного на два уровня, различные первообразные элементы поля GF(pn), являющиеся корнями одного и того же преобразования неприводимого над GF(p) полинома f(x) степени n, то соответствующие разностные множества будут автоморфными.

Действительно, пусть θ – первообразный элемент поля GF(p^n) и f(x)=0, тогда p – сопряженные элементы поля GF(p^n), θ^{p^k}, k=1,2,...,n–1, также первообразные элементы этого поля.

Обозначим через B_θ и $B_{\theta^{p^k}}$ разностные множества, сбалансированные на два уровня, построенные соответственно по первообразным элементам θ и θ_{p^k}, k=1,2,...,n–1. Тогда

$$B_{\theta^{p^k}} = \{i : \phi(\theta^i + 1) = 1, i = 0,1,..., p^n - 2\} = B_\theta.$$

Мультипликативно обратные первообразные элементы, если N=p–1, и взаимные первообразны неприводимые над полем GF(p) полиномы степени n, если $N=p^n-1$, n>1, приводят к инверсным изоморфизмам. Действительно, пусть B_θ и $B_{\theta^{-1}}$ – разностные множества, сбалансированные на два уровня, построенные соответственно по мультипликативно обратным элементам θ и θ^{-1} поля GF(p).

Тогда

$$B_\theta = \{i : \phi(\theta^i + 1) = 1, i = 0,1,..., p^n - 2\}$$

и

$$B_{\theta^{-1}} = \{i : \phi(\theta^{-i} + 1) = 1, i = 0,1,..., p^n - 2\} =$$

$$= \{p^n - 1 - i(\mathrm{mod}\, N) : \phi(\theta^i + 1) = 1, i = 0,1,..., p^n - 2\}.$$

Очевидно, что B_θ и $B_{\theta^{-1}}$ (mod N) автоморфны, и, следовательно, B_θ и $B_{\theta^{-1}}$ – инверсно-изоморфны. Аналогично доказывается, что взаимные полиномы приводят к инверсному изоморфизму. Изложение позволяет построить все неинверсно-изоморфные множества $B(N,K+,\lambda_1,\lambda_2)$ и, следовательно, все неинверсно-изоморфные усеченные коды μ^{t_n}, которые можно получить при помощи методов кодирования (3) и (4). Для каждого из кодов μ^{t_n} следует, путем циклической перестановки его символов, найти оптимальные по минимаксному критерию импульсные коды и отобрать среди них наилучшие.

Выводы

Характеристические коды, как было отмечено выше, существуют для всех $N = P^n - 1$ ($n \ge 1$). Например, на интервале длин от 50 до 1500, m-последовательности существуют только для пяти значений, доступное число последовательности Лежандра составляет 114, число характеристических кодов для этого интервала длин составляет 225.

Более того, мощность метода кодирования для данных последовательностей (ансамбль кодов для заданного $N = P^n - 1$) определяется числом классов неинверсно-изоморфных коэффициентов, которые могут быть получены разложением мультипликативной группы $T = \{t\}$ $\{t, N\} = 1$ на смежные классы по классу автоморфных коэффициентов и равна $\Psi(N)/2n$, где $\Psi(N)$ – функция Эйлера.

Так для характеристического кода с числом элементов $N = 2052$ существует 1030 изоморфизмов данного кода, в то время как для m-последовательностей ($N = 2047$) только 176 изоморфизмов.

Пусть количество простых чисел P, меньших x, задается функцией $\pi(x)$.

Впервые достаточно точные границы изменения функции $\pi(x)$ были установлены в 1850 году П.Л. Чебышевым:

$$a\frac{x}{\ln x} \le \pi(x) \le b\frac{x}{\ln x},\ x \ge 6, \qquad (29)$$

где $a = \frac{1}{2}\ln 2,\ b = 5\ln 2$.

Неравенства (29) были доказаны П.Л. Чебышевым с лучшими константами $a = 0{,}921\ldots,\ b = 1{,}105\ldots$, но при достаточно больших x.

Мы несколько ослабим его результат, упростив при этом вычисления согласно [7]:

$$\frac{x}{\ln x + 2} < \pi(x) < \frac{x}{\ln x - 4},\ x \ge 55. \qquad (30)$$

Например, для $x = 8000$, следует ожидать появления $728 < \pi(x) < 1604$ простых чисел.

Таким образом, в соответствии с (30), в интервале от 1 до 8000 могут быть синтезированы характеристические дискретные сигналы для 1604 значений длин сигнала.

В табл. 1 приведены значения мощности кодирования для наиболее широко применяемых систем дискретных последовательностей [6].

Анализ табл. 1 показывает, что несомненным достоинством характеристических сигналов являются их хорошие ансамблевые свойства.

К тому же, данный класс дискретных сигналов относится к оптимальным дискретным сигналам по периодической функции автокорреляции (ПФАК).

Таблица 1

Примеры ансамблей бинарных минимаксных последовательностей

Ансамбль	Длина L	Объем К	Квадрат максимума корреляции ρ^2_{max}
Голда	$2^n-1,\ n \neq 0 \bmod 4$ 7, 31, 63, 127, 511, 1023	$L+2=2^n+1$	$\frac{(\sqrt{2(L+1)}+1)^2}{L^2} \to \frac{2}{L}$, n – нечетное; $\frac{(2\sqrt{(L+1)}+1)^2}{L^2} \to \frac{4}{L}$, n – четное
Касами	2^n-1, n – четное 15, 63, 255, 123	$\sqrt{L+1}$	$\frac{(\sqrt{L+1}+1)^2}{L^2} \to \frac{1}{L}$
Камалетдинов 1	p(p – 1), p – простое 42, 110, 342, 506, 930	$p+1=\frac{\sqrt{4L+1}+3}{2} \to \sqrt{L}$	$\frac{(p+3)^2}{L^2} \to \frac{1}{L}$
Камалетдинов 2	p(p – 1), p – простое 12, 56, 132, 380, 552, 992	$p+1=\frac{\sqrt{4L+1}-3}{2} \to \sqrt{L}$	$\frac{(p+1)^2}{L^2} \to \frac{1}{L}$
Характеристические последовательности	$p^n-1,\ n \geq 1$ простое	$\psi(L)$	$\frac{4}{L}$, 0 для $L=4x+2$ $\frac{2}{L}$, для $L=4x$

Список литературы

1. Пестряков В.Б. Шумоподобные сигналы в системах передачи информации / В.Б. Пестряков, В.П. Афанасьев, В.Л. Гурвич и др.; Под ред. В.Б. Пестрякова. - М.: Сов. радио, 1973. - 424 с.

2. Горбенко И.Д. Синтез систем сигналов с заданными корреляционными свойствами, законами формирования, структурными и ансамблевыми свойствами / И.Д. Горбенко, А.А. Замула // Прикладная радиоэлектроника. – 2012. – Том 2. – С. 293-298.

3. Замула А.А. Предложения по построению широкополосных систем передачи со сложными сигналами / А.А. Замула // Радиотехника: всеукраинский научно-технический сборник. – 2012. – №171, вип. 4. – С. 177-185.

4. Замула А.А. Синтез одного класса дискретных сигналов в полях Галуа / А.А. Замула, Р.И. Киянчук, Т.Е. Ярыгина, Е.П. Колованова // Прикладная радиоэлектроника. – 2011. – Том 10, № 2. – С. 240-244.

5. Свердлик М.Б. Оптимальные дискретные сигналы / М.Б. Свердлик. - М., 1975. - 200 с.

6. Ipatov Valery P. Spread Spectrum and CDMA. Principles and Applications [Текст] / Valery P. Ipatov. University of Turku, Finland and St. Petersburg Electrotechnical University 'LETI', Russia. - John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, England, 2005. – 385 p.

7. Герман О.Н. Теоретико-числовые методы в криптографии: учебник для студ. учреждений высш. проф. образования / О.Н. Герман, Н.В. Нестеренко. – М.: Издательский центр "Академия", 2012. – 272с. - ISBN 978-5-7695-6786-5.

Поступила в редколлегию 7.02.2014

Рецензент: д-р техн. наук, проф. В.А. Краснобаев, Полтавский национальный технический университет шимени Ю. Кондратюка, Полтава.

ПОТУЖНІСТЬ МЕТОДА КОДУВАННЯ ХАРАКТЕРИСТИЧНИХ ДИСКРЕТНИХ ПОСЛІДОВНОСТЕЙ

А.А. Замула

Наводиться математична модель синтезу одного класу дискретних послідовностей. Аналізуються властивості різних дискретних послідовностей, а саме, кореляційні та ансамблеві властивості. Наводяться властивості об'єму (потужності кодування) характеристичних дискретних послідовностей.

Ключові слова: *дискретні послідовності, сигнал, об'єм системи сигналів, поле Галуа, правило кодування, потужність метода кодування, двозначний характер мультиплікативної групи.*

ENCODING METHOD POWER OF CHARACTERISTIC DISCRETE SEQUENCES

A.A. Zamula

The article presents a mathematical model of the discrete sequences class synthesis. There are analyzed the properties of the various discrete sequences, in particular correlation properties and ensemble properties in this article. There are represented research of characteristic discrete sequences volume (capacity coding) in this article.

Keywords: *discrete sequences, signal, signal system volume, Galua's field, encoding rule, power of encoding method, double character of multiplicative group.*