

УДК 681.32

МОДИФІКАЦІЯ ІТЕРАТИВНИХ МЕТОДІВ ДЕКОДУВАННЯ ЗАВАДОСТІЙКИХ КОДІВ

Войналович Олександр

Вінницький національний технічний університет

Анотація

Розглянуто властивості відомих ітеративних кодів. Запропоновано модифікацію ітеративного коду Елаеса за допомогою циклічної контрольної суми CRC. Показано, що модифікований код Елаеса дозволяє виправляти велику кількість подвійних і потрійних помилок. Перевагами запропонованого коду є проста програмно-апаратна реалізація і швидке декодування.

Abstract

Properties of known iterative codes are considered. It is proposed to modify the iterative Elias code using the cyclic checksum (CRC). It is shown that the modified Elias code allows to correct a large number of double and triple errors. Advantages of suggested code are simple software-hardware implementation and fast decoding.

Вступ

Під час передавання, обробки і збереження даних в комп'ютерних і телекомунікаційних мережах можливі різноманітні спотворення і втрати даних. Для боротьби з цими завадами та захисту даних від спотворень створені спеціальні завадостійкі коди, які суттєво підвищують достовірність операцій з даними.

Практичні потреби сприяли розробці нових теоретичних моделей каналів та нових завадостійких кодів. Як відомо, К. Шеннон не дав конструктивного методу побудови найкращих завадостійких кодів, а лише сформулював критерії оптимального передавання даних у вигляді своїх теорем. Оптимальним розв'язанням зазначеної проблеми стало використання в завадостійких кодах принципу ітеративності, який дозволяє розбити складну процедуру декодування на ряд відносно простих кроків (ітерацій).

Ітеративні завадостійкі коди

Найперший ітеративний код запропонував Елаес [1]. В цьому коді $(n \times m)$ -розрядне кодове слово записується у вигляді $(n \times m)$ -матриці, в якій використовуються перевіорчні рівняння по парності по рядкам та по стовпцям. Декодування починають відразу, не чекаючи надходження всього блоку інформації. Якщо перевірка по парності кодового слова в послідовному форматі дозволяє лише виявити помилки непарної кратності, тоді як перевірки по парності в матричному форматі дозволяють вже виправити поодинокі помилки і виявити помилки подвійної та непарної кратності.

Суттєво підвищити коректувальну здатність ітеративних кодів вдалось за допомогою турбо-кодів та LDPC-кодів [2]. Особливістю цих кодів стало те, що їм вдалось максимально наблизитись до границі Шеннона, що свідчило про максимальне використання ними пропускної здатності каналу зв'язку. Однак, ця видатна характеристика була досягнута занадто дорогою ціною: великої складності кодерів та декодерів, значної затримки результатів декодування, наявності порогу декодування. Все це є наслідком того, що турбо-коди і LDPC-коди використовують ймовірнісні оцінки, що вимагає математичних обчислень з рухомою комою.

В [3] було доведено, що ітеративне декодування може базуватись і на основі традиційних кодів і жорстких рішень, що вимагає використання цілочисельної математики. Таким математичним апаратом можуть бути обчислення в полях Галуа.

Всі згадані вище ітеративні коди вимагають відносно великого інтервалу часу для отримання результатів декодування. На практиці існують багато застосувань, коли потрібно швидке декодування для виправлення помилок малої кратності. Таку задачу

можна розв'язати за допомогою модифікації коду Елаеса. Такий код відрізняється від класичного коду Елаеса заміною однією з перевірок парності на контрольну суму CRC [4]. Доцільно замінити на CRC ту перевірку, яка містить більше елементів (рис. 1).

Якщо розглядати k -розрядну послідовність I як деякий поліном $h(x)$ степені $k-1$, тоді остача від його ділення на вибраний породжувальний поліном $g(x)$ степені r по правилам двійкового поля Галуа і дасть нам необхідну r -розрядну контрольну суму. Стандартні значення CRC: 16, 32, 64 розряди.

Як відомо, CRC самостійно виявляє всі поодинокі помилки та всі інші помилки з ймовірністю $p=2^{-s}$. Як видно із таблиці 1, поєднання CRC і коду Елаеса значно підвищує коректувальну здатність нового коду, який можна назвати модифікованим кодом Елаеса.

| | |
|-------------------|---|
| 0 1 1 0 1 0 1 1 0 | c |
| 0 1 0 1 1 1 0 1 0 | c |
| 1 0 1 0 0 1 1 0 0 | c |
| 0 1 0 0 1 0 1 1 0 | c |
| 1 1 0 1 1 0 1 1 0 | |

Рисунок 1 – Приклад модифікованого коду Елайса ($m=4, n=15$)

Таблиця 1 – Коректувальна здатність кодів Елаеса

| Типи помилок | Класичний код Елаеса | Модифікований код Елаеса |
|-----------------------------|----------------------|--------------------------|
| Поодинокі помилки | виправляються | виправляються |
| Подвійні помилки в рядках | виявляються | виправляються |
| Подвійні помилки в стовпцях | виявляються | виявляються |
| Потрійні помилки в рядках | виявляються | виправляються |
| Потрійні помилки в стовпцях | виявляються | виявляються |

Висновки

Використання ітеративних методів декодування дозволяє розбити складну процедуру декодування на відносно прості кроки (ітерації). Якщо класичний код Елаеса дозволяє виправити лише поодинокі помилки, тоді як модифікований код Елаеса дозволяє виправляти 100% поодиноких, та багато додаткових помилок великої кратності при несуттєвому збільшенні апаратних витрат.

Список використаних джерел

1. Кодирование информации (двоичные коды). Н. Т. Березюк и др. Харьков: Вища школа, 1978. 252 с.
2. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. Техносфера, 2006. 320 с.
3. Semerenko V. P. Iterative hard-decision decoding of combined cyclic codes, Eastern-European Journal of Enterprise Technologies. 2018. Vol. 1, issue 9 (91). P. 61–72.
4. Семеренко В. П. Теория и практика CRC кодов: новые результаты на основе автоматных моделей / В. П. Семеренко // Восточно-Европейский журнал передовых технологий. – 2015. – Т. 4, № 9 (76). – С. 38–48.