УДК 004.75

В. В. ЯЦКІВ

Тернопільський національний економічний університет, Тернопіль

ВИЯВЛЕННЯ ТА ВИПРАВЛЕННЯ БАГАТОКРАТНИХ ПОМИЛОК НА ОСНОВІ МОДУЛЯРНИХ КОРЕКТУЮЧИХ КОДІВ

Анотація. У вступі описано обмеження коректуючих кодів в системі залишкових класів. Визначено актуальність розробки коректуючих кодів на основі модулярної арифметики призначених для захисту від помилок даних представлених у двійковій системі числення. Сформульована мета та задачі досліджень для даної статті. Розроблено метод виявлення та виправлення двохкратних помилок за допомогою двох перевірочних символів. Розроблено алгоритм кодування та декодування даних на основі запропонованих модулярних кодів. Приведено приклад виправлення помилок в двох інформаційних символах. В кінці статті наведено список відомих наукових публікацій по даній темі.

Ключові слова: модулярна арифметика, система залишкових класів, коректуючі коди безпровідні сенсорні мережі.

Аннотация. Во введении описано ограничения корректирующих кодов в системе остаточных классов. Определены актуальность разработки корректирующих кодов основанных на модулярной арифметике и предназначенных для защиты от ошибок данных представленных в двоичной системе счисления. Сформулирована цель и задачи исследований для данной статьи. Разработан метод выявления и исправления двукратных ошибок с помощью двух проверочных символов. Разработан алгоритм кодирования и декодирования данных на основе предложенных модулярных кодов. Приведен пример исправления ошибок в двух информационных символах. В конце статьи приведен список известных научных публикаций по данной теме.

Ключевые слова: модулярная арифметика, система остаточных классов, корректирующие коды, беспроводные сенсорные сети.

Abstract. The restrictions of corrective codes in the Residue Number System is described in introduction. The relevance of development correcting codes based on modular arithmetic and designed to protect the data presented in the binary system from errors is determined. The objective and tasks of the research for this article is stated. A method for two errors detection and correction with the use of two check symbols is elaborated. The algorithm coding and decoding based on the proposed modular codes is elaborated. An example of two errors correction is shown. At the end of the article is a list of scientific publications on this topic

Key words: modular arithmetic, residue number system, corrective codes, wireless sensor networks.

Вступ

В безпровідних сенсорних мережах для підвищення надійності передачі даних використовують циклічний контроль парності (CRC – коди), який забезпечує ефективне виявлення помилок [1]. В [2] проведено аналіз методів виявлення та виправлення помилок та показано недоліки застосування існуючих коректуючих кодів в безпровідних сенсорних мережах (БСМ). БСМ є розділеною та самоорганізованою мережею сенсорів і виконавчих пристроїв, які об’єднані між собою безпровідними радіоканалами зв’язку.

Враховуючи переваги системи залишкових класів (СЗК) при обробці та передаванні даних, особливий інтерес, для використання в БСМ, представляють коректуючі коди на основі СЗК та модулярної арифметики [3, 4]. Однак для їх використання в існуючих цифрових системах оброблення та передавання даних, зокрема в БСМ, необхідно попередньо перетворити дані в СЗК, що потребує додаткових затрат часу та обчислювальних ресурсів [5, 6]. Коректуючі коди СЗК мають також обмеження, які накладаються умовою вибору зростаючої послідовності взаємно простих модулів. При цьому необхідно щоб перевірочні модулі були однакової розрядності. В іншому випадку виникає проблема ефективного (оптимального) збереження перевірочних символів.

Актуальність

З розвитком та широким впровадженням безпровідних технологій задача підвищення надійності передачі даних набуває все більш важливого значення. Відповідно, контроль цілісності даних, які передаються та обробляються сучасними цифровими системами є актуальною науковою задачею, зокрема в безпровідних сенсорних мережах.

В [7] розроблено та досліджено модулярні коректуючі коди, які забезпечують виправлення однократних помилок. Дані коди зберігають переваги коректуючих кодів СЗК, але обробляють вхідні дані представлені в позиційній системі числення (двійковій, десятковій), що значно спрощує процедури кодування / декодування та розширює область їх застосування. Отже, розробка коректуючих кодів на основі модулярної арифметики, які призначені для захисту даних представлених у двійковій системі числення від багатократних помилок є актуальною науковою задачею.

Мета

Метою статті є розробка коректуючих кодів на основі модулярної арифметики для виявлення та виправлення багатократних помилок.

Задачі

1. Для досягнення вказаної мети необхідно довести можливість виправлення помилок в двох інформаційних символах при використанні двох перевірочних модулів.
2. Розробити алгоритм виявлення та виправлення багатократних помилок.

Виявленння та виправлення помилок в одному інформаційному символі

Нехай $X \equiv (x_1, x_2, \ldots, x_i, \ldots, x_k)$ - кортеж символів заданої розрядності представлених в двійковій системі числення, які необхідно передати; $E_i \equiv (0,\ 0, \ldots, e_i, \ldots, 0)$ – код помилки; $X' \equiv (x_1', x_2', \ldots, x_i', \ldots, x_k')$ – кортеж символів в результаті дії завад:

$$(x_1', x_2', \ldots, x_i', \ldots, x_k') = (x_1, x_2, \ldots, x_i, \ldots, x_k) + \\ + (0, 0, \ldots, e_i, \ldots, 0) = (x_1, |x_2 + e_i|_P, \ldots, x_i, \ldots, x_k).$$

Значення контрольного символу обчислюється за формулою [8]

$$x_{k+1} = |(v_1 \cdot x_1 + v_2 \cdot x_2 + \ldots + v_i \cdot x_i + \ldots + v_k \cdot x_k)|_P, \quad (1)$$

де v_i – коефіцієнти взаємно прості з P, $|\bullet|_P$ – операція отримання залишку по модулю P.

Декодер по прийнятих даних $(x_1', x_2', \ldots, x_i', \ldots, x_k')$ обчислює значення контрольного символу:

$$x_{n+1}' = \left|(v_1 \cdot x_1' + v_2 \cdot x_2' + \ldots + v_i \cdot x_i' + \ldots + v_k \cdot x_k')\right|_P. \quad (2)$$

Для виявлення помилки обчислимо синдром δ, який представляє різницю між отриманим перевірочним символом і перевірочним символом обчисленим на приймальній стороні (в декодері):

$$\delta = \left|x_{k+1}' - x_{k+1}\right|_P,$$

якщо синдром дорівнює нулю, $\delta = 0$ то помилки немає, так як при відсутності помилки $x_i' = x_i$, відповідно і $x_{k+1}' = x_{k+1}$, якщо $\delta \neq 0$ – є помилка, відповідно $x_i' \neq x_i$ і, як наслідок $x_{k+1}' \neq x_{k+1}$.

Для виправлення помилок необхідно щоб значення синдрому δ було унікальне для всіх можливих варіантів помилки. Дана умова виконується при дотриманні правил: 1) значення контрольного модуля $P > 2 \cdot k \cdot (2^m - 1)$, де k – кількість інформаційних символів; 2) коефіцієнти v_i – взаємно прості з P.

Локалізація та виправлення помилки в одному інформаційному символі здійснюється шляхом порівняння синдрому δ з таблицею попередньо знайдених розв'язків рівняння $S_{ij} = \left|v_i \cdot e_{ij}\right|_P$, для всіх $-2^m - 1 < e_{ij} < 2^m - 1$, де $i = 1, \ldots, n$, $j = -2^m - 1, \ldots, 2^m - 1$.

На основі аналізу значень S_{ij} визначаємо символ в якому відбулася помилка.

Для виправлення помилки в одному символі необхідно розв'язати рівняння

$$\delta = \left|x_{k+1}' - x_{k+1}\right|_P = \left|v_i \cdot \left|x_i' - x_i\right|_P\right|_P,$$

так як $x_i' = \left|x_i + e_j\right|_P$ то $\left|v_i \cdot \left|\left|x_i + e_j\right|_P - x_i\right|_P\right|_P = S_{ij}$,

$$\left|v_i \cdot x_i + v_i \cdot e_j - v_i \cdot x_i\right|_P = S_{ij},$$

звідки слідує

$$S_{ij} = \left| v_i \cdot e_j \right|_P . \quad (3)$$

З рівняння (3) знаходимо значення помилки e_j. При цьому, правильне значення інформаційного символу дорівнює:

$$x_i = \left| x_i^{'} - e_j \right|_P .$$

Виявлення та виправлення помилок в двох інформаційних символах

В даній роботі розроблено метод виявлення та виправлення багатократних помилок на основі модурярних коректуючих кодів. Для забезпечення можливості виправлення помилок в двох інформаційних символах вибираємо взаємно прості коефіцієнти w_i і обчислимо додатковий перевірочний символ x_{k+2}.

Значення перевірочного символу обчислюється за формулою:

$$x_{k+2} = \left| (w_1 \cdot x_1 + w_2 \cdot x_2 + \ldots + w_i \cdot x_i + \ldots + w_k \cdot x_k) \right|_P . \quad (4)$$

В декодері по прийнятих даних обчислюється перевірочний символ $x_{k+2}^{'}$:

$$x_{k+2}^{'} = \left| (w_1 \cdot x_1 + v_2 \cdot x_2 + \ldots + w_i \cdot x_i^{'} + \ldots + w_k \cdot x_k) \right|_P .$$

В результаті отримали систему рівнянь:

$$\begin{cases} \left| (v_1 \cdot x_1 + v_2 \cdot x_2 + \ldots + v_i \cdot x_i + \ldots + v_k \cdot x_k) \right|_P = x_{k+1} \\ \left| (w_1 \cdot x_1 + w_2 \cdot x_2 + \ldots + w_i \cdot x_i + \ldots + w_k \cdot x_k) \right|_P = x_{k+2} \end{cases} .$$

Обчислюємо синдроми δ_1 і δ_2:

$$\delta_1 = \left| x_{k+1}^{'} - x_{k+1} \right|_P , \quad \delta_2 = \left| x_{k+2}^{'} - x_{k+2} \right|_P ,$$

або

$$\delta_1 = \left| v_1 \cdot (x_1^{'} - x_1) + v_2 \cdot (x_2^{'} - x_2) + \ldots + v_i \cdot (x_i^{'} - x_i) + \ldots + v_k \cdot (x_k^{'} - x_k) \right|_P , \quad (5)$$

$$\delta_2 = \left| w_1 \cdot (x_1^{'} - x_1) + w_2 \cdot (x_2^{'} - x_2) + \ldots + w_i \cdot (x_i^{'} - x_i) + \ldots + w_k \cdot (x_k^{'} - x_k) \right|_P . \quad (6)$$

При $\delta_1 = 0$ і $\delta_2 = 0$ – помилки відсутні, в іншому випадку наявні помилки.

Припустимо, що помилки відбулися в двох символах. Так як при відсутності помилки $x_i^{'} - x_i = 0$, то рівняння (5) і (6) набудуть вигляду:

$$\left| v_i \cdot (x_i^{'} - x_i) + v_{i+1} \cdot (x_{i+1}^{'} - x_{i+1}) \right|_P = \delta_1 , \quad (7)$$

$$\left| w_i \cdot (x_i^{'} - x_i) + w_{i+1} \cdot (x_{i+1}^{'} - x_{i+1}) \right|_P = \delta_2 . \quad (8)$$

З врахування виразів $e_1 = \left|x_1^{'} - x_1\right|_P$ і $e_2 = \left|x_2^{'} - x_2\right|_P$ рівняння (7) і (8) набудуть вигляду:

$$\left|v_1 \cdot e_1 + v_2 \cdot e_2\right|_P = \delta_1,$$

$$\left|w_1 \cdot e_1 + w_2 \cdot e_2\right|_P = \delta_2,$$

де e_1, e_2 – різниця між прийнятим і переданим значенням інформаційного символу.

Розв'язавши рівняння (7) і (8) отримаємо правильні значення інформаційних символів x_i і x_{i+1}.

Отже, даний коректуючий код виправляє помилки в t символах, якщо його мінімальна кодова відстань дорівнює: $d_{\min} \geq t+1$.

Алгоритм локалізації помилки складається з наступних кроків:

1. Обчислення перевірочних символів по прийнятих інформаційних символах: x_{k+1}, x_{k+2};
2. Обчислення синдрому δ_1, δ_2;
3. Якщо $\delta_1 = 0$, $\delta_2 = 0$ – помилки немає, зупинка і вихід. В іншому випадку продовження.
4. Припускаємо, що помилка відбулася в символах x_i і x_{i+1}, $i = 1,\ldots k$. Збільшуємо i, $i = i+1$.
5. Розв'язуємо рівняння (7) і (8);
6. Якщо знайдені $x_i < 2^m - 1$ і $x_{i+1} < 2^m - 1$. Перехід до пункту 2;
7. Збільшуємо i, $i = i+1$. Перехід до пункту 4.

Для виявлення помилки кратної r в кортежі даних, який складається із k інформаційних символів необхідно здійснити $C_k^r = \dfrac{k!}{r!(k-r)!}$ ітерацій, наприклад для $k = 8$, $r = 2$, $C_8^2 = 28$ ітерацій.

Розроблений метод та алгоритм виправлення помилок в двох інформаційних символах може бути використаний для виправлення багатократних помилок для цього необхідно збільшити кількість перевірочних символів.

Особливістю розроблених коректуючих кодів є можливість зміни кількості перевірочних символів x_{k+i}, $i = 1, \ldots, h$, де h – максимальна кількість перевірочних символів, без зміни принципів кодування. Тобто, при збільшенні ймовірності помилки в каналі зв'язку достатньо збільшити кількість перевірочних символів. Вказана можливість забезпечує високу надійність передавання даних при зміні характеристик каналу зв'язку.

Можливість виправлення двох помилок показано в наступному прикладі.

Приклад. Розглянемо коректуючий код, який складається з восьми інформаційних і двох перевірочних символів, і забезпечує виправлення помилок в будь-яких двох інформаційних символах. Розрядність інформаційних символів 4 біти. Кортеж даних, які необхідно передати має вигляд: $X = (5, 8, 10, 3, 7, 14, 12, 1)$.

Вибираємо модуль $P = 1021$ та взаємно прості коефіцієнти для обчислення першого перевірочного символу: $v_1 = 13$, $v_2 = 17$, $v_3 = 19$, $v_4 = 23$, $v_5 = 29$, $v_6 = 31$, $v_7 = 37$, $v_8 = 43$; взаємно прості коефіцієнти для обчислення другого перевірочного символу: $w_1 = 7$, $w_2 = 61$, $w_3 = 73$, $w_4 = 83$, $w_5 = 103$, $w_6 = 199$, $w_7 = 239$, $w_8 = 313$.

Значення перевірочних символів знаходимо за формулою (1):

$$x_{k+1} = \left|13 \cdot 5 + 17 \cdot 8 + 19 \cdot 10 + 23 \cdot 3 + 29 \cdot 7 + 31 \cdot 14 + 37 \cdot 12 + 43 \cdot 1\right|_{1021} = 563;$$

$$x_{k+2} = \left|7 \cdot 5 + 61 \cdot 8 + 73 \cdot 10 + 83 \cdot 3 + 103 \cdot 7 + 199 \cdot 14 + 239 \cdot 12 + 313 \cdot 1\right|_{1021} = 22.$$

Нехай прийняли дані $X^{'} = (5, 4, 6, 3, 7, 14, 12, 1)$. Обчислимо перевірочні символи по прийнятих даних за формулою (2):

$$x^{'}_{k+1} = \left|13 \cdot 5 + 17 \cdot 4 + 19 \cdot 6 + 23 \cdot 3 + 29 \cdot 7 + 31 \cdot 14 + 37 \cdot 12 + 43 \cdot 1\right|_{1021} = 419;$$

$$x^{'}_{k+2} = \left|7 \cdot 5 + 61 \cdot 4 + 73 \cdot 6 + 83 \cdot 3 + 103 \cdot 7 + 199 \cdot 14 + 239 \cdot 12 + 313 \cdot 1\right|_{1021} = 507.$$

Обчислюємо значення синдрому:

$$\delta_1 = \left|x^{'}_{k+1} - x_{k+1}\right|_P = \left|419 - 563\right|_{1021} = 877;$$

$$\delta_2 = \left|x^{'}_{k+2} - x_{k+2}\right|_P = \left|507 - 22\right|_{1021} = 485.$$

Так як синдроми δ_1 і δ_2 не дорівнюють нулю, отже наявні помилки.

Для виявлення помилки в двох інформаційних сиволах необхідно розв’язати рівняння (7) і (8) послідовно припускаючи, що помилки відбулися в двох символах.

Припустимо, що помилки в символах x_2 і x_3. Тоді рівняння (7) і (8) з врахуванням числових значень набудуть вигляду:

$$\left|17 \cdot e_2 + 19 \cdot e_3\right|_P = 877, \tag{9}$$

$$\left|61 \cdot e_2 + 73 \cdot e_3\right|_P = 485. \tag{10}$$

Помножимо рівняння (9) на 61 а рівняння (10) на 17:

$$\left|16 \cdot e_2 + 138 \cdot e_3\right|_P = 405, \tag{11}$$

$$\left|16 \cdot e_2 + 220 \cdot e_3\right|_P = 77, \tag{12}$$

і віднімемо рівняння (12) від рівняння (11): $\left|939 \cdot e_3\right|_P = 328$, за алгоритмом Евкліда знаходимо: $e_3 = 1017$.

Для знаходження e_2 підставимо значення e_3 в рівняння (10):

$$\left|61 \cdot e_2 + 73 \cdot 1017\right|_P = 485,$$

$\left|61 \cdot e_2\right|_P = 777$, отже $e_2 = 1017$.

Отже, правильні значення інформаційних символів дорівнюють:

$$x_2 = \left|x^{'}_2 - 1017\right|_{1021} = \left|4 - 1017\right|_{1021} = 8;\ x_3 = \left|x^{'}_3 - 1017\right|_{1021} = \left|6 - 1017\right|_{1021} = 10.$$

В таблиці 1 приведені результати обчислення значень інформаційних символів при всіх можливих варіантах помилок в двох інформаційних символах. Як видно з таблиці 1 значення інформаційних сим-

волів, в межах робочого діапазону, знаходяться тільки в першому рядку, що відповідає позиції помилок (u_i, u_j) в першому і другому інформаційному символі.

Таблиця 1 – Виявлення помилок в двох інформаційних символах

№	Позиція помилки		Значення інформаційних символів	
	u_i	u_j	x_i	x_i
1	1	2	871	131
2	1	3	616	724
3	1	4	990	74
4	1	5	860	192
5	1	6	988	331
6	1	7	621	103
7	1	8	108	176
8	**2**	**3**	**8**	**10**
9	2	4	978	44
		. . .		
28	7	8	944	754

Висновки

Розроблено коректуючі коди на основі модулярної арифметики, які дозволяють виявлення та виправлення багатократних помилок в пакетах даних. Дані коди забезпечують виправлення помилок в t - інформаційних символах при використанні t перевірочних символів. Представлено Алгоритм локалізації помилки.

Список літератури

1. IEEE Standard for Part 15.4: Wireless Medium Access Control Layer (MAC) and Physical Layer (PHY) specifications for Low Rate Wireless Personal Area Networks (LR-WPANs), IEEE Std 802.15.4- 2006.
2. Howard S. L. Error control coding in low-power wireless sensor networks: When is ECC energy-efficient? / Howard, S. L., Schlegel C., Iniewski K. // EURASIP Journal on Wireless Communications and Networking, №2. – 2006. – P.29-29.
3. Omondi A. Residue Number System: Theory and Implementation. / A.Omondi, B. Premkumar // Imperial College Press, vol. 2, 2007. – P. 296.
4. Акушский И.Я. Машинная арифметика в остаточных классах / И. Я.Акушский, Д.И. Юдицкий. – М.: Сов. радио. – 1968. – 460 с.
5. Goh Vik Tor. Multiple error detection and correction based on redundant residue number systems. /Goh, Vik Tor, and Mohammad Umar Siddiqi // Communications, IEEE Transactions, 2008. – P.325-330.
6. Tay Thian Fatt. A new algorithm for single residue digit error correction in Redundant Residue Number System / Tay Thian Fatt, Chang Chip-Hong //Circuits and Systems (ISCAS), IEEE International Symposium IEEE, 2014. – P. 1748-1751.
7. Яцків В.В. Модифіковані коректуючі коди системи залишкових класів та їх застосування / В.В. Яцків // Інформаційні технології та комп'ютерна інженерія. – 2013. – №2. – С.39-45.
8. Hu Zhengbing. Increasing the Data Transmission Robustness in WSN Using the Modified Error Correction Codes on Residue Number System / Hu Zhengbing, V. Yatskiv, A. Sachenko // *Elektronika ir Elektrotechnika.* Vol 21, No 1 (2015). Pp. 76-81.

Відомості про авторів

Яцків Василь Васильович, к.т.н., доцент, доцент кафедри спеціалізованих комп'ютерних систем Тернопільського національного економічного університету.