ISSN 2519-2310

COMPUTER SCIENCE AND CYBERSECURITY

ISSUE 2(6) 2017

V. N. Karazin Kharkiv National University Publishing

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УКРАИНЫ
MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені В.Н.КАРАЗІНА
ХАРЬКОВСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ имени В.Н. КАРАЗИНА
V.N. KARAZIN KHARKIV NATIONAL UNIVERSITY

КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА
КОМПЬЮТЕРНЫЕ НАУКИ И КИБЕРБЕЗОПАСНОСТЬ
COMPUTER SCIENCE AND CYBERSECURITY
(CS&CS)

Issue 2(6) 2017

Заснований 2015 року

Міжнародний електронний науково-теоретичний журнал
Международный электронный научно-теоретический журнал
International electronic scientific journal

The journal publishes research articles on theoretical, scientific and technical problems of effective facilities development for computer information communication systems and on information security problems based on advanced mathematical methods, information technologies and technical means.

Journal is published quarterly.
Approved for placement on the Internet by Academic Council of the Karazin Kharkiv National University (September 25, 2017, protocol No.13)

Editorial office:
Karazin Kharkiv National University
Svobody sq., 6, office 315a, Kharkiv, 61022, Ukraine
Phone: +38 (057) 705-10-83
E-mail: *cscsjournal@karazin.ua*
Web-page: *http://periodicals.karazin.ua/cscs (Open Journal System)*

Published articles have been internally and externally peer reviewed

TABLE OF CONTENTS

Issue 2(6) 2017

УДК 681.142

L-КОДЫ В СИСТЕМЕ ОСТАТОЧНЫХ КЛАССОВ

Виктор Краснобаев[1], Сергей Кошман[2], Алина Янко[3]

[1] Харьковский национальный университет имени В. Н. Каразина, пл. Свободы, 4, Харьков, Украина
krasnobaev@karazin.ua

[2] Харьковский национальный технический университет сельского хозяйства имени Петра Василенка, ул. Артема, 44 Харьков, Украина
s_koshman@ukr.net

[3] Полтавский национальный технический университет имени Юрия Кондратюка, Первомайский проспект 24, г. Полтава, 36011, Украина
al9_yanko@ukr.net

Рецензент: Ирина Лисицкая, д-р тех. наук, проф.,
член-корреспондент Академии наук прикладной радиоэлектроники,
Харьковский национальный университет имени В.Н. Каразина, площадь Свободы 4, г. Харьков, 61022, Украина
lisitska@karazin.ua

Поступила март 2017

Аннотация. *В статье разрабатывается метод коррекции ошибок данных в системе остаточных классов (СОК), основанный на применении корректирующих свойств L-кодов, которые образуются при использовании взаимно попарно не простых оснований. Данный метод позволяет расширить класс корректируемых ошибок, что расширяет корректирующие возможности L-кодов. Представлены примеры выполнения операции коррекции, а также описаны особенности реализации устройства для обнаружения ошибок данных.*

Ключевые слова: *система счисления, система остаточных классов, коррекция ошибок, компьютерная система, непозиционная кодовая структура.*

1 Введение

В настоящее время интенсивно исследуются возможности R-кодов для реализации арифметических операций, а также для коррекции ошибок в системе остаточных классов (СОК) [1,2]. Это объясняется простотой структуры R-кодов и хорошими корректирующими возможностями, а также сравнительной простотой их построения для любого заданного минимального кодового расстояния.

Представляется важным и интересным рассмотрение так называемых линейных кодов (L-кодов) в СОК. В литературе эти коды описываются скорее качественно, чем количественно. Дело в том, что до настоящего времени никто не занимался глубоким изучением свойств систем остаточных классов, основания которых не являются взаимно простыми числами. Подобная СОК также обладает определенными корректирующими свойствами, что обусловливает необходимость оценки возможности и целесообразности применения таких систем для повышения надежности компьютерных систем и компонент обработки целочисленных данных (КСКОЦД).

Цель статьи – разработка метода коррекции ошибок данных в СОК, расширяющего корректирующие возможности L-кодов.

2 Основная часть

Однако, если ограничить класс возможных ошибок в отдельных остатках кодовых слов, возможности L-кодов существенно расширяются.

Рассмотрим *лемму 1*. Для любого целого числа $A=(a_1, a_2, ..., a_n)$ в системе остаточных классов с основаниями m_i $(i=\overline{1,n})$ и для любой пары оснований m_i и m_j должно выполняться условие

$$(a_i - a_j) \equiv 0(\mathrm{mod}\, d_{ij}),$$

где $d_{ij}(m_i, m_j)$ наибольший общий делитель оснований m_i и m_j, а $i, j = \overline{1,n}$; $i \neq j$.

Для определения необходимых и достаточных условий для обнаружения однократных ошибок с помощью L-кодов по результатам леммы 1 сформулирована и доказана следующая теорема.

Теорема 1. Для обнаружения ошибок в остатке по произвольному основанию m_i $(i = \overline{1,n})$ числа $A = (a_1, a_2, ..., a_n)$, заданного в системе остаточных классов с основаниями $m_1, ..., m_n$, необходимо, чтобы основание m_i имело хотя бы один, отличный от единицы, общий делитель с остальными основаниями m_i $(i \neq j)$.

Доказательство. Пусть НОД $d_{ij}(m_i, m_j)$ определен для произвольных оснований МА $(i \neq j)$, и ошибка произошла по основанию m_i, т.е. $a_i = a_i + \Delta a_i$. Покажем, что выражение $(a_i - a_j) \bmod d_{ij}$ эквивалентно $\Delta a_i (\mathrm{mod}\, d_{ij})$. Согласно лемме выполняется следующее равенство

$$(a_i - a_j) = 0(\mathrm{mod}\, d_{ij}).$$

Запишем выражение

$$a_i + \Delta a_i = a_i (\mathrm{mod}\, m_i)$$

в виде

$$a_i + \Delta a_i = m \cdot m_i + a_i,$$

где m – целое число. Из последнего выражения определим искаженный остаток

$$a_i = a_i + \Delta a_i - m \cdot m_i.$$

Тогда можно записать

$$a_i - a_j = \left[(a_i - a_j) + (-mkd_{ij}) + \Delta a_i \right].$$

Так как

$$(a_i - a_j) \equiv 0(\mathrm{mod}\, d_{ij}) \text{ и } -mkd_{ij} \equiv 0(\mathrm{mod}\, d_{ij}),$$

где $m_i = kd_{ij}$, а k – натуральное число, то

$$(a_i - a_j) \equiv \Delta a_i (\mathrm{mod}\, d_{ij}).$$

Очевидно, что при отсутствии общих делителей, т.е. если $d_{ij} = 1$, тогда $\Delta a_i \equiv (\mathrm{mod}\, d_{ij})$. Это и доказывает необходимое условие теоремы.

Необходимое условие теоремы является достаточным, если ошибка не кратна делителю d_{ij}.

Действительно,

$$(md_{ij} + a_{ij}) \neq 0(\mathrm{mod}\, d_{ij}),$$

для $0 < a_{ij} < d_{ij}$.

Теорему 1 можно сформулировать еще следующим образом.

Для обнаружения ошибки в остатке по произвольному основанию m_i числа $A = (a_1, a_2, ..., a_n)$, заданного в СОК, необходимо и достаточно, чтобы ошибка Δa_i была не кратна делителям d_{ij} и $d_i = (d_{i1}, d_{i2}, ..., d_{in})$, где d_i – НОД делителей $d_i = (d_{i1}, d_{i2}, ..., d_{in})$.

На основании результатов теоремы 1 составим алгоритм обнаружения ошибок. Проверяем остаток по основанию m_i. Для этого определим совокупность значений

$$a_1 - a_2 = a_{12} (\mathrm{mod}\, d_{12}),$$
$$a_1 - a_3 = a_{13} (\mathrm{mod}\, d_{13}),$$

$$a_1 - a_n = a_{1n}(\mathrm{mod}\, d_{1n}).$$

Если $a_{1i} = (\mathrm{mod}\, d_{1i})$, то проверяется второй остаток и т. д.

2. Для получения значений a_{ij} $(i \neq j)$ составляем матрицу

$$G = \begin{vmatrix} a_{12} & a_{13} \ldots & a_{1n} \\ a_{21} & a_{23} \ldots & a_{23} \\ & \ldots & \\ a_{n1} & a_{n2} \ldots & a_{nn-1} \end{vmatrix}$$

При составлении матрицы G не обязательно указывать истинное числовое значение a_{ij}, достаточно представить его отличительный признак

$$a_{ij} = \begin{cases} 0, \textit{ если } a_i - a_j = 0(\mathrm{mod}\, d_{ij}), \\ 1, \textit{ если } a_i - a_j \neq 0(\mathrm{mod}\, d_{ij}). \end{cases}$$

Если определитель матрицы $|G| = 0$, то число $A = (a_1, a_2, ..., a_n)$ – правильное, а если $|G| \neq 0$, то число A – неправильное.

Рассмотрим соображения, позволяющие упростить вышеприведенный алгоритм.

Исходя из того, что

$$a_i - a_j \equiv [d_{ij} - (a_i - a_j)](\mathrm{mod}\, d_{ij}),$$

определитель $|G|$ можно не находить. Достаточно определить диагональные элементы матрицы G и добавить одно значение a_{n+1}, т.е.

$$a_{12}, a_{23}, a_{34}, ..., a_{n-1\,n}, a_{n1}.$$

Легко проверить, что при таких значениях a_{ij}, возможно, установить не только факт искажения кодового слова, но и определить номер искаженного остатка.

С целью определения необходимых и достаточных условий для исправления однократных ошибок с помощью L-кодов сформулирована и доказана следующая теорема.

Теорема 2. Для исправления ошибки в остатке по произвольному основанию m_i числа $A = (a_1, a_2, ..., a_n)$, заданного в системе остаточных классов с основаниями $m_1, m_2, ..., m_n$, необходимо, чтобы выполнялось условие

$$(d_{ik} - 1)(d_{ij} - 1) \geq m_i - 1 - (K_{d_{ik}} + K_{d_{ij}} - K_{[d_{ik}, d_{ij}]}), \qquad (1)$$

где $d_{ik} = (m_i, m_k)$, $d_{ij} = (m_i, m_j)$, $K_{d_{ik}}$ - количество делителей, кратных d_{ik}; $K_{d_{ij}}$ - количество делителей, кратных d_{ij};

$K_{[d_{ik}, d_{ij}]}$ - количество делителей, кратных наименьшему общему кратному (НОК) $[d_{ik}, d_{ij}]$ делителей d_{ik} и d_{ij}, $i \neq j$.

Доказательство. Вычислим значения a_{ij}, a_{ik}, a_{jk}. Если ошибка произошла по основанию m_i, то $a_{ik} = 0$, а $a_{ij} \neq 0$ и $a_{jk} = 0$. Число различных комбинаций a_{ij}, a_{ik} равно $(d_{ij} - 1) \cdot (d_{ik} - 1)$, где $(d_{ij} - 1)$ – число возможных значений величины a_{ij} $(a_{ij} \neq 0)$, $(d_{ik} - 1)$ – число возможных значений a_{ik} $(a_{ik} = 0)$, а число возможных значений ошибок по основанию m_i равно $m_i - 1$ $(\Delta a_i \neq 0)$ за вычетом числа необнаруженных ошибок. Число необнаруженных ошибок состоит из числа ошибок, кратных делителю $d_{ik} - K_{d_{ik}}$ и кратных делителю $d_{ik} - K_{d_{ik}}$. Таким образом, число возможных значений обнаруживаемых ошибок равно

$$m_i - 1 - (K_{d_{ik}} + K_{d_{ij}} - K_{[d_{ik},d_{ij}]}).$$

Для обеспечения соответствия возможным значениям ошибок по основанию m_i необходимо выполнение неравенства (1). Что и требовалось доказать.

Необходимое условие теоремы 2 является достаточным, если различным значениям ошибок Δa_i соответствуют различные значения произведения $a_{ik} \cdot a_{ij}$, и наоборот.

Действительно, в этом случае между возможными значениями Δa_i и значениями произведения $a_{ik} \cdot a_{ij}$ существует взаимно однозначное соответствие, что и определяет возможность однозначно определить величину ошибки.

На основании теоремы 2 составим алгоритм коррекции ошибок по произвольному основанию m_i:

1. Определим номер искаженного остатка. Для этого вычислим значения

$$a_1 - a_2 = a_{12} (\mathrm{mod}\, d_{12}),$$
$$a_2 - a_3 = a_{23} (\mathrm{mod}\, d_{23}),$$
$$\dots$$
$$a_{n-1} - a_n = a_{n-1n} (\mathrm{mod}\, d_{n-1n}),$$
$$a_n - a_1 = a_{n2} (\mathrm{mod}\, d_{n1}).$$

Если все остатки $a_{ij} = 0 (\mathrm{mod}\, d_{ij})$, то число A правильное. Если ошибка произошла по основанию m_i, то $a_{ij} \neq 0$ и $a_{ik} \neq 0$ и, таким образом, проверяемое число $A = (a_1, a_2, ..., a_i, ..., a_n)$ является неправильным.

2. По значениям a_{ij} и a_{ik} обращаемся в блок констант ошибок, где выбираем соответствующее значение Δa_i.

3. Производим коррекцию числа A в остатке a_i, и получаем правильное число $A = A - \Delta A$, т.е.

$$A = (a_1, a_2, ..., a_i, ..., a_n).$$

Если в сокращенной СОК за счет исключения основания, по которому произошла ошибка, можно однозначно представить число A, то вместо определения по значениям a_{ij} и a_{ik} величины ошибки Δa_i, непосредственно вычислим значения правильного остатка a_i.

Рассмотрим этот алгоритм коррекции ошибок.

1. Вычислим значение остатков $a_{12}, a_{23}, ..., a_{n1}$.

2. Определим номер искаженного остатка. Пусть ошибка произошла по m_i основанию. В этом случае это основание исключается, а число A представляется по основаниям $m_1, m_2, ..., m_n$, т.е.

$$A = (a_1, a_2, ..., a_{i-1}, a_{i+1}, ..., a_n).$$

3. Произведем свертку числа A в позиционный код.

4. Определим истинное значение искаженного остатка

$$a_i = A - \left[A / m_i\right] m_i,$$

где $[x]$ – целая часть x, не превосходящая x. Исправленное число

$$A_{исп} = (a_1, a_2, ..., a_i, ..., a_n).$$

Определим условия, при которых возможно исключение из СОК некоторых оснований. Для этого представим основания исходной СОК в каноническом виде

$$m_1 = \beta_{11}^{a_{11}} \beta_{12}^{a_{12}} \dots \beta_{1l_1}^{a_{1l_1}},$$

$$m_2 = \beta_{21}^{a_{21}} \beta_{22}^{a_{22}} \dots \beta_{2l_2}^{a_{2l_2}},$$
$$\dots$$
$$m_n = \beta_{n1}^{a_{n1}} \beta_{n2}^{a_{n2}} \dots \beta_{nl_n}^{a_{nl_n}},$$
$$M = \beta_1^{a_1} \beta_2^{a_2} \dots \beta_k^{a_k}.$$

Для однозначного определения числа A, заданного в СОК с основаниями $m_1, m_2, ..., m_n$, и лежащего в диапазоне $[0, M)$ можно исключить только те основания, для которых $\beta_m = \beta_{il_i}$, ($m = \overline{1,k}$, $i = \overline{1,n}$). При этом необходимо, чтобы $a_m \geq a_{il_i}$.

Таким образом, определены необходимые и достаточные условия коррекции ошибок методом исключения искаженного основания. Этими условиями является одновременное выполнение равенства и неравенства

$$\beta_m = \beta_{il_i},\ a_m \geq a_{il_i} \quad (2)$$

Пусть задана СОК основаниями $m_1 = 4$, $m_2 = 6$, $m_3 = 12$, $m_4 = 18$. При этом $M = [4, 6, 12, 18] = 36$. В соответствии с условием возможности коррекции ошибок (2) определим те основания СОК, которые можно исключить. Представим основания СОК в каноническом виде: $m_1 = 2^2$, $m_2 = 2 \cdot 3$, $m_3 = 2^2 \cdot 3$, $m_4 = 2 \cdot 3^2$ и $M = 2^2 \cdot 3^2$. Очевидно, что искомые основания - m_1, m_2, m_3. Произведем проверку, для чего составим частные значения НОК:

$$M_1 = [6, 12, 18] = 36,$$
$$M_2 = [4, 12, 18] = 36,$$
$$M_3 = [4, 6, 18] = 36,$$
$$M = [4, 6, 12] = 36.$$

Частное значение НОК $M_4 < 36$, что подтверждает правильность определения исключаемых оснований из заданной СОК.

Выше был представлен алгоритм обнаружения и исправления ошибок в СОК посредством L-кодов. Пусть при вычислении значений $(a_k - a_{k+1}) \bmod d_{kk+1}$ определено, что $a_{i-1\,i} \neq 0$, $a_{i\,i+1} \neq 0$, а все остальные значения равны

$$a_{k\,k+1} = (a_k - a_{k+1}) \bmod d_{k\,k+1} = 0.$$

Тогда утверждается, что число А неправильное, а ошибка присутствует в остатке по основанию m_i, т.е.

$$A = (a_1, a_2, ..., a_i, ..., a_n).$$

Обращаясь по значениям $a_{i-1\,i}$ и $a_{i\,i+1}$ в блок констант ошибок определим значение ошибки Δa_i и далее определим истинное значение остатка

$$a_{i\,ucn} = a_i - \Delta a_i.$$

Исправленное число представится в виде

$$A_{ucn} = (a_1, a_2, ..., a_{i\,ucn}, ..., a_n).$$

Для исправления ошибки с помощью разработанного метода, необходимо, чтобы ошибка Δa_i была одновременно не кратна двум делителям $d_{i-1\,i}$ и $d_{i\,i+1}$, что ограничивает класс корректируемых ошибок.

Таким образом, очевидна необходимость разработки эффективных методов и алгоритмов, позволяющих расширить класс возможных корректируемых ошибок.

Метод коррекции однократных ошибок, позволяющий исправлять ошибки, кратные одному из делителей $d_{i-1\,i}$ или $d_{i\,i+1}$, состоит в следующем.

Пусть задана СОК со взаимно не простыми основаниями, т.е. НОД

$$(m_1, m_2, ..., m_n) \geq 2.$$

И пусть задано число в СОК

$$A_{исп} = (a_1, a_2, ..., a_n).$$

Определим все значения $a_{k\,k+1}$, т.е. $a_{12}, a_{23}, a_{34}, ..., a_{n-1\,n}, a_{n\,1}$. Не нарушая общности рассуждений, будем считать, что $a_{i\,i+1} \neq 0$, а все остальные значения $a_{k\;k+1} \neq 0$.

Так как

$$a_{i\,i+1} = (a_i - a_{i+1}) \bmod d_{i\,i+1} \neq 0,$$

то ошибка может присутствовать только в остатках по основаниям m_i или m_{i+1}. В связи с этим возможны две гипотезы:

- ошибка присутствует в остатке a_i;

- ошибка присутствует в остатке a_{i+1}.

Прежде чем рассмотреть процесс коррекции ошибок предлагаемым методом, сформулируем и докажем теорему, результат доказательства которой используем при определении процесса сходимости совокупности чисел вида

$$A^{(k_i)} = (a_1, ..., a_{i-1}, a_{ik_i}, a_{i+1}, ..., a_n)$$

к правильному числу

$$A^{(\rho)} = (a_1, ..., a_{i-1}, a_{i\rho}, a_{i+1}, ..., a_n).$$

Предварительно рассмотрим лемму.

Лемма 2. Сумма, разность и произведение любых кодовых слов являются также кодовыми словами.

Теорема 3. Пусть в упорядоченной ($m_{i-1} < m_i; i = \overline{1, n}$) системе остаточных классов с основаниями $m_1, m_2, ..., m_n$ задано неправильное (искаженное в одном остатке) число

$$A = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n)$$

и пусть

$$\Delta a_i = a_i - a_i = k_i d_{i-1\,i}.$$

Тогда в совокупности значений

$$a_{ik_i} = (a_i - k_i d_{i-1\,i}) \bmod m_i$$

существует такое единственное значение $a_{i\rho}$, при котором число

$$A^{(\rho)} = (a_1, a_2, a_{i\rho}, ..., a_n)$$

является правильным числом, где $d_{i-1\,i}(m_{i-1}, m_i)$, а k_i может принимать значения $k_i = 1, 2, ..., m_i / d_{i-1\,i} - 1$.

Доказательство. Покажем, что существует такое значение $a_{i\rho_1}$, при котором число

$$A = (a_1, a_2, ..., a_{i\rho}, ..., a_n)$$

является правильным. По условию теоремы ошибка Δa_i кратна делителю $d_{i-1\,i}$. Выражение $k_i d_{i-1\,i}$ содержит все возможные числа кратные $d_{i-1\,i}$.

Таким образом, найдется хотя бы одно значение $k_i = \rho_1$, при котором

$$\Delta a_{i\rho_1} = \rho_1 d_{i-1\,i}, \text{ а } a_{1\rho_1} = a_i - \Delta a_{i\rho_1}.$$

Покажем, что $A^{(\rho_1)}$ единственное правильное число из совокупности чисел вида $A^{(k_i)}$.

Предположим, что существует такое значение $a_{1\rho_2} = a_i - \rho_2 d_{i-1\,i}$, при котором число $A^{(\rho_2)}$ также является правильным. Тогда в соответствии с леммой 2 число

$$A^{(\rho_1)} - A^{(\rho_2)} = (0, ..., a_{i\,\rho_1} - a_{i\,\rho_2}, ..., 0)$$

является правильным.

Если число $A^{(\rho_1)} - A^{(\rho_2)}$ правильное, то в соответствии с леммой 1 имеем

$$(\rho_2 - \rho_1)d_{i-1i} \equiv 0(\mathrm{mod}\, d_{1-i}),$$
$$(\rho_2 - \rho_1)d_{i-1i} \equiv 0(\mathrm{mod}\, d_{2-i}),$$
$$\dots$$
$$(\rho_2 - \rho_1)d_{i-1i} \equiv 0(\mathrm{mod}\, d_{n-i}).$$

Если $i \neq n$, то единственно правильным числом $A^{(\rho_1)} - A^{(\rho_2)}$ будет нулевое кодовое слово. Это обусловлено тем, что $d_{i-1i} \neq 0$ и d_{i-1i} не равно НОК делителей $d_{1i}, d_{2i}, ..., d_{ni}$. Причем неравенство $d_{i-1i} \neq [d_{1i}, d_{2i}, ..., d_{ni}]$ противоречит условию произвольного выбора оснований $m_1, m_2, ..., m_n$. Следовательно, выполняется следующее равенство

$$A^{(\rho_1)} - A^{(\rho_2)} = (0, 0, ..., 0, ..., 0).$$

Т.о., $\rho_1 = \rho_2$, что подтверждает единственность существования ρ_1, при котором

$$A^{(\rho_1)} = (a_1, a_2, ..., a_{i\rho_1}, ..., a_n)$$

является правильным. Что и требовалось доказать.

Разработаем алгоритм коррекции ошибок, основанный на результате теоремы 3.

Рассмотрим первую гипотезу. Так как $a_{i-1\ i} = 0$, то ошибка кратна делителю $d_{i-1\ i}$. Поэтому ошибка по основанию может принимать значения

$$\Delta a_i = kd_{i-1i},$$

для $k_i = 1, 2, ..., m_i / d_{i-1i} - 1$.

Вычислим совокупность значений

$$a_{ik_1} = (a_i - k_i d_{i-1i}) \bmod m_i.$$

Если в этой совокупности найдется такое значение a_{im}, при котором

$$A^{(m)} = (a_1, a_2, ..., a_{im}, ..., a_n)$$

правильное число, то первая гипотеза справедлива, т.е. ошибка присутствует в остатке по основанию m_i. В этом случае исправленным числом является,

$$A_{ucn} = A^{(m)},$$

где

$$a_{im} = (a_i - md_{i-1i}) \bmod m_i.$$

Если при всех значения a_{ik_i} число $A^{(k_i)}$ неправильное, то значение a_i истинно, а ошибка произошла в остатке по основанию m_{i+1}. Так как $a_{i+1\ i+2} = 0$, то ошибка по основанию m_{i+1} кратна делителю $d_{i+1\ i+2}$ т. е.

$$\Delta a_{i+1} = k_{i+1} d_{i+1\ i+2},$$

где $k_{i+1} = 1, 2, ..., m_{i+1} / d_{i+1i+2} - 1$.

Определим совокупность значений

$$a_{i+1k_{i+1}} = (a_{i+1} - k_{i+1} d_{i+1\ i+2}) \bmod m_{i+1}.$$

В соответствии с теоремой 3 в этой совокупности обязательно найдется такое единственное число a_{i+1N}, при котором $A^{(N)} = (a_1, a_2, ..., a_{i+1N}, ..., a_n)$ - правильное число.

Отметим, что очередность проверки гипотез произвольная и не влияет на вероятность коррекции ошибок. Однако с целью повышения быстродействия определения номера искаженного остатка, в первую очередь, необходимо проверить гипотезу, для которой значение $m_k / d_{k-1\ k}$ $(k = i, i+1)$ будет наименьшим.

Рассмотрим пример реализации разработанного алгоритма коррекции ошибок с помощью

L-кодов.

Пусть задана СОК основаниями $m_1 = 4$, $m_2 = 6$, $m_3 = 12$, $m_4 = 18$. При этом $M = 36$, $d_{12} = 2$, $d_{23} = 6$, $d_{34} = 6$, $d_{41} = 2$. Объем кодовых слов представлен в табл. 1.

Таблица 1 – Таблица кодовых слов

Число A в десятичном коде	Число A в СОК			
	m_1	m_2	m_3	m_4
0	0	0	0	0
1	1	1	1	1
2	2	2	2	2
3	3	3	3	3
4	0	4	4	4
5	1	5	5	5
6	2	0	6	6
7	3	1	7	7
8	0	2	8	8
9	1	3	9	9
10	2	4	10	10
11	3	5	11	11
12	0	0	0	12
13	1	1	1	13
14	2	2	2	14
15	3	3	3	15
16	0	4	4	16
17	1	5	5	17
18	2	0	6	0
19	3	1	7	1
20	0	2	8	2
21	1	3	9	3
22	2	4	10	4
23	3	5	11	5
24	0	0	0	6
25	1	1	1	7
26	2	2	2	8
27	3	3	3	9
28	0	4	4	10
29	1	5	5	11
30	2	0	6	12
31	3	1	7	13
32	0	2	8	14
33	1	3	9	15
34	2	4	10	16
35	3	5	11	17

Необходимо определить правильность числа $A = (3, 5, 7, 7)$, и в случае искажения исправить его.

1. Определим значения $a_{12} = 0$, $a_{23} = 2$, $a_{34} = 0$, $a_{41} = 0$. Так как $a_{23} \neq 0$, то число A неправильное, и ошибка произошла во втором либо в третьем остатках.

2. Так как $m_2 / d_{12} > m_3 / d_{34}$, то первая гипотеза состоит в том, что ошибка предполагается

в остатке по основанию m_3.

3. Вычислим значения $a_{3k_3} = a_3 - k_3 d_{23}$ для $k_3 = 1$.

Получим $a_{3k_3} = a_3 - k_3 d_{23} = 7 - 1 \cdot 6 = 1$. При этом полученное число $A^{(1)} = (3, 5, 1, 7)$ не являются кодовым словом (см. табл. 1), т. е. первая гипотеза не верна. Ошибка произошла в остатке по основанию m_2.

4. Исправим число A. Для этого по значениям $k_3 = 1, 2$ определим искомое значение $a_{2k_2} = a_2 - k_2 d_{21}$

$$k_2 = 1,\ a_{2k_2} = a_2 - k_2 d_{21} = 5 - 1 \cdot 2 = 3,$$
$$k_2 = 3,\ a_{2k_2} = a_2 - k_2 d_{21} = 5 - 2 \cdot 2 = 2.$$

В итоге, получим два кодовых слова: $A^{(1)} = (3, 3, 7, 7)$ и $A^{(2)} = (3, 1, 7, 7)$.

Из табл. 1 следует, что единственно правильным кодовым словом является значение $A^{(2)}$, т.е. $A_{ucn} = A^{(2)} = (3, 1, 7, 7)$.

Таким образом, разработанный метод коррекции ошибок в СОК позволяет расширить класс корректируемых ошибок. Это существенно расширяет корректирующие возможности L-кодов в СОК.

Рассмотрим работу устройства для обнаружения ошибок с помощью L-кодов, в соответствии с рассмотренным выше алгоритмом. Это устройство содержит входной регистр, сумматоры по модулю m_i и d_{1i} $(i = \overline{2, n})$ и $(n-1)$ – входной элемент ИЛИ. Работа этого устройства соответствует описанному выше алгоритму обнаружения ошибок.

Пусть СОК задана основаниями $m_1 = 4$, $a_{23} = 2$, $m_3 = 12$. При этом

$$\prod_{t=1}^{3} m_i = 288,\ L = M = [4, 6, 12] = 12,\ d_{12} = 2,\ d_{13} = 4.$$

Определим правильность числа

$$A = ((11), (001), (0111)).$$

На выходе сумматора по модулю m_2 получим $\overline{a_2} = m_2 - a_2 = 0101$, на выходе сумматора по модулю $m_3 - \overline{a_3} = m_3 - a_3 = 0101$. На выходе сумматора по модулю d_{12} получим

$$(a_1 + \overline{a_2}) = 0 (\mathrm{mod}\, d_{12}),$$

на выходе сумматора d_{13}

$$(a_1 + \overline{a_3}) = 0 (\mathrm{mod}\, d_{13}).$$

На выходе устройства отсутствует сигнал, т. е. число A правильное (см. Табл. 2).

Пусть число A искажено по основанию m_2 и пусть $\Delta a_2 = 011$, т.е.

$$A = ((0011), (0100), (0111)).$$

На выходе сумматора по модулю m_2 получим число $\overline{a_2} = m_2 - a_2 = 010$, а на выходе сумматора по модулю m_3 число $\overline{a_3} = m_2 - a_3 = 0101$.

На выходе сумматора по модулю d_{12} получим $a_1 + \overline{a_2} = 1 (\mathrm{mod}\, d_{12})$, а по модулю d_{13} - $a_1 + \overline{a_3} = 0 (\mathrm{mod}\, d_{13})$.

На выходе устройства получим операнд 0001, т.е. число неправильное.

Как следует из рассмотренных примеров выполнения операции коррекции ошибок, с помощью L-кодов достаточно просто реализуется процесс обнаружения ошибок. Время обнаружения ошибок для СОК, заданной любой системой оснований, всегда равно трем условным временным тактам и не зависит (как это наблюдается для R-кодов и помехоустойчивых кодов в позиционной системе счисления (ПСС)) от числа информационных оснований.

Таблица 2 - Таблица кодовых слов

A_i	Кодовые числа A в СОК		
	m_1	m_2	m_3
0000	00	000	0000
0001	01	001	0001
0010	10	010	0010
0011	11	011	0011
0100	00	100	0100
0101	01	101	0101
0110	10	000	0110
0111	11	001	0111
1000	00	010	1000
1001	01	011	1001
1010	10	100	1010
0101	11	101	1011

Приведем некоторые соображения, которые позволят упростить вышеприведенное устройство для обнаружения ошибок.

Вначале докажем соотношение $(a_1 + \overline{a_i}) = (\overline{a_1} + a_i) \bmod d_{1i}$, на основании которого составим алгоритм коррекции ошибок. Пусть в операнде $A = (a_1, a_2, ..., a_n)$ искажен остаток m_j, т. е. $a_j = (a_j + \Delta a_j) \bmod m_j$.

Запишем систему равенств:

$$k_1 = a_i - a_j = a_i + (m_j - a_j) = (a_i - a_j + m_j - \Delta a_j) \bmod m_j,$$

$$k_2 = a_j - a_i = a_j + \Delta a_j - a_i = (a_j - a_i + a_j) = \bmod m_j.$$

Сложим эти равенства и получим

$$k_1 + k_2 = m_j (\bmod m_j)$$

или

$$k_1 + k_2 = 0 (\bmod d_{ij}).$$

Таким образом, показано, что

$$(a_1 + \overline{a_i}) = (\overline{a_1} + a_i) \bmod d_{1i},$$

т. е. в устройстве для обнаружения ошибок вместо $n-1$ сумматоров по модулю m_i достаточно иметь всего один сумматор по модулю m_1.

Разработанный алгоритм реализация процесса обнаружения ошибок определяется следующими соотношениями:

$$a_2 + m_1 - a_1 = (a_2 + \overline{a_1}) \bmod d_{12},$$

$$a_3 + m_1 - a_1 = (a_3 + \overline{a_1}) \bmod d_{13}.$$

Вышерассмотренный вариант устройств для определения ошибок в СОК позволяет гарантировано обнаружить факт искажения числа A, однако при этом не определяется номер основания, по которому произошло искажение остатка.

Рассмотрим работу устройства, определяющего номер остатка, по которому произошло искажение числа A.

Пусть СОК задана основаниями $m_1 = 4$, $m_2 = 6$, $m_3 = 12$, $m_4 = 18$. При этом $L = M = [4, 6, 12, 18] = 36$, $d_{12} = 2$, $d_{23} = 6$, $d_{34} = 6$, $d_{41} = 2$, $A = (0, 2, 8, 2)$.

Пусть число A искажено по основанию m_4, т.е.

$$a_4 = (a_4 - \Delta a_4) \bmod m_4,$$

и пусть $\Delta a_4 = 5$.

На выходе сумматора по модулю m_2 получим значение $\overline{a_2} = m_2 - a_2 = 4$; по модулю m_3 получим - $\overline{a_3} = m_3 - a_3 = 4$, на выходе сумматора по модулю – $m_4 - \overline{a_4} = m_4 - a_4 = 11$. На выходе сумматора по модулю d_{12} получим $(a_1 + \overline{a_2}) = 0(\bmod d_{12})$,

по модулю d_{23} - $(a_1 + \overline{a_3}) = 0(\bmod d_{23})$,

по модулю d_{34} - $(a_3 + \overline{a_4}) = 0(\bmod d_{34})$,

по модулю d_{41} - $(a_4 + \overline{a_1}) = 1(\bmod d_{41})$.

На входах сумматоров по модулю d_{34} и d_{41} присутствует ненулевой результат операции $(a_m + \overline{a_j}) \bmod d_j$, поэтому открыт четвертый элемент И, т.е. на 4-й выходной шине присутствует сигнал. Отсюда следует, что ошибка произошла в четвертом остатке a_4 (Табл. 3). Данная процедура может быть использована в некоторых системах обработки данных [3,4].

На основании доказанной теоремы 2 необходимым условием обнаружения ошибки в остатке по модулю m_i является условие (1). Данное условие является и достаточным, если ошибка $\Delta a_i = a_i - a_i$ не кратна одновременно делителям $d_{i-1\,i}$, d_{ii+1}, т.е. следующим двум делителям $d_{\Delta a_i}^{(i-1)} = (d_{i-1\,i}, \Delta a_i) = 1$, $d_{\Delta a_i}^{(i+1)} = (d_{ii+1}, \Delta a_i) = 1$.

В соответствии с результатами теоремы 2 построим алгоритм коррекции ошибок по произвольному основанию m_i:

1. Определим все возможные значения типа $(a_i - a_{i+1}) = a_{i\,i+1}(\bmod d_{i\,i+1})$,

$$\begin{cases} a_1 - a_2 = a_{12}(\bmod d_{12}), \\ a_2 - a_3 = a_{23}(\bmod d_{23}), \\ \quad \cdots \\ a_{n-1} - a_n = a_{n-1\,n}(\bmod d_{n-1\,n}), \\ a_n - a_1 = a_{n1}(\bmod d_{n1}) \end{cases} \tag{3}$$

2. Если все значения (3) равны нулю, то либо ошибки нет, либо она кратна каждому из делителей d_{i-1}, $d_{i\,i+1}$, (предполагается однократная ошибка).

3. Если $a_{i-1\,i} \neq 0$, $a_{i\,i+1} \neq 0$, а все остальные значения $a_{ij} = 0$, то ошибка произошла по модулю m_i, т.е. $a_i = a_i + \Delta a_i$ $(1 \le \Delta a_i \le m_i - 1)$.

В соответствии с доказанной теоремой 3 необходимым условием для исправления ошибки в остатке a_i является условие (4), записанное в общем виде

$$(d_{ik} - 1)(d_{ij} - 1) \ge \delta(\Delta a_i), \tag{4}$$

где

$$\delta(\Delta a_i) = m_i - 1 - (K_{d_{ik}} + K_{d_{ij}} - K_{[d_{ik}, d_{ij}]}),$$

$K_{d_{ik}}$ - число возможных делителей ошибки Δa_i по основанию m_i (т.е. число возможных делителей числа $m_i - 1$), кратных значению d_{ik};

$K_{d_{ik\,j}}$ - число возможных делителей ошибки Δa_i по основанию m_i, кратных значению $d_{i\,j}$;

$K_{[d_{ik}, d_{ij}]}$ - число возможных делителей ошибки Δa_i по основанию m_i, кратных значению НОК чисел d_{ik} и $d_{i\,j}$.

Таблица 3 - Таблица кодовых слов для набора оснований СОК

A	Кодовые слова в СОК				A	Кодовые слова в СОК			
	m_1	m_2	m_3	m_4		m_1	m_2	m_3	m_4
0	0	0	0	0	18	2	0	6	0
1	1	1	1	1	19	3	1	7	1
2	2	2	2	2	20	0	2	8	2
3	3	3	3	3	21	1	3	9	3
4	0	4	4	4	22	2	4	10	4
5	1	5	5	5	23	3	5	11	5
6	2	0	6	6	24	0	0	0	6
7	3	1	7	7	25	1	1	1	7
8	0	2	8	8	26	2	2	2	8
9	1	3	9	9	27	3	3	3	9
10	2	4	10	10	28	0	4	4	10
11	3	5	11	11	29	1	5	5	11
12	0	0	0	12	30	2	0	6	12
13	1	1	1	13	31	3	1	7	13
14	2	2	2	14	32	0	2	8	14
15	3	3	3	15	33	1	3	9	15
16	0	4	4	16	34	2	4	10	16
17	1	5	5	17	35	3	5	11	17

Условие (4) является и достаточным, если различным возможным значениям $\delta(\Delta a_i)$ ошибок по основанию m_i $(i=\overline{1,n})$ соответствуют различные пары величин a_{ik} и a_{ij}.

Рассмотрим пример конкретного выполнения операции коррекции ошибок в СОК, заданной основаниями $m_1=4$, $m_2=6$, $m_3=12$. В этом случае таблица кодовых слов $L=[4,6,12]=12$ представляется в виде табл. 2. Отметим, что $d_{12}=(4,6)=2$, $d_{23}=(6,12)=6$, $d_{31}=(4,12)=4$; $\delta(\Delta a_1)=2$ (Табл. 4), $\delta(\Delta a_2)=3$ (табл. 5), $\delta(\Delta a_3)=8$ (Табл. 6), где

$$\delta(\Delta a_1)=m_1-1-(K_{d_{12}}+K_{d_{31}}-K_{[d_{12},d_{31}]}),$$
$$\delta(\Delta a_2)=m_2-1-(K_{d_{12}}+K_{d_{23}}-K_{[d_{12},d_{23}]}),$$
$$\delta(\Delta a_3)=m_3-1-(K_{d_{23}}+K_{d_{31}}-K_{[d_{23},d_{31}]}).$$

Пусть необходимо определить правильность числа $A=(11,100,0111)$. В первый и второй входные регистры заносится исходное число A. Первый сумматор первой группы определяет значение $\overline{a_1}=m_1-a_1=01$, второй – $\overline{a_2}=m_2-a_2=010$, а третий - $\overline{a_3}=m_3-a_3=0101$. Первый сумматор по модулю d_{ij} определяет значение $a_{12}=(a_1+\overline{a_2})\bmod_{12}$, второй - $a_{23}=(a_2+\overline{a_3})\bmod_{23}$, третий - $a_{31}=(a_3+\overline{a_1})\bmod_{13}$. Таким образом, с выходов соответствующих дешифраторов только на второй коммутатор поступают значения $a_{12}=1$, $a_{13}=3$, в соответствии с которыми (см. Табл. 6) он определяет значение инвертируемой по модулю m_2 ошибки, т.е. $\Delta\overline{a_2}=3$, которое через второй дешифратор в двоичном коде поступает на первый вход второго сумматора, на второй вход которого поступает значение $a_2=a_2+\Delta a_2=100$. Сумматор второй группы определяет результат операции

$$(\Delta\overline{a_2}+a_2)\bmod m_2=(m_2-\Delta a_2+a_2+\Delta a_2)\bmod m_2=001.$$

Таблица 4 – Таблица решений

a_{31}	$a_{12}=1$
1	$\Delta\overline{a_1}=1$
2	–
3	$\Delta\overline{a_1}=3$

Таблица 5 – Таблица решений

a_{23}	$a_{12}=1$
1	$\Delta\overline{a_2}=5$
2	–
3	$\Delta\overline{a_2}=3$
4	–
5	$\Delta\overline{a_2}=1$

Таблица 6 – Таблица решений

a_{31}	a_{23}				
	1	2	3	4	5
1	$\Delta\overline{a_3}=7$	–	$\Delta\overline{a_3}=3$	–	$\Delta\overline{a_3}=11$
2	–	$\Delta\overline{a_3}=2$	–	$\Delta\overline{a_3}=10$	–
3	$\Delta\overline{a_3}=1$	–	$\Delta\overline{a_3}=9$	–	$\Delta\overline{a_3}=5$

На вход устройства поступает исправленное число (см. Табл. 2) $A=(11,001,0111)$.

Рассмотренные выше алгоритмы и устройства могут быть использованы в [5, 6].

3 Выводы

Предложенные алгоритмы коррекции ошибок в СОК с взаимно попарно не простыми основаниями позволяют относительно просто реализовать процедуру обнаружения и исправления однократных ошибок в КСКОЦД. Рассмотренные алгоритмы обнаружения и исправления однократных ошибок позволяют локализовать ошибочное основание и исправить ошибку в одном остатке за пять условных временных тактов для любого числа оснований СОК. Основные достоинства L - кодов в СОК заключаются в технической и временной простоте процедуры обнаружения места ошибки и ее локализации. При этом, по простоте декодирующих схем L - коды не имеют аналогов, как в ПСС, так и в СОК.

Ссылки

[1] Krasnobayev V.A. A method for increasing the reliability of verification of data represented in a residue number system / V.A. Krasnobayev, S.A. Koshman, M.A. Mavrina // Cybernetics and Systems Analysis. – 2014. – Vol. 50. – Issue 6. – P. 969–976.

[2] Krasnobayev V.A. A method for arithmetic comparison of data represented in a residue number system / V.A. Krasnobayev, A.S. Yanko, S.A. Koshman // Cybernetics and Systems Analysis. – 2016. – Vol.52. – Issue 1. – P. 145–150.

[3] Karpenko O. Discrete Signals with Multi-Level Correlation Function / O. Karpenko, A. Kuznetsov, V. Sai, Yu. Stasev // Telecommunications and Radio Engineering. – 2012. – Vol. 71. – Issue 1. – P. 91–98.

[4] Stasev Yu.V. Formation of pseudorandom sequences with improved autocorrelation properties / Yu.V. Stasev, A.A. Kuznetsov, A.M. Nosik // Cybernetics and Systems Analysis. – 2007. – Vol.43. – Issue 1. – P. 1–11.

[5] Kuznetsov A.A. The statistical analysis of a network traffic for the intrusion detection and prevention systems / A.A. Kuznetsov, A.A. Smirnov, D.A. Danilenko, A. Berezovsky // Telecommunications and Radio Engineering. – 2015. – Vol.74 . – Issue 1. – P. 61–78.

[6] Naumenko N.I. Methods of synthesis of signals with prescribed properties / N.I. Naumenko, Yu.V. Stasev, A.A. Kuznetsov // Cybernetics and Systems Analysis. – 2007. – Vol. 43. – Issue 3. – P. 321–326.

Рецензент: Ірина Лисицька, д-р тех. наук, проф., член-кореспондент Академії наук прикладної радіоелектроніки, Харківський національний університет імені В.Н. Каразіна, Харків, Україна
E-mail: lisitska@karazin.ua

Надійшло: Березень 2017.

Автори:
Віктор Краснобаєв, д-р тех. наук, проф., Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: krasnobaev@karazin.ua

Сергій Кошман, к.т.н., доцент, Харківський національний технічний університет сільського господарства імені Петра Василенка, Харків, Україна.
E-mail: s_koshman@ukr.net

Аліна Янко, к.т.н., ст. викладач кафедри комп'ютерної інженерії, Полтавський національний технічний університет імені Юрія Кондратюка, Полтава, Україна.
E-mail: al9_yanko@ukr.net

L-коди у системі залишкових класів.

Анотація. У статті розроблено метод корекції помилок даних у системі залишкових класів, якій засновано на застосуванні коригувальних властивостей L-кодів, які утворюються при використанні взаємно попарно непростих основ. Даний метод дозволяє розширити клас коректованих помилок які коректуються, що розширює коригувальні можливості L-кодів. Наведені приклади виконання операції корекції, а також описані особливості реалізації пристрою для виявлення помилок даних.

Ключові слова: система числення, система залишкових класів, корекція помилок, комп'ютерна система, непозиційних кодова структура.

Reviewer: Irina Lisitska, Doctor of Sciences (Engineering), Full Prof., V. N. Karazin Kharkiv National University, Kharkov, Ukraine.
E-mail: lisitska@karazin.ua

Received: March 2017.

Authors:
Viktor Krasnobayev, Doctor of Sciences (Engineering), Full Prof., V. N. Karazin Kharkiv National University, Kharkov, Ukraine.
E-mail: krasnobaev@karazin.ua

Sergey Koshman, Ph.D., Associate Prof., Kharkov National Technical University of Agriculture named after Peter Vasylenko, Kharkov, Ukraine.
E-mail: s_koshman@ukr.net.

Alina Yanko, Ph.D., Senior Lecturer, Poltava National Technical Yuri Kondratyuk University, Poltava, Ukraine.
E-mail: al9_yanko@ukr.net.

L-codes in the system of residual classes.

Abstract. The method for correcting data errors in the residual class system, by applying the corrective properties of L-codes were developed in the article, which one are formed by using reciprocals pairwise not simple bases. This method allows you to extend the class of correctable errors, which expands the correcting possibilities of L-codes. The examples of the operation of correction were given, and features of the device to detect data errors were described.

Keywords: number system, the system of residual classes, error correction, the computer system, nonpositional code structure.

UDC 004.722:004.9

PRACTICAL CLASSIFICATION TOPOLOGICAL STRUCTURES OF COMMUNICATION NETWORKS FOR MULTIPROCESSOR COMPUTER SYSTEMS

Oleksii Tyrtyshnikov, Maryna Mavrina, Yuri Korzh

Poltava National Technical Yuri Kondratyuk University, 24, Pershotravnevyi Avenue, Poltava, 36011, Ukraine
alexey_it@ukr.net

Reviewer: Serghii Rassomakhin, Doctor of Sciences (Engineering), Full Prof., Department of Information Systems and Technologies Security, V. N. Karazin Kharkiv National University, Svobody sq., 4, Kharkov, 61022, Ukraine
rassomakhin@karazin.ua

Received April 2017

Abstract: *Proposed by the working version of practical classification topological structures of communication networks for multiprocessor computer systems. Any n-dimensional non-full mesh structure presented here as the result of some operations on any basic graph of the set, including one-dimensional non-full mesh simple graphs and n-dimensional realization of the generalized full mesh structure. The main classification criterion, which was refined earlier, is the notion of dimension topological structure that eliminates the shortcomings and contradictions of the, well-known, authors such classifications.*

Keywords: *multiprocessor computer system, communications network, classification of topological structures, the dimension of topological structure.*

1 Introduction

The apparent trend in the development of multiprocessor computer systems (MPCS) is a constant increase in the number of processing elements and computational nodes. Accordingly, becoming more complex their communication networks (CN). Early MPCS had a relatively a small amount of processors and memory modules, which are connected to each other by a simple CN types: bus, ring, binary tree, rectangular lattice [1-3]. CN of the modern MPCS based approach on more complex toroidal and tree types (for example, 3D-torus or "fat tree") [1, 4-7].

The initial stage of the designing CN MPCS is its topological synthesis, i.e. the choice of intermodule communication graph. The problem of the topological synthesis of CN is consider as a choice of the best variants of distribution some connections I between the predetermined amount nodes N of the topological structure (TS) graph by constraint-driven on the values of certain topological metrics (TM) network (for example, the order of nodes d). Well, it is generally, consider a variant of the graph, that has the least value of the maximum diameter D and the maximum width bisection B [2,8,10]. Methods of topological synthesis should be improved in connection with TS CN is complicated and increases.

Undoubtedly, at the stage of study selection an intermodule communication graph MPCS, highly desirable is practically meaningful classification of TS CN.

In order to classification TS CN was practically useful for designer, it is, in our opinion, should meet the following requirements:

- as the classification characteristics, to be used unambiguously defined and practically significant TM CN;
- classification should be sufficiently formalized and to allow its expansion and addition.

It is desirable that the direction of its extension is visible effective methods of topological synthesis CN, possibilities and rules optimum TS scaling, methods for producing complex structures that based on more simple.

In the absence, in the well-known authors of literature classification, fully meet these requirements, the research topic is quite relevant.

As previously indicated, the mathematical classification of the CN [8,9,11], in connection with the desire of the author to the highest completeness and generality, look complicated; classification characteristics are not always correlate with the main TM CN. As a rule, they can only tell designer to the approximate direction of the search.

On the other hand, common to the special and educational literature "practical" classifications of CN is too simplistic, incomplete and contradictory [1,3,5]. It has been shown [12] that the shortcomings and contradictions of the classifications of this type are due, in particular, with subjectivity (multivariate) imaging TS CN and, as a consequence, incorrect use a classification characteristic such as their dimension. Accordingly, they can be eliminate by clarifying the concept of the dimension of the TS and the rejection of their identification with the traditional representation about the dimension of the Euclidean space.

It was also asked to determine the dimension of the TS CN R as the absolute minimum connectivity structure, that is, the number of completely alternative ways (which do not overlap on any edge of the graph) of any length between any two nodes having the minimum order for this structure d_{min}. That is, by geometric dimension is can be expressed as the width of the section CN that crosses the minimum number of connections. Specify that if the width of any cut is not less than the minimum order of node for this structure d_{min} (this condition is satisfied for almost all TS CN), then $R=d_{min}$. It is obvious that for any univalent TS, all the nodes that have the same order, $R=d$.

Refined in this way the concept of dimension TS CN is an objective indicator, since it does not depend of way to imaging the structure. Furthermore, this criterion is practically important, because for the most common in modern MPCS univalent CN coincides with the order of the nodes, that is, with the number of communication ports.

Accordingly, it was propose [12] to classify TS by the dimensions as follows:

- 0-dimensional (trivial graph);
- 1-dimensional (line array, simple trees, star);
- 2-dimensional (ring, 2-dimensional realization of the n-dimensional topologies, for example, 2-dimensional lattice);
- n-dimensional (non-full mesh or structure of variable dimensional, specific implementations of which are, depending on the number of nodes, different dimension $n<N-1$: hypercubes, chordal ring structures (circulants), multidimensional lattice (n-lattice or hyperlattices), complex structure which based on star-shaped and tree base graphs (hypertrees and multitrees), toroidal TS (hypertors or n-tors) and so on);
- (N-1) - dimensional (full mesh).

This classification seems to be quite acceptable for educational applications, as it eliminated the ambiguity and contradictions mentioned earlier. However, from an engineering point of view, it seems haven't detailed, as almost all TS of modern MPCS on which the CN built are non-full mesh n-dimensional.

The aim of this work is to provide, based on the proposed approach, working (basic) version of the classification TS CN, which meets the requirements set earlier. For further detailed classification proposed an "evolutionary" approach, which based on a process for preparing TS from the simple to the complex of some generalized operations. In this case a group of 1-dimensional and full mesh structures of different dimensions can be seen as a group of basic graphs for construct TS by any dimension $2\leq R<N-1$.

2 Properties of basic graphs

The full mesh TS, in comparison with any other structures, has some unique topological properties [10,13,14]. Firstly, its dimension $R=d=N-1$ is identically determined by the number of nodes N and the structure a maximum possible for a concrete value N. The group of all full mesh graphs with any number of nodes may be define as a group of n-dimensional realization of the generalized full mesh structure. Then, for example, trivial graph is 0-dimensional its implementation, "segment" of the two nodes and one edge – 1-dimensional, "ring" of minimum size N=3 – 2-dimensional, etc.

Accordingly, compared to any non-full mesh n-dimensional TS, dimension of full mesh TS may be implementations in the widest range of $0 \le R \le N-1$.

Secondly, any non-full mesh TS, if adding it her links up to the maximum possible number (duplication excepted) becomes full mesh or vice versa – any non-full mesh TS may be obtained from full mesh of appropriate size by eliminating the "extra" links. The non-full mesh TS, obviously, can be have value of dimension within the somewhat narrow range of $1 \le R \le N-2$, as the dimension equal to the boundary values 0 and $N-1$ have only realization of full mesh topology.

These properties allow to consider the set of n-dimensional realizations of the generalized full mesh structure as the basis, "topological scale" for the construction of classification TS CN, since for any value of R of the previously specified range, obviously, there is only one implementation of a full mesh topology. For example, among the 1-dimensional structures such implementation is a "segment" of the two nodes and one edge.

The 1-dimensional non-full mash TS (linear TS, star or terminal topology, simple trees) has a number of common properties (nonunivalent, the minimum possible number of edges for connectivity of the graph $I=N-1$, no loops) [10,13,14]. However, they differ significantly in degree univalent for any sufficiently large number of nodes N.

To assess the degree of approximation nonunivalent to univalent TS, which has the same number of nodes and the dimension $R=d_{max}$, has previously been proposed [15] to use the coefficient of univalent:

$$K_u = \frac{2I}{d_{\max} N}.$$

It has been shown [15] that on the basis of trends changing coefficient of univalent with unlimited increase N, 1-dimensional non-full mesh structures can be divided into three classes:

- linear TS is "extremely univalent" (K_u increases and converges to one);
- a simple trees with any value of the parameter branch, which can be defined as the ratio of the number of nodes in two adjacent tiers of the structure are substantially nonunivalent (K_u increases and tends to the value, which is always much less than one);
- terminal topology is "extremely nonunivalent" (K_u decreases and converges to zero).

Plots of the function $K_u=f(N)$ for the 1-dimensional non-full mesh TS shown in Fig. 1 [15].

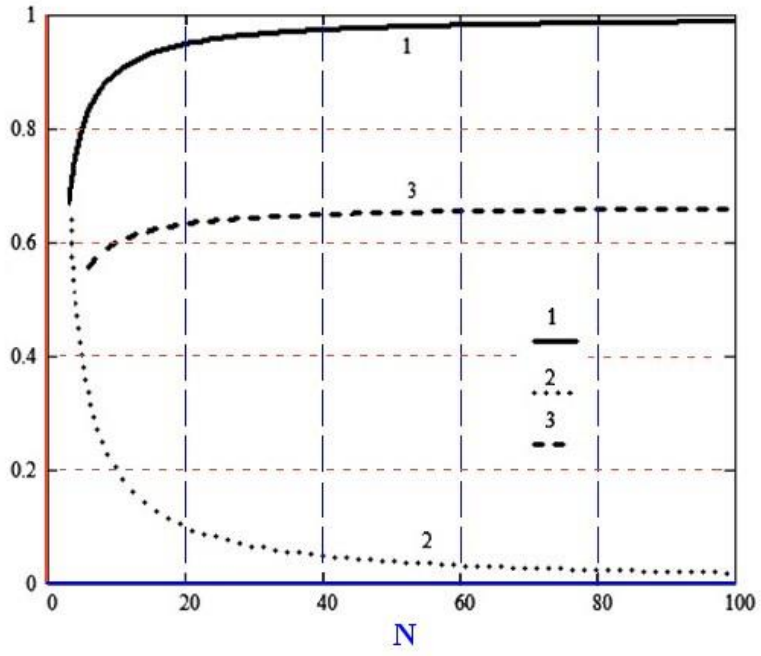

Fig. 1 – Plots of the function $K_u = f(N)$ for the 1-dimensional non-full mesh TS
(*1 – liner TS; 2 – terminal TS; 3 – binary tree*)

On the basis of the uniform-sized base graph with the help of copy operations (with "fusion" of nodes or without it [10]) and the next connection of some nodes received copies by introduction of additional toroidal linkages and so on, they can be prepared by various n-dimensional non-full mesh TS – as a univalent and nonunivalent.

Using nonunivalent TS CN in modern MPCS is considered inappropriate, in connection with their real nodes having the order of $d<d_{min}$, unused communication ports. The ratio of the number of unused communication ports to the total number of Nd_{max} regarded as a relative excess topological cost [8,15].

Converting nonunivalent TS in univalent made of quite simple and universal method – well-directed addition of these links annular (toroidal) type. Note that this conversion, in most cases, accompanied by improvement of the topological properties of the structure (a decrease in the maximum diameter and an increase in the width of the bisection [10]). Thus, nonunivalent TS may be considere as basic graphs for constructing of univalent structures [16]. That is why the presence of nonunivalent structures in practical classification TS CN, in our opinion, is fully justified, but division of TS on univalent and nonunivalent should not be seen as a major classification characteristic.

On the other hand, the effect of the topological properties of the basic graphs on properties of complex structures derived from them, no doubt. Accordingly, a plurality of 1-dimensional TS, along with a variety of implementations of the generalized full mesh structure can be use, as a group of basic elements for the construction of the general classification TS CN.

3 The version of the classification TS CN

The proposed working (basic) version of the classification TS CN shown on Fig. 2 in graphical format.

The sequence of n-dimensional realizations of the generalized full mesh TS, which arrange in order of increasing dimension, forms the left side of the classification, respectively, all non-full mesh structure – it is right side. The zero dimension has only a trivial graph, TS that has dimension $R=1$ form the level of simple basic graphs. Emphasize, that nontrivial graph of minimum size $N=2$, has topological properties is full mesh 1-dimensional TS, any non-full mesh structure is not contain fewer than three nodes. Accordingly, any class of non-full mesh TS has in its structure the simple structure by the size $N_{min}\geq 3$, the specific values of N_{min} for structures of different classes may also vary. For example, non-full mesh linear structure of minimum size $N=3$ can also be viewed as just a simple "star", however, in our opinion, should not consider it just a simple tree (said TS can be regarded as a basic graph for the binary tree by its multiple copy with merging some nodes).

The full mesh simple trees can be defined as TS, which has at least three tiers, where the root tier is only one node, whose order is equal to the branching parameter $k_t\geq 2$; nodes of intermediate tiers have the order k_t+1, and "leaves" are first-order nodes. The number of nodes on each tier is equal $k_t l$, where l – the ordinal number of tiers, if the root tier count by zero. Accordingly, the simplest TS of this class should be considered a three-tiered binary tree ($k_t=2$) by size of $N=7$.

In the incorrect determination of the linear structure the minimum size of which $N=3$ as a simple binary tree, is easy to be convinced, for example, analyzing the dependence of $K_u=f(N)$ for 1-dimensional non-full mesh topologies, graphics which are shown in Fig. 1. So, the graphics for linear and terminal TS have a common origin at the point $(N=3, K_u=2/3)$. However, it is obvious that this point does not belong to a binary tree graphic.

Most generic operations by which one TS can obtain from other (including the elimination part of links of the full mesh TS) are shown in Fig. 2 by arrows.

TS by dimension $R=2$ can be obtained by copying the basic 1-dimensional graphs, followed by a compound (or merge) some nodes of received copies, or the introduction of a toroidal (ring) link in a linear structure. Thus, at a level $R=2$ begin some classes of n-dimensional non-full mesh TS, namely rectangular n-lattice, complex structures on the basis of simple tree and star.

The full mesh TS size of which $N=4$, respectively, the dimensions $R=3$, is the basis of the class chordal ring structures or circulants.

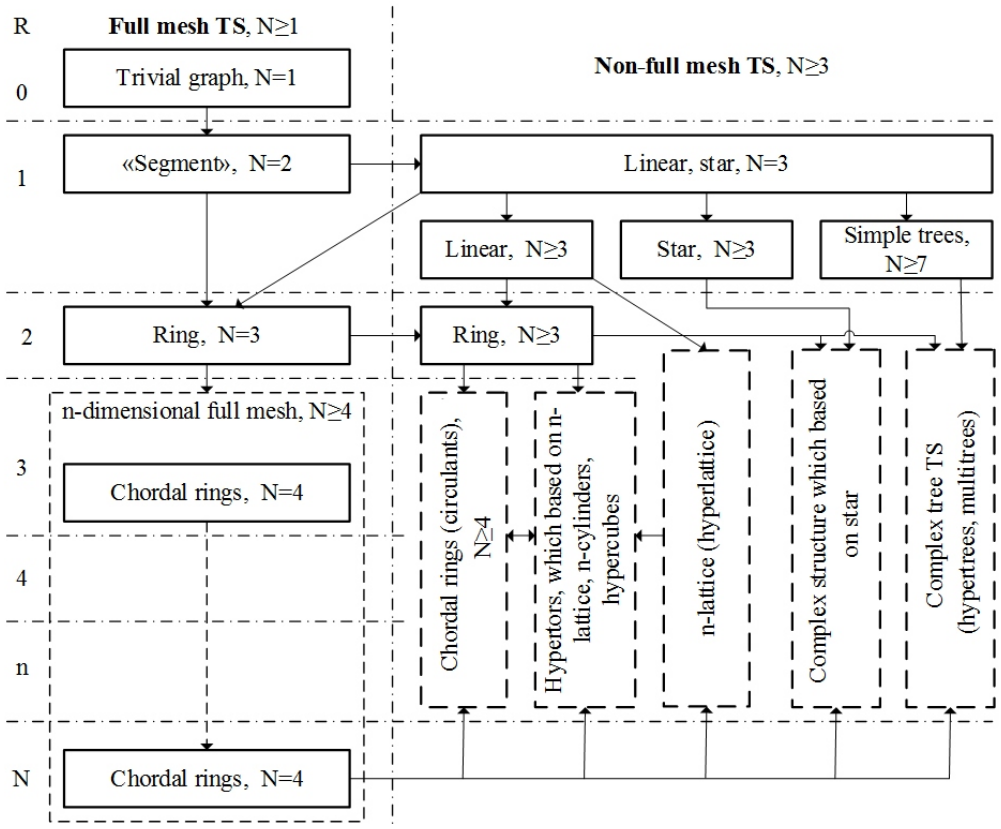

Fig. 2 – Working (basic) classification version TS CN

Also on this level it begins class of hypertorus, which basis on rectangular n-lattice, if consider the three-dimensional cube is the simplest instance of the specified class. In this class can be select a subclass of n-cylinders (non-full mesh hypertorus, which based on n-lattices, where the number of nodes at least in one dimension equal to two) [18]. Then hypercubes can be defined as the simplest hypertorus based on n-lattice (or simplest n-cylinders) in which all, without limitation, the number of nodes is two in all measurings. On the other hand, [17] hypercubes can be consider as a subclass of circulants. Accordingly, the composition of classes from non-full mesh TS allocated in Fig. 2 by dashed lines, and the connections between them may be refine by further research.

4 Conclusions

In the proposed classification TS CN MPCS a main feature is a refined concept of the dimension of the structure, which allows eliminating the shortcomings and contradictions of famous authors such classifications. Any n-dimensional non-full mesh TS is considered here as the result of some generalized operations on any basic graph of the set, including one-dimensional non-full mesh simple graphs and the n-dimensional realization of a full mesh structure. The main direction of future research is the development of advanced, indeed practically useful for designer classification TS CN that based the proposed working version, which requires its further detailing and formalization. In accordance with the proposed approach in the first place should be clarified and precisely the composition of classes n-dimensional non-full mesh TS and define a minimum set of generic operations for the construction of these structures on the basis of a set of basic graphs.

References

[1] Mel'nyk A.O. Arhitektura komp'jutera / A.O. Mel'nyk. – Luc'k: Volyns'ka oblasna drukarnja, 2008. – 470 s.
[2] Korneev V.V. Parallel'nye vychislitel'nye sistemy / V.V. Korneev. – Moskva: Nolidzh, 1999. – 320 s.
[3] Orlov S.A. Organizatsiya EVM i sistem / S.A. Orlov, B.Ya. Tsil'ker. – Sankt-Peterburg: Piter, 2011. – 688 s.
[4] Dally W.J. Principles and practices of interconnection networks / W.J. Dally, B.Towles. – Elsevier, 2004. – 550 p.
[5] Tanenbaum E. Arkhitektura komp'yutera / E. Tanenbaum, T. Ostin: per s angl. – Sankt-Peterburg: Piter, 2013. – 816 s.

[6] Sosa C. IBM System Blue Gene Solution: Blue Gene/P Application Development / C. Sosa, B. Knudson. – IBM Redbooks, 2009. – 382 p.
[7] 3D Torus for InfiniBand [Electronic resource]. – Access mode: http://www.hpcadvisorycouncil.com/events/2012/Switzerland-Workshop/ Presentations/Day_1/4_2_Mellanox.pdf.
[8] Artamonov G.T. Topologiya regulyarnykh vychislitel'nykh setei i sred / G.T. Artamonov. – Moskva: Radio i svyaz', 1985. – 192 s.
[9] Artamonov G.T. Topologiya setei EVM i mikroprotsessornykh sistem / G.T. Artamonov, V. D. Tyurin. – Moskva: Radio i svyaz', 1991. – 248 s.
[10] Kotsis G. Interconnection topologies and routing for parallel processing systems / G. Kotsis // Technical Report Series, ACPC / TR 92-19. – Wien: ACPC, 1992. – 95 p.
[11] Evreinov E.V. Odnorodnye vychislitel'nye sistemy, struktury i sredy / E.V. Evreinov. – Moskva: Radio i svyaz', 1981. – 207 s.
[12] Tyrtyshnikov O. I. Klasyfikacija komunikacijnyh merezh bagatoprocesornyh komp'juternyh system na osnovi utochnenogo ponjattja rozmirnosti / O. I. Tyrtyshnikov, Ju.M. Korzh, Botvin O.O. // Systemy obrobky informacii'. – 2016. – Vyp. 2 (139). – S. 126-131.
[13] Kharari F. Teoriya grafov / F. Kharari; per s angl. V.P. Kozyreva. – Moskva: Editorial URSS, 2003. – 296 s.
[14] Distel' R. Teoriya grafov / R. Distel': per s angl. – Novosibirsk: Izd-vo In-ta matematiki, 2002. – 336 s.
[15] Tyrtyshnikov O.I. Ocinjuvannja stupenju asymetrychnosti ta topologichnoi' vartosti statychnyh komunikacijnyh merezh / O.I. Tyrtyshnikov, O.O. Botvin, V.V. Sen'ko // Systemy obrobky informacii'. – 2015. – Vyp. 1 (126). – S. 162-165.
[16] Pinchuk V.P. Bazovye grafy dlya postroeniya topologii mnogoprotsessornykh sistem / V.P. Pinchuk // Iskusstvennyi intellekt. – 2004. – № 4. – S. 46-58.
[17] Monakhova E.A. Strukturnye i kommunikativnye svoistva tsirkulyantnykh setei / E. A. Monakhova // Prikladnaya diskretnaya matematika. – 2011. – № 3. – S. 92-115.
[18] Tyrtyshnikov O.I. Vlastyvosti statychnyh komunikacijnyh merezh toroi'dal'no-kubichnyh topologij / O.I. Tyrtyshnikov, I. V. Doduh // Systemy upravlinnja, navigacii' ta zv'jazku. – 2014. – Vyp. 2 (30). – S. 60-63.

Рецензент: Сергей Рассомахин, д.т.н., проф., ХНУ имени В.Н. Каразина, Харьков, Украина. E-mail: rassomakhin@karazin.ua

Поступила: Апрель 2017.

Авторы:
Алексей Тыртышников, к.т.н., доцент, Полтавский национальный технический университет имени Юрия Кондратюка, Полтава, Украина. E-mail: alexey_it@ukr.net
Марина Маврина, к.т.н., Полтавский национальный технический университет имени Юрия Кондратюка, Полтава, Украина.
Юрий Корж, кафедра компьютерной инженерии, Полтавский национальный технический университет имени Юрия Кондратюка, Полтава, Украина.

Практическая классификация топологических структур сетей связи для многопроцессорных компьютерных систем.

Аннотация: Предложен рабочий вариант практической классификации топологических структур коммуникационных сетей мультипроцессорных компьютерных систем. Любая *n*-размерная неполносвязная структура здесь рассматривается как результат выполнения некоторых операций над каким-либо базовым графом из множества, включающего одноразмерные неполносвязные простые графы и *n*-размерные реализации обобщенной полносвязной структуры. Основным классификационным признаком является уточненное ранее понятие размерности топологической структуры, что позволяет устранить недостатки и противоречия известных авторам подобных классификаций.

Ключевые слова: мультипроцессорная компьютерная система, коммуникационная сеть, классификация топологических структур, размерность топологической структуры.

Рецензент: Сергій Рассомахін, д.т.н., проф., ХНУ імені В.Н. Каразіна, Харків, Україна. E-mail: rassomakhin@karazin.ua

Надійшло: Квітень 2017.

Автори:
Олексій Тиртишніков, к.т.н., доцент, Полтавський національний технічний університет імені Юрія Кондратюка, Полтава, Україна. E-mail: alexey_it@ukr.net
Марина Мавріна, к.т.н., Полтавський національний технічний університет імені Юрія Кондратюка, Полтава, Україна.
Юрій Корж, кафедра комп'ютерної інженерії, Полтавський національний технічний університет імені Юрія Кондратюка, Полтава, Україна.

Практична класифікація топологічних структур мереж зв'язку для багатопроцесорних комп'ютерних систем.

Анотація: Запропонований робочий варіант практичної класифікації топологічних структур комунікаційних мереж мультипроцесорних комп'ютерних систем. Будь-яка *n*-розмірна неповнозв'язна структура тут розглядається як результат виконання деяких операцій над яким-небудь графом з множини, що складається з одноразмірних неповнозв'язних простих графів та *n*-розмірних реалізацій узагальненої повнозв'язної структури. Основною класифікаційною ознакою є уточнене раніше поняття розмірності топологічної структури, що дозволяє усунути недоліки та протиріччя відомих авторам подібних класифікацій.

Ключові слова: мультипроцесорна комп'ютерна система, комунікаційна мережа, класифікація топологічних структур, розмірність топологічної структури.

УДК 621.3.06

ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ НЕІН'ЄКТИВНИХ СХЕМ РОЗГОРТАННЯ КЛЮЧІВ СИМЕТРИЧНИХ БЛОКОВИХ ШИФРІВ

Марія Родінко, Роман Олійников

Харківський національний університет імені В. Н. Каразіна, майдан Свободи, 4, Харків, 61022, Україна
m.rodinko@gmail.com, roliynykov@gmail.com

Рецензент: Олександр Кузнецов, д.т.н., проф., Харківський національний університет імені В. Н. Каразіна, Харків, Україна.
kuznetsov@karazin.ua

Надійшло квітень 2017

Анотація. *Розглядаються неін'єктивні схеми розгортання циклових ключів, що застосовуються у багатьох відомих блокових шифрах («Калина», FOX, Twofish та ін.). Оцінюється ймовірність співпадіння потужностей множини послідовностей циклових ключів, які формуються неін'єктивною схемою розгортання ключів (СРК), і множини ключів шифрування, формулюється та доводиться теорема, що визначає таку ймовірність. Показується, що для повномасштабного шифру з неін'єктивною СРК ймовірність співпадіння потужностей множини послідовностей циклових ключів і множини ключів шифрування практично дорівнює 1. Таким чином, доводиться, що складність атак переборного типу на неін'єктивні СРК практично дорівнює складності атак на ін'єктивні схеми (складність перебірних атак не знижується), при цьому неін'єктивні СРК забезпечують додаткову стійкість до атак на реалізацію та деяких інших криптоаналітичних атак.*

Ключові слова: *симетричний блоковий шифр, схема розгортання ключів, еквівалентні ключі шифрування, блоковий шифр «Калина», ДСТУ 7624:2014.*

1 Вступ

Схема розгортання циклових ключів є одним із основних компонентів симетричного блокового шифру. Схема розгортання ключів (СРК) – це алгоритм, що розширює відносно короткий майстер-ключ (як правило, довжиною від 128-512 біт) до відносно великого розширеного ключа (як, правило декілька сотень чи тисяч бітів) для подальшого застосування в алгоритмах зашифрування/розшифрування [1].

Часто в основу СРК покладено деяке бієктивне перетворення, що дозволяє відобразити ключ шифрування у послідовність циклових ключів. Перші СРК були дуже простими і включали, наприклад, просту перестановку бітів ключа шифрування (DES, IDEA) або пряме чи рекурсивне лінійне перетворення з майстер-ключа [2]. Із розвитком технологій криптоаналізу розробники почали додавати до СРК нелінійні операції (наприклад, підстановки) з метою уникнення атак на зв'язаних ключах.

Використання простої бієктивної функції дозволяє забезпечити компактну реалізацію, відносно високу швидкодію та відсутність еквівалентних ключів шифрування. При цьому, суттєвим недоліком подібних СРК є відсутність властивості односпрямованості, тобто складність відновлення ключа шифрування при знанні одного або декількох підключів є не вищою за поліноміальну. Це робить шифр більш уразливим до атак на реалізацію.

СРК шифру «Калина» (ДСТУ 7624:2014 [3]) розроблялася з урахуванням необхідності захисту від атак на реалізацію та атаки на зв'язаних ключах [4]. З цією метою була розроблена односпрямована СРК, що забезпечує неможливість відновлення циклового ключа при знанні ключа шифрування або інших підключів. Особливістю односпрямованих СРК є те, що вони є неін'єктивними, тобто теоретично припускається існування еквівалентних ключів (таких, що формують однакову послідовність циклових ключів). Односпрямовані СРК застосовуються в таких відомих блокових шифрах, як FOX [5], Twofish [6] та ін. Оцінка ймовірності співпадіння потужностей множини послідовностей циклових ключів, які формуються неін'єктивною СРК, і множини ключів шифрування дозволила б додатково обґрунтувати стійкість односпрямованих СРК та доцільність їх використання у блокових шифрах.

2 Вимоги до схем розгортання ключів

Станом на сьогоднішній день не досягнуто консенсусу щодо необхідних та достатніх умов, яким повинна задовольняти СРК. Розробники приділяють більше уваги основному шифруючому перетворенню, ніж СРК [2]. Багато з існуючих правил проектування СРК є далекими від практичного застосування. Деякі з них є занадто слабкими з точки зору безпеки, деякі фокусуються лише на певних типах атак і є однобічними, інші є емпіричними і не мають достатнього обґрунтування [2].

Загальними принципами побудування СРК є відсутність слабких, напівслабких та еквівалентних ключів. Застосування циклових констант необхідно для попередження симетрії шифру, яка призводить до можливості реалізації слайд-атак [4].

Метою побудування сильної СРК є усунення будь-якої слабкості, яка гіпотетично або практично може бути використана для атаки на блоковий шифр [7]. Як і при проектуванні блокових шифрів, при розробці СРК часто застосовуються методи досягнення перемішування та розсіювання.

У роботі [8] показано, що шифри зі складними СРК є більш стійкими до атак диференціального та лінійного криптоаналізу, ніж шифри з більш простими СРК. Показано, що деякі ітеративні шифри з дуже простими СРК навіть при повному наборі циклів не досягають рівномірного розподілу ймовірностей диференціалів та лінійних корпусів. Водночас показано, що добре спроектовані шифри зі складними СРК досягають рівномірного розподілу швидше, ніж шифри з поганими СРК.

У роботі [9] Л. Кнудсен вважає, що сильна СРК повинна мати наступні загальні властивості, які можуть бути досягнуті водночас:

а) односпрямована функція, стійка до колізій (функція, яку неможливо інвертувати);
б) мінімальна взаємна інформація (між всіма бітами підключа та бітами майстер-ключа);
в) ефективна реалізація.

При розробці шифру «Калина» до СРК перспективного шифру були висунуті наступні вимоги [4]:

а) нелінійна залежність кожного біта кожного циклового ключа від кожного біта ключа шифрування;
б) циклові ключі суттєво відрізняються і мають складну нелінійну залежність;
в) захист від відомих криптоаналітичних атак, що орієнтовані на схему розгортання ключів;
г) відсутність слабких ключів, при яких погіршуються криптографічні властивості або знижується стійкість перетворення;
д) обчислювальна складність формування всіх циклових ключів не перевищує складності зашифрування трьох блоків;
е) простота програмної, програмно-апаратної і апаратної реалізації.

Як додаткові вимоги, розглядалися наступні [4]:

а) неможливість отримання ключа шифрування по одному або декільком цикловим ключам, що є доступними для криптоаналітика;
б) можливість формування циклових ключів у довільному порядку (однакова обчислювальна і просторова складність для зашифрування і розшифрування).

3 Атаки на схеми розгортання ключів

Слайд-атака. Слайд-атака вперше описана А. Бірюковим та Д. Вагнером у 1999 р. та є криптографічною атакою на основі підібраного відкритого тексту. При цьому, у більшості випадків атака дозволяє проводити криптоаналіз багатоциклових шифрів незалежно від числа циклів. Слайд-атака [10] експлуатує степінь самоподоби блокового шифру та в основному застосовується до ітеративних блокових шифрів з періодичною СРК.

Шифр розглядається як результат застосування ідентичних перетворень $F(x,k)$, де k є секретним ключем (при цьому F може складатися більше, ніж з одного циклу шифру) [10].

Ідея атаки полягає у зсуві однієї копії процесу зашифрування відносно іншої копії процесу зашифрування таким чином, що два процеси є зсунутими на один цикл. Це дає можливість легко отримати ключ шифрування після однієї ітерації F. Згідно парадоксу про день народження для здійснення атаки необхідно набрати $2^{n/2}$ пар (M_i, C_i) [10].

*Атака на зв'язаних ключах***.** Атака цього типу [11] припускає, що криптоаналітику відоме деяке математичне співвідношення, що зв'язує між собою ключі. Наприклад, співвідношення може бути простим значенням XOR з відомою константою $K_1 = K_2 \oplus C$ або більш складним зв'язком. Атака вперше була запропонована Е. Біхамом та нагадує слайд-атаку.

Атаки типу «зустріч посередині». Атаки цього типу [1] виникають, коли перша половина циклів шифру та друга половина циклів шифру залежать від різних наборів ключових бітів. Це дозволяє зловмиснику атакувати дві частини незалежно одна від одної і протидіє подвійному шифруванню з блоковим шифром та двома різними ключами.

Слабкі ключі [1]. Слабким вважається ключ K, для якого зашифрування є ідентичною функцією до розшифрування. Напівслабкими вважається пара ключів K та K', для яких зашифрування за допомогою K ідентичне розшифруванню за допомогою K' і навпаки. Якщо число слабких ключів відносно мале, вони можуть не представляти загрози для шифру, якщо той використовується для забезпечення конфіденційності. Однак в деяких режимах гешування (при використанні блокових шифрів), зловмисник може обрати вхідне значення ключа при спробі пошуку колізії. В таких режимах блоковий шифр не повинен мати слабких та напівслабких ключів.

Класи ключів, що виявляються [1]. Одним зі способів зменшення ефективного ключового простору є його поділ на класи і подальший пошук атаки, які показують, до якого класу належить ключ. У деяких випадках об'єм роботи із визначення приналежності ключа до певного класу дуже малий. Подібні ключі іноді називають слабкими [1]. Наприклад, певні ключі в алгоритмі Blowfish призводять до однакових входів у S-блок і можуть бути виявлені у зменшених за кількістю циклів варіантах шифру. Шифр IDEA має декілька класів ключів, що виявляються, лише за допомогою двох зашифрувань обраних відкритих текстів [1].

Прості зв'язки та еквівалентні ключі [1]. Простий зв'язок виникає між двома різними ключами і проявляється як співвідношення між відкритими текстами та шифртекстами. Блокові шифри DES та LOKI мають простий зв'язок, який виражається в наступному: якщо K зашифровує P у C, тоді побітове доповнення K зашифровує побітове доповнення P у побітове доповнення C. Це зменшує ефективний ключовий простір на один біт. Алгоритми DES та LOKI мають пари ключів, для яких простий зв'язок існує, щонайменше, для частини всіх відкритих текстів [1]. Два ключа є еквівалентними, якщо вони зашифровують усі відкриті тексти ідентично. Це може розглядатися як спеціальний вид простого зв'язку.

Атаки на СРК, що не є односпрямованими [1]. СРК не є односпрямованою, якщо маючи декілька циклових підключів, зловмисник може отримати інформацію про ключ шифрування або інші невідомі підключі. Так, відновлення декількох циклових підключів дозволяє відновити більшу частину майстер-ключа в СРК DES. Е. Біхам та А. Шамір використали це для оптимізації їхньої диференціальної атаки на DES. Крім того, це може зробити простішим пошук слабких та зв'язаних ключів для СРК, що не є односпрямованими.

4 Неін'єктивна схема розгортання ключів шифру «Калина»

Розглянемо приклад неін'єктивної СРК (шифр «Калина»). СРК шифру передбачає обчислення допоміжного ключа K_t, на основі якого формуються циклові ключі. Схематично алгоритм формування K_t наведений на рис. 1.

Застосування допоміжного ключа необхідне для забезпечення односпрямованості СРК та руйнування симетрії шифру [4]. Призначення початкового вектора *iv* полягає у забезпеченні унікальних послідовностей циклових ключів для кожної комбінації розміру блока та клю-

ча [4] (наприклад, для режима 128/128 і 128/256 циклові ключі будуть формувати унікальні псевдовипадкові послідовності, навіть якщо 256-бітовий ключ складається зі співпадаючих 128-бітових підблоків, які дорівнюють ключу режиму 128/128).

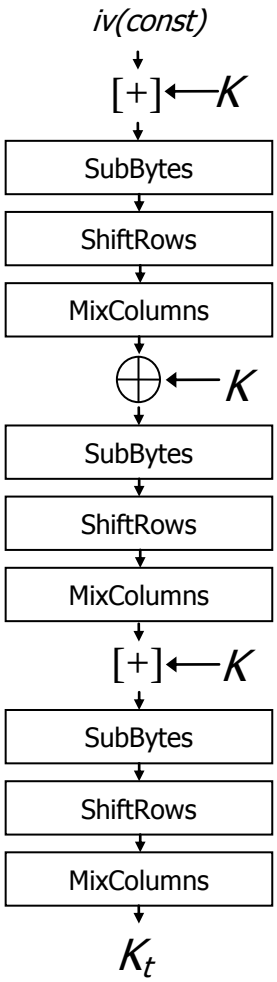

Рис. 1 – Формування допоміжного ключа K_t

Застосування двох ключів та константи забезпечує односпрямованість, унікальність кожного сформованого значення і додатково покращує криптографічні властивості як схеми розгортання, так і всього шифру для забезпечення стійкості до атак, що використовують нерухомі точки циклового перетворення [4]. Циклові ключі з парними індексами формуються на основі ключа шифрування, допоміжного ключа та константи *tmv* (див. Рис. 2), яка залежить від номеру циклу [4]. Циклові ключі з непарними індексами формуються шляхом циклічного зсуву парних. Цей підхід забезпечує як необхідний рівень запасу криптографічної стійкості, так і достатню швидкодію перетворення [4].

5 Оцінка властивостей неін'єктивних схем розгортання ключів

Розв'язання задачі оцінки потужності множини послідовностей циклових ключів було започатковано у [12]. Запропонуємо новий підхід до її вирішення, який дозволяє отримати більш точні оцінки та довести, що для неін'єктивних схем розгортання циклових ключів потужність множини циклових ключів не зменшується у порівнянні з ін'єктивними схемами. Введемо математичну модель оцінки ймовірності співпадіння потужностей множини послідовностей циклових ключів, які формуються неін'єктивною СРК, і множини ключів шифрування. Математична модель використовує припущення, що схема розгортання ключів представляє собою випадкове відображення, що випливає із конструкції та підтверджується результатами статистичного тестування. Тоді справедливою є наступна теорема.

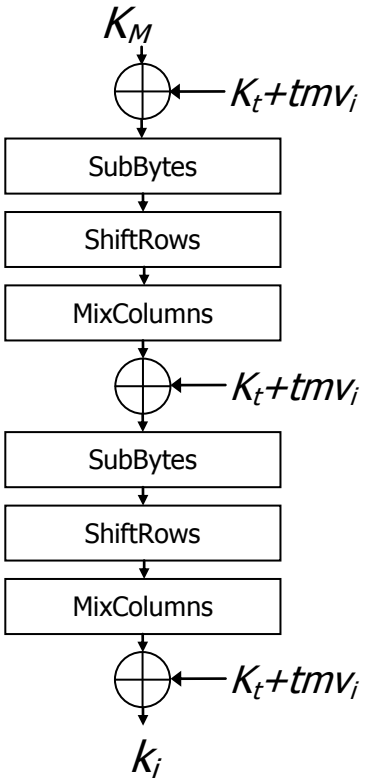

Рис. 2 – Формування циклових ключів з парними індексами

Теорема 1 (про ймовірність співпадіння потужностей множини послідовностей циклових ключів, які формуються неін'єктивною СРК, і множини ключів шифрування).

Нехай τ – неін'єктивна схема розгортання ключів, що реалізує випадкове відображення та має наступні параметри:

k – довжина ключа шифрування в бітах;

l – довжина циклового ключа в бітах;

t – кількість циклових ключів;

$K = 2^k$ – потужність множини ключів шифрування;

$L = 2^{tl}$ – потужність множини послідовностей циклових ключів.

Тоді ймовірність співпадіння потужностей множини послідовностей циклових ключів, які формуються неін'єктивною СРК, і множини ключів шифрування для τ обчислюється через наступне співвідношення:

$$P_\theta = \left(\frac{L}{L-K}\right)^{L-K+\frac{1}{2}} \cdot e^{(-K)}. \quad (1)$$

Доведення.

Нехай задано множину ключів шифрування $\Psi = \left\{K^{(i)} \mid i = 0,1,...,2^k - 1\right\}$ з потужністю $K = |\Psi|$ та множину послідовностей циклових ключів $\Lambda = \left\{L^{(i)} | i = 0,1,...,2^{tl} - 1\right\}$ з потужністю $L = |\Lambda|$.

Послідовність циклових ключів, що формується СРК, має вигляд $L^{(i)} = (L_0^{(i)}, L_1^{(i)}, ..., L_{t-1}^{(i)})$.

Генерація кожної послідовності ключів $L^{(i)}$ виконується за допомогою випадкової функції $f : \Psi \to \Lambda$.

Для кожного ключа шифрування $K^{(i)}$ формується послідовність циклових ключів, тобто всього з множини Λ обирається K послідовностей. Першу послідовність $L^{(0)} = (L_0^{(0)}, L_1^{(0)}, ..., L_{t-1}^{(0)})$ можна обрати L способами, другу $L^{(1)} = (L_0^{(1)}, L_1^{(1)}, ..., L_{t-1}^{(1)})$ *(так, щоб вона*

не співпадала з 1-ю) – $(L-1)$ способами, останню $L^{(K)}=(L_0^{(K)},L_1^{(K)},...,L_{t-1}^{(K)})$ – $(L-(K-1))$ способами. Таким чином, загальна кількість варіантів K послідовностей, що не повторюються,

$$L\cdot(L-1)\cdot...\cdot(L-(K-1))=\frac{L!}{(L-K)!}.$$

Число всіх можливих варіантів послідовностей циклових ключів дорівнює L^K. Тоді ймовірність співпадіння потужностей множини послідовностей циклових ключів, які формуються неін'єктивною СРК, і множини ключів шифрування визначається як

$$P_\theta=\frac{L!}{(L-K)!L^K}.$$

Згідно з формулою Стирлінга, наближене значення факторіала обчислюється як

$$n!\approx\sqrt{2\pi n}\left(\frac{n}{e}\right)^n.$$

Таким чином, отримуємо:

$$P_\theta=\frac{L!}{(L-K)!\cdot L^K}=\frac{\sqrt{2\pi L}\cdot\left(\frac{L}{e}\right)^L}{\sqrt{2\pi(L-K)}\cdot\left(\frac{L-K}{e}\right)^{L-K}\cdot L^K}=\sqrt{\frac{L}{L-K}}\cdot\frac{e^{-L}\cdot L^L}{e^{-L+K}\cdot(L-K)^{L-K}\cdot L^K}=$$

$$=\sqrt{\frac{L}{L-K}}\cdot e^{-K}\cdot(L-K)^{K-L}\cdot L^{L-K}=\sqrt{\frac{L}{L-K}}\cdot e^{-K}\cdot\left(\frac{L}{L-K}\right)^{L-K}=\left(\frac{L}{L-K}\right)^{L-K+\frac{1}{2}}\cdot e^{-K}.$$

Доведення закінчено.

В таблиці 1 представлені результати розрахунків за формулою (1).

Таблиця 1 – Результати розрахунків

k, біт	l, біт	t	P_θ
4	4	2	0,6197211
		3	0,9710922
		4	0,9981705
		5	0,9998856
		6	0,9999928
		7	0,9999996
		8	0,99999997
		9	0,999999998
		10	0,99999999989
8	8	2	0,6073225
		3	0,9980564
		4	0,9999924
		5	0,99999997
		6	0,99999999988
16	16	2	0,6065337
		3	0,9999924

Як слід з таблиці вже при $K = 2^4$ та $L = 2^{40}$ ймовірність співпадіння потужностей множини послідовностей циклових ключів, які формуються неін'єктивною СРК, і множини ключів шифрування дорівнює 0,99999999989. Зі зростанням довжин ключа шифрування та циклового ключа значення P_θ зростає. Для повномасштабного шифру практично $P_\theta \approx 1$. Цей факт

означає, що складність атак переборного типу на неін'єктивні СРК, практично дорівнює складності атак на ін'єктивні СРК.

6 Висновки

Застосування сильних схем розгортання ключів шифрування дозволяє усунути вразливості, які теоретично і практично можуть бути використані для атаки на шифр. Також, використання сильних СРК покращує характеристики шифру, зокрема диференціальні та лінійні.

До основних вимог, яким повинна задовольняти сильна СРК відносяться односпрямованість, нелінійна залежність між всіма бітами циклових ключів та ключа шифрування і ефективна реалізація.

Більшість відомих атак на схеми розгортання ключів не представляють практичної небезпеки, проте вони демонструють теоретичну слабкість, що може бути використана за певних обставин. При цьому найбільш небезпечними слід вважати атаку на зв'язаних ключах та атаки на СРК, що не є односпрямованими.

Запропонована математична модель оцінки ймовірності співпадіння потужностей множини послідовностей циклових ключів, які формуються неін'єктивною СРК, і множини ключів шифрування. Зокрема, отримано співвідношення, що дозволяє обчислити цю ймовірність. Доведено, що складність атак переборного типу на неін'єктивні схеми розгортання ключів практично дорівнює складності атак на ін'єктивні схеми (*складність перебірних атак не знижується*). При цьому, неін'єктивні СРК забезпечують додаткову стійкість до атак на реалізацію та інших криптоаналітичних атак. Таким чином, при побудуванні перспективного симетричного блокового шифру доцільно використовувати саме неін'єктивну схему розгортання циклових ключів.

Посилання

[1] Kelsey J. Key-Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES / J. Kelsey, B. Schneier, D. Wagner // Advances in Cryptology – CRYPTO'96. – Berlin; Heidelberg : Springer, 1996. – P. 237–251.

[2] Huang J. Revisiting Key Schedule's Diffusion In Relation With Round Function's Diffusion / J. Huang, X. Lai // Designs, codes and cryptography. – 2014. – Vol.73. – №1. – P. 85–103.

[3] Informacijni tehnologii'. Kryptografichnyj zahyst informacii'. Algorytm symetrychnogo blokovogo peretvorennja: DSTU 7624:2014. – [Chynnyj vid 2015–01–07]. – Kyi'v: Minekonomrozvytku Ukrai'ny, 2015. – 48 s.

[4] Olijnykov R. Pryncypy pobudovy i osnovni vlastyvosti novogo nacional'nogo standartu blokovogo shyfruvannja Ukrai'ny / R. Olijnykov, I. Gorbenko, O. Kazymyrov, V. Ruzhencev, Ju. Gorbenko // Zahyst informacii'. – 2015. – T. 17. – №2. – S. 142–157.

[5] Junod P. FOX: a new family of block ciphers / P. Junod, S. Vaudenay // Selected Areas in Cryptography. – Berlin; Heidelberg: Springer, 2005. – P. 114–129.

[6] Schneier B. Twofish: A 128-Bit Block Cipher / B. Schneier, et al. // AES algorithm submission. – June 15, 1998. – 68 p.

[7] May L. Strengthening the Key Schedule of the AES / L. May, M. Henricksen // Information Security and Privacy. – Berlin; Heidelberg: Springer, 2002. – P. 226–240.

[8] Knudsen R. Lars. On the Role of Key Schedules in Attacks on Iterated Ciphers / Lars R. Knudsen, John E. Mathiassen // Computer Security–ESORICS 2004. – Berlin; Heidelberg: Springer, 2004. – P. 322–334.

[9] Knudsen L. R. Practically secure Feistel ciphers / L. R. Knudsen // Fast Software Encryption. – Berlin; Heidelberg: Springer, 1993. – P. 211 – 221.

[10] Biryukov A. Slide attacks / A. Biryukov, D. Wagner // In Fast Software Encryption. – Berlin; Heidelberg: Springer, 1999. – P. 245–259.

[11] Biham Eli. New types of cryptanalytic attacks using related keys / Eli Biham // Journal of Cryptology. – Berlin; Heidelberg: Springer – Verlag, 1994. – Vol. 7. – №4 – P. 229–246.

[12] Olijnykov R.V. Metody analizu i syntezu perspektyvnyh symetrychnyh kryptografichnyh peretvoren': Dys. na zdobuttja nauk. st. doktora tehn. nauk po special'nosti 05.13.05 – Komp'juterni systemy ta komponenty. KhNURE / R.V. Olijnykov. – Kharkiv, 2014. – 423 s.

Reviewer: Alexandr Kuznetsov Dr., Full Professor, V.N. Karazin Kharkiv National University, Kharkov, Ukraine
E-mail: kuznetsov@karazin.ua

Received: April 2017

Authors:
M. Rodinko, PhD student, Department of Information Systems and Technologies Security, V.N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: m.rodinko@gmail.com

R. Oliynykov, Doctor of Sciences (Engineering), Ph.D. (Engineering), Full Prof., Department of Information Systems and Technologies Security, V.N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: roliynykov@gmail.com

The research of block ciphers non-injective key schedules properties.

Abstract. The considers non-injective key schedules used in many known block ciphers ("Kalyna", FOX, Twofish, etc.). It is estimated the probability of matching of round keys (formed by non-injective key schedule) set and encryption keys set cardinalities; a theorem which determines such a probability is formulated and proved. It is shown that for a full cipher with a non-injective key schedule, the probability of matching of round keys set and encryption keys set cardinalities is practically equal to 1. Thus, it is proved that the exhaustive search attacks complexity on non-injective key schedules is almost equal to injective ones (the exhaustive search attacks complexity does not decrease). At the same time, non-injective key schedules provide additional strength to attacks on the implementation and other attacks.

Key words: block cipher, key schedule, equivalent keys, block cipher "Kalyna", DSTU 7624: 2014.

Рецензент: Олександр Кузнецов, д.т.н., проф., Харківський національний університет імені В. Н. Каразіна, Харків, Україна.
E-mail: kuznetsov@karazin.ua

Поступила: Апрель 2017.

Авторы:
Мария Родинко, аспирантка, каф. «Безопасности информационных систем и технологий», Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина.
E-mail: m.rodinko@gmail.com
Роман Олейников, д.т.н., проф., каф. «Безопасности информационных систем и технологий», Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина.
E-mail: roliynykov@gmail.com

Исследование свойств неинъективных схем разворачивания ключей симметричных блочных шифров.

Аннотация. Рассматриваются неинъективные схемы разворачивания цикловых ключей, применяемые во многих известных блочных шифрах («Калина», FOX, Twofish и др.). Оценивается вероятность совпадения мощностей множества последовательностей цикловых ключей, которые формируются неинъективной схемой разворачивания ключей (СРК), и множества ключей шифрования; формулируется и доказывается теорема, которая определяет такую вероятность. Показывается, что для полномасштабного шифра с неинъективной СРК вероятность совпадения мощностей множества последовательностей цикловых ключей и множества ключей шифрования практически равна 1. Таким образом, доказывается, что сложность атак переборного типа на неинъективные СРК практически равна сложности атак на инъективные схемы (сложность переборных атак не снижается), при этом неинъективные СРК обеспечивают дополнительную стойкость к атакам на реализацию и другим криптоаналитическим атакам.

Ключевые слова: симметричный блочный шифр, схема разворачивания ключей, эквивалентные ключи шифрования, блочный шифр «Калина», ДСТУ 7624: 2014.

UDC 004.9: 621.391.7

SYNTHESIS OF DERIVED SIGNAL SYSTEMS FOR APPLICATIONS IN MODERN INFORMATION AND COMMUNICATION SYSTEMS

I. Gorbenko, A. Zamula, V. Morozov

V. N. Karazin Kharkiv National University, Svobody sq., 4, Kharkov, 61022, Ukraine
gorbenkoi@iit.kharkov.ua, zamylaaa@gmail.com, morozov@boiko.com.ua

Reviewer: Alexandr Potii, Doctor of Sciences (Engineering), Full Professor, Department of Information Systems and Technologies Security, V. N. Karazin Kharkiv National University, Svobody sq., 4, Kharkov, 61022, Ukraine
potav@ua.fm

Received on April 2017

Abstract: *The specified requirements for complex signal systems selection – data carriers for utilization in information and communication systems (ICT), with higher demand for noise immunity, noise resistance, secrecy and information security. Conceptual framework for new class of complex signals presented – cryptographic signals. Proved appropriateness of utilization cryptographic signals in information and communication systems, as well as, for derived signal systems formation, in order to improve values of noise immunity, noise resistance, secrecy and information security in protected ICT.*

Keywords:*: information security, noise immunity, signal system, broadband systems.*

1 Introduction

In circumstances of intense counteraction, rivalry could exhibit in wide range of areas, as well as, as last events show, in area of information and hybrid wars, use of protected information and communication systems (ICT) become question of particular importance. Under protection we should understand, in wide sense, ability to provide wanted values of noise immunity, imitation resistance, information, energy and structural secrecy of systems functioning.

To the ICT, there are increasingly stringent requirements to ensure the effectiveness of their operation in the face of complex external influences: natural and deliberate interference, interference from other radio systems operating at close frequencies or in the general frequency range. High profile for providing needed values of noise immunity and information security have research dedicated to use new types of signals, which called complex, wideband, multidimensional and noise-type.

Goal of creating protected ITC – is to create system that resistant to influence from many different, actual for that system, effects (noises). An objective problem is that in process of informational exchange correspondence: bit message-signal if fixed and as data carries used signals built with linear rules. Premises allows intruder, based on parametric estimating used in signal systems, to accomplish radio jamming with minimal power expense. There are threats to information security, namely, the possibility of: unauthorized access to information assets, violation of integrity, confidentiality, accessibility of data by intruders.

The main ways of the solution are to increase the noise immunity and information security of the ICT on the basis of improving the methodological foundations of ICT construction by creating new models, methods and technologies for managing telecommunications networks, information security, services and quality of service, developing methods for information exchange, methods for the synthesis of new classes of nonlinear discrete complex signals with the necessary ensemble, correlation and structural properties.

The article proposes a method for discrete sequences synthesis with given mutually correlative, structural and ensemble properties for use in telecommunication systems in which high demands are placed on secrecy, noise immunity, noise immunity, and information security of system operation.

The distinction or code division of subscribers of a multiuser ICS is based on the fact that each subscriber is allocated an alphabet of signals (code sequences) with which he transmits the information. The most commonly used criterion for distinguishability is the minimum of the Euclidean distance [1]. The criterion is that two signals are easily distinguishable if and only if the rms dis-

tance between them is large. The need for joint consideration of signals $Y(t)$ and $X(t)$ arises when using manipulation, for example, in cases where the signal $X(t)$ is modulated by a binary sequence or when it is modulated by some carrier itself. Thus, as a measure of signal distinctiveness, the following quantity is used:

$$T^{-1}\int_0^T [Y(t) \pm X(t)]^2 =$$

$$= -T^{-1}\{\int_0^T [Y^2(t) + X^2(t)]dt \pm 2\int_0^T X(t)Y(t)dt\}\ , \quad (1)$$

where T – signal period of $X(t)$ and $Y(t)$.

The first integral on the right-hand side of (1) is the sum of the energies of the signals $X(t)$ and $Y(t), 0 \le t \le T$. Consequently, for fixed energies, the signal $Y(t)$ is very different both from the signal $X(t)$, and from signal $-X(t)$ only if the parameter

$$R = \int_0^T X(t)Y(t)dt \quad (2)$$

is small.

Parameter *R*, when solving problems of search, detection, estimation of parameters (in this case, a consistent filtering or correlation reception is used), is a response consistent with the signal $Y(t)$ filter on the input signal $X(t)$. For example, if in a multiuser ICS with code division signals $X(t)$ and $Y(t)$ are allocated to two different stations (subscribers), then the parameter *R* is a measure of the level of mutual interference created by each of the signals to the reception of the other.

In the ICT, various systems (sets of linear recurrence sequences, Kasami, Gold, Kamaletdinov, etc.) that have relatively small values of the side lobes of auto and cross correlated functions have found application as a physical carrier of information [2]. However, these signals have low structural secrecy, limited ensemble properties, and also exist only for a limited number of signal period values. In the case of truncation (increase) in the period of such signals, their correlation properties deteriorate. Therefore, the actual task is to develop theory and practice of synthesis and analysis of discrete signal systems with the required correlation, structural, ensemble properties.

Studies have shown [3] that the required (in various conditions) performance indicators of the system can be realized, including through the use of broadband radio systems, for which the expansion of the spectrum is carried out using nonlinear discrete sequences.

In some ICS, the number of simultaneously used signals can exceed several hundred. We know of large sets of periodic sequences that have correlation functions with relatively small side-lobe values of the mutually correlated functions. To generate such sequences, shift registers with linear feedback are used. The rules for constructing these classes of sequences indicate a low structural concealment of the generated sequences, and, consequently, signals providing information transmission in telecommunication systems. Here, by structural concealment, is understood the complexity of determining by an attacker the rule (law) of constructing a discrete sequence used to manipulate information bits.

The need to use secure radio channels forces researchers to look at both the modes of functioning of protected radio channels and the aspects of the formation and application of complex signals. Therefore, in our opinion, today new approaches and new views are needed on the application processes and functions of complex signals in order to build secure ISS. Fundamental here, in our opinion, is a new understanding of the methods of providing information secrecy and imitating resistance, that is, functions that are implemented in traditional systems with the use of systems and means of cryptographic information protection. A productive step, from the point of view of a new direction in the use of complex signal systems, is the synthesis of so-called cryptographic signal systems. Synthesis of such signals is based on the use of key data.

For protected radio channels, the signal systems under consideration are determined by the applications in which they are applied. In particular, it can be either separate signals or signal pairs, or large sets of discrete signals with the necessary but objectively limited values of "tight packing", mutual-correlation and ensemble properties.

A cryptographic discrete signal is proposed to be understood as a sequence of symbols of an arbitrary alphabet and an arbitrary period, the only rule of construction of which is randomness or pseudo-randomness. Such a discrete signal has the necessary but limited values of "dense packing", correlation and ensemble properties. With this approach, the structural concealment of the signal is provided through randomness or pseudo randomness.

In work [4] the problem of synthesis of nonlinear cryptographic discrete signals was formulated and solved, providing the required values of noise immunity, information and structural stealth of the functioning of the telecommunication system. In general, the problem of synthesizing optimal binary cryptographic signals of a given period is formulated as follows. It is necessary to find a lot of discrete binary sequences - cryptographic sequences (CS) with a given number of symbols possessing the permissible level of maximum side lobes of the periodic autocorrelation function (PACF). Further, the solution of the synthesis problem is reduced to the preliminary selection of a certain limited set of discrete sequences, which seems promising in terms of providing the necessary cross-correlation properties.

It should be noted that in the process of research, a hypothesis was voiced about the possibility of using a cryptographic algorithm for the synthesis of a signal system. For these purposes, the choice of the National cryptographic standard of the block symmetric transformation of DSTU 7624: 2014, which determines the code "Kalina" [5], was justified.

Table 1 shows the results of the synthesis of CS for certain values of the sequence period. Analysis of the data in Table 1 shows that for a sequence period, for example, 63 the number of pairs of CSs corresponding to the established limit value 17 is more than 12×10^6 (12214869). For sequences with a three-level cross-correlation function (CCF), the number of pairs corresponding to this "boundary" is only 975 pairs. Thus, the ensemble of nonlinear CSs is more than 10^5 times exceeds the ensemble of said linear signals. Exceeding the volume of cryptographic signals over an ensemble composed of m-sequences is more than 10^7 times.

Table 1 – Ensemble properties of cryptographic signals

CS period	Boundary values (*Dense packing*)	**PACF**	**AACF**	**PCCF**		**ACCF**
		The number of CS satisfying the border "Dense packing"	The number of CS satisfying the border "Dense packing"	Total number of pairs of signals	The number of CS satisfying the border "Dense packing"	The number of CS satisfying the border "Dense packing"
31	9	7 743	3 622	29 977 024	1 465 137	14 537 423
63	17	10 868	7 166	59 056 712	12 214 869	54 822 445
127	23	3482	1302	6 062 162	47 053	1 619 780
511	59	3819	1951	7 292 380	122 835	3 466 713
1 023	100	8 513	6 194	36 235 584	5 293 538	35 083 491

2 Derived signal systems synthesis based on cryptography discrete symbol sequences

Among the systems of phase-shifted signals, many are formed on the basis of Walsh systems [2]. It is known that auto and mutually correlated functions of Walsh sequences have large lateral peaks. To improve the correlation properties of the signals, derivative signal systems (DSS) are generated

by multiplying Walsh sequences (source sequences) by a signal that has certain properties (producing a signal), in particular, have small side peaks of the autocorrelation function.

The authors formulated a hypothesis about the possibility of using nonlinear cryptographic sequences as production, the theoretical bases of their synthesis are given in [4]. The method of synthesizing derived signal systems based on the use of CS includes the following steps.

1. The selection of M cryptographic sequences of a fixed period N, which have the minimum values of the maximum side lobes (R_{max}.) PACF.

2. A set of Walsh codes (the matrix N · N) is formed in which each line corresponds to a separate code.

3. The sequences (each of the Walsh code lines of the original sequences) are multiplied by the cryptographic signal, forming N PSS.

4. Investigate the correlation properties of the generated PSS (in particular, PACF, AACF). To investigate the mutual correlation functions, they form a matrix of dimension N · N. The number of such matrices is L · N.

In Table 2, KP (M = 14), selected from the set of sequences, are given by the criterion of the minimum value of the maximum side lobes PACF (R_{max} < 10), on the basis of the Hadamar matrix (N = 64). The calculations of the statistical characteristics of the correlation functions (PACF) of the selected CS are also presented here.

Table 2 – CS having minimum values of the side lobes of PACF

1	1 1 1 0 0 0 1 1 1 1 1 0 1 0 0 0 0 1 1 1 1 1 0 1 1 1 0 0 1 1 0 0 1 1 0 0 0 1 0 1 0 0 0 1 1 0 1 0 1 1 0 1 0 0 1 0 0 1 1 0 0 1 0 1
2	1 0 0 0 0 1 0 0 1 0 0 0 0 1 0 0 1 0 1 1 1 0 0 1 1 0 1 0 0 0 0 0 0 0 1 1 0 0 1 0 0 1 0 0 0 0 0 1 0 1 1 1 0 0 1 1 1 0 0 1 1 1 0 1
3	0 0 0 0 1 0 0 1 0 0 0 0 1 0 0 1 0 1 1 1 0 0 1 1 0 1 0 0 0 0 0 0 0 1 1 0 0 1 0 0 1 0 0 0 0 0 1 0 1 1 1 0 0 1 1 1 0 0 1 1 1 0 1 1
4	0 0 0 0 1 0 0 1 0 0 0 0 1 0 0 1 0 1 1 1 0 0 1 1 0 1 0 0 0 0 0 0 0 1 1 0 0 1 0 0 1 0 0 0 0 0 1 0 1 1 1 0 0 1 1 1 0 0 1 1 1 0 1 1
5	0 0 0 1 0 0 1 0 0 0 0 1 0 0 1 0 1 1 1 0 0 1 1 0 1 0 0 0 0 0 0 0 1 1 0 0 1 0 0 1 0 0 0 0 0 1 0 1 1 1 0 0 1 1 1 0 0 1 1 1 0 1 1 0
6	0 1 0 0 1 0 0 0 0 1 0 0 1 0 1 1 1 0 0 1 1 0 1 0 0 0 0 0 0 0 1 1 0 0 1 0 0 1 0 0 0 0 0 1 0 1 1 1 0 0 1 1 1 0 0 1 1 1 0 0 1 1 0 1 1 0 0 0
7	0 0 0 0 1 0 0 1 0 1 1 1 0 0 1 1 0 1 0 0 0 0 0 0 0 1 1 0 0 1 0 0 1 0 0 0 0 0 1 0 1 1 1 0 0 1 1 1 0 0 1 1 1 0 1 1 0 1 1 0 0 0 0 1 0 1 1 0
8	0 0 0 1 0 0 1 0 1 1 1 0 0 1 1 0 1 0 0 0 0 0 0 0 1 1 0 0 1 0 0 1 0 0 0 0 0 1 0 1 1 1 0 0 1 1 1 0 0 1 1 1 0 1 1 0 1 1 0 0 0 1 0 1 1 0 1
9	0 0 1 0 0 1 0 1 1 1 0 0 1 1 0 1 0 0 0 0 0 0 0 1 1 0 0 1 0 0 1 0 0 0 0 0 1 0 1 1 1 0 0 1 1 1 0 0 1 1 1 0 1 1 0 1 1 0 0 0 1 0 1 1 0 1 0
10	0 1 0 0 1 0 1 1 1 0 0 1 1 0 1 0 0 0 0 0 0 0 1 1 0 0 1 0 0 1 0 0 0 0 0 1 0 1 1 1 0 0 1 1 1 0 0 1 1 1 0 1 1 0 0 0 1 0 1 1 0 1 0 0
11	0 0 0 0 0 0 0 0 1 0 1 0 0 0 1 0 0 1 1 0 0 0 0 0 1 1 1 1 1 0 0 0 0 1 1 0 1 1 0 1 1 1 0 0 0 1 1 0 1 0 0 0 0 1 0 1 1 1 1 0 0 1 0 1
12	0 0 0 0 0 0 0 1 0 1 0 0 0 1 0 0 1 1 0 0 0 0 0 1 1 1 1 1 0 0 0 0 1 1 0 1 1 0 1 1 1 0 0 0 1 1 0 1 0 0 0 0 1 0 1 1 1 1 0 0 1 0 1 0
13	0 0 0 0 0 0 1 0 1 0 0 0 1 0 0 1 1 0 0 0 0 0 1 1 1 1 1 0 0 0 0 1 1 0 1 1 0 1 1 1 0 0 0 1 1 0 1 0 0 0 0 1 0 1 1 1 1 0 0 1 0 1 0 0
14	0 1 0 0 0 1 1 1 1 0 0 0 1 1 0 0 0 0 0 1 0 0 1 1 0 0 1 0 0 0 0 0 0 0 0 1 1 0 1 1 1 1 1 0 1 1 1 0 0 1 0 1 0 1 1 0 0 0 0 0 1 0 1 1 0

Table 3 shows the results of studies of the statistical characteristics of the correlation functions of various classes of signals, including DSS when used as generating cryptographic signals. Calculations were carried out for the values of the sequence periods (from 30 to 2052).

Analysis of the data in Table 3 shows that the statistical characteristics of the DSS are close to the corresponding characteristics indicated in the table of linear and nonlinear signal classes. In this case, the values of the maximum side peaks of the PSS cross-correlation functions are less than for linear M-sequences commonly used in modern telecommunication systems.

Table 3 – Statistical characteristics of correlation functions of different signal classes

Signal Type	Characteristics	$\frac{R_{макс}}{\sqrt{N}}$	$\frac{m_{\lvert R\rvert}}{\sqrt{N}}$	$\frac{D^{1/2}_{\lvert R\rvert}}{\sqrt{N}}$	$\frac{D^{1/2}_{(R)}}{\sqrt{N}}$
Nonlinear characteristic sequences	AACF	1,6 - 2,4	0,3 - 3,4	1,4 - 7,7	1,9 - 10,8
	PACF	0,02 - 0,5	0,02 - 0,3	0,03 - 0,3	0,06 - 05
	ACCF	1,3 - 3,3	0,5 - 0,7	2,4 - 18,2	3,6 - 27
	PCCF	0,8 - 3,3	0,7 - 0,8	5,8 - 45,3	5,9 - 45,3
DSS	AACF	0,8 - 2,4	0,4 - 0,5	0,9 - 1	1 - 1,1
	PACF	0,7 - 2,5	0,2 - 0,7	0,2 - 0,5	0,3 - 0,9
	ACCF	1 - 2,5	0,2 - 0,7	0,2 - 0,5	0,3 - 0,7
	PCCF	1,4 - 2,8	0,2 - 0,7	0,4 - 0,5	0,6 - 0,9
Nonlinear cryptographic sequences	AACF	0,7 - 2,5	0,4 - 0,5	0,9 - 1	0,9 - 1,2
	PACF	0,9 - 2,5	0,3 - 0,7	0,2 - 0,5	0,3 - 0,9
	ACCF	1,2 - 2,7	0,4 - 0,7	0,3 - 0,5	0,5 - 0,7
	PCCF	1,5 - 2,8	0,5 - 0,7	0,3 - 0,5	0,8 - 0,9
Linear m-sequences	AACF	0,7 - 1,25	0,32	0,26	0,41
	PACF	$1/\sqrt{N}$	$1\sqrt{N}$	0	0
	ACCF	1,4 – 5,0	0,54	0,48	0,73
	PCCF	1,9 – 6,0	0,8	0,62	1

Calculation of statistical characteristics of correlation functions (PACF) CS

1) 64 0 -8 -4 -4 0 -8 0 0 4 0 4 4 -8 -4 8 -4 -4 0 4 4 -4 4 -4 0 8 4 4 -4 -8 -4 0 -8 0 -4 -8 -4 4 4 8 0 -4 4 -4 4 4 0 -4 -4 8 -4 -8 4 4 0 4 0 0 -8 0 -4 -4 -8 0 PFAKmin: -4 PFAKmax: -8 MO: -0.09375 |MO|: 0.46875
DISP: 0.5763694553724894 |DISP|: 0.3384787011890674

2) 64 4 -8 8 4 8 0 -8 8 0 0 -4 -4 4 0 4 0 -8 4 -4 -8 8 4 4 -8 4 4 4 8 4 4 8 -8 8 4 4 8 4 4 4 -8 4 4 8 -8 -4 4 -8 0 4 0 4 -4 -4 0 0 8 -8 0 8 4 8 -8 4 PFAKmin: 4 PFAKmax: -8 MO: 0.15625 |MO|: 0.59375
DISP: 0.6774495430488349 |DISP|: 0.3469815618916576

3) 64 4 -8 8 4 8 0 -8 8 0 0 -4 -4 4 0 4 0 -8 4 -4 -8 8 4 4 -8 4 4 4 8 4 4 8 -8 8 4 4 8 4 4 4 -8 4 4 8 -8 -4 4 -8 0 4 0 4 -4 -4 0 0 8 -8 0 8 4 8 -8 4 PFAKmin: 4 PFAKmax: -8 MO: 0.15625 |MO|: 0.59375
DISP: 0.6774495430488349 |DISP|: 0.3469815618916576

4) 64 4 -8 8 4 8 0 -8 8 0 0 -4 -4 4 0 4 0 -8 4 -4 -8 8 4 4 -8 4 4 4 8 4 4 8 -8 8 4 4 8 4 4 4 -8 4 4 8 -8 -4 4 -8 0 4 0 4 -4 -4 0 0 8 -8 0 8 4 8 -8 4 PFAKmin: 4 PFAKmax: -8MO: 0.15625 |MO|: 0.59375
DISP: 0.6774495430488349 |DISP|: 0.3469815618916576

5) 64 4 -8 8 4 8 0 -8 8 0 0 -4 -4 4 0 4 0 -8 4 -4 -8 8 4 4 -8 4 4 4 8 4 4 8 -8 8 4 4 8 4 4 4 -8 4 4 8 -8 -4 4 -8 0 4 0 4 -4 -4 0 0 8 -8 0 8 4 8 -8 4 PFAKmin: 4 PFAKmax: -8MO: 0.15625 |MO|: 0.59375
DISP: 0.6774495430488349 |DISP|: 0.3469815618916576

6) 64 4 -8 8 4 8 0 -8 8 0 0 -4 -4 4 0 4 0 -8 4 -4 -8 8 4 4 -8 4 4 4 8 4 4 8 -8 8 4 4 8 4 4 4 -8 4 4 8 -8 -4 4 -8 0 4 0 4 -4 -4 0 0 8 -8 0 8 4 8 -8 4 PFAKmin: 4 PFAKmax: -8 MO: 0.15625 |MO|: 0.59375
DISP: 0.6774495430488349 |DISP|: 0.3469815618916576

7) 64 4 -8 4 4 0 0 4 -4 4 0 -8 4 0 4 0 4 0 -8 0 0 8 0 0 -8 -4 -4 4 8 4 4 4 -4 4 4 4 8 4 -4 -4 -8 0 0 8 0 0 -8 0 4 0 4 0 4 -8 0 4 -4 4 0 0 4 4 -8 4 PFAKmin: 4 PFAKmax: -8 MO: 0.0703125 |MO|: 0.4296875
DISP: 0.5553298776598447 |DISP|: 0.350712702793093

8) 64 0 -8 4 4 0 -4 4 -8 8 4 -8 4 0 8 0 0 4 -8 0 -4 4 0 0 -8 -4 0 0 4 4 0 0 0 0 0 4 4 0 0 -4 -8 0 0 4 -4 0 -8 4 0 0 8 0 4 -8 4 8 -8 4 -4 0 4 4 -8 0 PFAKmin: 4 PFAKmax: -8 MO: 0.0 |MO|: 0.40625
DISP: 0.5634361794742422 |DISP|: 0.3836429502240921

9) 64 0 -8 4 4 0 -4 4 -8 8 4 -8 4 0 8 0 0 4 -8 0 -4 4 0 0 -8 -4 0 0 4 4 0 0 0 0 0 4 4 0 0 -4 -8 0 0 4 -4 0 -8 4 0 0 8 0 4 -8 4 8 -8 4 -4 0 4 4 -8 0 PFAKmin: 4 PFAKmax: -8 MO: 0.0 |MO|: 0.40625 DISP: 0.5634361794742422 |DISP|: 0.3836429502240921

10) 64 0 -8 4 4 0 -4 4 -8 8 4 -8 4 0 8 0 0 4 -8 0 -4 4 0 0 -8 -4 0 0 4 4 0 0 0 0 0 4 4 0 0 -4 -8 0 0 4 -4 0 -8 4 0 0 8 0 4 -8 4 8 -8 4 -4 0 4 4 -8 0 PFAKmin: 4 PFAKmax: -8 MO: 0.0 |MO|: 0.40625
DISP: 0.5634361794742422 |DISP|: 0.3836429502240921

11) 64 8 4 0 -8 -8 -4 4 8 8 4 0 0 -4 -8 4 8 8 0 8 4 0 0 -4 -4 -8 -4 0 0 4 -4 4 -4 4 -4 4 0 0 -4 -8 -4 -4 0 0 4 8 0 8 8 4 -8 -4 0 0 4 8 8 4 -4 -8 -8 0 4 8 PFAKmin: 4 PFAKmax: 8 MO: 0.0703125 |MO|: 0.5234375
DISP: 0.6476900319675074 |DISP|: 0.3767205345969094

12) 64 8 4 0 -8 -8 -4 4 8 8 4 0 0 -4 -8 4 8 8 0 8 4 0 0 -4 -4 -8 -4 0 0 4 -4 4 -4 4 -4 4 0 0 -4 -8 -4 -4 0 0 4 8 0 8 8 4 -8 -4 0 0 4 8 8 4 -4 -8 -8 0 4 8 PFAKmin: 4 PFAKmax: 8 MO: 0.0703125 |MO|: 0.5234375
DISP: 0.6476900319675074 |DISP|: 0.3767205345969094

13) 64 8 4 0 -8 -8 -4 4 8 8 4 0 0 -4 -8 4 8 8 0 8 4 0 0 -4 -4 -8 -4 0 0 4 -4 4 -4 4 -4 4 0 0 -4 -8 -4 -4 0 0 4 8 0 8 8 4 -8 -4 0 0 4 8 8 4 -4 -8 -8 0 4 8 PFAKmin: 4 PFAKmax: 8 MO: 0.0703125 |MO|: 0.5234375
DISP: 0.6476900319675074 |DISP|: 0.3767205345969094

14) 64 8 -4 4 4 0 0 4 -4 -4 4 -4 -8 0 -4 0 8 0 8 -4 -8 -4 -8 8 -8 0 0 4 0 -4 4 4 8 4 4 -4 0 4 0 0 -8 8 -8 -4 -8 -4 8 0 8 0 -4 0 -8 -4 4 -4 -4 4 0 0 4 4 -4 8 PFAKmin: -4 PFAKmax: 8 MO: 0.0 |MO|: 0.5
DISP: 0.6236095697723273 |DISP|: 0.3618734420321171

The results of the PCCF DSS study based on CS show that the number of pairs of signals for a sequence of 64 symbols for which the values R_{max} do not exceed 17 (*this, the so-called "tight packing" boundary, achieved in the class of the best, from the VKF viewpoint, sequences with a three-level PCCF*), is 604 pairs (*about 30% of the total number of possible combinations of pairs of signals*). Number of pairs of signals for which the values R_{max} do not exceed 20 – 1577, which is 77% of the total number of pairs of signals. At the boundary $R_{max} < 25$ - maximum number of selected pairs of signals is 1984 (96,8 %). Such values R_{max} occur for sequences that have become most widespread in modern telecommunication systems of the M-sequence.

3 Conclusions

The considered class of complex derivative signals obtained using the proposed method on the basis of the use of nonlinear cryptographic signals has, on the one hand, structural properties analogous to the properties of random (*pseudo-random*) sequences, on the other, the required ensemble and correlation properties.

The characteristics of their auto- and mutual correlation functions of such signals are not inferior to those of the best ones in terms of the correlation properties of discrete sequences (*M-sequences, Gold and Kasami sets, Kamaletdinov ensembles, etc.*). In addition, cryptographic signal systems exist and possess the above properties for a wide range of sequence period values. It is also necessary to note the special property of such signal systems - the possibility of their recovery in space and time with the use of keys and a number of other parameters that are used in the synthesis of signals. The characteristics of the signal systems synthesized using the developed method allow us to talk about improving the quality of the performance of the telecommunications system: noise immunity and information security.

Improvement of these indicators is achieved, in particular due to the possibility of forming, with the resulting method, large ensembles of discrete sequences of almost any period necessary (*for certain system applications*) values side lobe functions cars - mutually and butt-correlation function in a periodic and aperiodic modes, as well as the statistical characteristics of the correlation functions (CF) are not inferior to those of the best in terms of CF, linear to asses signals. Said allows to increase the noise immunity of the reception signals.

The mathematical and software providing the proposed method and computational algorithms for the synthesis of complex nonlinear discrete cryptographic signals systems as well as derivatives of signal systems for which the coprocessors are used as the producing ones are developed. Software and mathematical support obtained in the course of research, realizing the methods of synthesis and research of the properties of systems of non-linear signals, including PSS, is ready for possible use in the composition of prototypes and elements of modern digital communication means.

References

[1] Sarvate D.V. Crosleration Properties of Pseudorandom and Related Sequences / D.V. Sarvate, M.V. Pursley // IEEE Trans. Commun. – 1980. – Vol. Com. 68-5.

[2] Varakin L. E. Sistemy svyazi s shumopodobnymi signalami / L. E.Varakin. – Moskva: Radio i svyaz', 1985. – 384 s.

[3] Gorbenko I.D. Sintez sistem slozhnykh signalov s zadannymi svoistvami korrelyatsionnykh funktsii dlya prilozhenii mnogopol'zovatel'skikh sistem s kodovym razdeleniem abonentov / I.D. Gorbenko, A.A. Zamula, E.A. Semenko // Systemy obrobky informacii'. – 2014. – Vyp. 9 (125). – S. 25–30.
[4] Gorbenko I.D. Ensemble and correlation properties of cryptographic signals for telecommunication system and network applications / I.D. Gorbenko, A.A. Zamula, Ye.A. Semenko // Telecommunications and Radio Engineering. – 2016. – Vol. 75. – Issue 2. – P. 169–178.
[5] Informacijni tehnologii'. Kryptografichnyj zahyst informacii'. Algorytm symetrychnogo blokovogo peretvorennja: DSTU 7624:2014. – [Chynnyj vid 2015–01–07]. – Kyi'v: Minekonomrozvytku Ukrai'ny, 2015. – 48 s.

Рецензент: Олександр Потій, д.т.н., проф., Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: potav@ua.fm

Надійшло: Квітень 2017.

Автори:
Іван Горбенко, д.т.н., проф., лауреат Державної премії України, Харківський національний університет імені В.Н. Каразіна, Харків, Україна. E-mail: gorbenkoi@iit.kharkov.ua
Олександр Замула, д.т.н., доцент, Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: zamylaaa@gmail.com
Владислав Морозов, аспірант, Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: morozov@boiko.com.ua

Синтез похідних систем сигналів для додатків сучасних інформаційно-комунікаційних систем.

Анотація. Розглянуто спеціальні вимоги щодо вибору складних сигнальних систем - переносника інформації в інформаційно-комунікаційних системах з підвищеними вимогами до завадозахищеності, завадостійкості, скритності і безпеки інформації. Концептуальна основа для представлення нового класу складних сигналів - криптографічні сигнали. Вказана доцільність використання криптографічних сигналів в інформаційно-комунікаційних системах, а також для формування похідних сигнальних систем з метою підвищення рівня їх завадозахищеності, завадостійкості, скритності і інформаційної безпеки.

Ключові слова: Інформаційна безпека, перешкодостійкість, система сигналів, широкосмугові системи.

Рецензент: Александр Потий, д.т.н., проф., Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина.
E-mail: potav@ua.fm

Поступила: Апрель 2017.

Авторы:
Иван Горбенко, д.т.н., проф., лауреат Государственной премии Украины, Харьковский национальный университет имени В. Н. Каразина, Харьков, Украина.
E-mail: gorbenkoi@iit.kharkov.ua
Александр Замула, д.т.н., доцент, Харьковский национальный университет имени В. Н. Каразина, Харьков, Украина.
E-mail: zamylaaa@gmail.com
Владислав Морозов, аспирант, Харьковский национальный университет имени В. Н. Каразина, Харьков, Украина.
E-mail: morozov@boiko.com.ua

Синтез производных систем сигналов для приложений современных информационно-коммуникационных систем.

Рассмотрены специальные требования по выбору сложных сигнальных систем - переносчика информации в информационно-коммуникационных системах с повышенными требованиями к помехозащищенности, помехоустойчивости, скрытности и безопасности информации. Концептуальная основа для представления нового класса сложных сигналов - криптографические сигналы. Указана целесообразность использования криптографических сигналов в информационно-коммуникационных системах, а также для формирования производных сигнальных систем с целью повышения уровня их помехозащищенности, помехоустойчивости, скрытности и информационной безопасности.

Ключевые слова: Информационная безопасность, помехоустойчивость, система сигналов, широкополосные системы.

UDC 621.391:681.142

THE CONCEPT OF DIAGNOSTIC DATA ERRORS OF COMPUTING SYSTEMS WITCH FUNCTIONING IN THE SYSTEM OF RESIDUE CLASSES

Artem Moskalenko[1], Viktor Krasnobayev[2], Sergey Koshman[3]

[1] Poltava Institute of Business Academician Yuri Bugay International Science and Technical University, Sinna St., 7 Poltava, 36039, Ukraine
moskalenko_artem@ukr.net

[2] V. N. Karazin Kharkiv National University, Svobody sq.,4, Kharkov, 61022, Ukraine
krasnobaev@karazin.ua

[3] Kharkiv Petro Vasylenko National Technical University of Agriculture, Rizdviana st., 19, Kharkiv, 61052, Ukraine
s_koshman@ukr.net

Reviewer: Alexey Stakhov, Doctor of Sciences (Engineering), Full Prof., Academicians of the Academy of Engineering Sciences of Ukraine, International Club of the Golden Section, 6 McCreary Trail, Bolton, Ont., L7E 2C8, Canada
goldenmuseum@rogers.com

Received on May 2017

Abstract. *A method for diagnosing data of computer systems functioning in the system of residue classes (SRC) has been developed. This method is based on the use of orthogonal bases, which are formed from a complete base system. The presented method allows to increase the efficiency of control over the data submitted to the SRC. The examples of the implementation of this method are given in the article.*

Keywords*: reliability, data diagnostics, number system in residue classes, computer devices of the processing data.*

1 Introduction

The bases of the modern means for processing information of a communication node (CN) telecommunications network (TN) are computer devices of the processing data (CDPD).

The problem of achieving high efficiency of the telecommunications system as a whole is improved, especially such characteristics CDPD CN TN as the veracity, performance and reliability of the processing data. From the literature [1-3] it is known that the use of non-positional number system of residue classes (RC) can provide high performance custom implementation of numerical algorithms, consisting of a set of arithmetic operations. However, the need to ensure a reliable and fail-safe operation of the CDPD the development and implementation of new operational methods for effective monitoring and diagnostics data errors in RC, other than the methods used in conventional binary positional number systems (PNS) [4]. The aim of the research outlined in this article, is to increase the efficiency of the process diagnostic of data errors in the CDPD operating in RC. Thus, important and relevant researches for the development and improvement of method the rapid diagnostics of data errors in the CDPD operating in RC.

2 Main part

In general, the process of correction (detection and reclaim) errors in the code information structure of the data $\tilde{A}$ presented in RC consists of the following major steps:

– control data (process discovery of the existence errors in the non-positional code structure $\tilde{A} = (a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n)$ RC);

– diagnostics data (localization the place of errors with a given depth of diagnostics);

– reclaim errors in the code data structure (recovery distorted residues $\tilde{a}_j \left(j = \overline{1,n} \right)$ of the wrong number $\tilde{A}$ and obtain the correct number A).

The number $A=\left(a_1\|a_2\|...\|a_{i-1}\|a_i\|a_{i+1}\|...\|a_n\right)$ in non-redundant RC is represented by the set $\{a_i\}$ $\left(i=\overline{1,n}\right)$ of residues $a_i \equiv A(\mathrm{mod}\, m_i)$ for the system information bases (modules) $\{m_i\}$ in the numerical information interval $[0,M)$ (where $M=\prod_{i=1}^{n} m_i$ – the total number of information code words). Herewith the greatest common divisor (GCD) $(m_i,m_j)=1;\ i,j=\overline{1,n}\ (i\neq j)$.

In order to the fail-code RC has the necessary corrective abilities required to contain certain information redundancy. In this case, first, it is necessary to define (identify) and, if possible, quantify the pre-existing (natural) in the source code structure information redundancy. Secondly, with the task of providing additional data correction capabilities, introduce an additional (artificial) information redundancy (apply the method of information redundancy) by introducing additional (control) bases $\{m_k\}$ RC.

For solving the problem of ensuring the data in the RC additional correction capabilities, we assume that to n information bases added one additional $m_k=m_{n+1}$ control base is relatively prime to any of the existing information bases. In this case number $A=\left(a_1\|a_2\|...\|a_n\|a_{n+1}\right)$ in RC is represented by the set $\{m_j\}$ $(j=\overline{1,n+1})$ bases in full (working) numeric $[0,M_0)$ interval, where $M_0=M\cdot m_{n+1}$ – the total number of code words for a given RC.

It is known [1] that for non-positional coding structures in RC minimum code distance defined by the expression $d_{\min}=k+1$, it depends on the number k of control base and the amount of each of them. If the condition $\prod_{i=1}^{r} m_{z_i} \le m_k$ for control bases m_{z_i} is met, then the introduction in the system of bases RC one control $m_k=m_{n+1}$ base is equivalent to having r control bases $m_{z_1},m_{z_2},...,m_{z_r}$. Given the fact that all the numbers taking part in the processing of data in the CDPD (transmission and processing of information), as well as the result of the operation is in information numerical interval $[0,M)$, it is obvious that if the result of the data obtained by the final result that $A\ge M$, it means that the obtained number $\tilde{A}$ distorted (by incorrect). Thus, if $A<M$, it is concluded that the number A is correct, and if $A\ge M$, the number $\tilde{A}$ is wrong. Are assumed to be only single (only one of the residues $\{a_i\}$ of A) error or packet errors of length less than $l=\left[\log_2(m_i-1)\right]+1$ bits within one residue by modulo m_i. Note that the principle of comparing the value A with a value information numerical interval $[0,M)$ is base all existing methods of monitoring data in RC [3-5]. The essence of diagnosis non-positional code structure (NCS) in RC $A=\left(a_1\|a_2\|...\|a_{i-1}\|a_i\|a_{i+1}\|...\|a_n\|a_{n+1}\right)$ consists in revealing of distorted residues $m_{z_i}\left(i=\overline{1,r}\right)$.

Consider the list of scientific assertions, the results of the evidence which can form the basis of the method of diagnostic errors data presented in non-positional residue number system [1,4,5].

Recall that in the future will provide only single error (in one residue $a_i\left(i=\overline{1,n+1}\right)$, number $A=\left(a_1\|a_2\|...\|a_n\|a_{n+1}\right)$, presented in RC).

Assertion 1. Let an ordered system of bases in RC $m_i<m_{i+1}, i=\overline{1,n}$ with n information and one $m_k=m_{n+1}$ control bases, and let the number $A=\left(a_1\|a_2\|...\|a_{i-1}\|a_i\|a_{i+1}\|...\|a_n\|a_{n+1}\right)$ undistorted (right), $A<\mathrm{M}_0/m_{n+1}$, where $M_0=M\cdot m_{n+1}$ and $M=\prod_{i=1}^{n} m_i$. The value A does not change if the number will be represented in RC from which it is withdrawn one base m_i, i.e. if in the representa-

tion of A to remove the residue a_i. Thus obtained number $A_i = \left(a_1 \| a_2 \| ... \| a_{i-1} \| a_{i+1} \| ... \| a_n \| a_{n+1}\right)$ is called the projection of the number of A by modulo m_i.

Assertion 2. If in the ordered system bases of RC set the correct number A, then the projections $A_i \left(i = \overline{1, n+1}\right)$ of this number equal to each other, $A = A_1 = A_2 = ... = A_i = ... = A_n = A_{n+1} < \mathrm{M}_0 / m_{n+1}$.

Indeed, for the correct number A has relation holds $A < \mathrm{M}_0 / m_{n+1} < \mathrm{M}_0 / m_k < ... < \mathrm{M}_0 / m_i < ... < \mathrm{M}_0 / m_1$. Then, in accordance with the results of assertion 1, we have that $A = A_i$.

Assertion 3. Suppose that for an ordered system bases of RC all possible projections $A_i = \left(a_1 \| a_2 \| ... \| a_{i-1} \| a_{i+1} \| ... \| a_n \| a_{n+1}\right)$ $A_i \left(i = \overline{1, n+1}\right)$ number $A = \left(a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n \| a_{n+1}\right)$ coincide. In this case the number $A = \left(a_1 \| a_2 \| ... \| a_n \| a_{n+1}\right)$ is correct.

Show it. Assume that the number $A = \left(a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n \| a_{n+1}\right)$ is incorrect due to distortion residue a_i by modulo m_i. Replace in number A distorted residue a_i on the right $\tilde{a}_i$. In this case, received the correct number $\tilde{A} = \left(a_1 \| a_2 \| ... \| \tilde{a}_i \| ... \| a_n \| a_{n+1}\right)$. Then, in accordance with the result of assertion 3, we have $\tilde{A}_1 = \tilde{A}_2 = ... = \tilde{A}_i = ... = \tilde{A}_n = \tilde{A}_{n+1}$.

However, $A_i = \left(a_1 \| a_2 \| ... \| a_{i-1} \| a_{i+1} \| ... \| a_n \| a_{n+1}\right)$ and $\tilde{A}_i = \left(a_1 \| a_2 \| ... \| a_{i-1} \| a_{i+1} \| ... \| a_n \| a_{n+1}\right)$ concurrently, i.e. $A_i = \tilde{A}_i$. In this case the following relation must be performed $A = A_1 = \tilde{A}_1 = A_2 = \tilde{A}_2 = ... = A_n = \tilde{A}_n = A_{n+1} = \tilde{A}_{n+1}$. However, by the condition of assertion 2 projection $A_j \left(i \neq j\right)$ of the number A differs from projection A_i by the value of the residue a_i by the base m_i. Because of this $A_i \neq A_j$, this contradicts the hypothesis that number A is wrong.

Assertion 4. If in the ordered system of bases RC projection $A_i = \left(a_1 \| a_2 \| ... \| a_{i-1} \| a_{i+1} \| ... \| a_n \| a_{n+1}\right)$ number $A = \left(a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n \| a_{n+1}\right)$ satisfies the condition $A_i \geq \mathrm{M}_0 / m_{n+1}$, then this case is considered that the residue a_i of number A by modulo m_i authentically not distorted. Note again that will provide for single mistake.

Indeed, if residue a_i of number A by modulo m_i distorted, then the projection of A_i consisting of the undistorted $a_j \left(j = \overline{1, n+1}\right)$ and $i \neq j$ residues must be a wright number. However, by condition $A_i \geq \mathrm{M}_0 / m_{n+1}$ – a wrong number, which contradicts the assertion 2. In addition, we note that if all the values $A_i \geq \mathrm{M}_0 / m_{n+1}$ $\left(i = \overline{1, n}\right)$ then distorted residue a_{n+1}.

On the basis of the above scientific assertions, consider the method of diagnostics data presented in RC. Suppose given a number to be tested $A = \left(a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n \| a_{n+1}\right)$ in RC with n information $m_i (i = \overline{1, n})$ and one control $m_k = m_{n+1}$ bases. It is necessary, firstly, to inspect (to determine the correctness) of number A, and, secondly, to make a diagnosis residues $a_i \left(i = \overline{1, n+1}\right)$ of number A, i.e. identify distorted (or undistorted) residues. On the basis of evidence on the 3 and 4 assertions developed a method of diagnostic data presented in RC, which is shown on fig. 1,2.

The combination in time the process definition and analysis (comparison of the projections in the PNS $\tilde{A}_{jPNS}$ with module M) values $\underset{j=const}{\tilde{A}_{jPNS}} = \left(\sum_{i=1}^{n} a_i \cdot B_{ij}\right) \bmod M_j$ of the projections $\tilde{A}_j$ of the diagnosed number $A = \left(a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n \| a_{n+1}\right)$ allows increasing the efficiency of the procedure diagnosis data errors in the CDPD CN of TN in n time.

1	Definition the private M_i working bases RC
	$M_1 = m_2 \cdot m_3 ... m_{i-1} \cdot m_i \cdot m_{i+1} ... m_n \cdot m_{n+1},$ $M_2 = m_1 \cdot m_3 ... m_{i-1} \cdot m_i \cdot m_{i+1} ... m_n \cdot m_{n+1},$ . . . $M_i = m_1 \cdot m_2 ... m_{i-1} \cdot m_{i+1} ... m_n \cdot m_{n+1},$ . . . $M_n = m_1 \cdot m_2 ... m_{i-1} \cdot m_i \cdot m_{i+1} ... m_{n-1} \cdot m_{n+1},$ $M_{n+1} = M = M_0 / m_{n+1} = m_1 \cdot m_2 ... m_{i-1} \cdot m_i \cdot m_{i+1} ... m_{n-1} \cdot m_n.$
2	Definition the private $B_{ij} = M_i \cdot \bar{m}_{ij} / m_i = 1 (\mathrm{mod}\, m_i)$ orthogonal bases for this RC
	$M = \prod_{i=1}^{n} m_i$, $M_0 = \prod_{i=1}^{n+1} m_i = M \cdot m_{n+1}$, $M_i = \prod_{\substack{k=1 \\ k \neq i}}^{n+1} m_k$ $\bar{m}_{ij} = \overline{1, m_i - 1}$, $j = \overline{1, n+1}$ – number of bases by initial RC; $i = \overline{1, n}$ – number of bases RC in set of private working bases RC $(j = i+1)$ B_{11} B_{21} B_{31} $\cdots$ $B_{(n-1)1}$ B_{n1} B_{12} B_{22} B_{32} $\cdots$ $B_{(n-1)2}$ B_{n2} $\cdots$ $B_{1(n+1)}$ $B_{2(n+1)}$ $B_{3(n+1)}$ $\cdots$ $B_{(n-1)(n+1)}$ $B_{n(n+1)}$
3	Definition the projections $\tilde{A}_j$ number $\tilde{A} = (a_1 \| a_2 \| ... \| a_i \| ... \| a_n \| a_{n+1})$
	$\tilde{A}_1 = (a_2 \| a_3 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n \| a_{n+1}),$ $\tilde{A}_2 = (a_1 \| a_3 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n \| a_{n+1}),$ . . . $\tilde{A}_i = (a_1 \| a_2 \| ... \| a_{i-1} \| a_{i+1} \| ... \| a_n \| a_{n+1}),$ . . . $\tilde{A}_n = (a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_{n-1} \| a_{n+1}),$ $\tilde{A}_{n+1} = (a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_{n-1} \| a_n).$

Fig. 1 – Method of operative data diagnostic in RC

Consider the example using the method for the diagnosis in RC one-byte ($l = 1$) machine word (8 bits) the CDPD CN of TN. RC is given one control $m_k = m_{n+1} = 11$ and information $m_1 = 3$, $m_2 = 4$, $m_3 = 5$, $m_4 = 7$ bases.

In this case, provided the requirements of the uniqueness of the representation of the code words in this information numerically $[0, M)$ range.

For this RC we have: $M_0 = \prod_{i=1}^{n+1} m_i = 4620$ – the total number of code words in a given RC; $M = \prod_{i=1}^{n} m_i = 420$ – the number of information code words. In this case, the total (working) $[0, M_0)$ and the information $[0, M)$ numerical ranges defined respectively as $[0, 4620)$, and $[0, 420)$.

4	Calculation the value of projections $\tilde{A}_j$ in PNS $\underset{j=const}{\tilde{A}_{jPNS}} = (\sum_{\substack{i=1 \\ j=\overline{1,n+1}}}^{n} a_i \cdot B_{ij}) \bmod M_j$
	$\tilde{A}_{1PNS} = \left(\sum_{i=1}^{n} a_i \cdot B_{i1}\right) \bmod M_1 = \left(a_1 \cdot B_{11} + a_2 \cdot B_{21} + ... + a_n \cdot B_{n1}\right) \bmod M_1,$ $\tilde{A}_{2PNS} = \left(\sum_{i=1}^{n} a_i \cdot B_{i2}\right) \bmod M_2 = \left(a_1 \cdot B_{12} + a_2 \cdot B_{22} + ... + a_n \cdot B_{n2}\right) \bmod M_2,$ ... $\tilde{A}_{kPNS} = \left(\sum_{i=1}^{n} a_i \cdot B_{ik}\right) \bmod M_k = \left(a_1 \cdot B_{1k} + a_2 \cdot B_{2k} + ... + a_n \cdot B_{nk}\right) \bmod M_k,$ ... $\tilde{A}_{nPNS} = \left(\sum_{i=1}^{n} a_i \cdot B_{in}\right) \bmod M_n = \left(a_1 \cdot B_{1n} + a_2 \cdot B_{2n} + ... + a_n \cdot B_{nn}\right) \bmod M_n,$ $\tilde{A}_{(n+1)PNS} = \left(\sum_{i=1}^{n} a_i \cdot B_{i(n+1)}\right) \bmod M_{n+1} = \left(a_1 \cdot B_{1(n+1)} + a_2 \cdot B_{2(n+1)} + ... + a_n \cdot B_{n(n+1)}\right) \bmod M_{n+1}.$
5	Comparison the values $\underset{j=const}{\tilde{A}_{jPNS}} = \left(\sum_{\substack{i=1 \\ j=\overline{1,n+1}}}^{n} a_i \cdot B_{ij}\right) \bmod M_j$ with module $M = M_0 / m_{n+1}$.
6	Definition authentically undistorted $\{a_{z_j}\}$ and perhaps of distorted $\{\bar{a}_{z_j}\}$ residues of number $\tilde{A}$
	$\{a_{z_j}\}$ $j = \overline{l+1,\ n+1}$ $\tilde{A}_{1PNS} \geq M \to a_1,$ $\tilde{A}_{2PNS} \geq M \to a_2,$ ... $\tilde{A}_{nPNS} \geq M \to a_n.$
	$\{\bar{a}_{z_j}\}$ $j = \overline{1,\ l}$ $\tilde{A}_{1PNS} < M \to \bar{a}_1,$ $\tilde{A}_{2PNS} < M \to \bar{a}_2,$ ... $\tilde{A}_{nPNS} < M \to \bar{a}_n,$ $\tilde{A}_{(n+1)PNS} < M \to \bar{a}_{n+1}.$

Fig. 2 – Method of operative data diagnostic (*continuation Fig.1*)

All possible sets of private bases RC are shown in table 1.

Table 1 – Set of private working bases RC ($l = 1$)

i / j	m_1	m_2	m_3	m_4	M_j
1	4	5	7	11	1540
2	3	5	7	11	1155
3	3	4	7	11	924
4	3	4	5	11	660
5	3	4	5	7	420

Suppose that in the course of transmission or data processing instead of the correct result $A_{RC} = (1\|0\|0\|2\|1)$ of the operation $A_{PNS} = 100 < M = 420$ was obtained number form

$\tilde{A}_{RC} = (0\|0\|0\|2\|1)$, $\tilde{A}_{PNS} = 3180 > M = 420$. Necessary to conduct control and diagnostics of the number $\tilde{A}_{RC}$ (diagnosis his residues $a_i \left(i = \overline{1,5}\right)$).

2.1. The first stage.

1. Determine all values $B_i \left(i = \overline{1,5}\right)$ of orthogonal bases for a complete system of bases $m_1 = 3$, $m_2 = 4$, $m_3 = 5$, $m_4 = 7$ и $m_5 = 11$ RC (Table 2).

Table 2 – Orthogonal bases B_i RC

$B_1 = (1,0,0,0,0) = 1540, \quad \bar{m}_1 = 1$
$B_2 = (0,1,0,0,0) = 3465, \quad \bar{m}_2 = 3$
$B_3 = (0,0,1,0,0) = 3696, \quad \bar{m}_3 = 4$
$B_4 = (0,0,0,1,0) = 2640, \quad \bar{m}_4 = 4$
$B_5 = (0,0,0,0,1) = 2520, \quad \bar{m}_5 = 6$

2. Using the data in table 2, for the well-known [1] formula, determine the value of $\tilde{A}_{PNS}$:
$\tilde{A}_{PNS} = (0 \cdot 1540 + 0 \cdot 3465 + 0 \cdot 3696 + 2 \cdot 2640 + 1 \cdot 2520) \bmod 4620 = 3180 (\bmod 4620)$.

3. Perform comparison value number $\tilde{A}_{PNS}$ and $M = 420$. So, how $\tilde{A}_{PNS} > M = 420$, it is concluded that the obtained result $\tilde{A}$ distorted by any one of the residues a_i correct number $A_{RC} = (1\|0\|0\|2\|1)$.

2.2. The second stage.

1. We define the values private B_{ij} orthogonal bases for each of the 5 sets of bases RC. Thus, for $i = 4$ and $j = 5$, we have:

$$\begin{cases} B_{1j} = (1,0,0,0), \\ B_{2j} = (0,1,0,0), \\ B_{3j} = (0,0,1,0), \\ B_{4j} = (0,0,0,1). \end{cases}$$

In general, the values B_{ij} the private orthogonal bases determined according to the following comparison $B_{ij} = \dfrac{M_i \cdot \bar{m}_{ij}}{m_i} \equiv 1 (\bmod m_i)$, where $\bar{m}_{ij} \equiv \overline{1, m_i - 1}$ - the weight of an orthogonal basis B_{ij}. The results of calculations of values B_{ij} the private orthogonal bases are presented in table 3.

Table 3 – Private orthogonal bases B_{ij} for $l = 1$

B_{ij} i / j	1	2	3	4
1	385	616	1100	980
2	385	231	330	210
3	616	693	792	672
4	220	165	396	540
5	280	105	336	120

2.2. Determine the correct of residues number $\tilde{A}$. At first, we form all possible projection A_j number $\tilde{A}_{RC} = (0\|0\|0\|2\|1)$:

$$\begin{cases} \tilde{A}_1 = (0\|0\|2\|1), \\ \tilde{A}_2 = (0\|0\|2\|1), \\ \tilde{A}_3 = (0\|0\|2\|1), \\ \tilde{A}_4 = (0\|0\|0\|1), \\ \tilde{A}_5 = (0\|0\|0\|2). \end{cases}$$

Using the data from table 3, we represent the values of the projections $\tilde{A}_j \left(j = \overline{1,5} \right)$ number $\tilde{A}_{RC} = (0\|0\|0\|2\|1)$ in PNS:

$$\tilde{A}_{1PNS} = (a_1 \cdot B_{11} + a_2 \cdot B_{21} + a_3 \cdot B_{31} + a_4 \cdot B_{41}) \bmod M_1 =$$
$$(0 \cdot 385 + 0 \cdot 616 + 2 \cdot 1100 + 1 \cdot 980) \bmod 1540 = 100 < 420.$$
$$\tilde{A}_{2PNS} = (a_1 \cdot B_{12} + a_2 \cdot B_{22} + a_3 \cdot B_{32} + a_4 \cdot B_{42}) \bmod M_2 =$$
$$(0 \cdot 385 + 0 \cdot 231 + 2 \cdot 330 + 1 \cdot 210) \bmod 1155 = 870 > 420.$$
$$\tilde{A}_{3PNS} = (a_1 \cdot B_{13} + a_2 \cdot B_{23} + a_3 \cdot B_{33} + a_4 \cdot B_{43}) \bmod M_3 =$$
$$(0 \cdot 616 + 0 \cdot 693 + 2 \cdot 792 + 1 \cdot 672) \bmod 924 = 418 < 420.$$
$$\tilde{A}_{4PNS} = (a_1 \cdot B_{14} + a_2 \cdot B_{24} + a_3 \cdot B_{34} + a_4 \cdot B_{44}) \bmod M_4 =$$
$$(0 \cdot 220 + 0 \cdot 165 + 0 \cdot 396 + 1 \cdot 540) \bmod 660 = 540 > 420.$$
$$\tilde{A}_{5PNS} = (a_1 \cdot B_{15} + a_2 \cdot B_{25} + a_3 \cdot B_{35} + a_4 \cdot B_{45}) \bmod M_5 =$$
$$(0 \cdot 280 + 0 \cdot 105 + 0 \cdot 336 + 2 \cdot 120) \bmod 420 = 240 < 420.$$

Among all the obtained projections $\tilde{A}_i$ number $\tilde{A}$ projections $\tilde{A}_1$, $\tilde{A}_3$ and $\tilde{A}_5$ less than the value $M = 420$, but projections $\tilde{A}_2$ and $\tilde{A}_4$ is greater than $M = 420$. Consequently, the result of an incorrect diagnosis $\tilde{A}$ number will be the following assertion. Among the five residues number $\tilde{A}_{RC} = (0\|0\|0\|2\|1)$ is the residues of a_1, a_3 and a_5 may be wrong, and the residues of a_2 и a_4 – are not distorted.

It is known that the efficiency of diagnosis is convenient to characterize such a quantitative indicator, the depth D of diagnosis. In the RC depth D diagnosis data we mean the level of detail location of an error in the NCS on the form $A = (a_1\|a_2\|...\|a_{i-1}\|a_i\|a_{i+1}\|...\|a_n\|a_{n+1})$, consisting of a set of residues $\{a_i\}, i = \overline{1, n+1}$.

As noted above, it is assumed single (only one residue of NCS) error.

Quantitatively, the depth diagnostics data D in RC can be evaluated by the relation $D = 1/r$, where r – the number m_{z_i} of residues $\{m_{z_1}, m_{z_2}, ..., m_{z_r}\}$ that can be a mistake. The maximum value of depth $D_{\max}$ diagnosis is achieved when an error in NCS A is detected with accuracy to one residue. In this case, the maximum depth $D_{\max}$ diagnosis to mean the identification of one ($r = 1$) residue NCS A, which contains the error, i.e., $D_{\max} = 1/r = 1$. For the above example the number of diagnosis $\tilde{A}_{RC} = (0\|0\|0\|2\|1)$ we have that $r = 3$, i.e. $D = 1/3 \approx 0,33$.

3 Conclusions

In this article improved the method of diagnostic in RC, which basis on the use orthogonal bases B_{ij} of the private set of modules. Orthogonal bases B_{ij} formed from complete system of bases m_i $(i=\overline{1,n+1})$. Their use makes it possible to organize the process of parallel processing projections $A_i=(a_1\|a_2\|...\|a_{i-1}\|a_{i+1}\|...\|a_n\|a_{n+1})$ number $A=(a_1\|a_2\|...\|a_{i-1}\|a_i\|a_{i+1}\|...\|a_n\|a_{n+1})$ of the code structure in RC. This allows to raise the efficiency of diagnosis data in RC.

Implementation the process of diagnostic data errors in RC is shown in the example. The proposed method has allowed increasing the efficiency of the diagnostic data errors in the CDPD CN of TN operating in RC.

References

[1] Akushskii I.Ya. Mashinnaya arifmetika v ostatochnykh klassakh / I.Ya. Akushskii, D.I. Yuditskii. – Moskva: Sov. radio, 1968. – 440 s.

[2] Davis R.G. Residue coded signals and applications to space technology / R.G. Davis, R.A. Yocke // Proc. of the 6-th symposium on ballistic missile and aerospace technology. – 1961. – P. 215–245.

[3] Valach M. Origin of the code and number system of remainder classes / M. Valach // Stroje na zpracovani informaci. Sbornik III, 1955.

[4] Moroz S.A., Krasnobaev V.A. Metod kontrolya informatsii v nepozitsionnoi sisteme schisleniya klassa vychetov / S.A. Moroz, V.A. Krasnobaev // Systemy upravlinnja, navigacii' ta zv'jazku. – 2011. – Vyp. 2 (18). – S. 134–138.

[5] Krasnobaev V.A. Kontrol', diagnostika i ispravlenie oshibok dannykh, predstavlennykh kodom klassa vychetov / V.A. Krasnobaev, M.A. Mavrina, S.A. Koshman // Zbirnyk naukovyh prac'. Systemy obrobky informacii'. – 2013. – Vyp. 2. (109). – S. 48–54.

Рецензент: Олексій Стахов, д.т.н., проф., академік Академії інженерних наук України, Міжнародний Клуб Золотого Перетину, Онтаріо, Канада. E-mail: goldenmuseum@rogers.com

Надійшло: Травень 2017.

Автори:
Артем Москаленко, к.т.н., доц., Полтавський інститут бізнесу Міжнародного науково-технічного університету імені академіка Ю. Бугая, Полтава, Україна. E-mail: moskalenko_artem@ukr.net
Віктор Краснобаєв, д.т.н., проф., Харківський національний університет імені В. Н. Каразіна, Харків, Україна.
E-mail: krasnobaev@karazin.ua
Сергій Кошман, к.т.н., доц., Харківський національний технічний університет сільського господарства імені П. Василенка, Харків, Україна. E-mail: s_koshman@ukr.net

Концепція діагностування помилок даних обчислювальних систем, що функціонують у системі залишкових класів.

Анотація. Розроблено метод діагностування даних комп'ютерних систем, які функціонують у системі залишкових класів (СЗК). Даний метод заснований на використанні ортогональних базисів, які формуються з повної системи основ. Представлений метод дозволяє підвищити оперативність контролю даних, що представлені у СЗК. У статті наведено приклади реалізації даного методу.

Ключові слова: надійність, діагностика даних, система числення у залишкових класах, комп'ютерні пристрої обробки даних.

Рецензент: Алексей Стахов, д.т.н., проф., академик Академии инженерных наук Украины, Международный Клуб Золотого Сечения, Онтарио, Канада. E-mail: goldenmuseum@rogers.com

Поступила: Май 2017.

Авторы:
Артём Москаленко, к.т.н., доц., Полтавский институт бизнеса Международного научно-технического университета имени академика Ю. Бугая, Полтава, Украина. E-mail: moskalenko_artem@ukr.net
Виктор Краснобаев, д.т.н., проф., Харьковский национальный университет имени В. Н. Каразина, Харьков, Украина.
E-mail: krasnobaev@karazin.ua
Сергей Кошман, к.т.н., доц., Харьковский национальный технический университет сельского хозяйства имени П.Василенка, Харьков, Украина. E-mail: s_koshman@ukr.net

Концепция диагностирования ошибок данных вычислительных систем, функционирующих в системе остаточных классов.

Аннотация. Разработан метод диагностирования данных компьютерных систем, функционирующих в системе остаточных классов (СОК). Данный метод основан на использовании ортогональных базисов, которые формируются из полной системы оснований. Представленный метод позволяет повысить оперативность контроля данных, представленных в СОК. В статье приведены примеры реализации данного метода.

Ключевые слова: надежность, диагностика данных, система счисления в остаточных классах, компьютерные устройства обработки данных.

UDC 621.37:621.391

THE DIGITAL METHODS FOR DETECTION OF SELECTIVE SPECTRAL ANALYSIS OF COMPLEX SIGNALS

S. Veklych, S. Rassomakhin

V. N. Karazin Kharkiv National University, Svobody sq.,4, Kharkov, 61022, Ukraine
s.veklych@gmail.com, rassomakhin@karazin.ua

Reviewer: Vyacheslav Kharchenko, Doctor of Sciences (Engineering), Full Prof., Academicians of the Academy of Applied Radioelectronics Sciences, N.Ye. Zhukovskiy National Aerospace University – Kharkiv Aviation Institute (KhAI), 17 Chkalov St., Kharkiv, 61070, Ukraine.
v_s_kharchenko@ukr.net

Received on May 2017

Abstract. *The shortcomings of application of fast Fourier transformation algorithm at detection of separate tones of a signal are considered. The relevance of application of algebraic methods at demodulation of signals in modern information transmission systems is emphasized. The Goertzel algorithm of selective spectrum analysis is considered, the method of the linear algebraic processing of complex signal structures in case of detection of separate tones in a signal range is offered. The analysis of efficiency of the known and proposed method of selective spectrum analysis is carried out. It is concluded that the application of the method of linear algebraic processing of complex signal structures will allow us to calculate the parameters of the signal spectrum of only the needed nomenclature of frequencies by solving the system of linear algebraic equations without the use of fast Fourier transformation.*

Keywords*: fast Fourier transform (FFT), filter with infinite impulse response (IIR-filters), system of linear algebraic equations (SLAE), digital signal processing.*

1 Introduction

In the modern conditions characterized by complexity of the tasks solved by radio systems and a variety of an interfering situation development, enough perfect systems it is possible only on the basis of modern methods of optimization. The common problem of synthesis of radio engineering systems can conditionally be subdivided into two private tasks: the choice of the "best" signals for achievement of the required result taking into account a real situation and optimum processing of the accepted signals. The traditional method of the primary identification of parameters and demodulation of controlled signals is currently their analysis on the basis of the fast Fourier transform (FFT) algorithm. Use the FFT algorithms for processing of OFDM signal assumes the existence of exact information on the signal. At the solution of problems of radio monitoring and demodulation these data are, as a rule, unknown [1].

The device FFT optimized on computing expenses on the basis of decimation algorithms on the frequency or time not always is preferable from the point of view of excess dimensionality of the task. For example, if the signal range on an interval of discretization of the channel consists of small number quadrature frequency components $f_1, f_2, \ldots, f_m >> 0$, then for its complete processing it is enough to calculate only the amplitude coefficients. If to use a FFT, then based on properties of a computing algorithm determination will be carried out for $2 \cdot T \cdot f_m >> m$ amplitudes, i.e. excessively excess problem will be solved [2]. In this regard, development of the software and hardware tools of digital signal processing oriented only on use FFT algorithms not always is justified. Development of theoretical and practical bases of use of the ordinary apparatus of linear algebra for optimization of computing expenses and increase in characteristics of accuracy of recognition and demodulation of complex signals is of interest. We will consider some algorithms and methods of signals processing that allow to find separate tones of a signal, without solving an excess problem.

2 The Goertzel algorithm for detection of separate harmonious components

The Goertzel algorithm is a procedure for calculating the discrete Fourier transform. It makes it possible to reduce the number of necessary multiplications, but to a very small multiplier. The com-

plexity of this algorithm is equal to n^2 therefore it does not belong to FFT algorithms. Goertzel algorithm is useful when the Fourier transformation component is required to calculate small quantity, – as a rule, no more than $\log_2 n$ from n a component. As FFT algorithms calculate all components of transformation, in these cases it is necessary to discard unnecessary components [3].

Algorithm Goertzel allows to calculate the value of k-th bin of N dot DFT:

$$S_N(k) = \sum_{n=0}^{(N-1)} x(n) \cdot W_N^{kn}, \quad W_N^{kn} = \exp\left(-j\frac{2\pi}{N}nk\right) \tag{1}$$

It represents an IIR filter of the second order with two real coefficients in the feedback and one complex coefficient in the direct link of the filter. The structure of the Goertzel's digital filter is shown in Fig. 1.

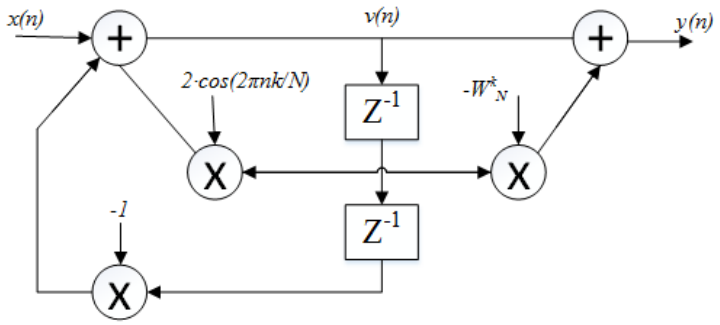

Fig. 1 – IIR filter implementation of the Goertzel algorithm

In order to obtain the indicated values of the k-th DFT coefficient in the Goertzel algorithm, only each $(N-1)$-th value of this coefficient is preserved, which provides one operation of complex multiplication in the filter straight chain and N real operations for calculating the intermediate results in the return circuit of the filter. Note that it is the refusal of receiving all output samples (therefore, their storage) in the straight filter circuit, which provides the Goertzel algorithm with saving in the number of computations in comparison with the definition of the nth DFT coefficient S, "*in the forehead*", according to the relation (1).

The filter's $y(n)$ output is equal to the DFT output frequency coefficient, $X(m)$, at the time index $n = N$, where the first time index value is $n = 0$. To be equivalent to the DFT, the frequency-domain index m must an integer in the range $0 \le m \le N-1$. The z-domain transfer function of the Goertzel algorithm is

$$H_G(z) = Y(z)/X(z) = \frac{1 - e^{-j2\pi m/N} \cdot z^{-1}}{1 - 2\cos(2\pi\, m/N) \cdot z^{-1} + z^{-2}}, \tag{2}$$

where $z^{-1} = e^{-j\omega t}$, and $z^{-2} = e^{-j2\omega t}$.

The differential equations of the filter Goertzel in a time domain are defined as follows:

1. The coefficients of return circuit of the filter are calculating:

$$v(n) = 2\cos(2\pi\, m/N) \cdot v(n-1) - v(n-2) + x(n). \tag{3}$$

2. The coefficients of straight filter chain are calculating:

$$y(n) = v(n) - W_N^k \cdot v(n-1). \tag{4}$$

Thus, the main advantages of the Goertzel algorithm over the standard radix-2 FFT for single tone detection consist in the following:

- N does not need to be an integer power of 2.
- The tone frequency can be any value between zero and sampling rate.
- The amount of filter coefficient storage is reduced.

- No storing a block of input data is needed before processing can begin (as with the FFT). Processing can begin with first input time sample.
- No data bit reversal is needed for Goertzel.
- If you implement the Goertzel algorithm M times to detect M tones, Goertzel is more efficient than FFT when $M < \log_2 N$.
- At computing an N -point $X(m)$ DFT bin value is that equation (3) need only be computed once after the arrival of the N -th input sample. Thus for real $x(n)$ inputs the filter requires $N+2$ real multiplies and $2N+1$ real adds to compute an N -point $X(m)$ [4].

One of disadvantages given an algorithm is that it does not allow to calculate a large number a component of Fourier coefficients. In tasks when it is necessary to calculate components of coefficients for several a component at once, this algorithm will not be effective. The use of FFT will also not allow to reduce the number of the calculated Fourier coefficients. In such cases it is proposed to use the method of linear algebraic processing of complex signal structures.

3 The method of linear algebraic processing of complex signal structures

Application of the Goertzel algorithm and the FFT method for calculating parameters of the signal spectrum is computationally cost and difficult to implement. To simplify the calculation of signals spectrum coefficients it is proposed to use the method of algebraic demodulation of complex signal structures. The idea of this method consists in statistical detection of amount of the observed fixed values of phases of harmonic oscillations on subcarrier frequencies.

For this the system of linear algebraic equations (SLAE) is composed:

$$A \cdot X = B, \tag{5}$$

where A - the matrix of amplitudes of the quadrature components on a modulation interval; B - the vector of the signal values in the digital representation in each sample of the modulation interval; X - the vector of required values of amplitude for a given modulation interval.

The dimension of the matrix A is defined by the number of samples N which are taken into account in the analysis of a signal on one interval of modulation and the number of considered quadrature of harmonics $(2 \cdot n_{f_{\max}})$. Depending on relation of vertical and horizontal the matrix's dimension the system (5) can be underdetermined $(N < 2 \cdot n_{f_{\max}})$, determined $(N = 2 \cdot n_{f_{\max}})$ and redefined $(N > 2 \cdot n_{f_{\max}})$. We will consider these cases in more detail.

The simplest case is when the system (5) can be strictly determined $(N = 2 \cdot n_{f_{\max}})$, so practically always SLAE is compatible and the solution of the system exists and the only. The number of the equations equals to the number of the required unknowns $(2 \cdot n_{f_{\max}})$ determining the amplitudes of quadrature signal's components. To solve the SLAE on the i-th modulation interval, it is necessary to select $(2 \cdot n_{f_{\max}})$ evenly located samples of the samples' array $P = \{p_0, p_1, ...\}$ beginning from the position where the full clock cycle of the signal begins to be observed. The square matrix of coefficients at unknown of SLAE is formed by the following rule:

$$\begin{aligned}
&\mathbf{A}_1 = \left\| a_{i,j} \right\|, \quad i, j = 0, \ldots, \left(2 \cdot n_{f\max} - 1\right); \\
&a_{i,j} = \sin\left[2\pi(f_0 + q \cdot \Delta f) \cdot t_i\right], \\
&0 \le j \le n_{f\max} - 1; \\
&a_{i,j} = \cos\left[2\pi(f_0 + q \cdot \Delta f) \cdot t_i\right], \\
&n_f \le j \le 2 \cdot n_{f\max} - 1;
\end{aligned} \quad , \tag{6}$$

where $q = 0, 1, ..., n_{f_{\max}}$.

The vector of the absolute terms is formed in the form a vector of signal's measurements on a duration of one modulation interval:

$$B_1 = \left\{ b_0, b_1, ..., b_{2n_{f\max}-1} \right\},\ b_i = p_i, \tag{7}$$

where $i = 0, ..., 2 \cdot n_{f_{\max}} - 1$.

The solution of the defined SLAE

$$A_1 \cdot X_1 = B_1 \quad \Rightarrow \quad X_1 = A_1^{-1} \cdot B_1 \tag{8}$$

gives the necessary estimate of the amplitudes' vector of the quadrature components $\mathbf{X}_1 = \left\{ x_0^1, \ldots, x_{(2 \cdot n_{f\max}-1)}^1 \right\}$ corresponding to the permissible values of the subcarriers of the frequencies. The next case when the system (5) is underdetermined $(N < 2 \cdot n_{f_{\max}})$ while at the such systems either have an infinite number of solutions, or do not have a solution at all. The underdetermined SLAE can be solved by the method of the pseudo-inverse matrix of Moore-Penrose. According of the method of the pseudo-inverse matrix among the set of the solutions by underdetermined SLAE the normal solution is chosen – the solution with minimum norm among the solutions satisfying condition $\|X_1\| = \min_{X_1}$. The normal solution exists and it is the only and is found by a formula:

$$X_1 = A_1^+ \cdot B_1, \tag{9}$$

where A^+ - the pseudo-inverse matrix of Moore-Penrose with dimension $2 \cdot n_{f_{\max}} \times 2 \cdot n_{f_{\max}}$.

The matrix A^+ is defined by the equation:

$$A_1 \cdot A_1^+ \cdot A_1 = A_1. \tag{10}$$

The solution (9) which is pertinent for writing down in the form of $X_1^+ = A_1^+ \cdot B_1$ gives a zero error $\left\| A_1 \cdot X_1^+ - B_1 \right\| = 0$, that is the solution is the pseudo-solution and among all pseudo-solution has as the normal solution, the minimum norm [5]. The most advantageous from the point of view of the maximum accounting of information on a signal is the case of the solution redefined SLAE $(N > 2 \cdot n_{f_{\max}})$. For formation redefined SLAE additional measurements of a signal from the sample containing P bigger quantity of the equations with the same number of unknown are used.

The degree of the redefined system is characterized by coefficient $\mu = W/2$ and describes asymmetry of the matrix dimensions $W \times 2$. This $W = \left\lfloor \frac{Fd}{V} \right\rfloor$, where Fd – a discretization frequency of the signal; V – a modulation rate; the sign $\lfloor \cdot \rfloor$ – means the rounding to the nearest smaller integer; the number 2 – means quantity used quadrature a component by means of which the signal, and, therefore, the number of unknown is set. The matrix A_2 and the vector B_2 are formed using the maximum number of measurements on a modulation interval T_p, determined by value $Num \approx T_p / t_d$:

$$\begin{aligned}
&\mathbf{A}_2 = \left\| a_{i,j} \right\|, \quad i = 0, \ldots, (Num - 1), \\
&j = 0 ... \left(2 \cdot n_{f\max} - 1 \right); \\
&a_{i,j} = \sin\left[2\pi (f_0 + q \cdot \Delta f) \cdot t_i \right], \\
&0 \le j \le n_{f\max} - 1; \\
&a_{i,j} = \cos\left[2\pi (f_0 + q \cdot \Delta f) \cdot t_i \right], \\
&n_f \le j \le 2 \cdot n_{f\max} - 1;
\end{aligned} \tag{11}$$

$$\mathbf{B}_2 = \left\{ b_0, \ldots, b_{(Num-1)} \right\}, \quad b_v = q_v, \\ v = 0, \ldots, (Num-1). \tag{12}$$

The SLAE has the form:

$$\mathbf{A}_2 \cdot \mathbf{X}_2 = \mathbf{B}_2 \tag{13}$$

The system (13) has the set of solutions. In practice most often use criterion of the least squares, leading to a assessment of the form:

$$\mathbf{X}_2^* = (\mathbf{A}_2{}^T \cdot \mathbf{A}_2)^{-1} \mathbf{A}_2{}^T \cdot \mathbf{B}_2 . \tag{14}$$

The solution of system (14) is the approximate, but the result turns out more exact, than at the solution of strict system (8). The noise stability of the solution is achieved by averaging the effect of the interference with a number of signal measurements exceeding the minimum necessary. The calculation of the phase angle vector by solving system (14) by the method of algebraic processing of complex signal structures requires approximately the same number of operations like when using the FFT method. When the dimension of the matrix A_2 equal to $Num \times 2$ the number of operations required to solve the system (14) is approximately equal to $Num \cdot \log_2 Num$. The main feature of this method is that for computation of parameters of a range of signals of the selected nomenclature of frequencies, there is no need to calculate all parameters of a signals spectrum.

Finally, we can consider the important case for practice when the SLAE is weakly determined. A weakly determined system is a system described by the matrix A with a determinant not equal to zero $|A| \approx 0$, but the number of conditionality $|A^{-1}| \cdot |A|$ is very large. As some equations appearing in such system are represented by a linear combination of other equations actually the system is underdetermined $(N < 2 \cdot n_{f_{\max}})$. Depending on a concrete type of a vector of right-side part B or exists an infinite set of solutions or none exists. For the solution of such type of systems the method of regularization is used. This method is based on the use of additional a priori information on the solution, which can be both qualitative and quantitative. The concept of regularization reduces to the replacement of the SLAE solution of the form (5) by the problem of minimization of a Tikhonov functional:

$$\Omega(X, \lambda) = |A \cdot X - B|^2 + \lambda \cdot |X - x0|^2 , \tag{15}$$

where λ – the small positive parameter of regularization; $x0$ – a priori estimate vector.

The problem of minimization of a Tikhonov functional can be reduced to solving another SLAE:

$$(A^T \cdot A + \lambda \cdot I) \cdot X = A^T \cdot B + \lambda \cdot x0 , \tag{16}$$

which at $\lambda \to 0$ passes into initial weakly determined system, and at big λ, being well defined, has the solution $x0$. Obviously, some intermediate value establishing a certain compromise between the acceptable conditionality and proximity to an initial task will be optimum [6]. The method of algebraic processing of complex signal structures allows carried out demodulation of signal by solving the SLAE without using FFT method. At demodulation of a signal by this method it is necessary that the SLAE was redefined since only the redefined SLAE allows to consider as much as possible information on a signal and gives the only solution of the system. Due to redefinition of SLAE the noise stability of this solution by averaging of action of noises at a large number of measurements of a signal is reached. The use of this method in case of demodulation of signals will allow to calculate parameters of a range of signals only of the necessary nomenclature of frequencies.

3 Conclusions

When processing complex signal structures for computation of parameters of a range of several tens tones in case of application of an algorithm of a FFT is solving a overly excess task. When using the Goertzel algorithm for the solution of this task which is implemented in the form of IIR fil-

ter of the second order the efficiency of the algorithm comes down to computing complexity of the FFT. To effectively solve this problem it is proposed to apply the method of algebraic processing of complex signal structures, which will allow us to calculate the parameters of the signal spectrum of only the needed nomenclature of frequencies by solving the SLAE without the use of FFT.

References

[1] Tikhonov V.I. Optimal'nyi priem signalov / V.I. Tikhonov. − M: Radio i svyaz', 1983. − 320 s.
[2] Feer K. Besprovodnaya tsifrovaya svyaz'. Metody modulyatsii i rasshireniya spektra / K. Feer; per. s angl. pod red. V.I. Zhuravleva. − Moskva: Radio i svyaz', 2000. − 520 s.
[3] Bleikhut R. Bystrye algoritmy tsifrovoi obrabotki signalov / R. Bleikhut; per. s angl. pod red. I.I. Grushko. − Moskva: Mir, 1989. − 448 s.
[4] Laions R. Tsifrovaya obrabotka signalov / R. Laions; per. s angl. pod red. A.A. Britova. − Moskva: Binom, 2006. − 635 s.
[5] Rabiner L. Teoriya i primenenie tsifrovoi obrabotki signalov / L. Rabiner, B. Gould; per. s angl. Yu. N. Aleksandrova. – Moskva: Mir, 1978. – 834 s.
[6] Vasil'ev K.K. Teoriya elektricheskoi svyazi: uchebnoe posobie / K.K. Vasil'ev, V.A. Glushkov, A.V. Dormidontov, A.G. Nesterenko. – Ul'yanovsk: UlGTU, 2008. – 452 s.

Рецензент: В'ячеслав Харченко, д.т.н., проф., академік Академії наук прикладної радіоелектроніки, Національний аерокосмічний університет ім. М. Є. Жуковського, Харків, Україна. E-mail: v_s_kharchenko@ukr.net

Надійшло: Травень 2017.

Автори:
Сергій Веклич, аспірант, Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: s.veklych@gmail.com
Сергій Рассомахін, д.т.н., проф., зав.каф. БІСТ, Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: rassomakhin@karazin.ua

Порівняльний аналіз алгоритму Герцеля та способу алгебраїчної обробки складних сигнальних конструкцій при виявленні окремих тонів сигналу.

Анотація. Розглянуто недоліки застосування алгоритму швидкого перетворення Фур'є при виявленні окремих тонів сигналу. Підкреслюється актуальність застосування алгебраїчних методів при демодуляції сигналів в сучасних системах передачі інформації. Розглянуто алгоритм селективного спектрального аналізу, запропонований спосіб лінійної алгебраїчної обробки складних сигнальних конструкцій при виявленні окремих тонів в спектрі сигналу. Зроблено аналіз ефективності відомого і запропонованого способу селективного спектрального аналізу. Зроблено висновок, що застосування способу лінійної алгебраїчної обробки складних сигнальних конструкцій дозволить обчислювати параметри спектру сигналів тільки потрібної номенклатури, шляхом вирішення СЛАР без використання швидкого перетворення Фур'є.

Ключові слова: ШПФ, НІХ-фільтри, СЛАР, цифрова обробка сигналів.

Рецензент: Вячеслав Харченко, д.т.н., проф., академик Академии наук прикладной радиоэлектроники, Национальный аэрокосмический университет им. М. Є. Жуковского, Харьков, Украина. E-mail: v_s_kharchenko@ukr.net

Поступила: Май 2017.

Авторы:
Сергей Веклич, аспирант, Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина.
E-mail: s.veklych@gmail.com
Сергей Рассомахин, д.т.н., проф., зав. каф. БИСТ, Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина.
E-mail: rassomakhin@karazin.ua

Сравнительный анализ алгоритма Герцеля и способа алгебраической обработки сложных сигнальных конструкций при определении отдельных тонов сигнала.

Аннотация. Рассмотрены недостатки применения алгоритма быстрого преобразования Фурье при обнаружении отдельных тонов сигнала. Подчеркивается актуальность применения алгебраических методов при демодуляции сигналов в современных системах передачи информации. Рассмотрен алгоритм селективного спектрального анализа, предложен способ линейной алгебраической обработки сложных сигнальных конструкций при обнаружении отдельных тонов в спектре сигнала. Произведен анализ эффективности известного и предложенного способа селективного спектрального анализа. Сделан вывод, что применение способа линейной алгебраической обработки сложных сигнальных конструкций позволит вычислять параметры спектра сигналов только необходимой номенклатуры, путем решения СЛАУ без использования быстрого преобразования Фурье.

Ключевые слова: БПФ, БИХ-фильтры, СЛАУ, цифровая обработка сигналов.

Статті пройшли внутрішнє та зовнішнє рецензування.

Наукове видання

КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА

Випуск 2(6) 2017

Міжнародний електронний науково-теоретичний журнал

Англійською, українською, російською мовами

Комп'ютерне верстання – Федоренко В.В., Кузнецова Т.В.

61022, Харків, майдан Свободи, 6
Харківський національний університет імені В.Н. Каразіна

V. N. Karazin Kharkiv National University Publishing