МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УКРАИНЫ

СУМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

СУМСКИЙ ФИЛИАЛ ХАРЬКОВСКОГО НАЦИОНАЛЬНОГО УНИВЕРСИТЕТА ВНУТРЕННИХ ДЕЛ

КАФЕДРА ЭЛЕКТРОНИКИ И КОМПЬЮТЕРНОЙ ТЕХНИКИ

ТЕЗИСЫ ДОКЛАДОВ

Третьей международной научной конференции

"Современные методы кодирования в электронных системах"

СМКЭС-2006

24-25 октября 2006 года

Сумы – 2006

Третья международная научная конференция

"Современные методы кодирования в электронных системах"

СМКЭС-2006

Свидетельство о регистрации № 528 от 06.12.2005

Целью конференции является обмен новыми идеями в области кодирования информации, обсуждение тенденций развития методов кодирования в электронных системах, установление контактов и сотрудничества в данной области.

Секции научной конференции:

1) ***кодирование в электронных моделях технических и естественных систем;***
2) ***защита информации от ошибок и несанкционированного доступа;***
3) ***сжатие информации;***
4) ***системы и устройства кодированя.***

Рабочие языки конференции:

украинский и русский.

УКАЗАТЕЛЬ ТЕЗИСОВ ДОКЛАДОВ

Секция 1: Кодирование в электронных моделях технических и естественных систем

Секция 2: Защита информации от ошибок и несанкционированного доступа

Секция 3: Сжатие информации

Секция 4: Системы и устройства кодирования

УДК 621.391

ИССЛЕДОВАНИЕ КОРРЕЛЯЦИОННЫХ СВОЙСТВ ДИСКРЕТНЫХ СИГНАЛОВ, ФОРМИРУЕМЫХ С ИСПОЛЬЗОВАНИЕМ КОДОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

А. А. Кузнецов, ктн, снс, А. М. Коваленко, А. М. Носик Харьковский университет Воздушных Сил им. Ивана Кожедуба

Как в коммерческих, так и в военных радиосетях все большее внимание в последнее время уделяется разработке и исследованию способов кодового разделения каналов как наиболее перспективных по многим характеристикам (высокие показатели помехозащищённости и скрытности радиосвязи, высокая энергетическая экономичность и экологичность терминального оборудования).

В системах радиодоступа с кодовым разделением каналов дискретные сигналы, поступающие на вход приемника, всегда обрабатываются с помощью корреляционных методов. В этой связи, разработка методов формирования больших ансамблей дискретных сигналов, исследование их корреляционных свойств является актуальной научной проблемой, имеющей важное научно-теоретическое значение, как для развития теории дискретных сигналов, так и для исследования прикладных вопросов построения цифровых систем связи.

Проведенные исследования показывают, что вопросу синтеза сложных сигналов, обладающих требуемыми корреляционными свойствами, посвящен ряд работ, в которых сформулирована задача синтеза сигналов в общем виде и рассмотрены характерные особенности синтеза. В тоже время, большинство известных методов обладает

рядом конструктивных недостатков, кроме того, не разработаны методы синтеза больших ансамблей слабо коррелированных между собой дискретных сигналов. Перспективным направлением в этом смысле являются методы, основанные на формировании дискретных сигналов с использованием кодовых последовательностей избыточных кодов. Этот подход позволяет, используя развитый математический аппарат алгебраической теории блоковых кодов, строить быстрые алгоритмы формирования псевдослучайных последовательностей. Кроме того, применение некоторых классов блоковых кодов позволяет получить улучшенные авто - и взаимно - корреляционные характеристики, аналитически связанные с конструктивными параметрами используемых кодов.

В докладе авторами излагаются основные результаты, полученные при разработке метода формирования дискретных сигналов на основе кодовых слов линейных блоковых кодов, результаты исследования их авто- и взаимно корреляционных свойств. Показано, что формируемые дискретные сигналы обладают улучшенными корреляционными свойствами, а методы их синтеза позволяют формировать большие ансамбли сигналов. Установлено, что повышение мощности ансамбля сигналов сопряжено со снижением дистанционных свойств сигналов, что, в конечном счете, приводит к увеличению уровней выбросов боковых лепестков функций корреляции синтезируемых сигналов. Разработана программная реализация предлагаемого метода синтеза, проведены экспериментальные исследования. Полученные результаты экспериментальных исследований совпадают с разработанными теоретическими положениями и подтверждают, таким образом, достоверность полученных результатов.

УДК 621.391

АЛГЕБРАИЧЕСКИЙ МЕТОД ДЕКОДИРОВАНИЯ ЛИНЕЙНЫХ БЛОКОВЫХ КОДОВ НА АЛГЕБРАИЧЕСКИХ КРИВЫХ В P^3

А. А. Кузнецов, ктн, снс, Харьковский университет Воздушных Сил им. Ивана Кожедуба,
И. В. Пасько, Военный институт ракетных войск и артиллерии СумГУ

Перспективным направлением в развитии теории помехоустойчивого кодирования являются коды, возникающие на алгебраических кривых (алгеброгеометрические коды). В ряде работ показано, что кодовые характеристики алгеброгеометрических кодов при большой длине лежат выше границы Варшамова-Гилберта. В тоже время известные методы декодирования алгеброгеометрических кодов ориентированы на узкий класс кодовых конструкций и, строго говоря, не позволяют реализовать их потенциальные свойства.

Следовательно, актуальным направлением исследований является разработка алгебраических методов декодирования алгеброгеометрических кодов, исследование сложности их практической реализации.

В докладе авторами излагаются основные научные и практические результаты, полученные при разработке алгебраического метода декодирования линейных блоковых кодов на алгебраических кривых в P^3. В основе предлагаемого подхода лежит алгебраическая процедура локализации ошибок, состоящая в поиске решений (точек) многочлена локаторов ошибок от трех неизвестных. Решения (точки) многочлена локаторов ошибок

однозначно локализуют (указывают месторасположение) ошибок в кодовом слове алгеброгеометрического кода.

Основное отличие от существующих методов состоит в рассмотрении алгебраических кривых в проективном пространстве P^3. Этот подход позволяет обобщить известные алгебраические процедуры декодирования алгебраических блоковых кодов на случай многочленов от трех переменных и расширить, таким образом, область их практического использования.

Разработанный метод позволяет свести задачу декодирования алгеброгеометрических кодов к решению системы линейных уравнений. Число неизвестных в системе уравнений задается конструктивными кодовыми характеристиками соответствующего кода. Разработан алгоритм, практически реализующий предлагаемый метод алгебраического декодирования. Оценена емкостная и временная сложность разработанного алгоритма. Показано, что сложность алгебраического декодирования предложенным методом растет полиномиально от длины и исправляющей способности кода.

Предложена программная реализация разработанного алгоритма декодирования, проведены экспериментальные исследования, результаты которых подтверждают достоверность полученных результатов.

Таким образом, в результате проведенных исследований получено общее решение задачи декодирования алгеброгеометрических кодов построенных по кривым в P^3. Перспективным направлением дальнейших исследований является исследование энергетического выигрыша от кодирования в каналах с независимыми и группирующимися ошибками.

УДК 681.32

КОДИРОВАНИЕ И ДЕКОДИРОВАНИЕ ДЛЯ МНОГОКАНАЛЬНЫХ СИСТЕМ ПЕРЕДАЧИ ДАННЫХ

Семеренко В. П., доцент
Винницкий национальный технический университет
sm@mail.vstu.vinnica.ua

Двоичные данные, которые параллельно передаются по q каналам связи можно рассматривать как многоканальный циклический $(q\times(n,k))$ код над полем Галуа $GF(2)$. Для упрощения математических преобразований целесообразно перейти от двоичного поля $GF(2)$ к полю расширения $GF(q)$, где $q=2^m$, m – положительное целое число. Основные свойства поля: количество элементов не превышает 2^m, каждый ненулевой элемент представляется как степень некоторого числа α, замкнутость всех элементов поля относительно операции умножения. Если каждый элемент поля $GF(q)$ представить в виде отдельного полинома степени m, тогда многоканальный циклический $(q\times(n,k))$ код является $(2^m-1,k)$ - кодом Рида-Соломона.

В отличие от традиционного трудоемкого описания кода Рида-Соломона с помощью алгебры полиномов предлагается использовать математический аппарат линейной последовательностной машины (ЛПМ), которая над полем Галуа $GF(q)$ может быть задана как автомат Мура с функцией состояний (переходов)

$$S(t+1)=A\times S(t)+B\times U(t) \qquad (1)$$

и функцией выходов

$$Y(t)=S(t), \qquad (2)$$

где A,B–характеристические матрицы;

U(t),Y(t),S(t)–векторы входной, выходной и состояний.

Если порождающий полином кода Рида-Соломона выразить через его корни α_j^i

$$g(x) = \alpha_0^i + \alpha_1^i X + \alpha_2^i X^2 + \ldots + \alpha_{2t-1}^i X^{2t-1} + X^{2t},$$

тогда характеристические матрицы ЛПМ можно записать следующим образом:

$$A = \begin{vmatrix} 0 & 0 & \cdots & 0 & \alpha_0^i \\ \alpha^0 & 0 & \cdots & 0 & \alpha_1^i \\ 0 & \alpha^0 & \cdots & 0 & \alpha_2^i \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \alpha^0 & \alpha_{2t-1}^i \end{vmatrix}, \qquad B = \begin{vmatrix} \alpha^0 \\ 0 \\ 0 \\ \cdots \\ 0 \end{vmatrix},$$

$i = 0,1,2,\ldots 2^m - 1$.

Процедура кодирования информационного k–разрядного вектора $I(x)$ над полем $GF(q)$ состоит из двух этапов. Вначале определяется вектор состояния $S(k)$ по формуле (1), когда в качестве вектора $U(t)$ используется вектор $I(x)$. Далее определяется вектор состояния $S(n)$ по формуле (1), когда в качестве вектора $U(t)$ используется $(n\text{-}k)$-разрядный нулевой вектор. Вектор $S(n)$ является контрольным вектором $R(x)$ для кодового вектора $C(x)=I(x)R(x)$. Процедура декодирования полученного из канала связи кодового вектора $C_e(x)$ также сводится к последовательному вычислению по формуле (1), векторов состояний ЛПМ той же структуры, которая использовалась при кодировании этого кодового вектора. Получение на n-м такте работы ЛПМ нулевого значения вектора $S(n)$ свидетельствует об отсутствии ошибок в кодовом векторе $C_e(x)$ в пределах корректирующей способности кода. В противном случае начинается поиск местоположения и значения ошибки.

УДК 681.518:004.93.1

ОЦІНКА ФУНКЦІОНАЛЬНОЇ ЕФЕКТИВНОСТІ ТЕЛЕКОМУНІКАЦІЙНОГО ІНФОРМАЦІЙНОГО ОСВІТНЬОГО СЕРЕДОВИЩА

В.О. Любчак, к.ф-м.н, Сумський державний університет

Вирішення проблеми підвищення ефективності функціонування телекомунікаційного інформаційного освітнього середовища (ТІОС) у зв'язку із стрімким розширенням мережі заочного та дистанційного навчання при збереженні кількості професорсько-викладацького складу та навчальних площ є першочерговою задачею вищої школи України. Оскільки на теперішній час існують необхідні технічні можливості створення систем керування (СК) навчальним процесом для різних форм навчання, то відставання у впровадженні таких систем пов'язано із методологічними та науково-теоретичними утрудненнями їх проектування. Складність розв'язання цієї задачі полягає в тому, що для оптимізації СК навчальним процесом для заочно-дистанційної форми необхідно розглядати узагальнений критерій ефективності, який враховує як інформаційну, так і технічну складові ТІОС. У цьому випадку перспективною може бути конструкція узагальненого критерію ефективності, запропонована І.В. Кузьміним, що враховує інформаційну спроможність системи та зведені витрати на функціонування системи. Пропонується узагальнений критерій ефективності ТІОС подати у вигляді добутку її перепускної інформаційної спроможності E_I та зведених витрат E_C на функціонування системи:

$$E = E_I E_B,$$

де

$$E_I = \sum_{l=1}^{L}\sum_{k=1}^{K}\{H_0^{(k,\,l)} - H_\gamma[D_1^{(k,\,l)},\ \beta^{(k,\,l)}]\ \}/\sum_{l=1}^{L}\sum_{k=1}^{K} t_{k,\,l}\,;$$

$$E_B = \sum_{m=1}^{M}\sum_{l=1}^{L}\sum_{k=1}^{K} C_{k,\,l,\,m}\,.$$

Тут $H_0^{(k,\,l)}$ – безумовна (апріорна) ентропія знань слухачів перед вивченням k-го модуля l-го дистанційного курсу (ДК); $H_\gamma(D_1^{(k,l)},\ \beta^{(k,\,l)})$ –апостеріорна ентропія, що характеризує залишкову невизначеність у слухачів після вивчення модуля; $D_1^{(k,l)}$, $\beta^{(k,\,l)}$ – точнісні характеристики належності векторів-реалізацій образу відповідним класам розпізнавання (рівням знань слухачів) за поточний модуль: перша достовірність та помилка другого роду відповідно; $t_{k,\,l}$ – час виконання модуля; $C_{k,\,l,\,m}$ – зведені витрати на функціонування ТІОС за один модуль; M, L, K – кількість режимів функціонування ТІОС, ДК і модулів відповідно. Нормований КФЕ ТІОС для рівноймовірних апріорних гіпотез $(\sum_{l=1}^{L}\sum_{k=1}^{K} H_0^{(k,\,l)} = L\log_2 K)$ подамо у вигляді:

$$E = \frac{L\log_2 K - \sum_{l=1}^{L}\sum_{k=1}^{K} H_\gamma[D_1^{(k,\,l)},\ \beta^{(k,\,l)}]\ \}\ \ C_{\min}T_{\min}}{L\log_2 K\ \ \sum_{l=1}^{L}\sum_{k=1}^{K} t_{k,\,l}\ \ \sum_{m=1}^{M}\sum_{l=1}^{L}\sum_{k=1}^{K} C_{k,\,l,\,m}}, \qquad (1)$$

де $C_{\min}$, $T_{\min}$ – вартість і час функціонування ТІОС у найбільш економічному режимі.

Аналіз критерію (1) показав, що він має глобальний екстремум в робочій області інформаційного критерію, значення якого, наприклад, при збільшенні витрат ТІОС за лінійною функцією змінюється за гіперболічним законом.

УДК 681.518:004.93.1

КОНЦЕПТУАЛЬНІ ПОЛОЖЕННЯ ТА ПЕРСПЕКТИВИ РОЗВИТКУ ІНФОРМАЦІЙНО-ЕКСТРЕМАЛЬНОЇ ІНТЕЛЕКТУАЛЬНОЇ ТЕХНОЛОГІЇ ПРОЕКТУВАННЯ СИСТЕМ КЕРУВАННЯ, ЩО НАВЧАЮТЬСЯ

А.С. Довбиш, д.т.н. (Сумський державний університет)

Перспектива подальшого розвитку автоматизованих систем керування (АСК) слабо формалізованими процесами різної природи полягає у переході від жорстких детермінованих методів керування до класифікаційних методів, що базуються на основі розпізнавання образів і самонавчання. Основною перевагою класифікаційного керування є надання АСК властивості адаптивності, що дозволяє системі ефективно функціонувати за умов апріорної невизначеності, інформаційних і ресурсних обмежень. На кафедрі інформатики Сумського державного університету розроблено науково-теоретичні та інструментально-практичні основи аналізу і синтезу адаптивних АСК, що навчаються, в рамках інформаційно-екстремальної інтелектуальної (ІЕІ) технології. За ІЕІ-технологією розроблено базовий метод синтезу таких АСК, який ґрунтується на оцінці інформаційної спроможності системи і дозволяє оптимізувати просторово–часові параметри її функціонування з метою побудови за навчальною матрицею безпомилкових вирішальних правил.

Основними принципами, на яких побудовано ІЕІ-технологію, є принципи максимізації кількості інформації шляхом введення додаткових обмежень на параметри функціонування системи, дуальності оптимального керування, редукції простору ознак розпізнавання (ОР), квантовості подання знань, рандомізації навчальної вибірки та інші.

IEI-технологія базується на детерміновано-статистичному підході до розпізнавання образів, її наукова новизна полягає в оптимізації структурованих просторово-часових параметрів функціонування АСК шляхом трансформації в процесі навчання відношення схожості на нечіткому розбитті простору ОР на класи у відношення еквівалентності. При цьому оптимізація параметрів функціонування здійснюється за ієрархічною ітераційною процедурою пошуку глобального максимуму інформаційного критерію функціональної ефективності (КФЕ) навчання АСК в робочій області визначення його функції. Побудова безпомилкового за навчальною матрицею класифікатора у дискретному субпарацептуальному просторі ОР на кожному кроці навчання здійснюється шляхом цілеспрямованих допустимих перетворень апріорного нечіткого розподілу реалізацій образу у чітке розбиття. При цьому одночасно здійснюється відновлення контейнерів класів розпізнавання в радіальному базисі, що характерно для задач контролю та керування, де розподіли реалізацій образу є уніномодальними. Таким чином, у рамках IEI-технології підвищення ефективності машинного навчання АСК за умови нечіткої компактності реалізацій образу досягається шляхом цілеспрямованої зміни значень ОР. У рамках IEI-технології за МФСВ розроблено та програмно реалізовано базові алгоритми компараторного розпізнавання, кластер-аналізу та самонавчання, класифікаційного самонастроювання та прогнозування.

Отримані у рамках IEI-технології наукові результати синтезу АСК, що навчаються, успішно апробовано при розв'язанні практичних задач підвищення ефективності керування хімічними процесами у ВАТ "Сумихімпром", автофокусування електронного мікроскопа (ВАТ "Selmi" м. Суми), оперативного діагностування онкопатологій та інше.

2000 MSC primary 00A05; sec. 00A69, 00A71, 03E99

QUANTISETS AND THEIR QUANTIRELATIONS

L.G.Gelimson, Ph.D., D.Sc., RUAG Munich, iasco@web.de

The sets with either unit or zero quantities of their possible elements, the fuzzy sets with intermediate quantities in the indeterminate case only, and the multisets whose element quantities are any cardinal numbers cannot express many typical collections, e.g., that of half an apple and a quarter of a pear. For concrete (mixed) quantities, e.g., "5 *l* fuel", there is no suitable mathematical model and no known operation, say between "5 *l*" and "fuel" (neither "5 *l*" × "fuel" nor "fuel" × "5 *l*"). Set operations with absorption are only restrictedly reversible and hinder constructing universal quantity degrees. Elastic mathematics by the author and its fundamental quantianalysis introduce corresponding adequate concepts.

Notation 1. A set quantioperation (quantirelation) is a set operation (relation) such that the actual quantity of each element of its operands (objects) is exactly taken into account, and can be denoted by the sign of a similar usual set operation (relation, respectively) with a little circle on the right above by noncoinciding results of the operation and the quantioperation.

Definition 2. A *quantiset* is a non-positional quantiunion of *quantielements* of the form ${}_qa$, each of them consisting of its *element* (*basis*), say a, with its *own quantity* (named: *uniquantity*), say q, inside in the quantiset, the elements and element quantities being any objects (possibly fuzzy etc.):
$A=^\circ\{...,\ {}_qa,...,\ {}_rb,...,\ {}_sc,...\}^\circ=^\circ...\cup^\circ{}_qa\cup^\circ...\cup^\circ{}_rb\cup^\circ...\cup^\circ{}_sc\cup^\circ...$.
Quantifying is a set quantioperation of the form ${}_q$: $a\to{}_qa$.
The *empty quantielement* ${}_0a=^\circ{}_q\#$ (# the *empty element*, $\#\in\varnothing$) is the empty set $\varnothing$ and has to be *reduced* to *canonical form* ${}_0\#$.

In a quantiset, all the quantielements with the same basis have to be *reduced* (*collected*) by adding their own quantities:

$$\dots \cup^{\circ}{}_{q}a \cup^{\circ} \dots \cup^{\circ}{}_{r}a \cup^{\circ} \dots \cup^{\circ}{}_{s}a \cup^{\circ} \dots =^{\circ}{}_{\dots + q + \dots + r + \dots + s + \dots} a.$$

Quantisets are *quantiequal* if, after the reduction, they contain all quantielements in common.

Outside quantifying a quantiset means multiplying the inside quantities by the outside one:

$${}_{t}A =^{\circ}{}_{t}\{\dots, {}_{q}a, \dots, {}_{r}b, \dots, {}_{s}c, \dots\}^{\circ} =^{\circ}\{\dots, {}_{tq}a, \dots, {}_{tr}b, \dots, {}_{ts}c, \dots\}^{\circ}.$$

Example 3. {$_{2\ loaves}$bread, $_{1.5\ kg}$meat, $_{1/2}$water-melon, $_{\$\ -25}$money, $_{-2\ h}$time, $_{-3\ l}$petrol} is a possible result of shopping.

Definition 4. An *ordinary set* is a reduced quantiset with unit element quantities only.

Definition 5. An *algebraic quantiunion of quantisets* is a quantiset quantiunifying all quantielements of the quantisets, each quantity in the subtrahends changing sign:

$$\dots \cup^{\circ} \{\dots, {}_{q}a, \dots\}^{\circ} \setminus^{\circ} \dots \setminus^{\circ} \{\dots, {}_{r}b, \dots\}^{\circ} \cup^{\circ} \dots \cup^{\circ} \{\dots, {}_{s}c, \dots\}^{\circ} \setminus^{\circ}$$
$$\dots \setminus^{\circ} \{\dots, {}_{t}d, \dots\}^{\circ} \cup^{\circ} \dots =^{\circ} \{\dots, {}_{q}a, \dots, {}_{-r}b, \dots, {}_{s}c, \dots, {}_{-t}d, \dots\}^{\circ}.$$

Definition 6. An *algebraic addition* or *unification* is called *algebraically commutative* and/or *associative* if it becomes commutative and/or associative provided that each negative operation sign is avoided by changing the own signs of the corresponding operands, say:

$$-3 - 5 + 2 - (-4) + (-1) = (-3) + (-5) + 2 + 4 + (-1),$$
$${}_{q}a \setminus^{\circ} {}_{r}b \cup^{\circ} {}_{s}c \setminus^{\circ} {}_{t}d =^{\circ} {}_{q}a \cup^{\circ} {}_{-r}b \cup^{\circ} {}_{s}c \cup^{\circ} {}_{-t}d.$$

Corollary 7. *If the quantities of each basis in quantisets form a commutative additive group, then the algebraic quantiunification of the quantisets is an algebraically commutative and associative set quantioperation, and the quantisets form a commutative additive group with zero* $_{0}\#$.

Notation 8. For a one-variable basis function (a completely algebraically additive one-variable quantity function), quantifying the preimage means quantifying (multiplying) the image, say $f({}_{q}x) = {}_{q}f(x)$ ($Q({}_{x}a) = xQ(a)$, respectively).

The introduced concepts apply to information problems etc.

УДК 621.391

СРЕДНЯЯ ДЛИНА ДВОИЧНЫХ БИНОМИАЛЬНЫХ ЧИСЕЛ ПРОИЗВОЛЬНОГО ДИАПАЗОНА

Кулик И.А., к.т.н. доц.
Сумский государственный университет
E-mail: kulik@pe.sumdu.edu.ua

Существуют методы биномиального кодирования, основанные на неравномерных биномиальных числах, не уступающие, а в некоторых случаях превосходящие по эффективности широко известные помехоустойчивые или экономичные коды. Распространению биномиальных кодов препятствует, в частности, неизученность вопроса о средней длине неравномерных биномиальных чисел. И если задача вычисления средней длины указанных чисел для полного диапазона биномиальной системы счисления с параметрами n и k автором была решена, то вопрос о средней длине биномиальных чисел для произвольного диапазона оставался нераскрытым.

В настоящем докладе предлагается анализ структуры двоичного неравномерного биномиального кода, на основании которого производится точная оценка его средней длины для произвольного диапазона чисел $X_z = (x_1 x_2 ... x_i ... x_r)$; где x_i – биномиальные разряды числа, $\max(k, n-k) \le r \le n-1$. В лексикографическом порядке неравномерных биномиальных чисел с параметрами n и k при каждом последующем исключении старшего по весу i-го биномиального разряда обнаруживается лексикографический порядок биномиальных чисел с параметрами $n-i$ и $k-q_i$, где $q_i = x_1 + x_2 + ... + x_{i-1}$. Это

обстоятельство позволяет воспользоваться уже известной формулой средней длины для полного диапазона, но уже при параметрах $n-i$ и $k-q_i$:

$$L(n-i,k-q_i)=\frac{(k-q_i)((n-i)-(k-q_i))((n-i)+2)}{((k-q_i)+1)((n-i)-(k-q_i)+1)}.$$

Обозначив через X_1 и X_2 соответственно начальное и конечное числа произвольного диапазона, среднюю длину принадлежащих ему неравномерных биномиальных чисел можно вычислить как:

1) для случая $X_1=0$, $X_2\le C_n^k$

$$L_{cp}[0,X_2]=\frac{\sum_{i=1}^{r} x_i\left[L(n-i,k-q_i)+1\right]\cdot N(n-i,k-q_i)}{X_2+1},$$

где $N(n-i,k-q_i)=C_{n-i}^{k-q_i}$ – количество двоичных неравномерных биномиальных чисел с параметрами $n-i$ и $k-q_i$; $x_1x_2...x_i...x_r$ – биномиальные разряды числа X_2+1;

2) для случая $X_1\le X_2$, $X_1\ne 0$, $X_2\le C_n^k$

$$L_{cp}[X_1,X_2]=\frac{(X_2+1)L_{cp}[0,X_2]-(X_1+1)L_{cp}[0,X_1]}{X_2-X_1}.$$

На основе полученных соотношений возможна разработка математически более строгих способов оценки сложностных характеристик алгоритмов биномиального кодирования и декодирования, которые оперируют неравномерными биномиальными числами произвольного диапазона, а также получение эффективных способов решения задач информационного характера таких, как определение степени биномиального сжатия, нахождение информационной избыточности биномиальных чисел, информационной нагрузки биномиальных разрядов и т.д.

УДК 681.518:004.93.1

РЕДУКЦІЯ ПРОСТОРУ ОЗНАК РОЗПІЗНАВАННЯ ПРИ НАВЧАННІ СИСТЕМ КЕРУВАННЯ ДИСТАНЦІЙНИМ НАВЧАННЯ

Шелехов І.В., асистент каф. інформатики СумДУ

Розвиток інформаційно-екстремальної інтелектуальної (ІЕІ) технології дозволяє знаходити нові застосування методам та алгоритмам навчання систем керування в соціальних, економічних та інших не технічних сферах. Крім класичних задач навчання та екзамену нову інтерпретацію отримали і проблеми, що тісно з ними пов'язані. Розглянемо задачу оптимізації словника ознак розпізнавання (ОР) в системах керування дистанційним навчанням (СКДН) в рамках методу функціонально-статистичних випробувань (МФСВ). Зважаючи на те, що словник ОР в СКДН представляє собою набір множин еквівалентних (взаємозамінних) тестів, які використовуються для перевірки рівня знань студентів після вивчення окремих модулів або матеріалу в цілому, реалізацією кожної ОР є певна відповідь, а алфавіт класів розпізнавання, відповідно до загальноприйнятої системи оцінювання, складається з чотирьох елементів („відмінно", „добре", „задовільно", „незадовільно"), то задача синтезу СКДН в рамках ІЕІ технології буде зводитися до побудови деяким оптимальним в інформаційному розумінні способом розбиття простору ОР на класи еквівалентності. При цьому актуальність задачі оптимізації словника ОР пов'язується не тільки з проблемами багатовимірності, надлишковості даних, втрати інформації, але й релевантності тестів, оптимізації їх кількості з точки зору навчального процесу, формування класів взаємозамінних

тестів, корекції матеріалів дистанційного курсу тощо.

Існують дві основні категорії методів, що використовуються для редукції простору ОР: зниження розмірності – спрощення гіперпростору шляхом трансформування його осей; селекція ОР – вибір підмножини інформативних ОР з початкового словника без зміни осей. Головна відмінність між ними полягає у відношенні до структурних зв'язків образів – семантики (*semantics*). Селекція ОР, на відміну від методів зниження розмірності не змінює семантику безповоротно, що є прийнятним для підвищення ефективності СКДН, що навчаються. За способами оцінки оптимальності словника методи селекції ОР поділяють на фільтри (*Filters*) – методи попередньої обробки та вкладені методи (*Wrappers*). Фільтри, використовуючи елементи теорії інформації, є найбільш універсальними методами оцінки, але вони безпосередньо не аналізують класифікаційні особливості ОР. Вкладені методи навпаки базуються на оцінці ефективності навчання, що вказує на наявність певних симбіотичних відносин між ними та алгоритмами навчання системи. Завдяки цьому вкладені методи характеризуються більш якісними, ніж фільтри, результатами, але втрачають в оперативності та універсальності. IEI-технологія дозволяє поєднати переваги даних груп методів селекції ОР при розв'язані задач аналізу і синтезу СКДН, що навчаються.

Практична реалізація алгоритму редукції простору ОР використовувала метод послідовної спадної селекції, який полягає в послідовному видаленні ОР з найменшою інформативністю. Оцінка інформативності проводилася безпосередньо в процесі навчання СКДН в рамках IEI технології за МФСВ, де як критерій функціональної ефективності використовувалась інформаційна міра Кульбака. Результати оптимізації словника з 28 тестів по дисципліні „Інтелектуальні системи", виявили 4 малоінформативні тести, видалення яких підвищує ефективність навчання.

УДК 681.518:004.93.1

КЛАСТЕРІЗАЦІЯ РЕЗУЛЬТАТІВ ТЕСТУВАННЯ ПРИ ДИСТАНЦІЙНОМУ НАВЧАННІ

С.О. Петров, асистент СумДУ

При синтезі адаптивних систем керування дистанційним навчанням (СКДН), на етапі формування початкової конфігурації розбиття простору ознак на класи розпізнавання доцільним є застосування алгоритмів кластер-аналізу, що дозволяє:

- автоматизувати процес формування навчальної матриці;
- підвищити ефективність функціонування СКДН, а відповідно й ефективність навчального процесу.

Існуючи методи кластерізації поділяють на дві групи: декомпозіційні, та ієрархічні. Декомпозіційні (k-кластеризація) – це методи, які базуються на однозв'язності об'єктів і контейнерів розпізнавання, ієрархічні – працюють в тих випадках якщо деяка достатньо велика група об'єктів включає в себе групу меншого розміру.

Особливість відомих алгоритмів ієрархічної класифікації (Single Link, Complete Link, Group Average) полягає в тому, що вони розбивають вектори реалізації на кластери, шляхом розбиття їх на ієрархічні групи, що дозволяє зменшити вплив багато вимірності. Такі методи кластеризації ще мають назву агломеративні, в загальному випадку, використовують махалонобіусову метрику, яка в частковому випадку має вигляд:

$$d_{ij}^2 = \sum_{k=1}^{q} \nu_k \left(z_j^{(k)} - z_j^{(k)} \right)^2 \qquad (1)$$

де $z_i^k = (U_k', X_i)$ – одновимірна проекція лінійних комбінацій вхідних змінних; $\nu_k = \varphi(Q_k)$ – лінійна

комбінація $U_i, \forall i$ в новому базисі коваріаційної матриці ковариационной матриці S; $\varphi(\cdot)$ - деяка монотонно-зростаюча функція Ідея алгоритмів декомпозиційної кластеризації (K-means) ідея яких полягає в представленні кластера у вигляді центроїда, який є центром мас усіх векторів що входять в кластер. Тут вхідними величинами є матриця S та число k, вводиться деяка оціночна функція $c:\{X:X\le S\}\to R^+$ – вартість кластера, потім ставиться оптимізаційна задача вибору такої множини векторів, яка буде мінімізувати вартість кластера.

$$\min \sum_i c(S_i),\ i=1...k \qquad (2)$$

Основними недоліками існуючих методів кластеризації є відсутність загального критерію оцінки оптимальності побудови начальної конфігурації класів та немає загальних рекомендацій по апріорному визначенню числа k.

Метод, який розроблений автором базується на гібридному алгоритмі, в якому комбінуються критерії (1) і (2), та проводиться обчислення ентропійного критерію Шенона, як показника якості розбиття, який обчислюється рамках інформаційно-екстремальної технології за методом функціонально статистичних випробувань. Цей метод дозволяє з заданою ефективністю розв'язувати задачу кластер-аналізу, маючи загальний критерій оцінки якості розбиття та не потребуючи апріорно визначеного значення числа k. Розроблено практичну реалізацію алгоритму, та проведено експеримент по кластеризації даних які отримані з відповідей студентів на тестові запитання. За результатами тестування було сформовано навчальну матрицю, яка була кластеризована на чотири класи, які відповідають оцінкам "відмінно ", "добре", "задовільно", "незадовільно".

УДК 681.518:004.93.1

КЛАСИФІКАЦІЙНЕ КЕРУВАННЯ ІНВЕСТИЦІЯМИ

В.А. Тронь, асп. (Сумський державний університет)

Складність і невизначеність процесів на ринках цінних паперів перетворили професійну діяльність на фондовому ринку скоріше на мистецтво ніж на науку. У доповіді розглядається задача застосування для оптимального формування інвестиційного портфелю здатної навчатися системи підтримки прийняття рішень (СППР), синтезованої в рамках інформаційно-екстремальної інтелектуальної (ІЕІ) технології за методом автоматичної класифікації – методом функціонально-статистичних випробувань (МФСВ), що ґрунтуються на прямій оцінці інформаційної спроможності системи за умов апріорної невизначеності, нечітких даних, інформаційних І ресурсних обмежень.

Нехай дано алфавіт класів розпізнавання $\left\{X_m^0 \middle| m=\overline{1,M}\right\}$, де M — кількість класів (портфелів), навчальна матриця $\left\|y_{m,i}^{(j)} \middle| i=1,N, j=1,n\right\|$, де N, n – кількість ознак розпізнавання (нормовані показники) і реалізацій образу відповідно, і відомий вектор параметрів функціонування СППР. Треба на етапі навчання побудувати оптимальне (тут і далі в інформаційному розумінні) розбиття простору ознак на класи за умови, що інформаційний критерій функціональної ефективності (КФЕ) набуває максимуму в робочій області визначення його функції, а на етапі екзамену за побудованим на етапі навчання СППР вирішальним правилом визначити належність реалізації образу, що розпізнається, до відповідного класу розпізнавання із заданого алфавіту. Нехай портфель інвестицій складається з п'яти типів активів: акції підприємств, облігації підприємств, ощадні сертифікати, кредитний договір, облігації державних позик. Кожен актив має дві ознаки: доходність і

ризик. Таким чином, структурований словник складався із 10 ознак розпізнавання функціонального стану ринку цінних паперів.

При формуванні навчальної матриці бралися показники 20 компаній, що представляють 60% ринку цінних паперів України які характеризували середні дохідності та ризики активів. Оптимізація просторово-часових параметрів навчання в процесі побудови гіперсферичного класифікатора за МФСВ здійснювалася за алгоритмом послідовної оптимізації контрольних допусків на ознаки розпізнавання із використанням базової процедури LERNING, що обчислює значення інформаційного критерію функціональної ефективності за Кульбаком, здійснює на кожному кроці навчання пошук його глобального максимуму в робочій області визначення функції критерію та визначає оптимальні геометричні параметри контейнерів класів розпізнавання. У результаті навчання СППР було побудовано оптимальні контейнери для трьох класів розпізнавання, що характеризують ринковий, агресивний і консервативний портфелі інвестицій. Аналіз результатів навчання СППР показав, що контейнери не перетинаються в просторі ознак розпізнавання. Це дозволяє стверджувати, що побудований гіперсферичний класифікатор є безпомилковим за навчальною матрицею і у режимі екзамену здатний забезпечити повну ймовірність правильного прийняття рішень, наближену до асимптотичної, яка характеризує ефективність навчання СППР. Умовою високої достовірності СППР в режимі екзамену є формування екзаменаційної навчальної матриці за тим самим правилом, що і для навчальної матриці, що забезпечує їх однакові структурованість, статистичну стійкість і однорідність.

Таким чином, вперше розроблено в рамках IEI-технології інформаційне та програмне забезпечення здатної навчатися СППР формування інвестиційного портфелю, яке дозволяє оперативно і з високою достовірністю в режимі екзамену приймати рішення на ринку цінних паперів.

УДК 681.518:519.718

КОНЦЕПТУАЛЬНАЯ СТРУКТУРА ЭКСПЕРТНОЙ СИСТЕМЫ ИТОГОВОЙ ОЦЕНКИ ЗНАНИЙ

В.С. Ноздренков, СумГУ, sfab@bk.ru

Интенсивное развитие процесса информатизации системы образования невозможно без применения современных информационных технологий. Для разработки и реализации автоматизированных обучающих систем необходимо использовать методы и средства, созданные в рамках исследований по нечеткой логике, нейровычислениям, генетическим вычислениям и вероятностным вынислениям, что позволяет существенно повысить функциональные возможности разрабатываемых систем.

Предлагается следующая структура экспертной системы итоговой оценки знаний (см. рис. 1).

База данных. В ней содержится информация о полученных оценках, весовые коэффициенты заданий, время, затраченное на выполнение конкретного задания, списки студентов в группах, модели предметных областей, графики модульно-рейтингового контроля и т.д.

База знаний. В базе знаний заложен опыт эксперта (преподавателя) в данной предметной области. База знаний должна быть выполнена в виде иерархической структуры, что позволит избежать проблемы размерности, которая обусловлена тем, что при большом количестве входных переменных построение системы высказываний о неизвестной зависимости «вход-выход» значительно усложняется. В связи с этим целесообразно выполнить классификацию входных переменных и построить на ее основе так называемое дерево вывода, которое будет

представлять собой систему иерархически связанных нечетких баз знаний меньшей размерности.

Подсистема нечеткая логика. В ней заложены лингвистические переменные и их термы, для которых определены соответствующие функции принадлежности. Реализован алгоритм нечеткого логического вывода.

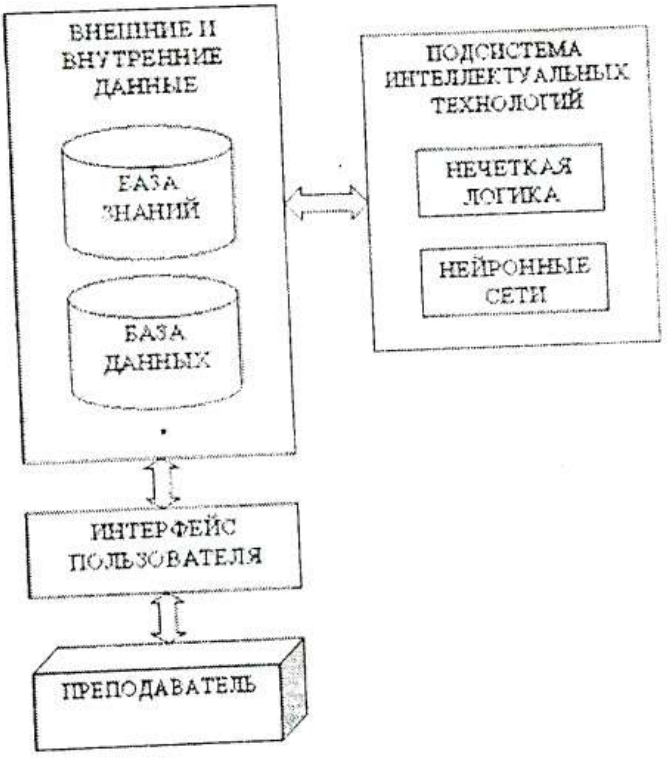

Рис. 1. Концептуальная структура экспертной системы

Подсистема нейронные сети. В ней определена структура нейронной сети и характеристики ее нейронов.

Интерфейс пользователя предоставляет преподавателю возможность вводить исходные данные, настраивать параметры системы, получать итоговые результаты в удобном для него виде.

УДК 681.3.07

СЕМЕЙСТВО СИММЕТРИЧНЫХ БЛОЧНЫХ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ ЗАЩИТЫ ИНФОРМАЦИИ С ДИНАМИЧЕСКИ УПРАВЛЯЕМЫМИ ПАРАМЕТРАМИ ШИФРОВАНИЯ

Белецкий А.Я., д-р техн. наук, профессор,
Белецкий А.А., мл. научный сотр., Национальный авиационный университет (E-mail: abel@nau.edu.ua)
А.А.Кузнецов, канд.техн.наук, ст. научный сотр.
Харьковский университет воздушных сил
(E-mail: kuznetsov_alex@rambler.ru)

В данном докладе предлагается достаточно гибкая к изменению параметров шифрования симметричная блочная криптосистема, названная системой ***RSB* - 32.**. Аббревиатура ***RSB*** происходит от ключевых слов ***R****ound,* ***S****tep,* ***B****lock* – подчеркивая тем самым, что основными для криптоалгоритма являются раундовые преобразования (***R***), разбитые на определенное число шагов (***S***), а действие алгоритма осуществляется над блоками (***B***) открытого или закрытого текстов, причем размер раундового ключа (как элемента общего ключа) составляет 32 бита. ***RSB*** – это итерационный блочный шифр, который доставляет уникальную возможностью по изменению как размеров секретных ключей, так и числа шагов (раундов) шифрования.

Отличительная особенность ***RSB*** алгоритма состоит в том, что в нем используется оригинальная функция шифрования типа *скользящего кодирования* (свертки), которая обеспечивает не только глубокое перемешивание открытого текста, но и участвует в формировании *блочного раундового ключа* для очередного шифруемого блока. Общий ключ в ***RSB*** шифре образуется конкатенацией (объединением) ***r*** 32–разрядных раундовых ключей, являющихся *базовыми раундовыми ключами.*

Основные параметры ***RSB*** шифра:

- Длина раундового ключа - 32 бита.
- Длина общего (шагового) ключа: $r * 32$, $r = 1, 2, \ldots$
- Число шагов шифрования: $s = 1, 2, \ldots$
- Общее число раундов шифрования: $r * s$.
- Размер блока: 256 бит.

- Размер элементов скользящего кодирования - 32 бита.
- Размер элементов нелинейной замены: 8 бит.

Основная идея составных, или композиционных, блочных шифров состоит в построении криптостойкой системы путем многократного применения относительно простых криптографических преобразований, которые называются *криптографическими примитивами* (функциями шифрования). В качестве криптографических примитивов в ***RSB*** алгоритме используются:

- стохастическая круговая прокрутка шифруемого блока;
- скользящее кодирование 32-разрядных элементов блока;
- стохастическая нелинейная замена байтов блока;
- стохастическая перестановка байтов в пределах блока.

Перечисленные криптографические примитивы обеспечивают в ***RSB*** шифре стохастические операции циклических сдвигов блоков, свертки, а также нелинейных замен и перестановок байтов в пределах блока, причем указанные преобразования выполняются в каждом блоке под управлением индивидуальных блочных раундовых ключей, зависящих не только от значения секретного базового раундового ключа, но и всего шифруемого текста, предшествующего преобразуемому блоку. Применение оригинальных примитивов типа лево- и правостороннего скользящего кодирования в ***RSB*** алгоритме позволило устранить один из серьезных недостатков классических блочных шифров, который проявляется в том, что одинаковым блокам открытого текста соответствуют одинаковые блоки шифротекста. В ***RSB*** шифре указанный недостаток устраняется как операциями скользящего кодирования (свертки 32-разрядного базового ключа с соответствующими по размеру элементами текста), так и за счет различия в двух любых блочных раундовых ключах, управляющих криптопреобразованиями соответствующих блоков шифруемого текста.

Как показали результаты статистических испытаний ***RSB*** криптосистемы, эффективность алгоритма зашифрования, оцениваемая количеством тестов в пакете ***NIST STS***, в котором тестирование успешно прошло больше 99% и соответственно 96 % последовательностей, оказалось на уровне не ниже российского алгоритма ***ГОСТ*** 28147-89 и превосходит в отдельных случаях эффективность широко используемых зарубежных стандартов криптографической защиты, таких как ***DES***, ***IDEA*** и ***AES*** (*Rijndael*).

УДК 681.3.07

УОЛША ГЕНЕРАТОРЫ ПОТОЧНОГО БЛОЧНО-СБАЛАНСИРОВАННОГО ШИФРОВАНИЯ

Белецкий А.Я., д-р техн. наук, профессор,
Белецкий А.А., мл. научный сотр.,
Национальный авиационный университет
(E-mail: abel@nau.edu.ua)
Кузнецов А.А.,,канд. техн. наук, ст. научный сотр.
Харьковский университет воздушных сил
(E-mail: kuznetsov_alex@rambler.ru)

При шифровании больших объемов данных (таких, например, как речь или «живое видео») в реальном времени применяются *поточные* криптографические системы (шифры, генераторы). Суть поточных шифров заключается в сложении по модулю 2 битов потока ключей с битами сообщений. В современных криптосистемах поток ключей (*поточный ключ*) генерируется из короткого основного (*базового*) ключа с помощью однозначно определенных детерминированных алгоритмов, осуществляющих так называемую процедуру *разворачивания ключа*.

Поточные шифры принято разделять на *синхронные* и *самосинхронизирующиеся* (или *асинхронные*). В синхронных поточных шифрах поточный ключ (*гаммирующая функция* или *гамма*) формируется независимо от входной последовательности, каждый элемент (бит, байт и т.п.) которой таким образом шифруется независимо от других элементов. Если же поточный ключ зависит от исходных данных и результата их шифрования, то шифрование называют самосинхронизирующимся. Большинство реализаций поточного шифрования являются синхронными.

В докладе предлагается ***WKG*** семейство поточных криптографических систем, размер секретного ключа ***K*** которых составляет 256 бит. Аббревиатура ***WKG*** порождается ключевыми словами ***W**alsh **K**eystream **G**enerator* (Уолша генератор гаммы). Отличительная особенность семейства ***WKG*** шифров состоит в том, что за один шаг шифрования в системе формируется 256-разрядный блок гаммы, образующийся в результате

стохастической перестановки и циклических сдвигов (перемешивания) элементов (битов) *сбалансированной* (1,0)-матрицы Уолша 16-го порядка. Блок битов (обязательно четного порядка) считается сбалансированным, если содержит одинаковое число нулей и единиц. Симметрическая матрица Уолша трансформируется в сбалансированную (1,0)-матрицу двумя приемами. Во-первых, заменой элементов –1 на 0. И, во-вторых, приведением элементов верхней строки матрицы (состоящей из одних положительных единиц) к сбалансированной последовательности, в качестве которой выбрана чередующаяся (0,1)-последовательность.

Алгоритмы ***WKG*** строятся из двух этапов: *управляющей фазы*, в ходе которой переопределяется состояние регистров ключевого поля и *вычислительной фазы*, в ходе которой формируется 256-битная гамма функция. Различные способы реализации этих двух фаз приводят к различным вариантам ***WKG*** генераторов, включая синхронные и самосинхронизирующиеся шифры. Перечисленным фазам функционирования ***WKG*** алгоритма отвечают два его базовых криптографических объекта. Первым объектом шифрующей системы является управляющий блок, представляющий собой квадратную *матрицу ключевого поля* 16-го порядка, в которую на этапе инициализации загружается базовый 256-битный секретный ключ ***K***. Вторым объектом также служит квадратная матрица 16-го порядка (***W***-матрица), предназначенная для формирования 256-битных блоков сбалансированных псевдо случайных последовательностей (гамма функций). На этапе инициализации в эту матрицу загружается стартовая сбалансированная матрица Уолша-Пэли. Состояние второго криптографического объекта (регистров ***W***-матрицы) находится в прямой зависимости от состояния первого объекта – матрицы (совокупности 16-разхрядных регистров) ключевого поля. Алгоритм изменения состояния регистров ***W***-матрицы сохраняется неизменным для всех типов семейства ***WKG*** шифров, в то время как алгоритм управления состоянием регистров матрицы ключевого поля меняется каждый раз при переходе к новому типу генератора.

В докладе приводится сравнительный анализ эффективности (по критерию качества статистических свойств псевдослучайных последовательностей) четырех типов Уолша генераторов, включая линейные и нелинейные, синхронные и асинхронные. В числе последних рассматривается поточный самосинхронизирующийся Уолша генератор с нелинейной обратной связью по шифротексту.

УДК 621.391

МЕТОД ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ КАСКАДНЫХ КОДОВЫХ КОНСТРУКЦИЙ

Кузнецов А. А., ктн, снс, Харьковский университет Воздушных Сил им. Ивана Кожедуба,
Грабчак В. И., Военный институт ракетных войск и артиллерии СумГУ

Перспективным направлением в развитии комплексных механизмов обеспечения информационной скрытности и достоверности передачи данных являются теоретико-кодовые схемы – секретные системы теоретической стойкости, сложность взлома которых сводится к решению теоретико-сложностной задачи декодирования случайного кода. Их практическое использование позволяет реализовать в одном устройстве методы канального кодирования и специального преобразования данных. В тоже время, как показывает проведенный анализ, для реализации известных методов необходимы огромные объемы ключевых данных (0,5 – 1,5 Мбит). Кроме того, неприемлемо высоки временная и емкостная сложности алгоритмов формирования и декодирования кодограмм.

Для устранения указанных недостатков предлагается использовать каскадные кодовые конструкции. Среди каскадных кодов наиболее общим классом являются обобщенные каскадные коды, применение которых, позволяет без значительного ухудшения кодовых параметров снизить сложность их практической реализации. Кроме того, как показано в докладе, применение обобщенных каскадных кодов для построения теоретико-кодовых схем позволяет обеспечить эффективную защиту информации со сравни-

тельно небольшими объемами ключевых данных. Проведенные исследования способов маскирования обобщенного каскадного кода показали, что наиболее приемлемым по соотношению «число переборов оптимального статистического опробования/объем ключа» является маскирование кодов второй ступени и использование обобщенных каскадных кодов высокого порядка. С учетом полученных результатов разработаны каскадные схемы защиты информации, позволяющие обеспечить требуемые показатели информационной стойкости и достоверности передачи данных. Проведенные исследования стойкости разработанных схем к криптоаналитическим атакам противника показали, что наилучшей стратегией противника является применение атаки с подобранным открытым текстом и с подобранной кодограммой. Однако удачная реализация любой из рассмотренных атак не позволит противнику однозначно получить правило быстрого декодирования кода для восстановления информационного содержания передаваемых сообщений. Анализ полученных экспериментальных результатов статистической безопасности показывает, что разработанные схемы позволяют эффективно выполнять криптографическое преобразование данных – по своим показателям статистический портрет предлагаемой схемы не уступает лучшим известным криптоалгоритмам, принятым в качестве национальных стандартов ведущих государств мира.

Таким образом, в результате проведенных исследований показано, что применение разработанных каскадных теоретико-кодовых схем позволяет эффективно обеспечить передачу сообщений в пункты приема с заданной точностью и сохранять в тайне от противника смысловое содержание передаваемых сообщений и, таким образом, обеспечить требуемые показатели достоверности и информационной скрытности передачи данных в АСУВ.

УДК 004.056.55

ОБ ОДНОЙ ВЕРСИИ ТЕОРЕТИКО - ЧИСЛОВОЙ ТЕОРЕМЫ ФЕРМА

В.А.Фильштинский к.ф-м.н., доцент, СумДУ
e-mail: father-4f@yandex.ru

Теорема Ферма утверждает, что в группе вычетов $\mathbb{Z}_p$ с простым модулем p

$$x^N \equiv 1(\mathrm{mod}\, p), \quad N = p-1$$

для любого $x \in \mathbb{Z}_p, x \neq 0$.

Здесь, вместо последовательности многочленов $x^0, x^1, x^2, \ldots$ рассматривается последовательность $P_0(x), P_1(x), P_2(x), \ldots$, заданная соотношением

$$P_{n+2}(x) = c \cdot x \cdot P_{n+1}(x) - P_n(x), \; P_0(x) = \alpha, P_1(x) = \beta \cdot x,$$

где $c, x, \alpha, \beta \in \mathbb{Z}_p$.

Доказано следующее предложение.

Если последовательность $\{P_n\}$ есть последовательность многочленов Чебышева, т.е. $c = 2, \alpha = 1, \beta = 1$, то

$$P_N(x) \equiv 1 = P_0(x)(\mathrm{mod}\, p), P_{N+1}(x) \equiv x = P_1(x)(\mathrm{mod}\, p),$$

где $N = \dfrac{p^2 - 1}{2}$.

Для любых других троек (c, α, β)

$$P_N(x) \equiv P_0(x)(\mathrm{mod}\, p), P_{N+1}(x) \equiv P_1(x)(\mathrm{mod}\, p),$$

где $N = \dfrac{p(p^2 - 1)}{2}$.

Это утверждение предполагается применить к созданию криптографического алгоритма, аналогичного алгоритму RSA.

УДК 621.391.019.3

МЕТОД ПЕРЕБОРНОГО ПОШУКУ ОПТИМАЛЬНИХ ЗГОРТКОВИХ КОДІВ ТА СИГНАЛЬНО-КОДОВИХ КОНСТРУКЦІЙ

Іщенко М.О., аспірант
Одеська Національна Академія Зв'язку ім. О.С. Попова
E-Mail: dima_ischenko@rambler.ru

Розв'язуючи проблему підвищення ефективності систем передачі інформації, важливим є одночасно підвищення частотної та енергетичної ефективності. Рішення цієї проблеми можливе за умови використання сигнально-кодових конструкцій. Важливим показником ефективності СКК, декодування яких проводиться за критерієм мінімуму ймовірності помилки (алгоритм Вітербі), являється вільна віддаль.

Автором пропонується ефективний метод переборного пошуку породжуючих поліномів оптимальних згорткових кодів (ЗК) та сигнально-кодових конструкцій (СКК) по критерію максимальної вільної віддалі. Розроблено алгоритм та блок-схему даного методу. Розроблена імітаційна модель алгоритму використовуючи пакет віртуального об'єктного програмування HP VEE. Проведено пошук оптимальних ЗК та СКК, на основі ФМ-8, при різних методах узгодження сигнально-кодових конструкцій.

В основі даного методу лежить находження вільної віддалі ЗК та СКК, що характеризує коректуючу здатність коду та визначає нижню границю завадостійкості кодів при використанні алгоритму Вітербі.

Пропонований метод базується на моделюванні емулятор кодера та отримав назву "*емуляційний метод*".

Даний метод передбачає:

– формування тест-пакету для тестування параметрів кодера;

– моделювання згорткового кодера з параметрами: швидкість коду R, довжина кодового обмеження ν, в якому проводиться перебір породжуючих поліномів;

– моделювання формувача маніпуляційного коду (код Грея або код, що формується підчас розбиття ансамблю сигналу на вкладені під ансамблі) та формувача в метриці Евкліда сигнального сузір'я багатопозиційних M-ічних сигналів;

– розрахунок для кожного породжуючого поліному вільної віддалі ЗК та СКК;

- вибір породжуючих поліномів ЗК та СКК з максимальною вільною віддалю.

Для перевірки коректності розробленого методу і програми на його основі проведено тестування на прикладі пошуку оптимальних згорткових кодів, оптимальних по критерію максимуму вільної віддалі в метриці Хемінга, оскільки в літературі опубліковані таблиці оптимальних згорткових кодів.

В результаті пошуку було найдемо ряд нових кодів, вільна віддаль яких збігається з оптимальними кодами. Це доводить ефективність даного методу.

Для аналізу СКК дослідження проводилось в два етапи:

- на першому етапі було проведено розрахунок вільної віддалі СКК (з-за допомогою імітаційної моделі) які містили відомі (оптимальні) згорткові коди.
- на другому етапі проводився пошук породжуючих поліномів оптимальних СКК.

Метод є універсальним оскільки пошук оптимальних СКК проводиться для різних методів узгодження кодера і модулятора та для різних ансамблів сигналів (ФМ-М, АФМ-М, КАМ-М, і т.д.).

УДК 681. 3. 06

АНАЛІЗ АЛГОРИТМІВ ПОБУДОВИ ПАРАМЕТРІВ ДЛЯ КРИПТОСИСТЕМ НА ЕЛІПТИЧНИХ КРИВИХ

О.Є. Ілясова, Харківський банківський інститут УАБС

Криптографічні системи на еліптичних кривих набули поширеного використання в різних криптографічних додатках завдяки забезпеченню належного захисту при достатньо малій, в порівнянні з другими системами, довжині ключа. Генерація загальносистемних параметрів криптосистеми є початковим етапом її використання. До параметрів криптосистеми, яка базується на перетвореннях в групі точок еліптичних кривих, належать параметри рівняння кривої та її порядок. Для забезпечення необхідного рівня стійкості параметри повинні задовольняти наступним умовам: порядок кривої повинен бути великим простим числом, параметри рівняння кривої повинні бути випадковими числами, обчислювальна складність перетворень має бути поліноміальною. Таким чином, виникає задача пошуку недетермінованого алгоритму з поліноміальною обчислювальною складністю, який забезпечував би генерацію криптостійких до відомих атак загальносистемних параметрів. В Україні розроблено стандарт цифрового підпису ДСТУ 4145-2002, що базується на перетвореннях в групі точок еліптичних кривих, які визначені над полем $GF(2^m)$. Згідно з даним стандартом необхідно виконати генерацію параметрів. Це можливо за рахунок використання алгоритму "комплексного множення". Цей алгоритм починається з вибору великого простого числа p так, щоб система мала

необхідний рівень безпеки. Другим кроком є обчислення параметрів рівняння еліптичної кривої. Недоліком вищенаведеного алгоритму є достатньо велика обчислювальна складність побудови мінімального полінома j - інваріанта кривої та пошук його дійсного кореня. Обчислення коефіцієнтів рівняння кривої виконується за умови, що корінь полінома відомий. Після цього перевіряється, чи має побудована крива заздалегідь заданий порядок. Перевірка пов'язана з обчислювальною складністю для поля GF(2^m), де m - велике число.

В зв'язку з цим в даній роботі обгрунтовано необхідність заміни алгоритму "комплексного множення" на інший, який був би більш ефективним за часом, оптимальним за обчислювальною складністю, а також знаходив порядок випадкової еліптичної кривої над вказаним полем. Для цього було проаналізовано три відомих алгоритма: Р. Скуфа, SEA, Т. Сатоха. Результат аналізу показав, що алгоритм Р. Скуфа хоча і має поліноміальну складність, але його практична реалізація займає багато часу. Наприклад, для поля в 2000 біт час реалізації складає 1500 годин. Алгоритм SEA в порівнянні з алгоритмом Р. Скуфа має значну перевагу в часі лише для полів GF(p^m), де $p \geq 3$, але ця умова не відповідає прийнятим в Україні стандартам. І саме алгоритм Т. Сатоха дозволяє обчислювати порядок випадково генерованої еліптичної кривої та є одним з швидких за часом алгоритмів. Його було розроблено для полів GF(p^m), але його можна використовувати і над полем GF(2^m). В результаті програмна реалізація алгоритму дозволить обчислювати порядок еліптичних кривих з випадковими коефіцієнтами з мінімальною за часом складністю. А сам алгоритм можна застосувати при розробці нового стандарту.

УДК 621,391.1 (075.8)

«ЗОЛОТЫЕ» МАТРИЦЫ И НОВЫЙ МЕТОД КРИПТОГРАФИИ

А.П. Стахов, доктор технических наук, профессор
e-mail: goldenmuseum@rogers.com

1. «Золотая» криптография

Суть «золотой» криптографии состоит в следующем. В качестве «криптографического ключа» используется некоторое значение переменной x. Это означает, что количество «криптографических ключей» для данного метода теоретически бесконечно. Метод может быть применен для криптографической защиты так называемых «дискретных сигналов», представляющих последовательность «отсчетов» некоторой непрерывной функции:

$$a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, \ldots \quad (1)$$

Шифрация сообщения состоит в последовательном представлении четверок «отсчетов» типа a_1, a_2, a_3, a_4 из (1) в виде квадратной матрицы:

$$M = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \quad (2)$$

и последующем ее умножении на прямую «золотую» матрицу. При этом образуется «кодовая матрица» E

$$M \times Q(2x) = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \times \begin{pmatrix} cFs(2x+1) & sFs(2x) \\ sFs(2x) & cFs(2x-1) \end{pmatrix} = \begin{pmatrix} e_{11} & e_{12} \\ e_{21} & e_{22} \end{pmatrix} = E(x), \quad (3)$$

которая представляет собой «зашифрованное сообщение», передаваемое затем по «каналу связи».

Дешифрация зашифрованного сообщения, полученного из «канала связи», состоит в умножении «кодовой матрицы» (3) на инверсную матрицу.

Между детерминантами исходной матрицы (2) и «кодовой матрицы» (3) существует следующая связь:

$$\mathrm{Det}\ E = \mathrm{Det}\ M, \qquad (4)$$

что непосредственно вытекает из свойства (5).

2. Преимущества «золотой» криптографии

Предложенный метод принадлежит к так называемой «симметричной» криптографии, то есть для его реализации «криптографический ключ» должен быть известен «получателю» зашифрованного сообщения. Для передачи «криптографического ключа» предлагается использовать существующие «асимметричные» криптографические системы, то есть «криптографическая способность» данного метода определяется «криптографической способностью» соответствующей «асимметричной» системы, используемой для передачи криптографического ключа.

Основным достоинством «золотой» криптографии является простота алгоритма шифрации-дешифрации, что обеспечивает высокую скорость шифрации-дешифрации и позволяет использовать метод для криптографической защиты «дискретных сигналов», работающих в реальном масштабе времени (телефонные, измерительные и другие телекоммуникационные системы). При этом частая смена «криптографического ключа», выбираемого по случайному закону, неизвестному «передатчику» и «приемнику» и передаваемого с помощью «асимметричных» систем, обеспечивает достаточно высокий уровень криптографической защиты. Еще одним достоинством метода является возможность контроля процесса шифрации и дешифрации, что основывается на уникальном математическом тождестве (4), связывающем детерминанты исходной матрицы (2) и «кодовой матрицы» (3).

Таким образом, с помощью предложенного метода можно создавать простые с точки зрения технической реализации, быстродействующие и высоконадежные криптографические системы, предназначенные для защиты информационных систем, работающих в реальном масштабе времени.

УДК 681.3.67

ТЕНДЕНЦИИ В СТРУКТУРЕ УГРОЗ И РИСКОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Фильштинский С.В. (Мельбурн, Австралия)

Считается общепризнанным, что в настоящее время целью большинства атак на системы информационной безопасности являются, в конечном итоге, деньги, в то время как несколько лет назад основной целью атак был престиж в узких кругах хакеров.

Это изменение произошло несколько лет назад. С одной стороны большое количество уязвимых систем в Интернете породило рынок предложений на украденную информацию, и в первую очередь на легко превращаемые в реальные деньги номера кредитных карточек. С другой стороны появление торговых платформ для торговли такой информацией привлекло любителей быстрых денег со всего мира и тем самым создало огромный спрос. Это обстоятельство до сих пор поддерживает чрезвычайную устойчивость криминальных торговых площадок, несмотря на непрерывную охоту на них со стороны мощнейших государственных спецслужб, структур безопасности ведущих платежных систем и корпораций.

Система торговых площадок, созданная для операций с краденными кредитными карточками привлекла к себе другие виды мошенничества – фишинг (phishing), кража личной информации с целью мошенничества (identity theft), шантаж.

Торговые площадки изменили те виды мошенничества, которые ранее требовали объединения в

одной группе лиц специалистов разного профиля, таких как

- хакеры
- спамеры
- программисты
- специалисты в банковском деле
- специалисты по отмыванию денег.

Возникло разделение труда, специализация, рынок услуг. Компьютерное мошенничество вошло в индустриальных век.

Это важно понимать, оценивая уровни рисков в области информационной безопасности.

Если раньше, к примеру, база данных клиентов компании представляла интерес только для прямых конкурентов, то теперь любая ценная информация превратилась в высоколиквидный товар, который можно с легкостью продать за реальные деньги.

В докладе предлагается:

- оценивать риски с учетом повышения вероятности их реализации;
- искать меры защиты, которые бы работали против используемой киберпреступниками бизнес - модели;
- не ограничивать способы защиты техническими методами, а также применять меры организационного характера.

УДК 681.142

ОБОБЩЁННЫЕ МУЛЬТИКАНАЛЬНЫЙ АЛГОРИТМ И ПОЗИЦИОННАЯ СИСТЕМА СЧИСЛЕНИЯ

А.Н. Лаврёнов
Институт современных знаний имени А.М. Широкова, Минск
E-mail: lanin99@mail.ru

Система счисления – система счёта или совокупность правил по упорядочиванию (перечислению) объектов, а также способов их представления с помощью некоторого конечного множества символов. История человечества показала возможность существование символической, непозиционной и позиционной систем счисления. Однако в практической деятельности только последняя доказала свою наибольшую результативность и получила широкое распространение. Само название позиционной системы счисления (ПСС) указывает на то, что значение (значимость) каждого разряда, представленного неким символом, зависит от его положения.

Пусть исходное множество объектов A разделено на n подмножеств A_n, т. е. на языке множеств это выразим так

$$A = \sum_n A_n .$$

В каждом A_n его элементы упорядочены с помощью алфавита α_n, и их общее количество или мощность алфавита α_n есть $P(\alpha_n) = p_n$. Следовательно, любой набор X элементов множества A можно записать следующим образом:

$$\{X\} = \sum_{m=1}^{m=n} \alpha_m A_m \equiv \alpha_n \alpha_{n-1} \dots \alpha_m \dots \alpha_2 \alpha_1 .$$

Назовём такую конструкцию обобщённой позиционной системой счисления (ОПСС). Если в качестве A_m рассматривать соответственно b^m, $m!$, $F_k(m)$ или C_{n-1}^m, то получим степенную с основанием b, факториальную, k-фибоначчиевую и биномиальную ПСС. В качестве своего примера ОПСС предложим в роли основания деформированные k- обобщенные матрицы Фибоначчи $Q_k = \begin{bmatrix} \vec{c} & c_k \\ I_{k-1} & 0 \end{bmatrix}$, где $\vec{c} = diag(c_1, c_2, \dots c_{k-1})$ и c_k - параметры деформации.

Из вышеприведенного построения ОПСС ясно, что мощность P_A множества A равна сумме мощностей P_{A_n} подмножеств A_n, т. е. $P_A \equiv \sum_{m=1}^{m=n} P_{A_m}$. Данный факт разложения P_A на слагаемые P_{A_n} можно использовать для классификации ОПСС.

Также, если установить изоморфизм между элементами n- разрядной ОПСС и элементами l-разрядных ОПСС ($1 \le l \le n$), то можно ввести обобщенный мультиканальный алгоритм. В виду того, что в общем случае $P_{A_i} \neq P_{A_j}$, то имеются запрещенные комбинации и (или) множественное представление числа. Последнее улучшает диффузионные характеристики обобщенного мультиканального алгоритма и служит дополнительным барьером по защите информации от несанкционированного доступа.

УДК 621.391.1

ФОРМИРОВАНИЕ КОДОВ-КОМПОЗИЦИЙ НА ОСНОВЕ МНОГОЗНАЧНЫХ БИНОМИАЛЬНЫХ ЧИСЕЛ

Онанченко Е.Л., к.т.н., доц.; Онанченко А.Е., студ.
Сумский государственный университет
E-mail: electron@sumdu.edu.ua

Проблема повышения скорости передачи информации становится одной из первостепенных и какой бы сложной не была логика обработки информации, она становится оправданной, если это приводит к повышению эффективности использования канала связи. Второй, не менее важной проблемой, является проблема достоверности информации, так как появление ошибок может привести к тяжелым последствиям. Требования к вероятности искажения данных с каждым годом ужесточаются. Обе проблемы являются противоречивыми и одна решается за счет другой.

К существующим кодам предъявляется несколько требований: возможность обнаруживать и исправлять ошибки заданной кратности, простота построения устройств кодирования и декодиования, малые аппаратурные затраты. Эти требования достигаются за счет возможности изменения избыточности, а значит и корректирующих возможностей в зависимости от уровня помех. Это позволяет строить адаптивные системы связи, меняющие скорость передачи в зависимости от уровня помех.

Указанным условиям во многих случаях удовлетворяют комбинаторные коды, использующие в своей основе известные комбинаторные соотношения - перестановки, размещения, сочетания, композиции. Однако специализированные устройства формирования

комбинаторных конфигураций получаются достаточно сложными, обладают относительно слабыми возможностями по изменению длины комбинаторных комбинаций, недостаточно надежными.

Комбинаторные коды имеют более сложную структуру, чем двоичные, алгоритмы их генерирования усложнены. В общем случае для преобразования исходного двоичного слова в комбинаторную конфигурацию и обратно используется специализированный преобразователь кода, реализуемый аппаратными средствами либо программным путем. Построение комбинаторных кодов целесообразно производить с использованием систем счисления, структура которых близка к структуре порождаемых ею кодов. Двоичная система счисления не позволяют генерировать комбинаторные коды с использованием простых и надежных алгоритмов. Существенно упростить алгоритмы генерирования комбинаторных кодов позволяют биномиальные системы счисления с многозначным алфавитом. Исходное двоичное число преобразуется в число биномиальной системы счисления, а затем уже биномиальное число преобразуется в соответствующую ей комбинаторную конфигурацию.

Известные системы счисления с комбинаторным основанием, в том числе и биномиальные, обладают двумя положительными свойствами – они помехоустойчивы и способны генерировать комбинаторные конфигурации типа сочетаний и композиций. Это делает их пригодными для построения помехоустойчивых устройств кодирования, сжатия информации, систем автоматизированного проектирования и контроля, систем связи. Такие устройства отличаются также повышенным быстродействием и надежностью.

УДК 621.3.011

ЗАВАДОСТІЙКЕ КОДУВАННЯ СИГНАЛІВ В СИСТЕМІ ДИСТАНЦІЙНОГО КЕРУВАННЯ ПЕРЕТВОРЮВАЧАМИ ПО ЛІНІЯМ ЕЛЕКТРОМЕРЕЖІ

В.Я. Жуйков д.т.н., проф.; Ю.В. Хохлов к.т.н.; В.М. Співак к.т.н., проф. Національний технічний університет України „Київський політехнічний інститут", e-mail: vspivak@list.ru

Узгоджене керування перетворювачами електроенергії, що розташовані на деякій відстані, сприяє підвищенню продуктивності та якості виробництва. Перспективним є передавання сигналів узгодженого керування по існуючим лініям електромережі (при цьому не потрібно прокладати додаткові кабелі, полегшується процедура приєднання до мережі зв'язку). Однак перетворювачі генерують в електромережу завади, тому для надійного керування актуальним є вирішення задачі підвищення завадостійкості систем передавання сигналів дистанційного керування [1].

Навіть з використанням загальноприйнятих методів зменшення завад від перетворювачів, їх рівень залишається істотним. Одним з найефективніших методів підвищення завадостійкості є метод передавання сигналів з розширенням спектру.

Показано варіанти використання базисних функцій відомих ортогональних спектральних перетворень, зокрема, перетворення Уолша, для надання сигналам дистанційного керування шумоподібної форми.

Поставлено задачу застосування нових спектральних перетворень, що характеризуються малою трудомісткістю і простотою реалізації, та розробки систем передавання сигналів дистанційного керування перетворювачами по лініях електроживлення з підвищеними завадостійкістю та швидкодією.

Показано, що відносна трудомісткість перетворення в орієнтованому базисі (ОБ) складає 44,3–95% від відносної трудомісткості перетворення Уолша при порівняних значеннях довжин інтервалів визначення N (див. рис.1)[2], тому доцільним є використання ОБ перетворення в системах передавання.

Вперше застосовано перетворення дискретних функцій в ОБ для забезпечення завадостійкого передавання сигналів дистанційного керування перетворювачами по лініях електромережі, що дозволяє підвищити завадостійкість та збільшити кількість каналів передавання у порівнянні з існуючими системами. Наприклад, кількість каналів у порівнянні з багатоканальними системами, які використовують перетворення Уолша, збільшується у $3''/2''$ разів. Запропоновано нові системи передавання сигналів дистанційного керування перетворювачами по лініях електромережі для синхронного та асинхронного керування за одноканальною, багатоканальною та комбінованою схемами.

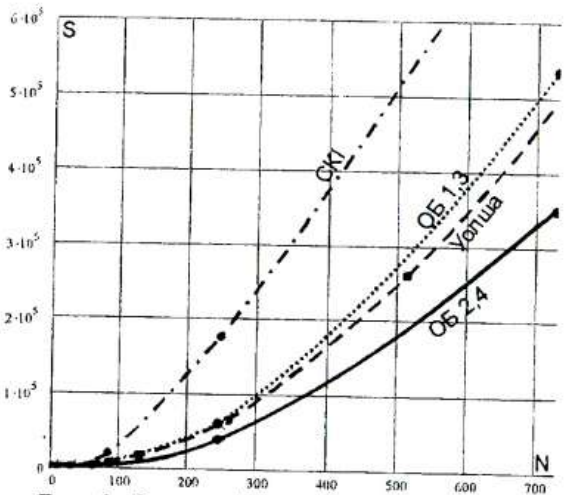

Рис.1. Залежність кількості операцій S від значення довжини інтервалу визначення N.

Математичне моделювання системи передавання [3] показало, що запропонований метод передавання сигналів дистанційного керування дозволяє підвищити завадостійкість у 2-3 рази.

Результати роботи апробовані в системі завадостійкого дистанційного керування по лініях електромережі режимами роботи перетворювачів в енергосистемі з фотогенераторами та трифазним випрямлячем.

1. Терещенко Т.О., Петергеря Ю.С., Хохлов Ю.В. Передача інформації у системах побутової автоматизації на основі узгоджених фільтрів // Технічна електродинаміка. Тематичний випуск "Силова електроніка та енергоефективність", частина 2. – 2002. – С. 61-65.
2. Петергеря Ю.С., Хохлов Ю.В., Хижняк Т.А. Порівняльний аналіз спектральних перетворень // Электроника и связь. – 2002. - №16. – С.71-75.
3. Хохлов Ю.В. Аналіз завадостійкості систем дистанційного керування перетворювачами електроенергії. Тематичний випуск "Силова електроніка та енергоефективність", частина 2. – 2005. – С.60-63.

УДК 621.396.6.019.3

МЕТОДЫ ОЦЕНКИ ДОСТОВЕРНОСТИ ФУНКЦИОНИРОВАНИЯ БИНОМИАЛЬНЫХ ЦИФРОВЫХ УСТРОЙСТВ

В.В. Гриненко, СумГУ,
grvital@list.ru

Возрастание сложности цифровых устройств приводит к ужесточению требований, предъявляемых к надежности узлов. Проблема обеспечения надежности систем включает задачи по разработке теоретических методов анализа надежности на стадии проектирования, выбору показателей надежности и их оценки по результатам испытаний.

Для оценки функциональной надежности цифровых устройств по отношению к сбоям и отказам используются различные подходы, основанные на вероятностно-статистических и расчетных методах, с применением математических моделей. При анализе схем состоящих из одной ступени элементов возможно применение метода основанного на использовании моделей сбоев логических элементов. Достоверность работы устройства определяется вероятностями появления помех на входах элементов приводящих к их ошибочному переключению. При моделировании возможно использование соотношений по оценке достоверности передачи данных по каналу связи с асимметричным уровнем одиночных помех.

Для оценки отказоустойчивости в более сложных устройствах, в которых отказ одного элемента может привести к появлению двух и более ошибок на выходе, используется модель оценки достоверности работы цифрового устройства со схемой встроенного контроля.

Так, к примеру, если схема контроля не контролируется, то вероятности правильной работы $P_{пр.}(t)$, вероятность неправильной работы устройства $P_{о.о.}(t)$, вероятность, что устройство работает неправильно, но сигнал ошибки отсутствует $P_{н.о.}(t)$, вероятность правильной работы, при наличии сигнала ошибки $P_{о.н.}(t)$ определяются по следующим соотношениям

$$P_{пр.}(t) = P_{исх}(t)P_{к}(t),$$

$$P_{о.о.}(t) = P_{обн.}(1 - P_{исх.}(t)),$$

$$P_{н.о.}(t) = (1 - P_{исх.}(t)P_{к.}(t)) - P_{обн.}(1 - P_{исх.}(t)P_{к.}(t)),$$

$$P_{о.н.}(t) = P_{обн.}P_{исх.}(t)(1 - P_{к.}(t)).$$

где $P_{исх.}(t), P_{к.}(t)$ – вероятности безотказной работы исходной схемы и схемы контроля определяются по экспоненциальному закону распределения.

Вероятность обнаружения ошибки для различного модуля кратности ошибок определяется соотношением

$$P_{обн.} = 1 - \frac{N}{2^{n-1} - 1}$$

$N = C_n^k$ – количество кодовых комбинаций,

где n, k – параметры биномиальной системы счисления.

Описанные подходы позволяют производить оценку показателей надежности цифровых устройств на основе биномиальных кодов под воздействием сбоев и отказов в логических элементах.

УДК 621.3.011: 621.314

ВЫБОР ОПТИМАЛЬНОГО ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ ДЛЯ СЖАТИЯ СИГНАЛОВ В РЕАЛЬНОМ ВРЕМЕНИ

Петергеря Ю. С., к.т.н., доц., Колотов Н. В. , НТУУ «КПИ», кафедра «Промышленной электроники»
e-mail: nick@voliacable.com

Известно, что дискретные вейвлет-преобразования (ВП) широко используются для сжатия цифровых сигналов в реальном времени путем устранения высокочастотных флуктуаций. В зависимости от характера сигналов и задачи обработки применяются различные ВП. Оптимальный вейвлет должен обеспечить минимально возможные количество циклов для достижения необходимого коэффициента сжатия и время выполнения одного цикла, а также простую схемотехническую реализацию алгоритмов.

Рассмотрим эффективность применения ВП Хаара, Добеши 2 порядка и ВП в ориентированном базисе (ОБ ВП) на примере сжатия сигнала (рис.1), который содержит 243 отсчета, имеет два изменения значений в низкочастотной области и высокочастотные составляющие, за счет устранения которых производится сжатие сигнала.

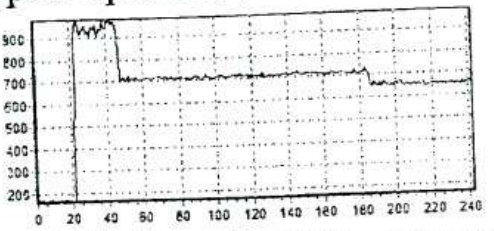

Рис. 1. Цифровой сигнал - оригинал

Первым критерием сравнения служит максимальный уровень разложения, приводящий к исключению большинства высокочастотных составляющих без искажения низ-

кочастотных колебаний. Для определения такого уровня был рассчитан коэффициент подобия сигнала для рассмотренных ВП (рис.2) и выбрано его пороговое значение 0.96. Из рис.2 видно, что, для Хаара и Добеши третий, а для ОБ ВП – второй, являются уровнями, которые соответствуют данному пороговому значению.

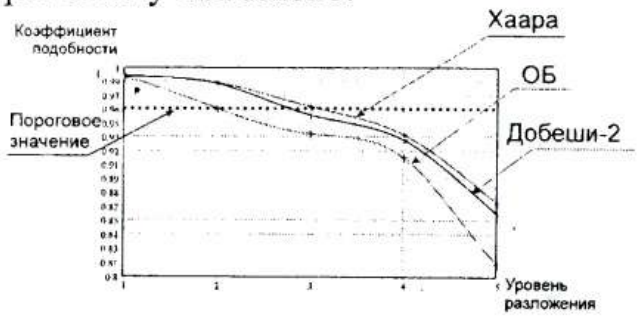

Рис. 2. Зависимость коэффициента подобия сигналов от уровня разложения

Последующее сравнение связано с определением трудоемкости преобразований. Схемы разложений ВП Хаара и ОБ ВП представлены на рис.3,а и рис.3,б соответственно.

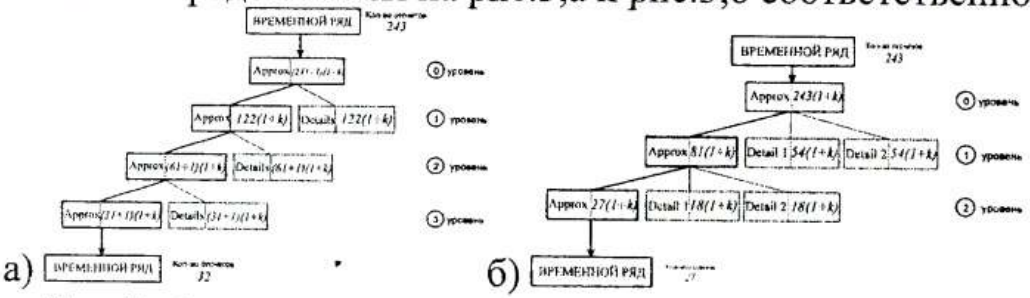

Рис. 3. а) схема разложения сигнала ВП Хаара и Добеши, б) схема разложения сигнала ОБ ВП.

Вычисления, проведенные по схемам показали, что для достижения заданного коэффициента подобия 0.96 при ОБ ВП требуется на 23.7 % операций меньше, нежели при использовании ВП Хаара. Результат разложения при использовании ОБ ВП содержит также меньшее количество отсчетов (27 при ОБ ВП и 32 при Хаара). Полученные данные свидетельствуют о перспективности применения ОБ ВП для решения задач сжатия сигналов в реальном времени.

УДК 621.382(07) + 681.32(07)

ФОРМУВАННЯ ПСЕВДОВИПАДКОВИХ РОЗПОДІЛІВ НА ОСНОВІ КОДІВ ГАЛУА

Лаврів М.В., аспірант каф. Інформатики Прикарпатського національного університету ім. В.Стефаника (м. Івано-Франківськ) dlya_marii@mail.ru

Одним із ефективних шляхів розширення смуги спектру сигналу аналого-цифрового перетворення на основі інтегрального методу є використання методу статистичних досліджень Монте-Карло. Широке застосування останнього обмежувалось складністю якісних алгоритмів і засобів генерування псевдовипадкових сигналів та значними коштами виготовлення, що і визначило актуальність здійснення досліджень по розробці таких генераторів, які б володіли конкуруючими техніко-економічними характеристиками.

Запропоновано метод і розроблено генератор псевдовипадкових чисел на основі циклічних кодів типу послідовностей максимальної довжини, який полягає в тому, що в кодовій послідовності всі елементи володіють рекурсивною взаємозалежністю, а кожен із n-розрядних кодових фрагментів та їх аналогове представлення має псевдовипадковий характер розподілу на одиничному періоді. Технічна реалізація такого генератора полягає у застосуванні регістра зсуву, охопленого логічним зворотним зв'язком згідно примітивних невироджених поліномів, до цифрових виходів якого підключено цифро-аналоговий перетворювач, що по аналоговому виходу формує аналогову розгортку псевдовипадкового сигналу.

Здійснено оцінку якості псевдовипадкового розподілу за допомогою емпіричних та теоретичних методів

тестування. Зокрема, у групі емпіричних тестів проведено: - перевірку рівномірності розподілу між нулем і одиницею; - перевірку серій, згідно якої досліджується рівномірність і незалежність пар суміжних випадкових чисел; - перевірку інтервалів між моментами появи суміжних значень; - перевірку комбінацій, що досліджує розподіл n груп із k наступних один за одним чисел і обчислює число груп, в яких міститься r різних чисел; - перевірку перестановок, що розділяє початкову послідовність на n груп з t елементів в кожній і визначає скільки раз зустрічається кожне розміщення, після чого застосовується критерій χ^2. З метою визначення потенційної верхньої спектральної частотної складової проведено спектральне тестування отриманого розподілу.

За допомогою графічних тестів, зокрема гістограми розподілу елементів оцінено рівномірність розподілу символів у послідовності та визначено частоту їх появи. Тест оцінки розподілу на площині дозволив визначити залежності між елементами досліджуваної послідовності, а перевірки на монотонність - рівномірність розподілу символів. За допомогою графічного спектрального тестування здійснено перевірку послідовності на розподіл 0 і 1 в досліджуваній послідовності на основі аналізу висоти викидів перетворення Фур'є.

За допомогою статистичних критеріїв, зокрема χ^2 та Колмогорова - Смірнова проведено статистичні дослідження отриманих розподілів для визначення закону розподілу випадкових чисел, які дозволили визначити тип емпіричного розподілу як рівномірний, а сукупність всіх наведених тестів ствердити високі якісні показники у порівнянні з відомими методами генерування псевдовипакових розподілів за співвідношенням критеріїв "якість розподілу – вартість реалізації".

УДК 621.382(07) + 681.32(07)

АНАЛІЗ ТА ОБҐРУНТУВАННЯ ЕФЕКТИВНОСТІ ЗАСТОСУВАННЯ АНАЛОГО-ЦИФРОВОГО ПЕРЕТВОРЕННЯ МОНТЕ-КАРЛО

Лаврів М.В., аспірант каф. Інформатики Прикарпатського національного університету ім. В.Стефаника (м. Івано-Франківськ) dlya_marii@mail.ru
Овчар І.Є., аспірант каф. Інформатики Прикарпатського національного університету ім. В.Стефаника (м. Ів-Франківськ) iovchar@ukrpost.net

Перспектива розвитку методів та засобів аналого-цифрового (АЦ) перетворення полягає у тенденції зменшенні застосування інтегральних перетворювачів, при цьому спостерігається впровадження спеціалізовано орієнтованих щодо типу джерел повідомлень перетворювачів. З метою визначення галузей ефективного застосування АЦ перетворювачів проаналізовано методи перетворення: паралельного, інтегрування, послідовного наближення, дельта-сигма, багатоетапних ітерацій.

Паралельні АЦ перетворювачі володіють максимальною швидкодією, однак їх широке застосування обмежується складністю архітектури, високою вартістю та енергоспоживанням. З іншого боку інтегруючі перетворювачі характеризуються простотою, низькими коштами реалізації та енергоспоживанням, проте володіють низькою швидкодією.

З метою підвищення техніко-економічних параметрів АЦ перетворення, зокрема розширення смуги вхідного сигналу перетворення та уникнення необхідності застосування пристроїв вибірки-зберігання запропоновано

метод Монте-Карло, який класифікується до інтегруючих методів і володіє їх перевагами. Широке впровадження АЦ перетворювачів Монте-Карло обмежувалось складністю реалізації якісних дешевих генераторів псевдовипадкових сигналів.

У доповіді наведено результати розробки методів генерування псевдовипадкових послідовностей на основі циклічних зсувів, охоплених логічним зворотним зв'язком, що реалізовані на регістрах зсуву та із рандомізацією вагових двійкових розрядів на основі двійкових лічильників, складність та кошти виготовлення яких порівнянні зі складністю та коштами виготовлення генератора пилоподібного опорного сигналу інтегруючих АЦ перетворювачів. Розроблено математичний апарат, алгоритми, методичні та принципові рішення побудови генераторів псевдовипадкових сигналів сканування Монте-Карло, здійснено оцінку якості статистичних розподілів, порівняння із відомими методами та визначено ефективність їх застосування.

Проаналізовано нові функціональні розширення методу, які полягають у можливості безпосереднього перетворення двополярних сигналів без їх попереднього лінійного випрямлення, виводу результатів перетворення окремо для «+»- та «-»- складових, а також у векторному перемноженні двох довільних двополярних сигналів із формуванням усередненого на визначеному періоді результату їх добутку, а також «+»- та «-»- складових результату.

Практичного застосування запропонований метод набув в розподілених інфосистемах обліку енергоносіїв, а також в лічильниках електроенергії, в яких здійснюється обчислення інтегрального значення спожитої енергії, що визначається векторним добутком діючого значення напруги та струму споживання.

УДК 621.382

АДАПТИВНЕ ЗМЕНШЕННЯ НАДЛИШКОВОСТІ ДАНИХ НА БАЗІ МЕТОДІВ ПЕРЕДБАЧЕННЯ НУЛЬОВОГО ТА ПЕРШОГО ПОРЯДКУ

Іляш Ю.Ю., аспірант кафедри інформатики Прикарпатського національного університету ім. В.Стефаника (м. Ів-Франківськ)
yurchuk-il@rambler.ru

Адаптивні методи зменшення надлишковості даних передбачають, що відліки вхідного потоку даних поступають в систему через однакові проміжки часу Δt, основним із завдань для яких є формування істотних відліків. При аналізі вхідного потоку, представленого точними значеннями деякої аналогової функції, відбувається порівняння відліку, отриманого в даний момент часу t_i, з останнім істотним відліком $f^*(t_j)$ і, в разі невідповідності, - різницею $[f^*(t_j) - f(t_i)]$ деякої заданої величини ε, отриманий відлік $f(t_i)$ формується як істотний.

Існує також клас алгоритмів, в яких істотні відліки заміняються своїми наближеними значеннями. В алгоритмах передбачення в якості апроксимуючої функції найчастіше використовують поліноми m-го степеня, а методи визначають як поліномні. Їх основу складають методи скінчених різниць, за допомогою яких можна відтворити поліном n-го степеня за $n+1$ значенням відліку

$$s(t) = b_0 + b_1 t + \ldots + b_n t^m .$$

В алгоритмах передбачення для кожного наступного відліку S_{i+1} формується оцінка $\hat{S}_{i+1}$ на основі попередніх відліків $y_i, y_{i-1}, \ldots$ Оцінки формуються згідно виразу

$$\hat{S}_{i+1} = \sum_{j=0}^{m} (-1)^j C_{m+1}^{j+1} y_{i-j}, \text{ чи}$$

$$\hat{S}_{i+1} = y_i + \Delta y_i + \Delta^2 y_i + \ldots + \Delta^n y_i,$$

де Δy_i - скінченні різниці відповідного порядку, а

$$\Delta y_i = y_i - y_{i-1}, \qquad \Delta^n y_i = \Delta^{n-1} y_i - \Delta^{n-1} y_{i-1}.$$

Значення S_i замінюється значенням оцінки $\hat{S}_i$, якщо похибка наближення $\left|S_i - \hat{S}_i\right|$ не перевищує допустимої похибки ε.

Найпростішим методом реалізації поліномного передбачення є передбачення нульового порядку, за якого оцінка кожного наступного відліку чисельно рівна значенню попереднього відліку. Тому для передбачення наступних відліків достатньо пам'ятати значення останнього істотного відліку.

Дещо складнішим за технічною реалізацією є передбачення першого порядку. В алгоритмах передбачення першого порядку для аналізу значень вибірок використовується поліном першого порядку

$$\hat{S}_{i+1} = 2y_i - y_{i-1},$$

згідно якого відбираються істотні відліки та встановлюється значення апертури розмірності 2ε.

В доповіді наведено результати аналізу алгоритмів передбачення нульового та першого порядку. Здійснено оцінку ефективності вказаних методів при стисненні сигналів різних стандартизованих форм.

УДК 621.382

АНАЛІЗ ЕФЕКТИВНОСТІ АДАПТИВНИХ МЕТОДІВ ЗМЕНШЕННЯ НАДЛИШКОВОСТІ ДАНИХ

Іляш Ю.Ю.; аспірант кафедри інформатики Прикарпатського національного університету ім. В.Стефаника (м. Ів-Франківськ)
yurchuk-il@rambler.ru

В техніці кодування повідомлень актуальною задачею є зменшення обсягів інфопотоків, що циркулюють в інфосистемі, без втрат інформаційного змісту.

Одним з ефективних методів полягає у зменшенні природної надлишковості, інакше - "стисненні даних". Основою стиснення даних є «економічний» опис даних, згідно якому можливе відновлення їх початкових значень із контрольованим значенням похибки відтворення.

Методи зменшення надлишковості полягають в виключенні тих вибірок даних, які можуть бути відновлені за допомогою аналізу попередніх чи наступних вибірок (передбачення та інтерполяція), або шляхом порівняння з вибраними базисними функціями чи коливаннями.

Методи передбачення ґрунтуються на наближених оцінках, які ефективні за умови, що потік даних характеризується відносною стабільністю в межах різних часових проміжків. Якщо ж дані змінюються випадковим чином, або піддаються впливу завад, то ефективність зменшення надлишковості методами передбачення при заданій точності буде незначною. В практиці набули широкого застосовуються інтерполяційні методи, що відносяться до класу адаптивних апертурних методів зменшення надлишковості з однопараметричною адаптацією.

Розрізняють методи інтерполяції нульового та першого порядку. Застосування інтерполяції вищих порядків на практиці недоцільно внаслідок значних апаратурних та затрат часу. На відміну від методів передбачення, в інтерполяційних методах значення апертури не є постійним, а змінюється з формуванням кожного наступного відліку і триває поки не буде визначено такого значення апертури, що не вміщує отриманих значень сигналу. Перший відлік, який не потрапляє в межі апертури вважатиметься істотним і передається по каналах зв'язку. Починаючи з наступного значення побудова апертури починається заново. При цьому в якості початку нового інтервалу інтерполяції може бути використаний як відлік, що передається (алгоритм із з'єднаними відрізками, або інтерполяція першого порядку із 2 ступенями вільності), або ж перший відлік, який слідує за відліком, що передавався (алгоритм із нез'єднаними відрізками, або інтерполяція першого порядку із 4 ступенями вільності). Цей спосіб отримав широке застосування завдяки своїй ефективності і простоті практичної реалізації. Використання вказаних методів характеризується складністю технічної реалізації. Досліджено ефективність і інших інтерполяційних методів стиснення повідомлень, таких як методи інтерполяції з фіксованою апертурою із зсувом, метод найменших квадратів, багатоступеневої ітераційної інтерполяції.

Наведено результати аналізу алгоритмів інтерполяції, їх ефективність при застосуванні до різних типів сигналів на базі порівняння загальної кількості відліків та кількості істотних відліків, які формуються після застосування інтерполяції. При порівнянні досліджуваних методів стиснення інформації слід вказати на найкращі результати при стисненні сигналів типу телеметричних на базі інтерполяції першого порядку.

УДК 621.391(075.8)

ВИЗНАЧЕННЯ КОДОВИХ СИСТЕМ ГАЛУА ТА ЇХ ОСНОВНИХ ВЛАСТИВОСТЕЙ

Л.Б. Петришин - проф., д.т.н., зав. каф. Інформатики Прикарпатського національного університету ім. В.Стефаника (м. Івано-Франківськ) petryshynl@mail.ru

Застосування ефективних методів реалізації системних функцій інфотехнології на основі рекурсивних методів кодування дозволяє зменшити інтенсивність інфопотоків, що циркулюють в інфосистемі, та затрати обчислювальної потужності. Рекурсивне кодування Галуа класифікується до блокових поліномних циклічних повних методів кодування і характеризується скінченністю ряду розкладу, симетрією індексу і аргументу, та ізоморфізмом з лінійними Булевими функціями відповідної розмірності.

Вихідною є *рекурсивна* кодова система Галуа, що формується на базі послідовностей із звичайним логічним взаємозв'язком $n+1$ кодових елементів g між собою згідно

$$g_{i+1} = \sum_{i}^{i+n-1} a\, g_i \ (mod\ 2),$$

де a – значення вектора зворотних зв'язків.

Наведений метод кодування дозволяє реалізувати наступні переваги порівняно з існуючими системами кодування: - маршрутизацію повідомлень із розподіленим доступом до джерел повідомлень; - відбір даних про поточний стан джерела повідомлень в довільний момент часу; - самокоректування прийнятого спотвореного коду; - скорочення часу ідентифікації інтегрального стану джерела; - зменшення об'ємів оброблюваних повідомлень.

Проте, рекурсивній кодовій системі властивий

значний час ідентифікації стану джерел із низькою активністю. Автором вперше розроблена та досліджена кодонна кодова система Галуа, позбавлена вказаного недоліку. Математична модель синтезу кодових елементів кодонної системи визначається в векторній формі

$$N_i = f(g_{i0}, g_{i1}, \dots, g_{ij}, \dots, g_{i\,n-1}),$$

де g_{ij} - синхронізовані по знакомісцю елементи Галуа, j - номер кодона відліків.

Кодове поле породжується послідовністю, вектор-кодони якої утворюють байторієнтоване тривимірне упорядкування витків абстрактної спіралі n-розрядних $N-1$ кілець Галуа, замкнутих послідовно між собою в тор з циклом $M=n(N-1)=n(2^n-1)$. Час ідентифікації інтегральної характеристики зменшується до періоду слідування інформаційних повідомлень.

При мікроміниатюризації перетворювачів переміщень на основі кодових шкал виникають технологічні труднощі зчитування. Рознесення зчитувачів через постійну кількість кодових елементів дозволяє уникнути технологічних проблем. Автором вперше розроблена та досліджена система Галуа з дискретним розрідженням кодових послідовностей, що описується виразом

$$N_i = f(g_i, g_{i+v}, g_{i+2v}, \dots, g_{j+(n-1)v}),$$

де N_i - поточне значення відліку, v - коефіцієнт розрідження.

Поле Галуа; породжене розглянутим методом, володіє основними властивостями кодонної моделі при ноніусному зчитуванні та властивостями рекурсивної моделі - при звичайному.

Таким чином, використовуючи математичний апарат кодування Галуа, реальним є добір кодової системи, що кращим чином задовольняє техніко-економічні вимоги до перетворювачів форми інформації та враховує структуру сигналу перетворення.

УДК 621.391.837, 681.327.22

ОЦІНКА ЕФЕКТИВНОСТІ МЕТОДІВ КОДУВАННЯ

Л.Б. Петришин - проф., д.т.н., зав. каф. Інформатики Прикарпатського національного університету ім. В.Стефаника (м. Івано-Франківськ) petryshynl@mail.ru

Сучасний розвиток та широке впровадження інфотехнологій спричиняють значне зростання обсягів інфопотоків. При цьому об'єктивні обмеження щодо обчислювальної потужності систем чи пропускної здатності каналів та мереж інфообміну не дозволяють перевищити закладені значення вказаних параметрів. Одним із основних факторів виникнення такої кризи є домінуюче застосування двійкового числення. Як вказують результати проведеного аналізу, головним напрямком підвищення техніко-економічних параметрів є перехід до більш ефективних систем кодування.

Визначено, що в інфосистемах існує природна впорядкованість зміни форми інформації при її перетворенні із фізичного параметру в цифровий код. При перетворенні інформації з аналогової форми в цифрову явно чи опосередковано здійснюється перетворення в унітарний чи розрядно-позиційний код. З метою підвищення ефективності здійснюється кілька проміжних теоретико-числових перетворень (зокрема дискретно-фазових через коди Лібова-Крейга) та перехід до двійкового та кодування Грея. Проте останні відносяться до паралельних методів кодування, що накладає певні природні обмеження, елімінувати які та підвищити ефективність кодування можна при переході до рекурсивних методів формування інфопотоків. Такі

теоретико-числові перетворення здійснюються в полях Галуа із застосуванням рекурсивного кодування Галуа.

З метою визначення ефективності здійснено оцінку інформаційної потужності P кожного із методів кодування

$$P = N\,m,$$

де N - модуль кодової системи; m - мінімальна кількість розрядів однозначної ідентифікації повідомлення.

Значення P для основних методів кодування наведено в таблиці 1, а відповідні графіки - на рисунку 1.

Таблиця 1

код / система	**розрядність *m***	**потужність *P***
унітарна, Хаара	$m = N$	$P = m^2 = N^2$
Лібова-Крейга	$m = N/2$	$P = m\,N/2 = N^2/2$
двійкова, Грея	$m = log_2 N$	$P = log_2 N\,N$
Галуа (кодон., розр.)		
Галуа (рекурсив.)	$m_{min} = 1$	$P_{min} = N$

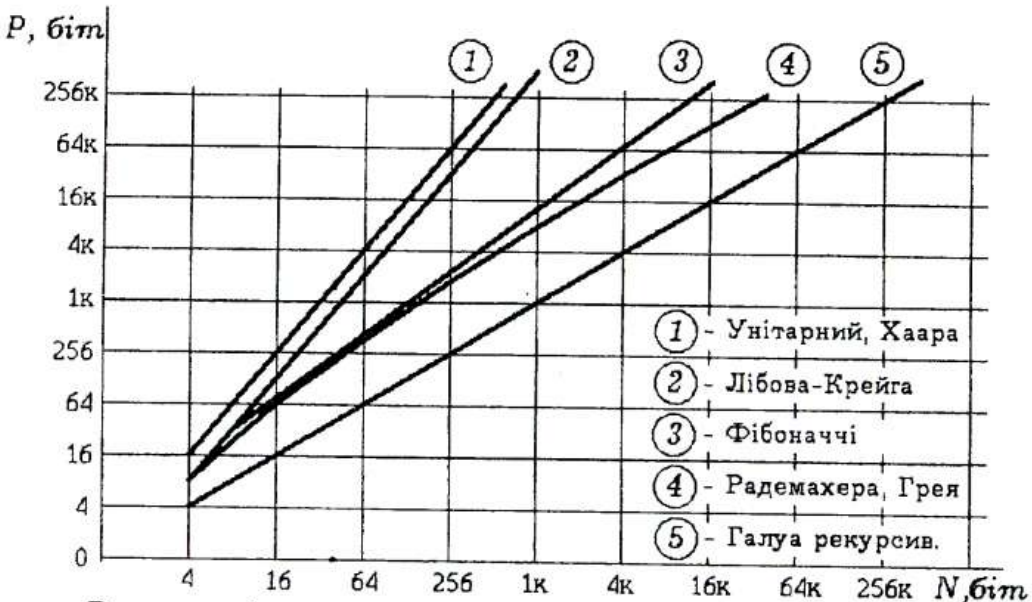

Рисунок 1

За отриманими результатами можна підсумувати меншу кодову потужність і, як наслідок, вищу ефективність кодування Галуа порівняно з відомими методами кодами.

УДК 621.038

СЖАТИЕ ДВОИЧНЫХ КОДОВ НА ОСНОВЕ БИНОМИАЛЬНЫХ ЧИСЕЛ

Чередниченко В. Б., ст. преподаватель
Национальный университет внутренних дел, филиал в г. Сумы. *E- mail* <chered_ukr@ukr.net>

В разнообразных электронных системах нередко применяется сжатие информации. Для сжатия равновесных кодов ранее были предложены простые алгоритмы, которые несложно реализовать аппаратными средствами. При этом исходные комбинации сначала превращаются в двоичные биномиальные коды, а затем последние преобразуются в номера.

Для расчета среднего числа тактов преобразования равновесных кодов в номера была предложена формула:

$$\overline{N} = (n - \frac{k(n-k)(n+2)}{(k+1)(n-k+1)}) + \frac{C_n^k - 1}{2} \qquad (1)$$

где n – длина кодовых комбинаций,

k – число единиц в комбинации.

Максимум среднего количества тактов преобразования кода в номер $\overline{N}_{max}$ находится в точке $k = n/2$ для четных значений n, а для нечетных n имеется два одинаковых максимума в точках $k = n/2 + 1/2$ и $k = n/2 - 1/2$. Два минимума этой функции находятся в точках k=1 и k= n- 1. Первым слагаемым в (1) можно пренебречь при $k \geq 3$.

Когда в коде неодинаковы вероятности $p_0, p_1, \ldots p_i, \ldots p_N$ появления различных кодовых комбинаций $b_0, b_1, \ldots b_i, \ldots b_N$, тогда среднее количество тактов нумерации $\overline{N}$ при

различной вероятности появления кодовых комбинаций равно:

$$\overline{N} = \sum_{i=0}^{N} p_i b_i = p_0 0 + p_1 1 + \ldots + p_i b_i + \ldots + p_N N \qquad (2)$$

Коэффициент уплотнения равновесных кодов равен:

$$S = n / log_2 C_n^k \qquad (3)$$

Этот коэффициент имеет максимальную величину при двух крайних значениях $k = 1$ и $k = n - 1$. Минимальный коэффициент уплотнения имеет место при $k = n/2$ для четных значений n, а для нечетных n минимум находится в двух точках $k = n/2 + 1/2$ и $k = n/2 - 1/2$.

Таким образом, при использовании описанных алгоритмов максимальное сжатие получается при минимальных затратах времени на преобразование.

Предлагается использовать данный метод для сжатия любых двоичных кодов длиной n. Для этого каждую из исходных кодовых комбинаций можно считать равновесной с количеством единиц k в ней. Тогда все сжатые комбинации будут содержать полученный после преобразования код и дополнительные данные о количестве единиц в каждой исходной последовательности $q = log_2 n$. При этом коэффициент уплотнения уменьшится:

$$S = n / log_2 C_n^k + log_2 n \qquad (4)$$

Проведенные расчеты показывают, что в окрестности точки $k = n/2$ имеется интервал, где сжатия не происходит. Для n=16 его относительная ширина равна 0,5n, а для n= 128 она уменьшается до 0,28n. Тогда при количестве единиц в исходной комбинации, соответствующем этому интервалу удлинения, целесообразно «пропускать» исходной код без обработки. Это улучшает характеристики сжатия и значительно уменьшает суммарное время преобразования.

УДК 004.627

МНОГОПОЛЬЗОВАТЕЛЬСКАЯ СИСТЕМА СЖАТИЯ ДАННЫХ С ОБЩИМ СЛОВАРЕМ

Ю.А. Зубань, доцент, к. т. н., СумГУ, yuza@ukr.net;
В.В. Петров, інженер, институт прикладной физики АН Украины

На сегодняшний день существует много подходов к сжатию информации и алгоритмов, их реализующих. Наиболее распространенными являются словарные методы. Наиб лее эффективные из них (семейство алгоритмов LZ78) основываются на замене строки символов в сжимаемом потоке на соответствующий номер элемента в словаре. Эффективность сжатия непосредственно зависит от размера словаря и его содержимого. Словарь, как правило, создается по мере. просмотра сжимаемого потока символов, поэтому начальные последовательности символов сжимаются менее эффективно, чем последние, когда словарь сформирован и в него входит достаточное количество записей, повторяющихся в сжимаемом потоке.

Эффективность словарных методов сжатия можно существенно повысить, если начинать процесс сжатия с готовым словарем, учитывающим наиболее вероятные последовательности символов в сжимаемом потоке, например слова украинского, английского или русского алфавита. По мере работы со словарем его содержимое может пополняться новыми словами и фразами.

Совместное использование словаря многими пользователями позволит динамически корректировать информацию о часто употребляемых фразах, а также обеспечит доступ к сжатым данным только в пределах группы пользователей, имеющих доступ к словарю. Это может быть востребовано в корпоративных информационных системах

УДК 681.32

ОЦЕНКА ЭФФЕКТИВНОСТИ СЖАТИЯ ИЗОБРАЖЕНИЙ МЕТОДОМ ЛОКАЛЬНЫХ СРЕЗОВ

Т.А. Протасова, ст. преп. каф. ЭКТ СумГУ

Под сжатием информации понимают операцию, в результате которой данному коду или сообщению ставится в соответствие более короткий код или сообщение. Особенно важным становится сжатие при передаче, хранении и обработке изображений.

В основе предложенного метода лежит нумерация локальных срезов – двоичных последовательностей, полученных в результате разложения многоуровневого сигнала.

Каждую отдельно взятую двоичную последовательность можно рассматривать как равновесную кодовую комбинацию. В результате каждое из 2^n двоичных сообщений источника A^* представляется в виде числа k, содержащихся в этом сообщении единиц, и относящейся к нему равновесной кодовой комбинации. Таким образом, осуществляется преобразование вероятностного источника A^*, генерирующего двоичные сообщения длиной n из их общего числа 2^n, в два других - источники A и B. Смысл такого преобразования состоит в том, что исходное множество из 2^n двоичных последовательностей разбивается на $(n+1)$ классов эквивалентности. Представителем класса эквивалентности в этом случае выступает число k единиц в двоичных кодовых комбинациях. Соответственно, источник A генерирует эти комбинации, а источник B - числа k. При этом число генерируемых сообщений в источниках A и B сокращается от 2^n до n.

Кроме того, равновесные кодовые комбинации, принадлежащие к одному и тому же классу эквивалентности, будут равновероятными и, следовательно, к ним можно применять структурные методы сжатия, использующие коды с равной длиной слов.

Наиболее эффективным в данном случае является применение специальной структурной системы счисления - биномиальной системы счисления с многозначным алфавитом. Двоичные последовательности, полученные в результате разложения по срезам, необходимо преобразовать в сочетание. Для этого последовательно в порядке возрастания запишем адреса (номера разрядов) единиц в кодовых комбинациях. Полученная монотонно возрастающая последовательность представляет собой сочетание. По разработанному алгоритму происходит переход от сочетания к многозначному биномиальному числу, и затем осуществляется нумерация этого биномиального числа.

Коэффициент сжатия для метода срезов характеризуется выражением:

$$K_{сж} = \frac{n \cdot m}{H(A,B)}$$

где n – длина кодовой последовательности,

m – количество срезов,

$H(A,B)$ – взаимная энтропия, определяется из следующего соотношения:

$$H(A,B) = H(A/B) + H(B) = -\sum_{k=0}^{n} C_n^k p_k \log_2 p_k$$

В зависимости от свойств изучаемого объекта коэффициент сжатия может достигать значительных величин от десяти и выше.

УДК: 621.391

РЕАЛІЗАЦІЯ ДИСКРЕТНИХ ТЕОРЕТИКО-ЧИСЛОВИХ ПЕРЕТВОРЕНЬ НАД ПОЛЯМИ ГАЛУА

Превисокова Н.В., асистент кафедри інформатики Прикарпатського національного університету імені Василя Стефаника, м. Івано-Франківськ, natvolo@rambler.ru

Для виконання основних завдань цифрового оброблення інформації (ЦОІ) розробляються методи дискретних теоретико-числових перетворень. Зростання обсягів інфопотоків зумовлює необхідність збільшення ефективності використання обчислювальних потужностей засобів ЦОІ, яка залежить від методу формування, перетворення, оброблення, схемотехнічної реалізації, форми подання інформації та, зокрема, від швидкості виконання арифметичних операцій при реалізації перетворень.

Для подання чисел в цифрових системах найчастіше використовується двійкова система числення. Проте, час виконання арифметичних операцій в двійковій системі залежить від розрядності пристрою внаслідок формування та поширення міжрозрядних переносів. Аналіз результатів розробки сучасних методів ефективних обчислень вказав на існування альтернативних методів кодування, зокрема, розроблений метод виконання арифметичних операцій додавання-віднімання та перемноження, що ґрунтується на паралельній обробці операндів із використанням рекурсивного упорядкування кодування Галуа.

З метою встановлення ефективності застосування методу кодування Галуа проаналізовано особливості виконання арифметичних модульних операцій, тобто

операцій додавання та множення за модулем $2^n - 1$ над розширеними полями Галуа GF(p^n), де p – просте, n – натуральне, у двійковій системі та операцій із використанням кодування Галуа і визначено час їх виконання.

Тривалість виконання операції додавання із поданням інформації у двійковій системі залежить від типу двійкового суматора. Проаналізовано час виконання додавання двійковими суматорами для паралельних операндів з паралельними переносами, які забезпечують досягнення максимальної швидкодії.

Порівняно із звичайним перемножувачем двійкових чисел, модульний перемножувач містить матрицю із n суматорів. Час виконання перемноження визначається сумою часу виконання операції перемноження двох чисел без приведення результату за модулем та часу зведення добутку за модулем $2^n - 1$.

Специфіка рекурсивного упорядкування методу кодування Галуа передбачає реалізацію арифметичних операцій додавання та перемноження на основі матриці програмованих логічних елементів, час доступу до яких не перевищує часу виконання відповідних операцій в двійковій системі числення.

Проаналізовано швидкодію пристроїв виконання арифметичних операцій двійковій системі числення та при Галуа-кодуванні. Встановлено, що час виконання арифметичних операцій в кодових системах Галуа менший, ніж при використанні двійкової системи числення. Проведені дослідження доводять ефективність за показником часу застосування Галуа-кодування для виконання арифметичних операцій над полями Галуа.

УДК: 621.391

МІЖСИСТЕМНІ ПЕРЕТВОРЕННЯ ФУНКЦІЙ ТА КОДОВИХ СИСТЕМ

Превисокова Н.В., асистент кафедри інформатики Прикарпатського національного університету імені Василя Стефаника, м. Івано-Франківськ, natvolo@rambler.ru

Останнім часом невпинно розширюються галузі застосування складних інформаційних систем, які включають засоби формування, перетворення, передавання та оброблення повідомлень. При реалізації системних функцій в цифрових системах використовуються різні коди, та виникає потреба у їх перетворенні. Розробка та реалізація ефективних процедур перетворення форми та оброблення інформації зумовлює необхідність встановлення методів, відповідності та взаємозалежностей перетворень між системами функцій і кодами чи системами кодування.

На першому етапі реалізації системної функції перетворення інформації в більшості систем використовуються унітарні та розрядно-позиційні коди, які породжуються відповідно унітарними та функціями Хаара. Вказана група кодів при реалізації функції перетворення інформації вимагає великих апаратурних затрат, оскільки для кодування N дискретних повідомлень потребує повної N–бітової розрядної мережі кодового подання. Зменшити розрядність коду до $N/2$ дозволяють коди Лібова-Крейга, які породжуються дискретно-фазовими функціями. Необхідність зменшення апаратурних затрат зумовила

перехід до ефективніших методів кодування із зменшеною розрядністю кодів до $n=log_2N$.

Дискретно-фазові функції дозволяють здійснити перехід до систем Радемахера та Грея, на основі яких творяться n-розрядні двійковий та код Грея, котрі набули широкого застосування при реалізації функцій перетворення та цифрового оброблення повідомлень в сучасних інфосистемах.

Аналіз ефективності реалізації системних функцій та сучасних методів кодування дозволив визначити одним із найбільш ефективних метод Галуа-кодування. Проведені дослідження дозволили встановити процедури переходу із систем Радемахера та Грея, а також двійкового та коду Грея до системи Галуа через проміжне перетворення до базису Уолша.

На підставі аналізу зазначених систем дискретних функцій і відповідних кодових систем визначено методи їх формування та перетворень між ними, встановлено аналітичні та логічні взаємозалежності. Доведено відповідність логічних залежностей методів перетворень кодів аналітичним залежностям методів перетворень породжуючих систем функцій. Синтезовано схеми відповідних перетворювачів кодів, які можуть використовуватись у засобах перетворення та оброблення повідомлень, здійснено аналіз їх складності та швидкодії.

З єдиних позицій здійснено аналіз та встановлено ряд проміжних систем дискретних функцій та базисів та творених відповідних кодів чи кодових систем, що лежать в основі подання, перетворення форми та оброблення інформації. Встановлені методи перетворень, логічні та аналітичні залежності між кодовими системами та системами функцій дозволяють аналітично описати та реалізувати відповідні процедури перетворення форми інформації.

УДК 519.7

АНАЛІЗ ЕФЕКТИВНОСТІ ВИКОНАННЯ ЕЛЕМЕНТАРНИХ АРИФМЕТИЧНИХ ОПЕРАЦІЙ В РІЗНИХ СИСТЕМАХ КОДУВАННЯ

Монастерецький В.В., аспірант,
Прикарпатський національний університет
імені Василя Стефаника
E-mail:vvn@il.if.ua

В галузі цифрової обробки повідомлень вирішуються задачі кодування, цифрового прийому, декодування та обробки інфопотоків на основі арифметико-логічних та дискретних теоретико-числових перетворень. При цьому техніко-економічна ефективність цифрової обробки інформації визначається формою подання вхідних даних, методами кодування та закладеними алгоритмами. Актуальність завдання розробки сучасних методів ефективних обчислень зумовлена невпинним зростом точності подання даних та результатів, який спричиняє до розширення їх розрядності (в системах радіолокації і обробки зображень) та розмірності вирішуваних задач (в комп'ютерній томографії, сейсмодіагностиці і метеорології), що в процесі обробки зумовлює до значного зростання об'ємів обчислень і вимагає розробки та впровадження швидких високоефективних алгоритмів.

Основною перевагою арифметики Галуа над іншими системами кодування полягає у відсутності міжрозрядних переносів і можливості обчислення кожного із бітів цілого слова результату як суми за модулем 2 за один такт.

Відомо, що найвищою швидкодією володіють методи із розпаралеленням обчислення результатів цифрової

обробки. Той факт, що на сьогоднішній день не відомі методи паралельного виконання арифметичних операцій безпосередньо в кодах Ґалуа, зумовив актуальність проведення досліджень щодо можливості реалізації та розробки основ бінарної арифметики реального часу в полях Ґалуа.

Результати досліджень вказали на ефективність теоретико-числових перетворень із застосуванням теорії полів Ґалуа, які дозволяють реалізувати швидкі прямі алгоритми обчислень, що зумовлені простотою апаратної реалізації на базі процедур зсуву. Коди Ґалуа володіють одними із кращих характеристиками кодової і кореляційних функцій, а також множинністю алгоритмів декодування, які реалізуються на основі високорегулярних послідовних структур.

Розроблений метод виконання основних арифметичних операцій в кодах Ґалуа ґрунтується на безпосередній паралельній обробці операндів на підставі синтезованих логічних функцій порозрядного сумування за *mod p*. Прикладне застосування пропонованого методу виконання арифметичних операцій полягає у розробці кодових матриць визначеного перетворення системи кодів.

Аналіз вказує на вищу швидкодію процесорів Ґалуа, Виграш в швидкодії досягається за рахунок нарощування потужності апаратних засобів, оскільки потребує використання масиву програмованих логічних елементів ємністю $n \times n^2$, поля n^2 ключів комутації і n-входових пристроїв сумування за *mod 2*.

Перевагою структур арифметичних процесорів Ґалуа є високий ступінь однорідності обчислювального середовища, що визначає перспективу їхньої реалізації в мікроелектронному виконанні.

УДК 621.375

МЕТОД СКАНУЮЧОГО АНАЛОГО-ЦИФРОВОГО ПЕРЕТВОРЕННЯ НА БАЗІ КОДУВАННЯ ГАЛУА

Овчар І.Є. - аспірант каф. Інформатики Прикарпатського національного університету ім. В.Стефаника (м. Ів-Франківськ) iovchar@mail.ru

Процедура аналого-цифрового (АЦ) перетворення є однією із основних системних функцій інфотехнології при перетворенні форми інформації. В більшості випадків АЦ перетворення здійснюється безпосередньо біля джерела повідомлень із наступною передачею цифрових даних по каналах зв'язку в систему обробки. Оскільки відомі методи АЦ перетворення передбачають формування вихідних повідомлень у паралельному форматі, а передача інформації в розподіленій системі здійснюється в послідовному, то виникає необхідність додаткового перетворення паралельних кодів у послідовні, що потребує додаткових затрат часу та апаратури. Підвищити ефективність інфообміну дозволяє реалізація безпосереднього АЦ перетворення в послідовному форматі та передача повідомлень до каналу зв'язку на базі рекурсивних методів кодування повідомлень, зокрема, кодування Галуа.

Кодові елементи послідовностей Галуа володіють основними властивостями рекурсивної упаковки, логічного взаємозв'язку та неповторимості довільних n-розрядних кодових фрагментів в повному кільці Галуа розмірності $N=2^n$, які вперше дозволили розробити новий клас методів скануючого АЦ перетворення Галуа та паралельних АЦ перетворювачів Галуа із послідовним виходом, звузити діапазон розгортки від $0 \div N-1$ для

інтегруючих перетворювачів до n для скануючих АЦ перетворювачів Галуа.

На рис. 1 наведено приклад сканування послідовності Галуа $GF(2^n)$. Динамічний діапазон зміни вхідної вимірюваної аналогової величини $U_{x\,min} \div U_{x\,max}$ квантується на кількість рівнів, відповідну довжині $0 \div N-1$ послідовності Галуа.

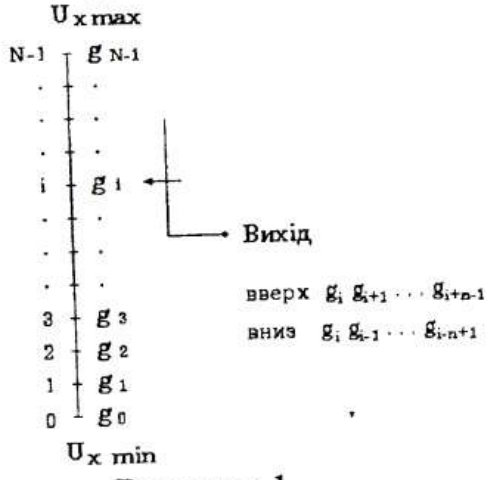

Рисунок 1

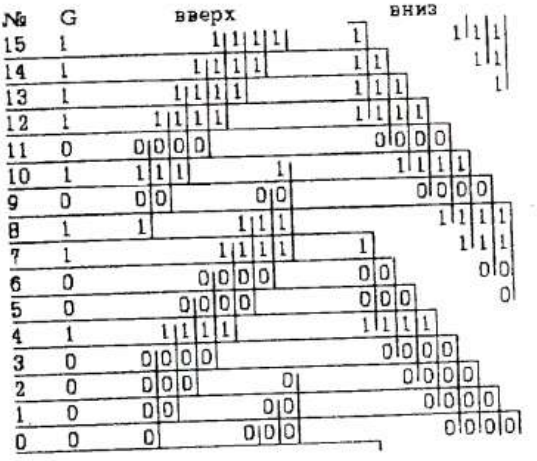

Рисунок 2

Кожному із квантованих рівнів аналогової величини U_x надається кодова ознака $g_0, g_1, \ldots, g_i, \ldots, g_{N-1}$ із послідовності Галуа. Для АЦ перетворення i-го значення U_{xi} достатньо здійснити вольтзміну із послідовною в часі розгорткою n квантів вхідної величини. Можна проводити зміну як самої вхідної величини U_x, так і значення опорної напруги U_{on}, також інваріантним є напрямок вольтдобавки, що необхідно враховувати при декодуванні коду перетворення. На рис. 2 наведено приклад формування кодових відліків перетворення внаслідок розгортки n-розрядних фрагментів послідовності Галуа $GF(2^4)$.

Таким чином, наведено результати розробки методичних, принципових та схемотехнічних рішень побудови засобів АЦ перетворення із скануванням по вимірюваному сигналу U_x та по опорному U_{on}.

УДК 681.518

БИНОМИАЛЬНАЯ СИСТЕМА ГЕНЕРИРОВАНИЯ РАВНОВЕСНЫХ КОДОВ

Кулик И.А., к.т.н., доцент, Лысенко М.А. магистр
Сумский государственный университет
e–mail: Kulik@pe.sumdu.edu.ua

Для асимметричных каналов связи эффективными являются равновесные коды. При полностью асимметричном канале данные коды считаются идеальными. При построении n–разрядного кода с постоянным весом отношение единиц m к количеству нулей $(n–m)$ выбирается так, чтобы обеспечить необходимое количество разрешенных комбинаций. Таким образом, количество комбинаций может быть найдено как число сочетаний из n элементов по m: C^n_m.

Преобразование двоичной информации в равновесный код сопряжено с трудностями схемотехнического характера. Для упрощения аппаратурной реализации предлагается проводить преобразование не за один этап, а за два. Такое кодопреобразование осуществляется с использованием биномиальных кодов, формируемых на основе двоичной биномиальной системы счисления. Двоичной k – биномиальной системой счисления называется числовая функция:

$$F = x_{i-1} \cdot C_{n-1}^{k-q_{n-1}} + \ldots + x_i \cdot C_{n-r+i}^{k-q_i} + \ldots + x_1 \cdot C_{n-r+1}^{k-q_1} + x_0 \cdot C_{n-r}^{k-q_0}$$

с системами кодообразующих ограничений:

$$\begin{cases} k \le r \le n-1, \\ q = k, \\ x_0 = 1 \end{cases} \quad \text{и} \quad \begin{cases} q-k = r-q, \\ 0 \le q \le k-1, \\ x_0 = 0 \end{cases}$$

где r – количество разрядов биномиального числа (длина), $r \in 1,2,...$; k – максимальное количество единиц в биномиальном числе; i – порядковый номер разряда, $i = 0, 1,..., r\text{-}1$; x_i – биномиальная двоичная цифра – 0 или 1; n – целочисленный параметр системы счисления; q – число единиц в биномиальном числе; q_i – сумма единичных значений цифр x_i от $(r\text{-}1)$ – го разряда до $(i+1)$ – го включительно:

$$q_i = \sum_{j=i+1}^{r} x_j$$

где $i = 0, 1, ...,r\text{-}1$; $x_r = 0$.

В предлагаемом алгоритме используются равномерные двоичные биномиальные кодовые комбинации, которые содержат или n нулей, или k единиц, или $(n\text{-}k)$ нулей в старших разрядах перед младшей единицей. Количество n–разрядных биномиальных чисел: $N = C_{n+1}^{k}$

Обобщенная структура биномиальной системы генерирования равновесных кодов будет иметь следующий вид (рис. 1):

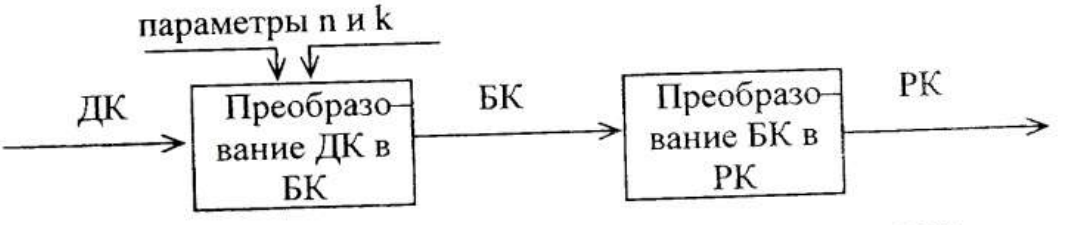

Рис. 1 – Структура биномиальной системы генерирования равновесных кодов (ДК–двоичный код, БК–биномиальный код, РК–равновесный код)

Полезными свойствами биномиальной системы счисления являются: 1) помехоустойчивость при передаче, хранении и обработке информации; 2) способность перебирать, генерировать и нумеровать комбинации кодов с постоянным весом; 3) возможность построения помехоустойчивых цифровых устройств.

УДК 681.5

ОЦЕНКА ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ НЕЙРОПОДОБНОГО КЛАССИФИКАТОРА СООБЩЕНИЙ В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТИ

Полонский А. Д., доц., Бражник И.Е., СумГУ
e-mail: electron@sumdu.edu.ua

Широкое применение систем передачи данных (СПД) явилось толчком к развитию методов исследования функционирования нейроподобных классификаторов (НПК) сообщений. Известные подходы к определению эффективности функционирования НПК базируются на методах теории статистических решений. В то же время НПК функционирует в условиях действия большого количества факторов не стохастического характера. В связи с этим возникает проблема оценивания эффективности функционирования НПК в условиях неопределенности (УН) нестатистической природы.

В докладе сформулирована задача оценивания эффективности функционирования НПК в УН на множестве нечетких отношений типа нестрого порядка. В качестве критерия эффективности использована функция принадлежности максимального числа сообщений нечеткому множеству, которые может распознать НПК в единицу времени с допустимым уровнем вероятностей ошибок. Показано, что с уменьшением нечеткости представлений о потоках информации в СПД и возможностях НПК критерий эффективности вырождается в единичную функцию. Это соответствует детерминированной оценке эффективности НПК при точном задании исходных данных.

Научное издание

Третья международная научная конференция

"СОВРЕМЕННЫЕ МЕТОДЫ КОДИРОВАНИЯ В ЭЛЕКТРОННЫХ СИСТЕМАХ"

СМКЭС-2006

(24-25 октября 2006)

ТЕЗИСЫ ДОКЛАДОВ

Ответственный за выпуск проф. А.А. Борисенко

Компьютерный набор И.Е. Бражник

Стиль и орфография авторов сохранены.

Подп. в печ.18.10.2006 г.
Формат 60x84/16.
Усл.печ.л. 4,88. Тираж 60 экз. Заказ № 633.
Уч.-изд.л. 3,27.
Издательство СумГУ. Свидетельство ДК№2365 от 08.12.2005
40007, г.Сумы, ул. Р.-Корсакова, 2.
Типография СумГУ. 40007, г.Сумы, ул. Р.-Корсакова, 2.