УДК 004.75

Н.Г.Яцків, канд. техн. наук, доц., Т.Г.Цаволик, Р.В. Деркач
Тернопільський національний економічний університет, Україна

МЕТОД ФОРМУВАННЯ КОРЕГУЮЧИХ КОДІВ В СИСТЕМІ ЗАЛИШКОВИХ КЛАСІВ

N.G.Yatskiv, Ph.D., Assoc. Prof., T.G.Tsavolyk, R.V. Derkach

THE METHOD OF CORRECTING CODES FORMATION IN THE RESIDUE NUMBER SYSTEM

З широкомасштабним розвитком та впровадженням безпровідних технологій стає більш актуальною проблема забезпечення високої надійності передачі даних в безпровідних комп'ютерних мережах. Одним з підходів вирішення даної проблеми є використання корегуючих кодів. На даний час розроблено значну кількість корегуючих кодів, які функціонують у позиційних системах числення і знаходять практичне застосування в безпровідних комунікаціях, зокрема коди Ріда – Соломона, Боуза - Чоудхурі – Хоквінгема, турбо - коди та інші [1]. Окремо необхідно виділити корегуючі коди, які функціонують в системі залишкових класів (СЗК) [2 - 4]. Дані коди характеризуються високою корегуючою здатністю та можливістю адаптивної зміни кількості та значень перевірочних символів в залежності від стану каналу зв'язку. Однак використання корегуючих кодів СЗК потребує додаткового перетворення даних з двійкової системи числення в систему залишкових класів, в якій дані представляються залишками від ділення на вибрану систему взаємно простих модулів, що знижує швидкодію формування корегуючих кодів [2].

В роботі пропонується новий метод формування корегуючих кодів СЗК, суть якого полягає в наступному. Послідовність бітів, яка підлягає передачі, розділяється на k частин по 4 або 8 біт:

$$\left(a_1^1\, a_2^1 \ldots a_i^1 \ldots a_m^1,\; a_1^2\, a_2^2 \ldots a_i^2 \ldots a_m^2, \cdots, a_1^j\, a_2^j \ldots a_i^j \ldots a_m^j, \cdots, a_1^k\, a_2^k \ldots a_i^k \ldots a_m^k\right), \qquad (1)$$

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

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

Так як значення тетрад або байтів в позиційному представленні менші, ніж відповідні модулів p_i, то їх можна вважати залишками.

Перевірочні символи обчислюються за формулою [4]:

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

де X – повідомлення в позиційній системі числення, $X = \sum_{i=1}^{k} (x_i \cdot M_i \cdot \delta_i) \bmod P_K$, $x_i = \sum_{i=1}^{m} a_i \cdot 2^i$, $M_i = \dfrac{P_K}{p_i}$, $\delta_i = M_i^{-1} \bmod p_i$.

Кодове слово складається з інформаційних і перевірочних символів і має вигляд:

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

Виявлення помилок. Якщо в прийнятому повідомленні $X' = (x_1', x_2', \dots, x_i', \dots, x_k, x_{k+1}, \dots, x_n')$ відбулась помилка, то його позиційне представлення вийде за межі робочого діапазону, тобто $X' > P_K$.

Виявлення помилок базується на обчислення проекцій числа. Нехай $X = (x_1, x_2, \dots, x_i, \dots, x_k, x_{k+1}, \dots, x_n)$ правильне число, тоді значення X не зміниться, якщо його представити в системі модулів, із якої вилучено модуль p_i. Значення X_i отримане із X без модуля p_i називають проекцією числа X за модулем p_i. Відповідно, якщо число $X = (x_1, x_2, \dots, x_i, \dots, x_k, x_{k+1}, \dots, x_n)$ правильне, то проекції цього числа за всіма модулями рівні: $X_1 = X_2 = \dots = X_i = \dots = X_n < P_k$ [2].

Приклад. Нехай $X = 1010011101011001$ – повідомлення, яке необхідно передати. Розділимо дане повідомлення X на тетради: $x_1 = 1010$, $x_2 = 0111$, $x_2 = 0101$, $x_4 = 1001$. Виберемо модулі, згідно умови $p_i > 2^4$: $p_1 = 17$, $p_2 = 19$, $p_3 = 23$, $p_4 = 29$ – інформаційні, $p_5 = 31$ – перевірочний модуль. Робочий діапазон становить $P_K = 17 \cdot 19 \cdot 23 \cdot 29 = 215441$. Загальний діапазон $P = P_K \cdot p_5 = 215441 \cdot 31 = 6678671$. Оскільки значення x_1, x_2, x_3, x_4 в десятковій системі числення менші за відповідні модулі, то їх можна вважати залишками за даними модулями. Переведемо повідомлення $X = (x_1, x_2, x_3, x_4)$ в 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 $M_1 - M_4$ 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 обчислюється за формулою $x_5 = X \bmod p_5 = 153622 \bmod 31 = 17$.

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

Запропонований метод формування корегуючих кодів в системі залишкових класів не потребує перетворення повідомлення в систему залишкових класів, таким чином, підвищує швидкодію обчислень і значно розширює область застосування за рахунок обробки повідомлень, які представлені в позиційних системах числення.

Література

1. Беспроводные линии связи и сети.: Пер. с англ. – М.: Издательський дом «Вильямс», 2003. – 640 с.

2. Модулярные параллельные вычислительные структуры нейропроцессорных систем /Н. И. Червяков, П. А. Сахнюк, А. В. Шапошников, С. А. Ряднов. Под редакцией Н.И. Червякова. – М.: Физматлит, 2003. – 288 с.

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

4. Goh Vik Tor, Mohammad Umar Siddiqi. Multiple error detection and correction based on redundant residue number systems. *Communications, IEEE Transactions on*, 2008, 56.3, p.325-330.