УДК 621.39

Ю.В. Стасев[1], А.А. Кузнецов[1], А.М. Носик[2], Л.Н. Качур[3]

[1]*Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков*
[2]*Метрологичский центр военных эталонов ВС Украины, Харьков*
[3]*Кировоградский национальный технический университет, Кировоград*

ФОРМИРОВАНИЕ БОЛЬШИХ АНСАМБЛЕЙ ДИСКРЕТНЫХ СИГНАЛОВ С ИСПОЛЬЗОВАНИЕМ ИЗБЫТОЧНЫХ КОДОВ

Исследуется проблема синтеза больших ансамблей дискретных сигналов с улучшенными корреляционными свойствами. Предлагается метод формирования псевдослучайных последовательностей с использованием избыточных кодов. Развиваемое направление синтеза дискретных сигналов позволяет, используя развитый математический аппарат алгебраической теории блоковых кодов, строить быстрые алгоритмы построения больших ансамблей псевдослучайных последовательностей с улучшенными авто- и взаимокорреляционными свойствами.

Ключевые слова: *дискретный сигнал, избыточный код, блоковый код, корреляционные свойства.*

Постановка проблемы в общем виде и анализ литературы

Эффективное функционирование современных систем и сетей связи сопряжено с обеспечением многостанционного доступа к различным информационным ресурсам и технологиям [1 – 3]. Одним из перспективных направлений в этом смысле являются системы многостанционного доступа с кодовым разделением каналов [1].

Метод кодового разделения каналов основан на одновременной передаче в полосе частот ретранслятора сигналов нескольких станций, модулированных информационным сигналом и кодовым сигналом – длинной последовательностью псевдослучайных чисел (ППСЧ). На приемной стороне информационная составляющая выделяется путем умножения принятого сигнала на копию ППСЧ. Надежное разделение каналов достигается благодаря ортогональности (квазиортогональности) кодовых сигналов отдельных станций. Этот подход широко используется в системах военной и в радиосвязи с кодовым разделением каналов CDMA (Code Division Multiple Access) как наиболее перспективный по многим характеристикам [1 – 3]: высокая помехозащищённость каналов и обеспечение конфиденциальности передаваемых сообщений; высокая скорость передачи и эффективность использования спектра частот; высокая энергетическая экономичность и экологичность терминального оборудования; высокая абонентская емкость сети и др.

Эффективность кодового разделения каналов определяется, прежде всего, свойствами применяемых ППСЧ: апериодической (АФАК) и периодической (ПФАК) функцией автокорреляции, апериодической (АФВК), периодической (ПФВК) и стыковой (СФВК) функцией взаимной корреляции. Абонентская емкость системы многостанционного доступа характеризуется мощностью ансамбля кодовых сигналов (количеством используемых ППСЧ). Таким образом, решение проблемы построения эффективных систем и сетей радиосвязи с кодовым разделением каналов сопряжено с формированием больших ансамблей дискретных сигналов с улучшенными авто- и взаимокорреляционными свойствами.

В данной работе исследуется проблема синтеза больших ансамблей дискретных сигналов с улучшенными корреляционными свойствами. Предлагается метод формирования псевдослучайных последовательностей с использованием избыточных кодов. Развиваемое направление синтеза дискретных сигналов позволяет, используя развитый математический аппарат алгебраической теории блоковых кодов, строить быстрые алгоритмы построения больших ансамблей ППСЧ с улучшенными авто- и взаимокорреляционными свойствами.

1. Постановка задачи синтеза больших ансамблей дискретных сигналов с улучшенными корреляционными свойствами

Для формализации задачи синтеза больших ансамблей дискретных сигналов с улучшенными авто- и взаимокорреляционными свойствами введем некоторые определения и обозначения.

Пусть $S_i = \left(S_{i_0}, S_{i_1}, ..., S_{i_{n-1}}\right)$ – двоичная ППСЧ (кодовый сигнал) из множества $S = \{S_0, S_1, ..., S_{M-1}\}$ мощности $|S| = M$. Элементы двоичной ППСЧ принимают одно из значений $S_{i_z} = \begin{cases} +1 \\ -1 \end{cases}$, $z = 0, ..., n-1$.

Определим нормированную апериодическую функцию взаимной корреляции (АФВК) для двоичных ППСЧ $S_i = \left(S_{i_0}, S_{i_1}, ..., S_{i_{n-1}}\right)$ и $S_j = \left(S_{j_0}, S_{j_1}, ..., S_{j_{n-1}}\right)$ выражением:

$$R_{i,j}^{АФВК}(l)=\frac{1}{n}\left(S_{i_0}S_{j_l}+S_{i_1}S_{j_{l+1}}+\cdots+S_{i_{n-1}}S_{j_{l+n-1}}\right)=\\ =\frac{1}{n}\sum_{z=0}^{n-1}S_{i_z}S_{j_{l+z}}, \quad (1)$$

где l – число тактов, на которые две последовательности сдвинуты одна относительно другой, причем

$$l=-n+1,...,-1,0,1,...,n-1,\ S_{j(n-l)<x<0}=0.$$

АФВК характеризует отклик оборудования на отличный от ожидаемого сигнал, сдвинутый во времени на l символов влево. Очевидно, что ее значения лежат в пределах: $-1,...,+1$.

Нормированная периодическая функция взаимной корреляции (ПФВК) характеризует отклик оборудования на периодическую последовательность сигналов, отличных от ожидаемого сигнала и определяется по выражению:

$$R_{i,j}^{ПФВК}(l)=\frac{1}{n}\left(S_{i_0}S_{j_{(l)\bmod(n)}}+S_{i_1}S_{j_{(l+1)\bmod(n)}}+\cdots+\right.\\ \left.+S_{i_{n-1}}S_{j_{(l+n-1)\bmod(n)}}\right)=\frac{1}{n}\sum_{z=0}^{n-1}S_{i_z}S_{j_{(l+z)\bmod(n)}}. \quad (2)$$

Отклик оборудования на последовательность отличных от ожидаемого сигнала и ожидаемого сигнала характеризует нормированная стыковая функция взаимной корреляции (СФВК).

Для оценки меры подобности последовательности ей самой, сдвинутой во времени на l символов влево, подобности ППСЧ ей самой, введем нормированную апериодическую функцию автокорреляции (АФАК):

$$R_{i,i}^{АФАК}(l)=\frac{1}{n}\left(S_{i_0}S_{i_l}+S_{i_1}S_{i_{l+1}}+\cdots+S_{i_{n-1}}S_{i_{l+n-1}}\right)=\\ =\frac{1}{n}\sum_{z=0}^{n-1}S_{i_z}S_{i_{l+z}}. \quad (3)$$

Эта функция имеет максимальное значение при $l=0$:

$$R_{i,i}^{АФАК}(0)=\frac{1}{n}\left(S_{i_0}S_{i_0}+S_{i_1}S_{i_1}+\cdots+S_{i_{n-1}}S_{i_{n-1}}\right)=\\ =\frac{1}{n}\sum_{z=0}^{n-1}\left(S_{i_z}\right)^2=\frac{1}{n}n=1.$$

Нормированная периодическая функция автокорреляции (ПФАК) характеризует отклик оборудования на периодическую последовательность ожидаемых сигналов и определяется по выражению:

$$R_{i,i}^{ПФАК}(l)=\frac{1}{n}\left(S_{i_0}S_{i_{(l)\bmod(n)}}+S_{i_1}S_{i_{(l+1)\bmod(n)}}+\cdots+\right.\\ \left.+S_{i_{n-1}}S_{i_{(l+n-1)\bmod(n)}}\right)=\frac{1}{n}\sum_{z=0}^{n-1}S_{i_z}S_{i_{(l+z)\bmod(n)}}. \quad (4)$$

Задача синтеза больших ансамблей дискретных сигналов с улучшенными ансамблевыми и корреляционными свойствами состоит в построении такого множества $S=\{S_0,S_1,...,S_{M-1}\}$, чтобы при наибольшем значении мощности M множества S минимально и максимально допустимые уровни боковых лепестков функций авто и взаимной корреляции лежали в установленных пределах:

$$\left\{\begin{array}{c} R_{min}^{АФВК}\le R_{i,j}^{АФВК}(l)\le R_{max}^{АФВК}\\ R_{min}^{ПФВК}\le R_{i,j}^{ПФВК}(l)\le R_{max}^{ПФВК}\\ R_{i,i}^{АФАК}(0)=1\\ R_{min}^{АФАК}\le R_{i,i}^{АФАК}(l\ne 0)\le R_{max}^{АФАК}\\ R_{i,i}^{ПФАК}(0)=1\\ R_{min}^{ПФАК}\le R_{i,i}^{ПФАК}(l\ne 0)\le R_{max}^{ПФАК}\end{array}\right\}, \quad (5)$$

где $R_{min}^{АФВК}$ и $R_{max}^{АФВК}$ – минимально и максимально допустимые уровни боковых лепестков апериодической функций взаимной корреляции кодовых сигналов; $R_{min}^{ПФВК}$ и $R_{max}^{ПФВК}$ – минимально и максимально допустимые уровни боковых лепестков периодической функций взаимной корреляции кодовых сигналов; $R_{min}^{АФАК}$ и $R_{max}^{АФАК}$ – минимально и максимально допустимые уровни боковых лепестков апериодической функций автокорреляции кодовых сигналов; $R_{min}^{ПФАК}$ и $R_{max}^{ПФАК}$ – минимально и максимально допустимые уровни боковых лепестков периодической функций автокорреляции кодовых сигналов.

Проанализируем известные методы решения поставленной научно-технической задачи, сравним полученные результаты по ансамблевым и корреляционным свойствам формируемых дискретных сигналов.

2. Исследование корреляционных и ансамблевых свойств дискретных сигналов, формируемых известными методами синтеза

Проведенные исследования показывают, что вопросу синтеза сложных сигналов, обладающих требуемыми корреляционными свойствами, посвящен ряд работ [3 – 11], в которых сформулирована задача синтеза сигналов в общем виде и рассмотрены характерные особенности синтеза. Отметим, что в настоящее время существуют различные направления решения данной научной задачи.

В [4, 7] предложены процедуры синтеза дискретных сигналов асимптотическими методами в спектральной области по периодической функции автокорреляции, которые позволяют получить неплохие приближения к требуемым значениям функции автокорреляции. Однако эти методы позволяют синтезировать отдельные сигналы, обладающие требуемыми периодическими функциями автокорреляции при двоичном основании алфавита. Кроме того, синтезируемые в [4, 7] сигналы обладают ступенчатой структурой, что приводит к использованию дополнительной амплитудной модуляции.

В [5] исследуются вопросы синтеза р-ичных сигналов во временной области по апериодической функции автокорреляции на основе решения системы уравнений вида (3).

В [5] решение системы (3) сведено к простому перебору компонент

$$S_{i_z} = \begin{cases} +1 \\ -1 \end{cases}, \; z = 0,\ldots,n-1,$$

при котором соответствующие значения $R_{i,i}^{АФАК}(l)$, $l \neq 0$ лежат в пределах

$$R_{min}^{АФАК} \le R_{i,i}^{АФАК}(l \neq 0) \le R_{max}^{АФАК}.$$

В работах [6, 7] предложены методы синтеза дискретных сигналов по функции неопределенности в спектральной области. Использование этих методов позволяет получить, как и в случае синтеза дискретных сигналов по периодической функции автокорреляции, двоичные сигналы ступенчатой формы. Метод синтеза сигналов с требуемыми спектральными свойствами, изложенный в [6, 7], позволяет получать сигналы с малым уровнем "боковых составляющих" амплитудного спектра. Однако в [6, 7] не рассматриваются ансамблевые и авто- и взаимокорреляционные свойства синтезированных сигналов.

В [8] синтезированы дискретные сигналы с хорошими авто- и взаимокорреляционными свойствами на основе решения совокупности систем нелинейных неравенств вида (5) со значениями функций авто- и взаимокорреляции, определенных по выражениям (1 – 4). Предложенные в [8] процедуры синтеза дискретных сигналов позволяют, в отличие от других методов синтеза дискретных сигналов, синтезировать не отдельные сигналы, а ансамбли сигналов, обладающие требуемыми авто- и взаимокорреляционными свойствами. Однако предложенные в [8] методы синтеза фазоманипулированных сигналов обладают рядом недостатков: не все сигналы, синтезированные в результате решения системы неравенств относительно значений функции автокорреляции, удовлетворяют решению системы неравенств относительно значений функции взаимной корреляции, что приводит к большим временным затратам синтеза ансамбля сигналов; решение системы неравенств (5) получено лишь для двоичного случая; нельзя заранее (до окончания решения задачи синтеза сигналов) определить объем ансамбля сигналов.

Таким образом, к настоящему времени не разработаны методы синтеза больших ансамблей слабо коррелированных между собой дискретных сигналов. Большинство известных методов основано на использовании переборных процедур и не дает гарантированного результата синтеза сигналов с заданными ансамблевыми и корреляционными свойствами. Оценку свойств формируемых ансамблей сигналов проводят в таких случаях с использованием методов теории вероятностей и математической статистики.

Методика проведения статистических исследований свойств дискретных последовательностей подробно изложена в [3, 5], в соответствии с которой, в ходе статистических исследований для каждой пары последовательностей оцениваются следующие параметры ПФВК:

– максимальный выброс бокового лепестка $R_{max}^{ПФВК}$;

– среднее значение уровня боковых лепестков:

$$m_{ПФВК} = \frac{1}{n}\sum_{l=1}^{n} R_{i,j}^{ПФВК}(l); \qquad (6)$$

– среднее значение уровня модуля боковых лепестков;

$$m_{|ПФВК|} = \frac{1}{n}\sum_{l=1}^{n} \left| R_{i,j}^{ПФВК}(l) \right| \qquad (7)$$

– дисперсия уровня боковых лепестков;

$$d_{ПФВК} = \frac{1}{n-1}\sum_{l=1}^{n} \left(R_{i,j}^{ПФВК}(l) - m_{ПФВК} \right)^2 \qquad (8)$$

– дисперсия уровня модуля боковых лепестков;

$$d_{|ПФВК|} = \frac{1}{n-1}\sum_{i=1}^{n} \left(\left| R_{i,j}^{ПФВК}(l) \right| - m_{|ПФВК|} \right)^2. \qquad (9)$$

Естественной оценкой для математического ожидания m случайной величины X является среднее арифметическое ее наблюдаемых значений:

$$\tilde{m} = \frac{1}{N}\sum_{i=1}^{N} X_i, \qquad (10)$$

где N – количество реализаций.

Оценка дисперсии определяется выражением:

$$\tilde{D} = \frac{1}{N-1}\sum_{i=1}^{N} (X_i - \tilde{m})^2. \qquad (11)$$

Далее, исходя из вышесказанного и согласно методике приведенной в [5], производились статистические исследования следующих параметров ПФВК: $M_{|ПФВК|}$ – МО модулей уровня боковых лепестков; $M_{ПФВК}$ – МО уровня боковых лепестков; $\sqrt{D_{m_{|ПФВК|}}}$ – СКО модуля среднего значения уровня боковых лепестков; $\sqrt{D_{m_{ПФВК}}}$ – СКО среднего значения уровня боковых лепестков; $D_{ПФВК}$ – дисперсия уровня боковых лепестков; $D_{|ПФВК|}$ – дисперсия модуля уровня боковых лепестков; $\sqrt{D_{d_{ПФВК}}}$ – СКО дисперсии уровня боковых лепестков; $\sqrt{D_{d_{|ПФВК|}}}$ – СКО дисперсии модуля уровня боковых лепестков; $U_{max_{ПФВК}}$ – МО максимального выброса боковых лепестков; $\sqrt{D_{U_{max_{ПФВК}}}}$ – СКО максимальных выбросов боковых лепестков.

Количество реализаций N при проведении статистических исследований выбирается исходя из положений центральной предельной теоремы теории вероятностей: при больших значениях N среднее арифметическое будет иметь распределение, близкое к нормальному, с математическим ожиданием:

$$M[\tilde{m}] \approx \tilde{m} \qquad (12)$$

и средним квадратическим отклонением:

$$\sigma[\tilde{m}] \approx \sigma / \sqrt{N}, \qquad (13)$$

где σ – среднее квадратическое отклонение оцени-

ваемого параметра. При этом вероятность того, что оценка $\tilde{m}$ отклоняется от своего математического ожидания меньше чем на ε (доверительная вероятность), равна:

$$P(|\tilde{m} - m| < \varepsilon) \approx 2\Phi\left(\varepsilon / \sigma[\tilde{m}]\right), \qquad (14)$$

где – $\Phi(x)$ функция Лапласа, определяемая как

$$\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_0^x e^{-t^2/2} dt . \qquad (15)$$

Доверительный интервал с пределами, соответствующий доверительной вероятности P:

$$\tilde{m} - t_\rho \cdot \sigma[\tilde{m}] < m < \tilde{m} + t_\rho \cdot \sigma[\tilde{m}], \qquad (16)$$

где t_ρ – корень уравнения $2\Phi(t_\rho) = P$.

Для примера в табл. 1 сведены некоторые статистические показатели ПФВК дискретных сигналов, полученные различными методами синтеза.

Статистические характеристики ПФВК, представленные в табл. 1, были получены при 10^5 реализациях.

Для определения доверительной вероятности полученных оценок воспользуемся выражением (14). Как видно из выражения (14), наихудшим является случай для n=31. В этом случае при $\varepsilon = 0,001$ для количества реализаций $N = 10^5$:

$$P(|\tilde{m} - m| < \varepsilon) \approx 2 \cdot \Phi\left(0,001 \cdot \sqrt{10^5} / 0,088\right) \approx 0,99967 .$$

Если задаться точностью $\varepsilon = 5 \cdot 10^{-4}$, получим значение, равное

$$P(|\tilde{m} - m| < \varepsilon) \approx 0,92763 .$$

Анализ данных табл. 1 показывает, что по взаимокорреляционным свойствам формируемые ансамбли сигналов обладают сопоставимыми характеристиками.

Таблица 1

Статистические свойства ПФВК ансамблей дискретных сигналов

Линейные рекуррентные последовательности максимального периода					
Параметры ПФВК	Число элементов в сигнале				
	15	63	255	511	1023
$M_{ПФВК}$	$0,24$	$0,85 \cdot 10^{-1}$	$0,46 \cdot 10^{-1}$	$0,32 \cdot 10^{-1}$	$0,93 \cdot 10^{-2}$
$\sqrt{D_{m_{ПФВК}}}$	$0,5 \cdot 10^{-1}$	$0,94 \cdot 10^{-1}$	$0,2 \cdot 10^{-1}$	$0,63 \cdot 10^{-2}$	$0,54 \cdot 10^{-2}$
$D_{ПФВК}$	$0,21 \cdot 10^{-1}$	$0,91 \cdot 10^{-2}$	$0,17 \cdot 10^{-2}$	$0,93 \cdot 10^{-3}$	$0,67 \cdot 10^{-3}$
$\sqrt{D_{d_{ПФВК}}}$	$0,3$	$0,31 \cdot 10^{-1}$	$0,14 \cdot 10^{-1}$	$0,7 \cdot 10^{-2}$	$0,8 \cdot 10^{-2}$
$U_{max_{ПФВК}}$	$2,9/\sqrt{n}$	$2,5/\sqrt{n}$	$2,9/\sqrt{n}$	$3,1/\sqrt{n}$	$3,1/\sqrt{n}$
$\sqrt{D_{U_{max_{ПФВК}}}}$	$0,51 \cdot 10^{-1}$	$0,6 \cdot 10^{-1}$	$0,63 \cdot 10^{-1}$	$0,55 \cdot 10^{-2}$	$0,53 \cdot 10^{-2}$
Характеристические последовательности					
Параметры ПФВК	Число элементов в сигнале				
	16	60	256	508	1020
$M_{ПФВК}$	$0,21$	$0,82 \cdot 10^{-1}$	$0,51 \cdot 10^{-1}$	$0,34 \cdot 10^{-1}$	$0,89 \cdot 10^{-2}$
$\sqrt{D_{m_{ПФВК}}}$	$0,71 \cdot 10^{-1}$	$0,98 \cdot 10^{-1}$	$0,29 \cdot 10^{-1}$	$0,73 \cdot 10^{-1}$	$0,59 \cdot 10^{-2}$
$D_{ПФВК}$	$0,27 \cdot 10^{-1}$	$0,81 \cdot 10^{-2}$	$0,27 \cdot 10^{-2}$	$0,11 \cdot 10^{-1}$	$0,75 \cdot 10^{-3}$
$\sqrt{D_{d_{ПФВК}}}$	$0,34$	$0,35 \cdot 10^{-1}$	$0,19 \cdot 10^{-1}$	$0,66 \cdot 10^{-2}$	$0,84 \cdot 10^{-2}$
$U_{max_{ПФВК}}$	$3,1/\sqrt{n}$	$3/\sqrt{n}$	$3,8/\sqrt{n}$	$3,2/\sqrt{n}$	$3,1/\sqrt{n}$
$\sqrt{D_{U_{max_{ПФВК}}}}$	$0,61 \cdot 10^{-1}$	$0,67 \cdot 10^{-1}$	$0,68 \cdot 10^{-1}$	$0,66 \cdot 10^{-1}$	$0,61 \cdot 10^{-2}$
Производные ортогональные последовательности					
Параметры ПФВК	Число элементов в сигнале				
	16	60	256	508	1020
$M_{ПФВК}$	$3,8 \cdot 10^{-2}$	$3,3 \cdot 10^{-2}$	$2,9 \cdot 10^{-2}$	$0,35 \cdot 10^{-1}$	$0,25 \cdot 10^{-1}$
$\sqrt{D_{m_{ПФВК}}}$	$7,5 \cdot 10^{-5}$	$0,5 \cdot 10^{-4}$	$8,7 \cdot 10^{-6}$	$0,9 \cdot 10^{-3}$	$0,69 \cdot 10^{-3}$
$D_{ПФВК}$	$5,6 \cdot 10^{-2}$	$1,5 \cdot 10^{-2}$	$4,4 \cdot 10^{-3}$	$0,71 \cdot 10^{-3}$	$0,36 \cdot 10^{-3}$
$\sqrt{D_{d_{ПФВК}}}$	$0,4 \cdot 10^{-1}$	$6,4 \cdot 10^{-7}$	$1,2 \cdot 10^{-6}$	$0,64 \cdot 10^{-3}$	$0,57 \cdot 10^{-3}$
$U_{max_{ПФВК}}$	$1,5/\sqrt{n}$	$2,6/\sqrt{n}$	$3/\sqrt{n}$	$3,2/\sqrt{n}$	$3,8/\sqrt{n}$
$\sqrt{D_{U_{max_{ПФВК}}}}$	$2,1 \cdot 10^{-3}$	$1,8 \cdot 10^{-3}$	$1,1 \cdot 10^{-3}$	$0,85 \cdot 10^{-1}$	$0,77 \cdot 10^{-3}$
Последовательности, образованные псевдослучайной перестановкой элементов кодовых слов регистрового кода максимальной длины					
Параметры ПФВК	Число элементов в сигнале				
	31	63	127	255	511	1023
$M_{ПФВК}$	$1,1 \cdot 10^{-3}$	$0,26 \cdot 10^{-3}$	$6,24 \cdot 10^{-5}$	$1,54 \cdot 10^{-5}$	$3,74 \cdot 10^{-6}$	$9,85 \cdot 10^{-7}$
$\sqrt{D_{m_{ПФВК}}}$	$0,28 \cdot 10^{-2}$	$0,1 \cdot 10^{-2}$	$0,35 \cdot 10^{-3}$	$0,12 \cdot 10^{-3}$	$4,32 \cdot 10^{-5}$	$1,53 \cdot 10^{-5}$
$D_{ПФВК}$	$0,34 \cdot 10^{-1}$	$0,16 \cdot 10^{-1}$	$0,8 \cdot 10^{-2}$	$0,39 \cdot 10^{-2}$	$0,2 \cdot 10^{-2}$	$0,98 \cdot 10^{-3}$
$\sqrt{D_{d_{ПФВК}}}$	$0,85 \cdot 10^{-2}$	$0,29 \cdot 10^{-2}$	$0,1 \cdot 10^{-2}$	$0,35 \cdot 10^{-3}$	$0,12 \cdot 10^{-3}$	$0,1 \cdot 10^{-3}$
$U_{max_{ПФВК}}$	$2,1/\sqrt{n}$	$2,3/\sqrt{n}$	$2,6/\sqrt{n}$	$2,8/\sqrt{n}$	$3/\sqrt{n}$	$3,3/\sqrt{n}$
$\sqrt{D_{U_{max_{ПФВК}}}}$	$0,88 \cdot 10^{-1}$	$0,57 \cdot 10^{-1}$	$0,37 \cdot 10^{-1}$	$0,24 \cdot 10^{-1}$	$0,16 \cdot 10^{-1}$	$0,11 \cdot 10^{-1}$

Для подтверждения данного вывода на рис. 1 приведены зависимости среднего значения максимального выброса бокового лепестка $U_{max_{ПФВК}}$ от длины сигнала n для различных методов синтеза.

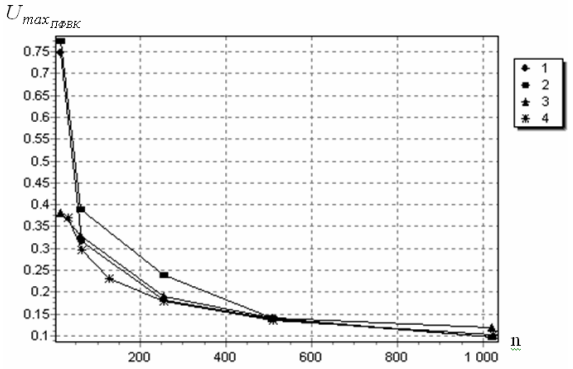

Рис. 1. Зависимость среднего значения максимального выброса бокового лепестка $U_{max_{ПФВК}}$ от длины сигнала n

На рис. 1. приведены: 1) линейные рекуррентные последовательности максимального периода (ЛРПМ); 2) характеристические последовательности; 3) производные ортогональные последовательности; 4)последовательности, образованные псевдослучайной перестановкой элементов кодовых слов регистрового кода максимальной длины.

В то же время ансамблевые свойства дискретных сигналов, формируемых различными методами синтеза, существенно различаются. На рис. 2 приведены зависимости мощности M ансамбля сигналов от длины n. Как видно из приведенных зависимостей, последовательности, образованные псевдослучайной перестановкой элементов кодовых слов регистрового кода максимальной длины, имеют улучшенные ансамблевые свойства. При сравнимых значениях уровней боковых лепестков функции взаимной корреляции мощность ансамблей дискретных сигналов, формируемых с использованием методов псевдослучайной перестановки и избыточного кодирования, превосходит известные в $10^{10}-10^{10^{10}}$ раз (!). Фактически, мощность формируемых ансамблей сигналов сопоставима с мощностью множества всех равновесных последовательностей длины n и веса n/2. Точная оценка мощности ансамблей дискретных сигналов, формируемых с использованием методов псевдослучайной перестановки и избыточного кодирования, определяется выражением:

$$M = \frac{n!}{\left(\frac{n+1}{2}\right)!\cdot\left(\frac{n-1}{2}\right)!}. \qquad (17)$$

Таким образом, применение методов избыточного кодирования позволяет получить ансамбли сигналов с хорошими корреляционными свойствами, псевдослучайные перестановочные преобразования позволяют добиться высоких ансамблевых характеристик.

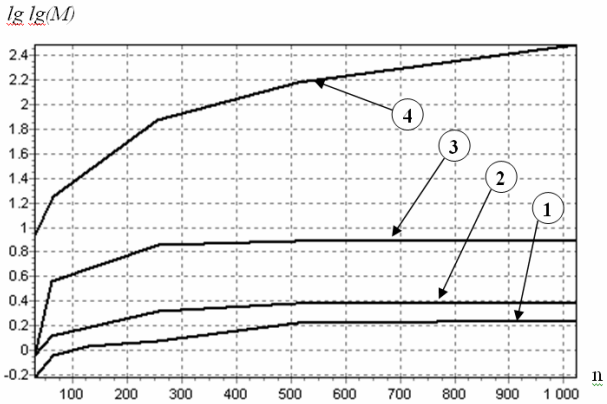

Рис. 2. Зависимость мощности ансамбля сигналов M от длины сигнала n

Из результатов анализа ансамблевых и корреляционных свойств дискретных сигналов следует, что последовательности, образованные псевдослучайной перестановкой элементов кодовых слов регистрового кода максимальной длины, обладают улучшенными свойствами, а соответствующий метод синтеза является одним из наиболее перспективных с точки зрения дальнейшего развития и практического применения для решение проблемы построения эффективных систем и сетей радиосвязи с кодовым разделением каналов.

Рассмотрим метод синтеза дискретных последовательностей, основанный на псевдослучайной перестановке элементов кодовых слов регистрового кода максимальной длины, исследуем особенности его реализации и возможности дальнейшего развития.

3. Синтез ансамблей дискретных сигналов с использованием методов избыточного кодирования

Впервые предложенный в работах [11] подход к построению двоичных псевдослучайных последовательностей на основе методов кодирования позволяет математически обобщить решение задачи синтеза больших ансамблей сигналов и в общей постановке решить для случая двоичных ППСЧ.

Зафиксируем двоичный циклический линейный блочный (n, k, d) код, исследуем авто- и взаимокорреляционные свойства дискретных сигналов, формируемых с использованием кодовых последовательностей этого кода.

В соответствии с общими положениями теории помехоустойчивого кодирования двоичный линейный (n, k, d) код C есть подпространство в $GF^n(2)$, т.е. непустое множество n-последовательностей (кодовых слов) над GF(2), k – размерность линейного подпространства, d – минимальное кодовое расстояние (минимальный вес ненулевого кодового слова). Циклический код является частным случаем подпространства, так как обладает дополнительным свойством цикличности. Каждый вектор из $GF^n(q)$ можно представить многочленом от формальной переменной x степени не выше n – 1. Компоненты вектора отождествляются с коэффициентами много-

члена. Множество многочленов обладает структурой векторного пространства, идентичной структуре пространства $GF^n(q)$, а также структурой кольца многочленов $GF(q)[x]/(x^n - 1)$. Код является циклическим, если вместе с кодовым словом c(x) он содержит также многочлен $x \cdot c(x)$. Справедлива следующая теорема, дающая конструктивный механизм построения циклических кодов.

Теорема 1 [12]. Единственный приведенный ненулевой многочлен g(x) наименьшей степени $r = n - k$ однозначно задает (n, k, d) циклический код над GF(2) и обозначается порождающим многочленом, причем $g(x) = \prod_i (x - \beta^i)$, где $\beta^i \in GF(2^m)$.

В [11] предложено решение задачи синтеза дискретных сигналов на основе использования кодовых последовательностей циклических кодов. Основные результаты представим в виде следующих утверждений.

Утверждение 1 [11]. Пусть задан ансамбль дискретных сигналов S, каждая последовательность которого образована кодовыми словами C^i циклического (n, k, d) кода. Тогда периодические авто- и взаимокорреляционные свойства удовлетворяют следующим выражениям

$$\begin{cases} R_{i,j}^{\text{ПФАК}}(l) = 1, \text{ если } l = 0 \bmod(n); \\ R_{i,j}^{\text{ПФАК}}(l) \le \dfrac{n - 2 \cdot d}{n}, \text{ если } l \ne 0 \bmod(n), \end{cases} \quad (18)$$

$$\begin{cases} R_{i,j}^{\text{ПФВК}}(l) = 1, \text{ если } C^i = C^j_{\to l}; \\ R_{i,j}^{\text{ПФВК}}(l) \le \dfrac{n - 2 \cdot d}{n}, \text{ если } C^i \ne C^j_{\to l}, \end{cases}, \quad (19)$$

где $C^j_{\to l}$ – кодовое слово C^j, циклически сдвинутое на l символов.

В соответствии с общей постановкой задачи синтеза ансамбля дискретных сигналов с требуемыми авто- и взаимокорреляционными свойствами необходимо сформировать множество ППСЧ, функции корреляции которых удовлетворяют системе ограничений (5). Предлагаемый подход на основе методов кодирования позволяет математически обобщить решение задачи синтеза и в общей постановке решить систему (5), в части, касающейся ограничений на значения периодических функций корреляции.

Действительно, если весовой спектр кода ограничен сверху некоторым значением d*, т.е. для всех $w(C^i) > d^*$ весовой спектр равен нулю (табл. 2), тогда периодические авто- и взаимокорреляционные свойства синтезируемых последовательностей удовлетворяют системе ограничений (5), а минимально и максимально допустимые уровни боковых лепестков функции автокорреляции задаются утверждением 2.

Таблица 2

Весовой спектр несовершенного кода

$w(C^i)$	0	1	…	d - 1	d	d + 1	…	d*	d* + 1	…	n
Число кодовых слов	1	0	…	0	# d	#d + 1	…	# d*	0	…	0

Утверждение 2 [11]. Пусть задан ансамбль дискретных сигналов S, каждая последовательность которого образована кодовыми словами циклического (n, k, d) кода с весовым спектром кода как в табл. 2. Тогда периодические авто- и взаимокорреляционные свойства удовлетворяют системе ограничений (5), причем:

$$R_{\min}^{\text{ПФАК}} \ge \frac{n - 2 \cdot d^*}{n}; \; R_{\min}^{\text{ПФВК}} \ge \frac{n - 2 \cdot d^*}{n}; \quad (20)$$

$$\begin{cases} R_{\max}^{\text{ПФАК}} = 1, \text{ если } l = 0 \bmod(n); \\ R_{\max}^{\text{ПФАК}} \le \dfrac{n - 2 \cdot d}{n}, \text{ если } l \ne 0 \bmod(n), \end{cases}$$

$$\begin{cases} R_{\max}^{\text{ПФВК}} = 1, \text{ если } C^i = C^j_{\to l}; \\ R_{\max}^{\text{ПФВК}} \le \dfrac{n - 2 \cdot d}{n}, \text{ если } C^i \ne C^j_{\to l}. \end{cases} \quad (21)$$

Таким образом, сигналы, сформированные в соответствии с предложенным в [11] способом, обладают улучшенными автокорреляционными свойствами. Взаимокорреляционные свойства сформированных сигналов имеют теоретически обоснованные выбросы. Остальные значения боковых выбросов лежат в узких пределах, являющихся одними из лучших на сегодняшний день результатов.

Для устранения основного недостатка рассмотренного подхода, а именно – наличия одного максимального выброса боковых лепестков функции взаимной корреляции предлагается использовать перестановочные преобразования, получившие широкое развитие в теории защиты информации. Суть перестановочного преобразования состоит в изменении нумерации входных символов, т.е. выходной вектор – суть перенумерованый входной.

Предположим, что $a = \{a_1, a_2, ..., a_n\}$ – входной вектор, а $a^* = \{a^*_1, a^*_2, ..., a^*_n\}$ – выходной вектор, $\forall a_i$, $a^*_i \in GF(q)$. Тогда перестановочное преобразование можно представить в виде:

$$a^* = a \cdot P, \quad (22)$$

где P – перестановочная матрица, т.е. квадратная матрица размером n×n ячеек, в каждой строке и в каждом столбце которой находится только по одной единице.

Очевидно, что перестановочное преобразование сохраняет вес Хемминга $w_h(a)$, т.е. справедлива

Лемма 1.

$$w_h(a^*) = w_h(a). \quad (23)$$

Сохранение веса Хемминга наблюдается также для разницы двух произвольных векторов равной длины, т.е. в результате перестановочного преобразования над двумя векторами сохраняется расстояние по Хеммингу между ними. Действительно, зафиксируем два вектора a и b равной длины:

$a = \{a_1, a_2, ..., a_n\}$, $b = \{b_1, b_2, ..., b_n\}$, $\forall a_i, b_i \in GF(q)$

и соответствующие им вектора a* и b* после выполнения перестановочного преобразования:

$$a^* = \{a^*_1, a^*_2, ..., a^*_n\}, \; b^* = \{b^*_1, b^*_2, ..., b^*_n\},$$

$$\forall a^*_i, b^*_i \in GF(q).$$

Пусть $w_h(x, y)$ – расстояние по Хеммингу между векторами x и y, тогда справедлива

Лемма 2.

$$w_h(a, b) = w_h(a^*, b^*). \qquad (24)$$

Зафиксируем перестановочное преобразование P. Применим полученные результаты к произвольному линейному блоковому (n, k, d) коду над GF(q). Справедливо следующее утверждение.

Утверждение 3. Перестановочное преобразование P над всеми кодовыми словами линейного блокового (n, k, d) кода над GF(q) образует новый линейный блоковый код с теми же параметрами и весовым спектром.

Таким образом, перестановочное преобразование над всеми кодовыми словами (n, k, d) кода переведет последовательности из $GF^k(q)$ в необязательно другие последовательности из $GF^n(q)$. При этом q^k последовательностей из $GF^n(q)$, полученных в результате перестановочного преобразования, в силу линейности перестановочного преобразования образуют линейное подпространство $GF^k(q)$ пространства $GF^n(q)$ – новый линейный блоковый (n, k, d) код с параметрами, равными исходному коду, а при условии сохранения расстояния по Хеммингу между произвольными кодовыми словами (лемма 2) – с тем же весовым спектром.

В результате проведенных исследований выявлены следующие основные свойства перестановочного преобразования: линейность – следует из выражения (22); сохранение веса Хемминга произвольного вектора – следует из леммы 1; сохранение расстояния по Хеммингу между двумя произвольными векторами – следует из леммы 2; сохранение дистанционных свойств линейного блокового кода – следует из утверждения 3. Кроме того, как можно убедиться на примере, перестановочное преобразование не обязательно сохраняет свойство цикличности кодовых слов. Практически это означает, что после выполнения перестановочного преобразования над всеми кодовыми словами циклический (n, k, d) код преобразуется в необязательно циклический (n, k, d) код с тем же весовым спектром. Исключение свойства цикличности или значительное снижение вероятности его сохранения позволяет, в свою очередь, избавиться или существенно снизить вероятность возникновения боковых выбросов в функции взаимной корреляции дискретных сигналов, формируемых с использованием линейных блоковых кодов.

Рассмотрим циклический (n, k, d) код над GF(q) как в условии утверждений 1, 2. Весовой спектр кода в общем случае может быть представлен в виде набора множеств кодовых слов с фиксированным весом:

$$\{V_0, V_1, ..., V_{d-1}, V_d, V_{d+1}, ..., V_n\}, \qquad (25)$$

где V_i – множество кодовых слов веса i.

Из определения (n, k, d) кода следует, что $|V_0| = 1$, а $V_1, ..., V_{d-1}$ – суть пустые множества.

Рассмотрим множества $V_{d+1}, ..., V_n$. Пусть мощность множества V_i для всех i = d, d+1, … n равно $|V_i| = v_i$. Каждое множество V_i содержит все циклические сдвиги всех кодовых слов (n, k, d) кода веса i. Таким образом, в произвольном циклическом (n, k, d) коде содержится $\frac{v_i}{n}$ ненулевых кодовых слов веса i и все их циклические сдвиги (по n сдвигов для каждого слова).

Рассмотрим теперь полное множество W_i последовательностей из $GF(q)^n$ веса i. Всего таких последовательностей

$$N_i = C_n^i = \frac{n!}{i! \cdot (n-i)!}.$$

Разобьем множество W_i на $\frac{N_i}{n}$ подмножеств $W_{i,j}$, каждое из которых содержит все n циклических сдвигов одной последовательности из $GF(q)^n$ веса i,

$$W_i = W_{i,1} \cup ... \cup W_{i,\frac{N_i}{n}}, \ |W_{i,j}| = n, \ j = 1, 2, ..., \frac{N_i}{n}. \qquad (26)$$

Анализ выражений (25) и (26) показывает, что множество V_i кодовых слов циклического кода является или пустым множеством или объединением конечного числа множеств $W_{i,j}$.

Перестановочное преобразование над всеми кодовыми словами согласно утверждению 3 сохраняет дистанционные свойства кода. Другими словами, в результате выполнения перестановочного преобразования при равновероятно и независимо сформированной перестановке P кодовые слова из множества V_i преобразуются в последовательности веса i, принадлежащие любому из множеств $W_{i,j}$. Схематично представим процесс перестановочного преобразования над всеми кодовыми словами циклического кода на рис. 3.

Проанализируем влияние процесса перестановочного преобразования на корреляционные свойства формируемых дискретных последовательностей.

Максимальный боковой выброс функции взаимной корреляции дискретных сигналов соответствует случаю принадлежности ансамблю помимо исходной дискретной последовательности ее циклической сдвижки. Это полностью соответствует случаю использования в качестве последовательностей сигналов кодовых слов циклического кода.

В результате выполнения перестановочного преобразования (см. рис. 3) кодовые слова циклического кода преобразуются в последовательности такого же веса. Сохранение свойства цикличности в результате такого преобразования соответствует попаданию двух и более преобразованных последовательностей в одно подмножество $W_{i,j}$, не обязательно отличное от исходного подмножества кодовых слов циклического кода. Так, например, для случая, приведенного на рис. 3, в результате перестановочного преобразования два кодовых слова преобразованы в последовательности, принадлежащие $W_{d,1}$.

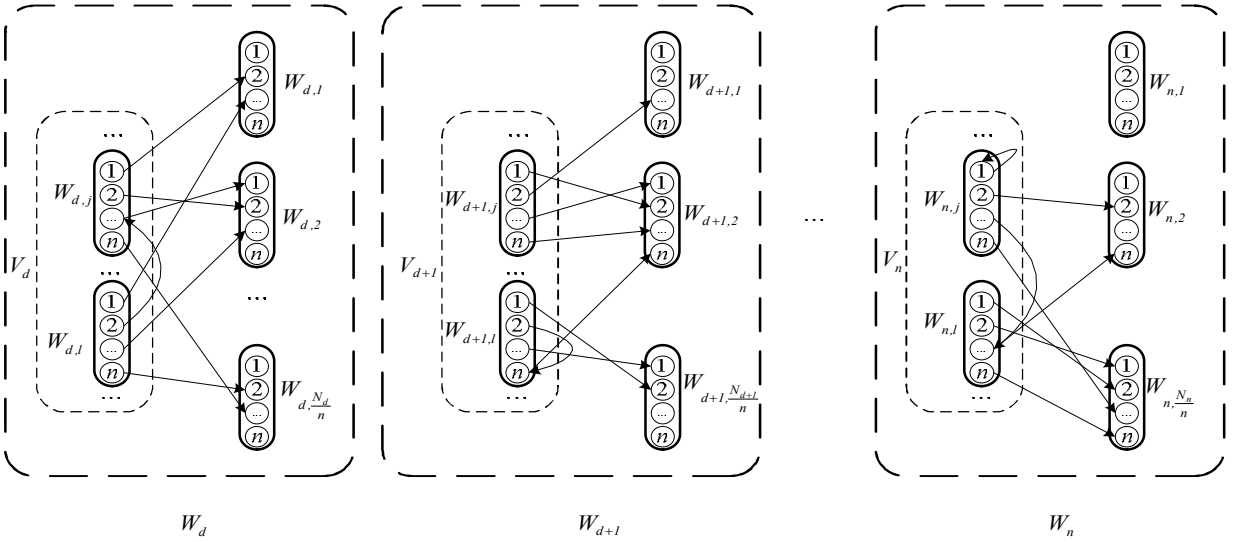

Рис. 3. Схема процесса перестановочного преобразования над кодовыми словами циклического кода

Это означает в сохранении цикличности для этой пары последовательности. В множество $W_{d,2}$ переведены три последовательности, откуда следует сохранение между ними свойства цикличности, но при этом свойство цикличности с первыми двумя последовательностями потеряно.

Выводы

Таким образом, установлено, что максимальный выброс бокового лепестка функции взаимной корреляции для формируемых в соответствии с рассматриваемым методом дискретных сигналов будет наблюдаться в случае сохранения свойства цикличности преобразуемых последовательностей. Сохранение цикличности последовательностей суть случайная величина, ее вероятность зависит от мощности множества слов фиксированного веса в $GF(q)^n$ и от весового спектра используемого кода. Как показали статистические исследования, полученные ППСЧ на основе кодовых слов блокового кода и блока перестановок обладают улучшенными корреляционными и ансамблевыми свойствами, что согласуется со сделанными теоретическими выводами. Следовательно, наиболее перспективным направлением в решении задачи синтеза больших ансамблей слабокоррелированных дискретных сигналов является применение методов избыточного (помехоустойчивого) кодирования в сочетании с псевдослучайными перестановочными преобразованиями элементов формируемых последовательностей. Данный подход позволяет формировать большие ансамбли ППСЧ с улучшенными авто- и взаимокорреляционными свойствами.

Перспективным направлением дальнейших исследований является разработка методов синтеза недвоичных ППСЧ, основанных на обобщенном перестановочном преобразовании элементов кодовых слов недвоичных избыточных (помехоустойчивых) кодов. По мнению авторов, в этом направлении могут быть получены новые научные результаты, вносящие существенный вклад в развитие теории синтеза больших ансамблей дискретных недвоичных сигналов для решения проблемы построения эффективных систем и сетей радиосвязи с кодовым разделением каналов.

Список литературы

1. Гряник М.В., Фролов В.И. Технология CDMA – будущее сотовых систем в Украине // Мир связи. – 1998. – № 3. – С. 40-43.

2. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. – М.: Вильямс, 2003. – 1104 с.

3. Стасев Ю.В., Горбенко И.Д., Макаренко Б.И., Ивашкин А.В., Воронов Д.Н. Применение сложных сигналов в командно-телеметрических радиолиниях // Космічна наука і технологія. – 1997. – Т. 3. – № 5/6. – С. 104-108.

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

5. Варакин Л.Е. Системы связи с шумоподобными сигналами. – М.: Сов. радио, 1985. – 384 с.

6. Дядюнов Н.Г., Сенин А.И. Ортогональные и квазиортогальные сигналы. – М.: Связь, 1977. – 244 с.

7. Вакмай Д.Е., Седлецкий Р.М. Вопросы синтеза радиолокационных сигналов. – М.: Сов. радио, 1973. – 312 с.

8. Горбенко И.Д., Стасев Ю.В., Замула А.А. Теория дискретных сигналов. Ортогональные сигналы. – МО СССР, 1988. – 119 с.

9. Стасев Ю.В., Брыдня Е.А. Производные ортогональные системы сигналов // Збірник наукових праць ІПМЕ. – К.: ІПМЕ, НАН України, 2004. – Вип. 25. – С. 230-237.

10. Стасев Ю.В. Метод обробки сигналів з мінімальним зсувом фази // Системи озброєння і військової техніки. – 2005. – № 1 (1). – С. 79-85.

11. Стасев Ю.В., Кузнецов А.А., Носик А.М. Формирование псевдослучайных последовательностей с улучшенными автокорреляционными свойствами // Кибернетика и системный анализ. – 2007. – № 1. – С. 3-16.

12. Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки. – М.: Связь, 1979. – 744 с.

Поступила в редколлегию 18.06.2008

Рецензент: д-р техн. наук, проф. В.И. Карпенко, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

ФОРМУВАННЯ ВЕЛИКИХ АНСАМБЛІВ ДИСКРЕТНИХ СИГНАЛІВ З ВИКОРИСТАННЯМ НАДМІРНИХ КОДІВ

Ю.В. Стасєв, О.О. Кузнецов, О.М. Носик, Л.М. Качур

Досліджується проблема синтезу великих ансамблів дискретних сигналів з покращуваними кореляційними властивостями. Пропонується метод формування псевдовипадкових послідовностей з використанням надмірних кодів. Напрям синтезу дискретних сигналів, що розвивається, дозволяє, використовуючи розвинений математичний апарат теорії алгебри блокових кодів, будувати швидкі алгоритми побудови великих ансамблів псевдовипадкових послідовностей з покращуваними авто- і взаємокореляційними властивостями.

Ключові слова: *дискретний сигнал, надмірний код, блоковий код, кореляційні властивості.*

FORMING OF LARGE BANDS OF DISCRETE SIGNALS WITH THE USE OF SURPLUS CODES

Yu.V. Stasev, A.A. Kuznetsov, A.M. Nosik, L.N. Kachur

The problem of synthesis of large bands of discrete signals is explored with the improved properties of correlations. The method of forming of pseudo-random sequences is offered with the use of surplus codes. The developed direction of synthesis of discrete signals allows, using the developed mathematical vehicle of algebraic theory of codes of blocks, to build the rapid algorithms of construction of large bands of pseudo-random sequences with improved auto- and cross-correlation properties.

Keywords: *discrete signal, surplus code, block code, properties of correlations.*