УДК 681.32

В. П. Семеренко
Ю. С. Халіна

НЕАЛГЕБРАЇЧНІ МЕТОДИ ДЕКОДУВАННЯ ЦИКЛІЧНИХ КОДІВ

Вінницький національний технічний університет

Анотація
Проведено порівняльний аналіз неалгебраїчних методів декодування циклічних кодів (Меггіта, мажоритарного та порогового декодування). Розглянуто математичне обгрунтування для декодування циклічних кодів на основі перестановок розрядів кодового слова. Проаналізовані вимоги до автоматного генератора перестановок.

Ключові слова: циклічні коди, перестановочне декодування, лінійна послідовнісна схема.

Abstract
Comparison analysis of non-algebraic methods for decoding of cyclic codes (Meggitt decoding, majority decoding, threshold decoding) is considered. A mathematical substantiated for decoding cyclic codes based on permutations of codeword bits is considered. The requirements to automaton generator of the permutations are analyzed.

Keywords: cyclic codes, permutation decoding, linear finite-state machine

Суть операції декодування завадостійких кодів полягає в обчисленні деякого синдрому та його аналізі. В термінах математики таким синдромом є функція $f(Z,\Theta)$, аргументами якої є кодове слово Z й структура даних Θ, що визначає спосіб представлення коду. Ця функція вибирається таким чином, щоб при відсутності помилок її значення було нульовим, а при кодовому слові Z_{err} з помилками її значення було іншим.

На практиці виявлення лише факту помилки недостатньо і необхідно мати точніший результат декодування, тобто знаходження помилкових розрядів в слові Z_{err}. В циклічних кодах існує декілька методів визначення параметрів помилки по її синдрому.

Найвідомішим методом декодування циклічних кодів, як і інших лінійних кодів, є алгебраїчний метод декодування Берлекемпа-Мессі [1]. Це багатоступеневий метод декодування, що включає розв'язання системи лінійних рівнянь та знаходження коренів полінома помилки. Складність цього методу швидко зростає зі збільшенням довжини коду та кратності помилки. Тому частіше стали використовувати неалгебраїчні методи декодування.

Особливістю циклічних кодів є відносно мала кількість синдромів, які треба зберігати для подальшого зберігання з метою точної локалізації помилки – на цьому базується метод Меггіта [2]. Ще простішим є так званий метод "виловлювання помилок": якщо довжина конфігурації помилки не перевищує довжини синдрому, тоді при деякому циклічному зсуві слова Z_{err} синдром буде дорівнювати помилці. В цьому випадку взагалі немає потреби в зберіганні додаткової інформації. Недоліками цих методів є невисока кодова швидкість.

При матричному представленні циклічних кодів (на основі перевіряльної та породжувальних матриць) використовуються мажоритарний та порогові методи декодування, які характеризуються високою продуктивністю роботи та простою апаратною реалізацією. Ці методи основані на складанні перевірочних рівнянь і знаходженні помилкових розрядів в слові Z_{err} на основі аналізу коректності зазначених рівнянь. Якщо мажоритарний метод аналізує лише двійкові значення, то пороговий метод порівнює результати перевірочних рівнянь з деяким пороговим значенням. Головним недоліком останніх методів є можливість їх застосування для обмеженого класу кодів [3].

Найбільш універсальними неалгебраїчними методами декодування є декодування на основі циклічних перестановок, які в загальному вигляді можна описати формулою [1]:

$$i \to (i+\upsilon) \bmod n, \quad GF(2), \quad \upsilon = 2, 3, 4, \ldots$$

Формування перестановок можна розглядати як результат роботи деякого генератора перестановок і представити його функціонування скінченим автоматом Λ. Початковий стан $S(0)$ автомату Λ збігається з початковим значенням кодового слова Z. На кожному такті t обчислюються нові (переставлені) позиції кодового слова Z, що еквівалентно переходу автомата Λ зі стану $S(t)$ в наступний стан $S(t+1)$. Формування чергового стану автомата Λ будемо йменувати ітерацією.

Суть запропонованого методу декодування циклічного (n,k)-коду нагадує метод "виловлювання помилок", однак, відрізняється від нього використанням операції циклічної перестановки замість операції циклічного зсуву [4]. На кожній ітерації відбувається переміщення позицій розрядів кодового слова: від середини слова до країв та навпаки. Задачею декодера є пошук такого способу переміщення, щоб помилкові розряди попали в $(n-k)$-розрядне перевірочне вікно і були виправлені.

Для ефективного декодування методом перестановок необхідно гарантувати виправлення всіх помилок в межах коректувальної здатності коду за мінімальний час та мінімальних апаратних витратах. Для досягнення цієї мети було проведено дослідження математичних властивостей автоматного генератора перестановок.

Теоретичний аналіз показав, що циклічні перестановки мають відповідати трьом вимогам:

– період перестановок має бути максимальним, тобто n;

– розмірність стану $S(t)$ має бути максимальною, тобто n;

– протягом одної ітерації всі розряди слова Z мають переміщатись по всім $(n-1)$ позиціям.

Таким вимогам буде відповідати генератор перестановок, наприклад, з такими параметрами: n – просте число, а інтервал перестановок $\upsilon = 2$.

Особливістю циклічних перестановок є наявність при деяких умовах порогу корекції. Цей ефект виникає, коли зустрічаються пари розрядів кодового слова, які тільки взаємно міняються місцями або постійно залишаються на місці. Для таких розрядів, назвемо їх маятниковими, необхідно вводити додаткові перевірки.

В роботі проведено дослідження ситуацій, при яких виникають маятникові розряди і сформульовані пропозиції по їх уникненні.

Варто зазначити, що циклічні перестановки лежать також в основі норменного методу декодування. Для представлення циклічних кодів використовується перевіряльна матриця, а сам метод декодування передбачає складні операції з великими масивами даних, що призводить до складної апаратної реалізації [5].

Значно спростити програмно-апаратну реалізацію декодування а також використати паралельну обробку даних можна при автоматному представленні циклічних кодів. Для цього використовується автоматна модель на основі спеціального типу лінійних скінчених автоматів – лінійних послідовнісних схем (ЛПС) [6].

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Кларк, Дж., мл., Кейн. Дж. Кодирование с исправлением ошибок в системах цифровой связи. М. : Радио и связь,1987. – 392 с.
2. Блейхут Р. Теория и практика кодов, контролирующих ошибки. М. : Мир, 1986. 576 с.
3. Золотарев В.В., Зубарев Ю.Б., Овечкин Г.В. Многопороговые декодеры и оптимизационная теория кодирования. М. : Горячая линия - Телеком, 2012. – 239 с.
4. Semerenko V.P. On the error-correcting capabilities of iterative error corection codes, Eastern-European Journal of Enterprise Technologies, vol. 1, issue 4 (97), pp. 31–39, 2019.
5. Конопелько В.К., Липницкий В.А. Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов. Минск, Едиториал УРСС, 2004. – 239 с. – 176 с.
6. Семеренко В. П. Теорія циклічних кодів на основі автоматних моделей : монографія. Вінниця : ВНТУ, 2015. – 444 с.

Василь Петрович Семеренко – канд. техн. наук, доцент кафедри обчислювальної техніки, Вінницький національний технічний університет, Вінниця, e-mail: vasilsemerenko@gmail.com

Юлія Сергіївна Халіна – студентка групи 2КІ-15б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця

Vasyl P. Semerenko – PhD, Associate Professor, Department of computer technique, Vinnytsia National Technical University, Vinnytsia, e-mail: vasilsemerenko@gmail.com

Yulia S. Khalina – student, Department of computer technique, Vinnytsia National Technical University, Vinnytsia. e-mail: sk8ergirl1007@gmail.com