УДК 621.39

А.А. Кузнецов[1], Ал. М. Носик[2], А.А. Смирнов[3], Ан. М. Носик[2], Л.Н. Качур[3]

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

РАЗРАБОТКА МЕТОДА И АЛГОРИТМОВ СИНТЕЗА БОЛЬШИХ АНСАМБЛЕЙ НЕДВОИЧНЫХ ДИСКРЕТНЫХ СИГНАЛОВ НА ОСНОВЕ ОБОБЩЕННЫХ ПЕРЕСТАНОВОЧНЫХ ПРЕОБРАЗОВАНИЙ

Исследуются методы формирования дискретных сигналов для систем радиосвязи с кодовым разделением каналов, анализируются способы повышения абонентской емкости за счет применения больших ансамблей недвоичных псевдослучайных последовательностей. Разрабатывается метод и алгоритмы синтеза больших ансамблей недвоичных дискретных сигналов на основе обобщенных перестановочных преобразований элементов кодовых слов недвоичных избыточных кодов.

Ключевые слова: *дискретные сигналы, кодовое разделение каналов, перестановочное преобразование.*

1. Постановка проблемы в общем виде и анализ литературы

Системы радиосвязи с кодовым разделением каналов обладают рядом существенных преимуществ по сравнению с другими стандартами радиосвязи [1 – 3]. Наряду с высокой помехоустойчивостью, спектральной эффективностью и высокой абонентской емкостью они позволяют обеспечить скрытность передачи данных и имитостойкость на уровне цифровой обработки сигналов [4 – 6]. В то же время, резкое увеличение числа абонентов сетей мобильной связи, расширение спектра и качества предоставляемых услуг выдвигают повышенные вероятностно-временные требования к перспективным радиосистемам [1, 5]. Первоочередным заданием в этом смысле является повышение абонентской емкости широкополосных систем радиосвязи с кодовым разделением каналов за счет применения больших ансамблей дискретных сигналов.

Проведенный анализ известных методов синтеза ансамблей дискретных сигналов [1 – 7], результаты исследований корреляционных и ансамблевых свойств псевдослучайных последовательностей, формируемых с использованием различных методов синтеза, показали, что к настоящему времени не разработаны методы формирования больших ансамблей слабо коррелированных между собой дискретных сигналов.

Перспективным направлением в этом смысле является разработка методов синтеза недвоичных дискретных сигналов, основанных на обобщенном перестановочном преобразовании элементов кодовых слов недвоичных избыточных (помехоустойчивых) кодов. Развитие этого направления позволит формировать большие ансамбли недвоичных дискретных сигналов с улучшенными авто- и взаимокорреляционными свойствами.

2. Разработка метода формирования недвоичных псевдослучайных последовательностей для построения дискретных сигналов

Для построения больших ансамблей недвоичных дискретных сигналов на основе обобщенных перестановочных преобразований элементов кодовых слов недвоичных избыточных кодов рассмотрим методы алгебраической теории блоковых кодов и комбинаторики [2, 8].

Зафиксируем конечное поле GF(q). Рассмотрим векторное пространство $GF^n(q)$ как множество n-последовательностей элементов из GF(q) с покомпонентным сложением и умножением на скаляр. *Линейный* (n, k, d) *код* V есть подпространство $GF^k(q)$ в пространстве $GF^n(q)$, т.е. непустое множество n-последовательностей (*кодовых слов*) над GF(q), k – *размерность* линейного подпространства, d – *минимальное кодовое расстояние* (минимальный вес ненулевого кодового слова). Линейный код как линейное подпространство в $GF^n(q)$ однозначно задается набором базисных векторов – *порождающей матрицей* G кода V, т.е. матрицей ранга $\mathrm{rank}(G) = k$, размерности $k \times n$. Любое кодовое слово есть линейная комбинация строк из G. Для кодирования может использоваться любое взаимно однозначное соответствие информационных k-последовательностей и n-последовательностей кодовых слов, задающее отображение: $\phi : GF^k(q) \to GF^n(q)$. Наиболее простое соответствие информационного k-разрядного *информационного слова* $I = (I_0 \;\; I_1 \;\; ... \;\; I_{k-1})$, $I_i \in GF(q)$, $i = 0, 1, ..., k-1$ и n – разрядного кодового слова $C = (C_0 \;\; C_1 \;\; ... \;\; C_{n-1})$, $C_i \in GF(q)$, $i = 0, 1, ..., n-1$, задается выражением

$$C = I \cdot G . \qquad (1)$$

Для некоторых (циклических) линейных кодов, допускающих формальное математическое описание многочленами от одной формальной переменной (полиномиальное описание) соответствие информационного и кодового слов удобно задавать через произведение многочленов в кольце многочленов, идентичном по своей структуре пространству $GF^n(q)$ [8]. Действительно, циклический код является частным случаем подпространства, обладающего дополнительным свойством цикличности. Каждый вектор из $GF^n(q)$ можно представить в виде многочлена от формальной переменной x степени не выше $n-1$. Компоненты вектора отождествляются с коэффициентами многочлена. Множество многочленов обладает структурой векторного пространства, идентичной структуре пространства $GF^n(q)$, а также структурой кольца многочленов $GF(q)[x]/(x^n-1)$. В кольце многочленов определено умножение над многочленами: $p_1(x)\cdot p_2(x) = R_{x^n-1}[p_1(x)\cdot p_2(x)]$, где $R_b[a]$ – остаток от деления многочлена a на многочлен b. Циклический сдвиг в терминах алгебры многочленов запишется в виде $x\cdot p(x) = R_{x^n-1}[x\cdot p(x)]$. Если кодовые слова (n, k, d) кода над $GF(q)$ задаются в виде многочленов, то код V является подмножеством кольца $GF(q)[x]/(x^n-1)$. Код V является циклическим, если вместе с кодовым словом $C(x)$ он содержит также многочлен $x\cdot C(x)$. Единственный приведенный ненулевой многочлен $g(x)$ наименьшей степени $r = n-k$ однозначно задает (n, k, d) циклический код над GF(q) и обозначается порождающим многочленом, причем $g(x) = \prod_i (x-\beta^i)$, где $\beta^i \in GF(q^m)$.

Аналогично выражению (1), определим соответствие информационного многочлена $I(x) = I_0 + I_1\cdot x + ... + I_{k-1}\cdot x^{k-1}$, $\deg(I(x)) = k-1$, $I_i \in GF(q)$, $i = 0, 1, ..., k-1$ и кодового многочлена $C(x) = C_0 + C_1\cdot x + ... + C_{n-1}\cdot x^{n-1}$, $\deg(C(x)) = n-1$, $C_i \in GF(q)$, $i = 0, 1, ..., n-1$, таким выражением:

$$C(x) = I(x)\cdot g(x). \qquad (2)$$

Если $g(x) = g_0 + g_1\cdot x + ... + g_{n-k}\cdot x^{n-k}$, $\deg(g(x)) = n-k$, $g_i \in GF(q)$, $i = 0, 1, ..., n-k$, то в матричной форме циклический код задается своей порождающей матрицей:

$$G = \begin{pmatrix} 0 & ... & g_{n-k} & g_{n-k-1} & ... & g_1 & g_0 \\ 0 & ... & g_{n-k-1} & ... & g_1 & g_0 & 0 \\ ... & ... & ... & ... & ... & ... & ... \\ g_{n-k} & g_{n-k-1} & ... & ... & ... & 0 & 0 \end{pmatrix}$$

и имеем эквивалентность выражений (1) и (2).

Линейное подпространство, отождествляющее код V, имеет ортогональное дополнение, базис которого задается *проверочной матрицей* H кода V, т.е. матрицей ранга $\mathrm{rank}(H) = r, r = n-k$. Размерность проверочной матрицы $r\times n$, причем

$$G\cdot H^T = 0, \qquad (3)$$

где под «0» понимается $k\times r$ матрица нулевых элементов $GF(q)$.

Для полиномиальных кодов условие (3) эквивалентно равенству $g(x)\cdot h(x) = x^n - 1$, или, что эквивалентно,

$$R_{x^n-1}[g(x)\cdot h(x)] = 0, \qquad (4)$$

где многочлен $h(x)$ – проверочный многочлен кода V, $h(x) = h_0 + h_1\cdot x + ... + h_k\cdot x^k$, $\deg(h(x)) = k$, $h_i \in GF(q)$, $i = 0, 1, ..., k$.

Выражение (4) – суть условие взаимообратности многочленов $g(x)$ и $h(x)$ в кольце $GF(q)[x]/(x^n-1)$. Соответствующая проверочная матрица примет вид:

$$H = \begin{pmatrix} 0 & 0 & ... & ... & ... & h_{k-1} & h_k \\ ... & ... & ... & ... & ... & ... & ... \\ 0 & h_0 & h_1 & ... & h_k & 0 & 0 \\ h_0 & h_1 & ... & h_k & ... & 0 & 0 \end{pmatrix}.$$

Если рассматривать матрицу H как набор базисных векторов некоторого линейного подпространства, получим линейный код $V^\perp$, называемый дуальным к V. Произвольная n-последовательность $C = (C_0\ C_1\ ...\ C_{n-1})$ является кодовым словом кода V тогда, если она ортогональна каждой строке проверочной матрицы H, т.е.

$$C\cdot H^T = 0. \qquad (5)$$

Для полиномиальных кодов выражение (5) перепишется в виде:

$$R_{x^n-1}[C(x)\cdot h(x)] = 0. \qquad (6)$$

Наиболее распространенными алгебраическими методами построения помехоустойчивых кодов являются методы построения кодов БЧХ (Боуза-Чоудхури-Хоквингема). Данный класс кодов привлекателен простотой алгебраических методов построения и позволяет для сравнительно небольшой длины кодового слова добиться высоких конструктивных кодовых характеристик. Порождающий многочлен g(x) недвоичных кодов БЧХ над GF(q) есть многочлен

$$g(x) = \prod_i (x-\beta^i), \text{ где } \beta^i \in GF(q^m). \qquad (7)$$

Рассмотрим структуру конечного поля $GF(q^m)$ как множество многочленов степени $\le m$ с коэф-

фициентами из GF(q), т.е. структуру кольца многочленов $GF(q)[x]/(x^m - 1)$. В соответствии с общими положениями теории полей Галуа кольцо многочленов $GF(q)[x]/(x^m - 1)$ с операциями по модулю неприводимого многочлена является расширенным полем Галуа $GF(q^m)$. Такое поле состоит из совокупности циклотомических классов (классов сопряженных элементов), схематично представленных в табл. 1 в виде соответствующих степеней примитивного элемента поля.

Таблица 1

Классы сопряженных элементов и соответствующие им минимальные многочлены

Элементы циклотомических классов					Минимальные многочлены
α^0					$f_0(x) = (x - \alpha^0)$
α^1	α^q	α^{q^2}	…	α^{q^m}	$f_1(x) = f_q(x) = ... = f_{q^m}(x) = (x - \alpha^1)\cdot(x - \alpha^q)\cdot(x - \alpha^{q^2})\cdot(x - \alpha^{q^m})$
…	…	…	…	…	…
α^i	α^{iq}	α^{iq^2}	…	α^{iq^m}	$f_i(x) = f_{iq}(x) = ... = f_{iq^m}(x) = (x - \alpha^i)\cdot(x - \alpha^{iq})\cdot(x - \alpha^{iq^2})\cdot(x - \alpha^{iq^m})$
…	…	…	…	…	…

Анализ табл. 1 показывает, что выражение (7) можно переписать в виде:

$$g(x) = \prod_i f_i(x), \qquad (8)$$

причем, в соответствии с теоремой БЧХ параметры циклического кода, заданного порождающим многочленом (7) связаны соотношениями: $n = q^m - 1$, $k = n - r = n - 2mt$, $d = 2t$.

Введем в рассмотрение обобщенную перестановочную матрицу, как основной механизм формирования псевдослучайных последовательностей из кодовых слов группового кода. Пусть D – диагональная матрица с ненулевыми на диагонали элементами, P – перестановочная матрица размера $n \times n$. Перестановочная матрица реализует перестановку координат вектора в виде матричного умножения, а именно, элемент p_{ij} матрицы P равен 1 тогда и только тогда, когда координата с номером i переходит посредством перестановки в координату с номером j. В остальных случаях $p_{ij} = 0$. Таким образом, матрица P содержит в каждом столбце и в каждой строке только одну единицу.

Произведение матриц $\Lambda = P \cdot D$ задает обобщенную перестановочную матрицу Λ с ненулевыми элементами поля GF(q). Если D – единичная матрица, то $\Lambda = P$ задает обычную перестановку символов.

Суть обобщенного перестановочного преобразования поясним следующим образом. 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 обобщенное перестановочное преобразование можно задать в виде:

$$a^* = a \cdot \Lambda. \qquad (9)$$

Для удобства матрицей Λ будем обозначать в дальнейшем некоторое фиксированное обобщенное перестановочное преобразование. Справедлива следующая лемма, задающее простейшее свойство обобщенного перестановочного преобразования – сохранение веса произвольной последовательности из n символов из GF(q).

***Лемма* 1.**

$$w_h(a^*) = w_h(a). \qquad (10)$$

Доказательство. По определению, вес Хемминга $w_h(a)$ вектора a – число ненулевых элементов вектора a. Обобщенное перестановочное преобразование изменяет нумерацию элементов вектора с умножением на ненулевые элементы – собственные значения матрицы Λ. Следовательно, число ненулевых элементов вектора a* равно числу ненулевых элементов вектора a, т.е. выполняется равенство (10).

Сохранение веса Хемминга наблюдается также для разницы двух произвольных векторов равной длины, т.е. в результате обобщенного 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 преобразования Λ: $a^* = \{a^*_1, a^*_2, ..., a^*_n\}$, $b^* = \{b^*_1, b^*_2, ..., b^*_n\}$, $\forall a^*_i$, $b^*_i \in$ GF(q). Обозначим $w_h(x, y)$ – расстояние по Хеммингу между векторами x и y, тогда справедлива лемма 2, задающая второе свойство – сохранение расстояния по Хеммингу между двумя произвольными векторами из n символов из GF(q).

***Лемма* 2.**

$$w_h(a, b) = w_h(a^*, b^*). \qquad (11)$$

Доказательство. По определению $w_h(a, b) = w_h(a - b)$, $w_h(a^*, b^*) = w_h(a^* - b^*)$.

Из выражения (9) следует, что обобщенное перестановочное преобразование суть линейная операция. Следовательно, справедливо равенство

$$a^* - b^* = a \cdot \Lambda - b \cdot \Lambda = (a - b) \cdot \Lambda = (a - b)^*.$$

Но, как следует из леммы 1, $w_h(a - b)^* = w_h(a - b)$, откуда имеем цепочку равенств: $w_h(a, b) = w_h(a - b) = w_h(a - b)^* = w_h(a^* - b^*) = w_h(a^*, b^*)$, что и завершает доказательство.

Применим полученные результаты к произвольному линейному блоковому (n, k, d) коду над GF(q). Справедлива следующая теорема.

***Теорема* 1**. Обобщенное перестановочное преобразование Λ 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.

Доказательство. По определению, каждый линейный блоковый (n, k, d) код над GF(q) является подпространством $GF^k(q)$ пространства $GF^n(q)$, т.е. $GF^k(q) \subseteq GF^n(q)$. В результате обобщенного перестановочного преобразованиями над всеми кодовыми словами линейного блокового кода вес полученных последовательностей в соответствии с леммой 1 не изменится. В соответствии с леммой 2 сохраниться так же расстояние по Хеммингу между двумя произвольными кодовыми словами.

Таким образом, преобразование Λ 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 преобразования Λ над q^k кодовыми словами (n, k, d) кода над GF(q), в силу его линейности 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 – с тем же весовым спектром.

Таким образом, использование преобразования Λ позволяет реализовать отображение $\Lambda : C \to C^*$, т.е. по заданному коду C строить новый код C* (возможен случай C* = C, например, когда Λ – единичная матрица), причем весовой спектр и (n, k, d) параметры кода C* соответствуют коду C.

Для построения кода C* достаточно преобразовать базис линейного подпространства $GF^k(q) \subseteq GF^n(q)$ (базис кода C), например, умножением порождающей матрицы G кода C на матрицу Λ: $G^* = G \cdot \Lambda$.

Выполнение обобщенного перестановочного преобразования по случайно сформированной обобщенной перестановочной матрице Λ позволяет получить множество псевдослучайных последовательностей (кодовых слов кода C*). Дистанционные свойства кода C* по теореме 1 задаются дистанционными свойствами кода C, псевдослучайные свойства формируемых последовательностей задаются свойствами матрицы Λ.

Таким образом, предлагаемый метод синтеза больших ансамблей недвоичных дискретных сигналов состоит из совокупности приемов и операций алгебраической теории блоковых кодов, комбинаторики и теории чисел, теории вероятности, методов корреляционного и спектрального анализа и позволяет за конечное число операций сформировать множество псевдослучайных последовательностей с требуемыми ансамблевыми и корреляционными свойствами. На первом этапе предлагаемого метода с помощью метода алгебраической теории блоковых кодов по введенным исходным данным формируются кодовые слова недвоичных блоковых кодов. На втором этапе с использованием методов комбинаторики и теории чисел по введенным ключевым данным выполняются обобщенные перестановочные преобразования кодовых слов недвоичных блоковых кодов. Ключевые данные (обобщенные перестановочные матрицы) формируются случайно, равновероятно и независимо. На третьем этапе с использованием методов корреляционного и спектрального анализа исследуются корреляционные свойства формируемых последовательностей. После выполнения всех этапов предлагаемого метода имеем множество псевдослучайных последовательностей с требуемыми ансамблевыми и корреляционными свойствами.

3. Разработка алгоритмов формирования псевдослучайных последовательностей для построения дискретных сигналов

В результате проведенных исследований разработан метод синтеза больших ансамблей недвоичных дискретных сигналов на основе псевдослучайных последовательностей, образованных обобщенным перестановочным преобразованием элементов кодовых слов недвоичных избыточных кодов. В соответствии с разработанным методом синтез псевдослучайных недвоичных последовательностей осуществляется поэтапно, с использованием методов алгебраической теории блоковых кодов и комбинаторики. Исследуем особенности синтеза больших ансамблей недвоичных дискретных сигналов с использованием предложенного метода, рассмотрим вычислительные аспекты построения дискретных сигналов с использованием различных методов кодирования.

Алгоритм построения дискретных недвоичных сигналов в общем виде представим в виде последовательности следующих шагов.

Шаг 1. Ввод исходных данных (длина последовательности n, мощность ансамбля сигналов M, мощность алфавита символов дискретных последовательностей q).

Шаг 2. Выбор используемого алгебраического блокового кода и расчет его (n, k, d) параметров над $GF(q)$, $q^k \geq M$.

Шаг 3. Формирование обобщенной перестановочной матрицы Λ размером $n \times n$ символов из $GF(q)$.

Шаг 4. Формирование M кодовых слов алгебраического блокового (n, k, d) кода над $GF(q)$.

Шаг 5. Выполнение обобщенно-перестановочного преобразования над M кодовыми словами алгебраического блокового (n, k, d) кода над $GF(q)$.

Шаг 6. Формирование ансамбля дискретных сиг-

налов мощности M, вывод полученных результатов.

Анализ приведенного алгоритма показывает, что основными и наиболее вычислительно сложными шагами являются: формирование M кодовых слов алгебраического блокового (n,k,d) кода над $GF(q)$ (шаг 4); выполнение обобщенно-перестановочного преобразования над M кодовыми словами алгебраического блокового (n,k,d) кода над $GF(q)$ (шаг 5). Очевидно, что при больших значениях длины n и мощности ансамбля формируемых сигналов M выполнение этих шагов алгоритма крайне затруднительно. В то же время, исходя из опыта построения и эксплуатации многоадресных систем цифровой связи с кодовым разделением каналов [1 – 7] следует, что наиболее целесообразным приемом является поочередное формирование дискретных последовательностей (кодовых сигналов) различными абонентами информационного обмена. Другими словами, для многоадресных систем связи не стоит задача формирования и хранения всего ансамбля сложных сигналов. Требуется в заданное время для i-го абонента информационного обмена сформировать i-ю дискретную последовательность (кодовый сигнал). При такой постановке задачи в алгоритме формирования дискретных сигналов должна быть предусмотрена возможность формирования дискретной псевдослучайной последовательности по введенному номеру (идентификационному коду) абонента, что исключает возможность совпадения кодовых сигналов для различных абонентов информационного обмена. Эту особенность формирования дискретных сигналов можно реализовать следующим образом.

Предположим, что алгебраический блоковый код, используемый на шаге 4 разработанного алгоритма, задан своей порождающей матрицей G. По своей сути помехоустойчивое кодирование реализует всюду определенное отображение множества информационных k-последовательностей $I=(I_0 \quad I_1 \quad ... \quad I_{k-1})$ в множество n-последовательностей кодовых слов $C=(C_0 \quad C_1 \quad ... \quad C_{n-1})$ с символами из $GF(q)$: $\phi: GF^k(q) \to GF^n(q)$, которое может быть задано, например, произведением (1).

Рассмотренное выше и используемое на шаге (5) обобщенно-перестановочное преобразование реализует биективное отображение множества n-последовательностей кодовых слов $C=(C_0 \quad C_1 \quad ... \quad C_{n-1})$ в множество n-последовательностей кодовых слов $C^*=(C^*_0 \quad C^*_1 \quad ... \quad C^*_{n-1})$ с символами из $GF(q)$ некоторого линейно эквивалентного кода. Таким образом, дискретная псевдослучайная последовательность $C^*=(C^*_0 \quad C^*_1 \quad ... \quad C^*_{n-1})$, используемая в качестве кодового сигнала в многоадресной системе радиосвязи – результат последовательного выполнения двух линейных преобразований: операции помехоустойчивого кодирования линейных блоковым кодов и операции обобщенно-перестановочного преобразования, т.е. запишем:

$$C^* = C \cdot \Lambda = I \cdot G \cdot P \cdot D, \qquad (12)$$

где P и D – рассмотренные выше перестановочная и диагональная матрицы.

Анализ выражения (12) показывает, что при заданных значениях G (правило помехоустойчивого кодирования), P и D (правило обобщенно-перестановочного преобразования) дискетная последовательность $C^*=(C^*_0 \quad C^*_1 \quad ... \quad C^*_{n-1})$, используемая в качестве кодового сигнала, может быть однозначно получена по информационной k-последовательности $I=(I_0 \quad I_1 \quad ... \quad I_{k-1})$ с символами из $GF(q)$. Кроме того, как следует из основных положений линейной алгебры, это отображение исключает возможность совпадения кодовых сигналов $C^*=(C^*_0 \quad C^*_1 \quad ... \quad C^*_{n-1})$ для различных информационных последовательностей $I=(I_0 \quad I_1 \quad ... \quad I_{k-1})$.

Таким образом, имеем возможность реализовать правило формирования дискретной псевдослучайной последовательности по введенному номеру (идентификационному коду) абонента, в качестве которого будем использовать искомую последовательность $I=(I_0 \quad I_1 \quad ... \quad I_{k-1})$. Алгоритм формирования дискретных недвоичных сигналов по введенному номеру представим в виде последовательности следующих шагов.

Шаг 1. Ввод исходных данных (длина последовательности n, мощность алфавита символов дискретных последовательностей q, идентификационный номер в виде последовательности I).

Шаг 2. Выбор используемого алгебраического блокового кода и расчет его (n,k,d) параметров над $GF(q)$, формирование порождающей матрицы G размером $k \times n$ символов из $GF(q)$.

Шаг 3. Формирование обобщенной перестановочной матрицы Λ размером $n \times n$ символов из $GF(q)$.

Шаг 4. Формирование кодового слова $C = I \cdot G$ алгебраического блокового (n,k,d) кода над $GF(q)$.

Шаг 5. Выполнение обобщенно-перестановочного преобразования $C^* = C \cdot \Lambda$ над кодовым словом алгебраического блокового (n,k,d) кода над $GF(q)$.

Шаг 6. Формирование дискретного сигнала $C^*=(C^*_0 \quad C^*_1 \quad ... \quad C^*_{n-1})$, вывод полученных результатов.

Оценим сложность реализации данного алгоритма на основных шагах: формирование кодового слова $C = I \cdot G$ алгебраического блокового (n,k,d) кода над $GF(q)$ (шаг 4); выполнение обобщенно-перестановочного преобразования $C^* = C \cdot \Lambda$ над

кодовым словом алгебраического блокового (n,k,d) кода над $GF(q)$. Формирование кодового слова линейного блокового кода может быть реализовано несколькими способами. Для общего случая линейного блокового кода (код задан порождающей матрицей G размером $k \times n$ символов из $GF(q)$) формирование кодового слова может быть реализовано с помощью устройства, реализующего элементарные арифметические операции над символами из $GF(q)$. По правилу умножения матриц для формирования кодового слова C необходимо умножить k-последовательность $I = (I_0 \quad I_1 \quad ... \quad I_{k-1})$ с символами из $GF(q)$ на $k \times n$ матрицу G с символами из $GF(q)$. Всего необходимо выполнить $k \times n$ умножений и $(k-1) \times n$ сложений в арифметике поля $GF(q)$.

Выполнение обобщенно-перестановочного преобразования над кодовым словом алгебраического блокового кода также может быть реализовано с помощью устройства, реализующего элементарные арифметические операции над символами из $GF(q)$. По правилу умножения матриц для формирования дискретной последовательности $C*$ необходимо умножить n-последовательность $C = (C_0 \quad C_1 \quad ... \quad C_{n-1})$ с символами из $GF(q)$ на $n \times n$ матрицу Λ с символами из $GF(q)$. Всего на этом этапе алгоритма необходимо выполнить $n \times n$ умножений и $(n-1) \times n$ сложений в арифметике поля $GF(q)$.

Таким образом, сложность реализации разработанного алгоритма растет полиномінально от длины дискретных последовательностей, что позволяет говорить о низкой вычислительной сложности реализации.

Выводы

В результате проведенных исследований разработан метод синтеза больших ансамблей недвоичных дискретных сигналов посредством обобщенных перестановочных преобразований элементов кодовых слов недвоичных избыточных кодов. Установлено, что применение алгебраических методов помехоустойчивого кодирования позволяет строить быстрые алгоритмы формирования дискретных сигналов, а использование обобщенных перестановочных преобразований обеспечивает псевдослучайность формируемых последовательностей. Разработаны вычислительные алгоритмы формирования недвоичных псевдослучайных последовательностей, установлено, что сложность реализации предложенных алгоритмов растет полиномінально от длины дискретных последовательностей, что позволяет эффективно реализовать устройства синтеза в программном и аппаратном виде. **Перспективным направлением** дальнейших исследований является исследование корреляционных и ансамблевых свойств формируемых ансамблей дискретных сигналов.

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

4. Стасев Ю.В., Брыдня Е.А. Производные ортогональные системы сигналов // Збірник наукових праць інституту проблем моделювання в енергетиці ім. Г.Є. Пухова. – К.: ІПМЕ НАНУ, 2004. – Вип. 25. – С. 230-237.

5. 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.

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

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

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

Поступила в редколлегию 1.08.2008

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

РОЗРОБКА МЕТОДУ І АЛГОРИТМІВ СИНТЕЗУ ВЕЛИКИХ АНСАМБЛІВ НЕДВІЙКОВИХ ДИСКРЕТНИХ СИГНАЛІВ НА ОСНОВІ УЗАГАЛЬНЕНИХ ПЕРЕСТАНОВОЧНИХ ПЕРЕТВОРЕНЬ

О.О. Кузнецов, Ал.М. Носик, О.А. Смирнов, Ан.М. Носик, Л.М. Качур

Досліджуються методи формування дискретних сигналів для систем радіозв'язку з кодовим розділенням каналів, аналізуються способи підвищення абонентської місткості за рахунок застосування великих ансамблів недвійкових псевдовипадкових послідовностей. Розробляється метод і алгоритми синтезу великих ансамблів недвійкових дискретних сигналів на основі узагальнених перестановочних перетворень елементів кодових слів недвійкових надмірних кодів.

Ключові слова: *дискретні сигнали, кодове розділення каналів, перестановочне перетворення.*

DEVELOPMENT OF METHOD AND ALGORITHMS OF SYNTHESIS OF LARGE BANDS OF UNBINARY DISCRETE SIGNALS ON BASIS OF THE GENERALIZED INTERCHANGEABLE TRANSFORMATIONS

A.A. Kuznetsov, Al.M. Nosik, A.A. Smirnov, An.M. Nosik, L.N. Kachur

The methods of forming of discrete signals are explored for the systems of radio contact with the code division of channels, the methods of increase of subscriber capacity are analysed due to application of large bands of unbinary pseudo-random sequences. A method and algorithms of synthesis of large bands of unbinary discrete signals is developed on the basis of the generalized interchangeable transformations of elements of words of codes of unbinary surplus codes.

Keywords: *discrete signals, code division of channels, interchangeable transformation.*