ISSN 1994-7836 (print)
ISSN 2519-2477 (online)

УДК 004.75

Article info
Received 17.03.2017 р.

Т. Г. Цаволик, В. В. Яцків
Тернопільський національний економічний університет, м. Тернопіль, Україна

МЕТОД ФОРМУВАННЯ КОРЕГУВАЛЬНИХ КОДІВ У СИСТЕМІ ЗАЛИШКОВИХ КЛАСІВ

Запропоновано новий метод формування перевірочних символів у корегувальних кодах системи залишкових класів. Проведено експериментальне дослідження апаратної складності та часу формування перевірочних символів корегувальних кодів системи залишкових класів для відомого та запропонованого методу при їх реалізації на програмованих логічних інтегральних схемах. Запропонований метод забезпечує зменшення апаратних затрат, використовує переваги корегувальних кодів системи залишкових класів, при цьому не потребує перетворення повідомлення у систему залишкових класів.

Ключові слова: корегувальні коди, система залишкових класів, безпровідні сенсорні мережі.

Вступ. Із широкомасштабним розвитком та впровадженням безпровідних технологій стає дедалі актуальнішою проблема забезпечення високої надійності передачі даних у безпровідних комп'ютерних мережах. Одним з підходів вирішення цієї проблеми є використання корегувальних кодів. На цей час розроблено значну кількість корегувальних кодів, які функціонують у позиційних системах числення і набувають практичного застосування у безпровідних комунікаціях, зокрема коди Ріда – Соломона, Боуза – Чоудхурі – Хоквінгема, турбокоди та ін. (Stallings, 2003). Окремо потрібно виділити корегувальні коди, які функціонують у системі залишкових класів (СЗК) (Chervjakov et al., 2003; Yatskiv, Tsavolyk & Zhengbing, 2015; Tor, Siddiqi, 2008). Ці коди характеризуються високою корегувальною здатністю та можливістю адаптивної зміни кількості та значень перевірочних символів залежно від стану каналу зв'язку. Однак використання корегувальних кодів СЗК потребує додаткового перетворення даних з позиційної системи числення (двійкової) у систему залишкових класів, в якій дані представляються залишками від ділення на вибрану систему взаємно простих модулів, що знижує швидкодію формування корегувальних кодів (Chervjakov et al., 2003).

Мета роботи полягає у підвищенні ефективності формування корегувальних кодів системи залишкових класів.

Формування перевірочних символів. У роботі пропонуємо новий метод формування перевірочних символів корегувальних кодів СЗК, суть якого полягає в такому. Послідовність бітів, яка підлягає передачі, розділяється на k частин по 4 або 8 біт:

$$\left(a_i^j, i=\overline{1,m},\ j=\overline{1,k}\right), \qquad (1)$$

де a^i – розряд даних у двійковому коді, $m=4,8$.

Кожній частині двійкового коду ставляться у відповідність прості числа (модулі) p_i ($p_1<p_2<\ldots<p_i<\ldots<p_n$), з яких перші k модулів інформаційні, n – загальна кількість модулів, $r=n-k$ – перевірочні модулі. Значення модулів вибираємо з умови $p_i>2^m$. Перші k модулів визначають робочий діапазон $P_k=\prod_{i=1}^{k}p_i$, повний діапазон дорівнює $P=\prod_{i=1}^{n}p_i$.

Оскільки значення тетрад або байтів у позиційному представленні менші за відповідні модулі p_i, то їх можна вважати залишками. Внаслідок вказаного перетворення повідомлення набуде вигляду

$$\left(x_i, i=\overline{1,k}\right), \qquad (2)$$

де x_i – частини повідомлення, які одночасно є залишками по вибраних модулях p_i, $x_i=\sum_{i=1}^{m}a_i\cdot 2^i$.

Для обчислення перевірочних символів повідомлення (2) перетворимо в позиційну систему числення

$$X=\sum_{i=1}^{k}(x_i\cdot M_i\cdot\delta_i)\bmod P_k, \qquad (3)$$

де: $M_i=\frac{P_k}{p_i}$; $\delta_i=M_i^{-1}\bmod p_i$.

Перевірочні символи обчислюють за формулою (Tor & Siddiqi, 2008)

$$x_{k+i}=X \bmod p_{k+i},\ i=\overline{1,(n-k)},$$

де X – повідомлення в позиційній системі числення.

Внаслідок цього кодове слово складається з інформаційних і перевірочних символів і має такий вигляд:

$$(x_1, x_2, \ldots x_i, \ldots x_k, x_{k+1}, \ldots x_n).$$

Для використання відомих корегувальних кодів СЗК потрібно перевести вхідне повідомлення у систему залишкових класів за формулою (Chervjakov et al., 2003; Tor & Siddiqi, 2008)

$$x_i=X \bmod p_i,\ i=\overline{1,k},$$

а після виявлення та виправлення помилок виконати обернене перетворення за формулою (3), що потребує додаткових затрат часу.

Приклад. Нехай X = 1010011101011001 – повідомлення, яке потрібно передати. Розділимо це повідомлення X на чотири тетради: $x_1=1010$, $x_2=0111$, $x_2=0101$, $x_4=1001$. Виберемо модулі, згідно з умовою $p_i>2^4$: $p_1=17$, $p_2=19$, $p_3=23$, $p_4=29$ – інформаційні, $p_5=31$ – перевірочний модуль. Робочий діапазон становить $P_k=17\cdot19\cdot23\cdot29=215441$. Загальний діапазон $P=P_k\cdot p_5=215441\cdot31=6678671$.

Оскільки значення x_1, x_2, x_3, x_4 у десятковій системі числення менші за відповідні модулі, то їх будемо

Цитування за ДСТУ: Цаволик Т. Г. Метод формування корегувальних кодів у системі залишкових класів / Т. Г. Цаволик, В. В. Яцків // Науковий вісник НЛТУ України. – 2017. – Вип. 27(3). – С. 191–194

Citation APA: Tsavolyk, T. G., & Yatskiv, V. V. (2017). The Method of Correcting Codes Formation in the Residue Number System. *Scientific Bulletin of UNFU, 27*(3), 191–194. Retrieved from: http://nv.nltu.edu.ua/index.php/journal/article/view/260

вважати залишками за цими модулями.

Переведемо повідомлення $X=(x_1,x_2,x_3,x_4)$ у десяткову систему числення. Для цього обчислимо ортогональні базиси: $M_1=\frac{P_K}{p_1}=12673$, $M_2=11339$, $M_3=9367$, $M_4=7429$. Обернені числа до $M_1 \div M_4$ рівні $\delta_1=15$, $\delta_2=14$, $\delta_1=4$, $\delta_4=6$. Отже, $X=\sum_{i=1}^{k}(x_i \cdot M_i \cdot \delta_i) \bmod P_K=153622$.

Перевірочний символ обчислюємо за формулою

$$x_5=X \bmod p_5=153622 \bmod 31=17.$$

Отже, повідомлення після кодування має вигляд $X'=(10,\ 7,\ 5,\ 9,17)$, або $X'=(1010,\ 0111,\ 0101,\ 1001,10001)$.

Результати експериментального дослідження. У цьому розділі наведено результати експериментального дослідження апаратних затрат (кількість логічних елементів, ЛЕ) та часу обчислення перевірочних символів за різної розрядності вхідних даних, за відомого методу формування перевірочних символів корегувальних кодів СЗК (метод 1) та запропонованого методу формування перевірочних символів у корегувальних кодах СЗК (метод 2). Експериментальні дослідження проводили з використанням програмного забезпечення Quartus фірми Intel (Altera). Відомий та запропонований метод формування корегувальних кодів СЗК, описані на мові програмування апаратних засобів Verilog-HDL та синтезовані в мікросхемах Cyclone IV.

Під час проведення експериментів змінювалися такі дані: розрядність вхідних даних: від 16 до 48 біт; кількість інформаційних модулів: 2-6; кількість перевірочних модулів – 1, 2; значення модулів залежить від розрядності повідомлення.

На рис. 1, 2 наведено результати експериментального дослідження апаратних затрат (кількість логічних елементів) та часу обчислення перевірочних символів за різної розрядності вхідних даних, для корегувальних кодів СЗК (метод 1) та для запропонованого методу (метод 2) з одним перевірочним модулем.

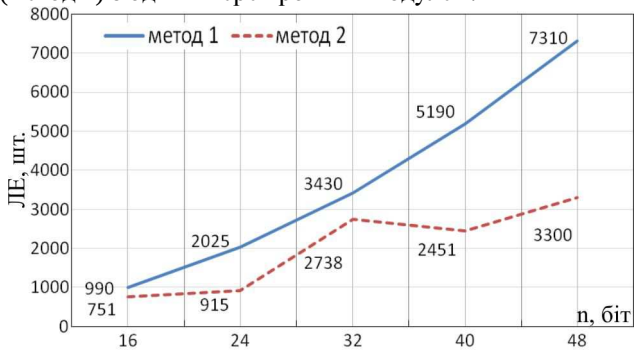

Рис. 1. Залежність апаратних затрат від розрядності вхідних даних за одного перевірочного модуля для методу 1 і методу 2

Як видно з рис. 1, запропонований метод забезпечує зменшення апаратних затрат у середньому на 35 % залежно від розрядності вхідних даних. При цьому часові затрати зростають у середньому на 46 % (рис. 2).

На рис. 3, 4 наведено результати експериментального дослідження апаратних затрат (кількість логічних елементів) та часу обчислення перевірочних символів за різної розрядності вхідних даних, для коревальних кодів СЗК (метод 1) та для запропонованого методу (метод 2) за використанням двох перевірочних модулів, що забезпечує виправлення помилки в залишку за будь-яким модулем.

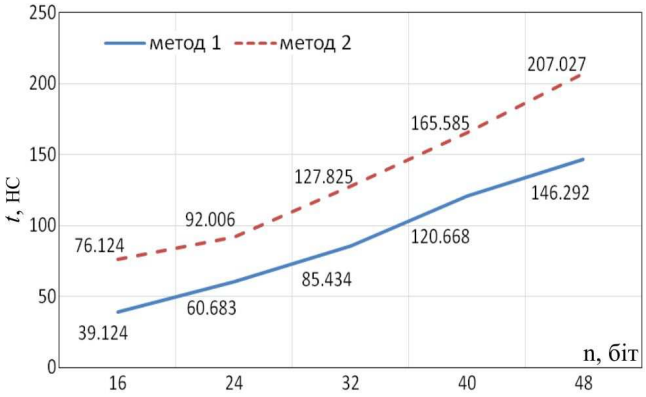

Рис. 2. Залежність часу обчислення перевірочних символів від розрядності вхідних даних за одного перевірочного модуля для методу 1 і методу 2

Як видно з рис. 3, запропонований метод забезпечує зменшення апаратних затрат у середньому на 29 % залежно від розрядності вхідних даних. При цьому часові затрати зростають у середньому на 47 % (див. рис. 4).

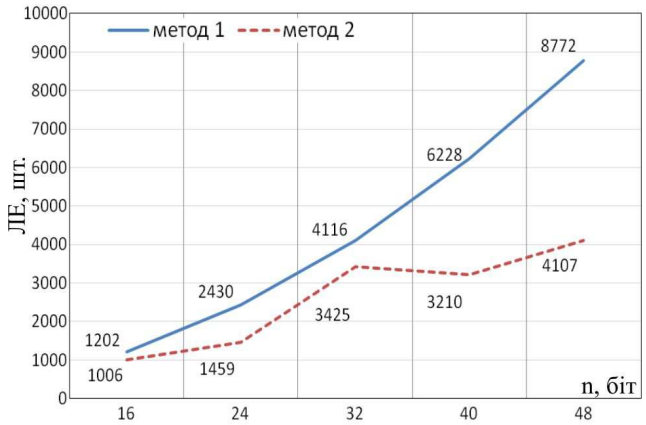

Рис. 3. Залежність апаратних затрат від розрядності вхідних даних за двох перевірочних модулів для методу 1 і методу 2

Також проведено дослідження апаратних затрат (рис. 5) та часу обчислення перевірочних символів (рис. 6) за розрядності вхідних даних 8 біт. При цьому значення всіх модулів вибираємо більші за 256.

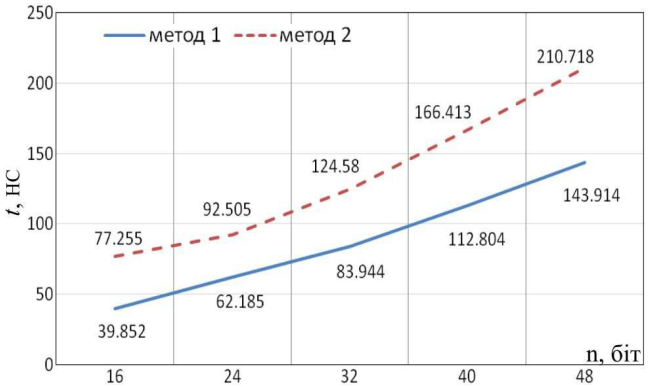

Рис. 4. Залежність часу обчислення перевірочних символів від розрядності вхідних даних за двох перевірочних модулів для методу 1 і методу 2

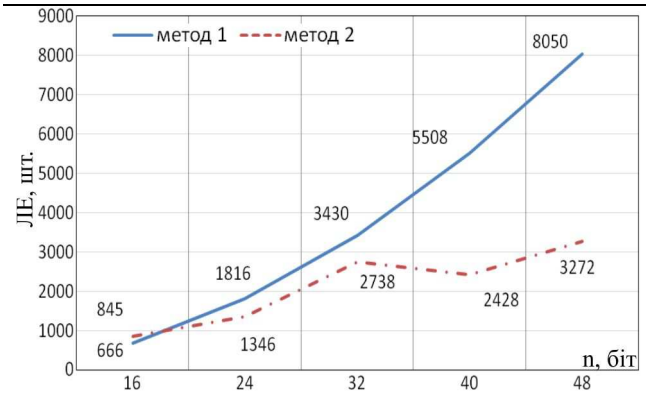

Рис. 5. Залежність апаратних затрат від розрядності вхідних даних за одного перевірочного модуля для методу 1 і методу 2 (розрядність блоку даних 8 біт)

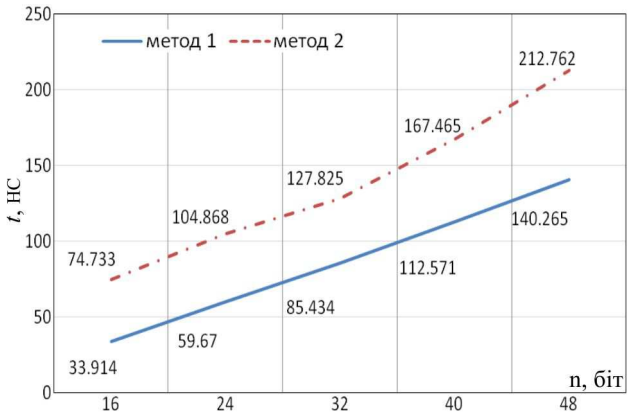

Рис. 6. Залежність часу обчислення перевірочних символів від розрядності вхідних даних за одного перевірочного модуля для методу 1 і методу 2 (розрядність блоку даних 8 біт)

Як видно з рис. 5, запропонований метод забезпечує зменшення апаратних затрат у середньому на 23 % і залежить від розрядності повідомлення (розрядність блоку даних 8 біт). При цьому час обчислення перевірочних символів зростає у середньому на 58 % (див. рис. 6).

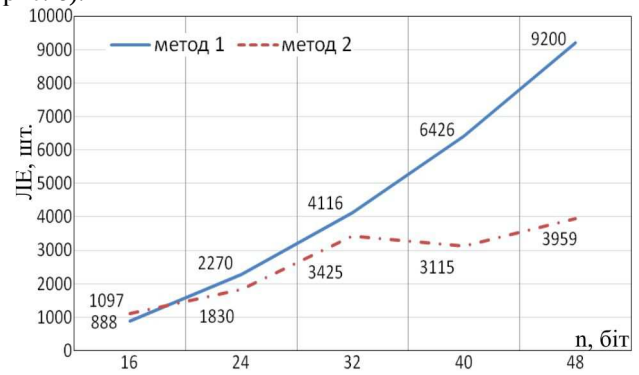

Рис. 7. Залежність апаратних затрат від розрядності вхідних даних за двох перевірочних модулів для методу 1 і методу 2 (розрядність блоку даних 8 біт)

Як видно з рис. 7, запропонований метод забезпечує зменшення апаратних затрат у середньому на 20 % і залежить від розрядності вхідних даних (розрядність блоку даних 8 біт). Часові затрати на формування перевірочних символів у запропонованому методі зростають у середньому на 59 % (рис. 8) порівняно з відомим методом. Однак у відомому методі повідомлення знаходиться у системі залишкових класів, що потребує додаткового часу на зворотне перетворення в позиційну систему числення.

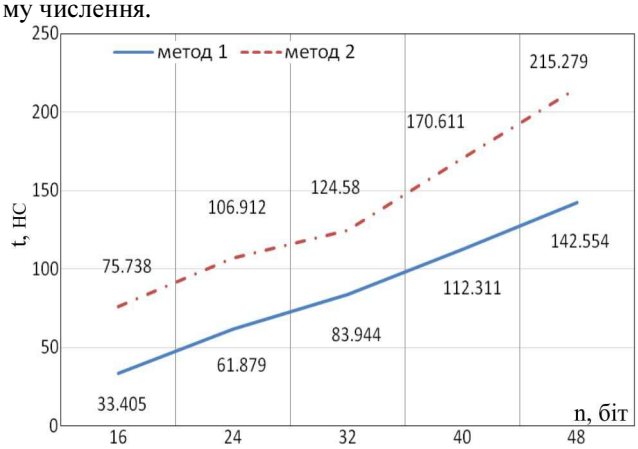

Рис. 8. Залежність часу обчислення перевірочних символів від розрядності вхідних даних за двох перевірочних модулів для методу 1 і методу 2 (розрядність блоку даних 8 біт)

Висновки. Запропонований метод формування корегувальних кодів системи залишкових класів забезпечує зменшення апаратних затрат у середньому на 20 % залежно від розрядності повідомлення. При цьому основною перевагою запропонованого методу є те, що вхідне повідомлення обробляється в позиційній системі числення тобто не потребує перетворення в систему залишкових класів. Отже, розроблений метод формування перевірочних символів значно розширить область застосування корегувальних кодів системи залишкових класів унаслідок оброблення повідомлень, які представлено у позиційних системах числення.

У подальших роботах плануємо підвищити швидкодію формування перевірочних символів унаслідок використання спеціальної системи модулів та оптимізації часу виконання операції модулярного множення.

Перелік використаних джерел

Chervjakov, N. I. (Ed.), Sahnjuk, P. A., Shaposhnikov, A. V., & Rjadnov, S. A. (2003). *Moduljarnye parallelnye vychislitelnye struktury nejroprocessornyh sistem*. Moscow: Fizmatlit, 288 p. [in Russian].

Stallings, W. (2003). *Besprovodnye linii svjazi i seti*: per. s angl. Moscow: Izd. dom "Viljams", 640 p. [in Russian].

Tor, G. V., & Siddiqi, M. U. (2008). Multiple error detection and correction based on redundant residue number systems. *Communications, IEEE Transactions on*, *56*(3), 325–330.

Yatskiv, V., Tsavolyk, T., & Zhengbing, Hu. (2015). Multiple Error Detection and Correction Based on Modular Arithmetic Correcting Codes. *Proceedings of the 8-th 2015 IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS'2015)*, *2*, 850–854. Warszawa, Poland.

Т. Г. Цаволик, В. В. Яцкив

МЕТОД ФОРМИРОВАНИЯ КОРРЕКТИРУЮЩИХ КОДОВ В СИСТЕМЕ ОСТАТОЧНЫХ КЛАССОВ

Предложен новый метод формирования проверочных символов в корректирующих кодах системы остаточных классов. Проведено экспериментальное исследование аппаратной сложности и времени формирования проверочных символов корректирующих кодов системы остаточных классов для известного и предложенного метода при

их реализации на программируемых логических интегральных схемах. Предложенный метод обеспечивает уменьшение аппаратных затрат, использует преимущества корректирующих кодов системы остаточных классов, при этом не требует преобразования сообщения в систему остаточных классов.

Ключевые слова: корректирующие коды; система остаточных классов; беспроводные сенсорные сети.

T. G. Tsavolyk, V. V. Yatskiv

THE METHOD OF CORRECTING CODES FORMATION IN THE RESIDUE NUMBER SYSTEM

The problem of high reliability of data transmission in wireless computer networks becomes more urgent with the widespread development and implementation of wireless technology. One of the approaches to solve this problem is using of correcting codes. A significant amount of correcting codes was developed. They operate in positional number systems and have practical application in wireless communications. It is necessary to highlight the correcting codes that operate in the Residue Number System (RNS). These codes are characterized by high corrective ability and the possibility of adaptive changes in the number and values of check symbols depending on the channel's state. However, the usage of RNS correcting codes requires additional data conversion from the binary system into the RNS. Thus, the aim of the work is to increase the efficiency of correcting codes formation based on Residue Number System. The essence of a proposed method of RNS correcting codes formation is as follows. The transmitted sequence of bits is divided into segments of 4 or 8 bits. Each part of the binary code is associated with prime numbers (modules) p_i ($p_1<p_2<...<p_i<...<p_n$). The value of the modules is chosen from the condition $p_i>2^m$. The authors present the following results of experimental studies. Firstly, the experimental studies of hardware costs (number of logic gates) and computation time for the check symbols are conducted for different digit capacity of the input data for RNS correcting codes and proposed method for the RNS correcting codes formation. Secondly, the study was conducted using the Quartus software by the Intel (Altera) company. Both known and proposed methods of RNS correcting codes coding are described using the Verilog-HDL, synthesized in Cyclone IV chips. Thirdly, the following parameters were choosen for the experiment: digit capacity of the input data from 16 to 48 bit; the number of information modules – 4; the number of check modules – 1, 2; the modules' values depend on the digit capacity of the message. Finally, the proposed method reduces hardware costs by an average of 20 % and depends on the digit capacity of the input data (block capacity is 8 bit). At the same time, the computation time costs rise by an average of 59 %. However, in the known method the message is represented in Residue Number System, which requires additional time for transformation in positional system. The conclusions are as follows. The proposed method of the RNS correcting codes formation reduces the hardware costs by 20 % depending on the digit capacity of the message and improves performance through the necessary transformation of the messages into RNS. Also the method of forming check symbols will expand the scope of RNS correcting codes usage by processing the messages represented in positional systems.

Keywords: Correction Codes; Residue Number System; Wireless Sensor Networks.

Інформація про авторів:

Цаволик Тарас Григорович, аспірант, Тернопільський національний економічний університет, м. Тернопіль, Україна.
Email: calisto2292@ukr.net

Яцків Василь Васильович, д-р техн. наук, доцент, Тернопільський національний економічний університет, м. Тернопіль, Україна.
Email: jazkiv@ukr.ne