УДК 004.415.3(043.2)

ПРОГРАМНИЙ КОМПЛЕКС ЗАВАДОСТІЙКОГО АЛГОРИТМУ РІДА–СОЛОМОНА

А. Я. Білецький, д-р техн. наук, проф.; ***О. О. Волівач***,
М. А. Якимчук, С. О. Чалайдюк

Національний авіаційний університет

email: abelanu@ukr/net

У статті розглянуто алгоритм кодування і декодування текстового файлу Ріда–Соломона. Запропоновано метод кодування-декодування є оптимальним, ефективним та раціональним алгоритмом для виправлення помилок у блоках даних. Досліджена структура процесу приймання-передавання інформації. Даний алгоритм реалізований у середовищі C++, Qt.

Ключові слова: код Ріда–Соломона, поля Галуа, кодування, декодування, алгоритм, програма, помилки, біт, файл, C++, *Qt*.

Thealgorithm ofencoding anddecodingtext fileby Reed–Solomon has been considered in the article.The proposedmethod ofencoding-decoding ofRSis optimal,effective and efficientalgorithmforcorrecting errorsindata blocks.The structureof the processof receptionand transfer ofinformation was investigated.This algorithmis implementedin the environment ofC++, Qt.

Keywords: Reed–Solomon code, Galois fields, encoding, algorithm, error, bit, file, C++, *Qt*.

Вступ

У сучасній ері цифрового зв'язку збільшення попиту на традиційні послуги стало важливим чинником у розвитку телекомунікаційних технологій. Такий розвиток подій у поєднанні з більш загальними досягненнями в галузі електроніки та обчислювальної техніки зробили можливим надання зовсім нових послуг зв'язку.

Що особливого в кодах Ріда–Соломона?

Ці коди мають більш високі можливості виправлення помилок, ніж будь-які інші [1]. «Елегантні» і складні математичні структур и дозволяють отримати точний математичний аналіз.

Постановка завдання

Коди Ріда–Соломона належать до FEC (*Forward Error Correction*) — кодів системи корекції помилок способом попередження. FEC використовується для виправлення помилок при передачі даних шляхом додавання в потоці надлишкової інформації, на основі якої може бути відновлене початкове значення даних [3].

Процедура корекції помилок передбачає два процеси: виявлення помилки і визначення її місця (ідентифікація повідомлення і позиції в повідомленні). Після вирішення цих двох завдань треба інвертувати значення помилкового біта.

Актуальною проблемою для практичної реалізації корекції помилок є технічне переозброєння кодером і декодером, підвищення ефективності процесів під час виявлення та достовірної корекції спотворених символів повідомлення.

Мета — вирішення питання щодо кодування і декодування кодів Ріда–Соломона. Згідно з метою були поставлені такі задачі:

− аналіз достовірності правильного результату при оптимальному виборі алгоритмів;

− проведення аналізу роботи кодера, декодера РС.

– ілюстрація програми кодування-декодування РС текстового файлу.

Аналіз досліджень

Існує кілька підходів до визначення кодів Ріда–Соломона. Вперше РС коди були зосереджені на оцінюванні поліномів над елементами в кінцевому полі [2; 3]. Цей підхід був узагальнений на алгебрично-геометричному визначенні за участі раціональних кривих. Інші вчені запропонували вивчати коди Ріда–Соломона у світлі полів Галуа та перетворення Фур'є. Нарешті, коди Ріда–Соломона можна розглядати як природне продовження кодів БЧХ, яке використовується в цій роботі.

Розв'язання поставлених завдань

Коди Ріда–Соломона — недвійкові циклічні коди, що дозволяють виправляти помилки в блоках даних. Діаграма, що представлена нижче, показує типове кодове слово РС (n, k) коду (рис. 1): n — розмір кодового слова; k — інформаційні символи; n-k = 2t — контрольні символи; t — максимальна кількість помилок, що може бути скоригована.

Довжина кодового слова — $n = 2^m - 1$.

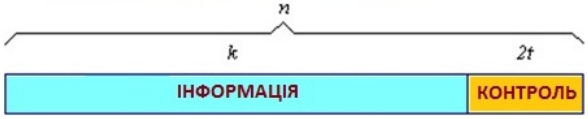

Рис. 1. Структура (n,k) коду

Сьогодні важливим є не лише швидкість, але і якість переданих даних.

Усі види інформації, такі як звук, відео-, графіка або текст зображуються у вигляді нулів та одиниць. Так само, як фотографія зазнає подряпин

або звук — шуму, цифрова інформація схильна до помилок.

Інша характеристика RS-кодування — систематичне або несистематичне застосування. При систематичному застосуванні виробляється кодове слово, яке складається з потоку незмінених первинних вхідних даних у перших n-k символах кодового слова.

У систематичному застосуванні, навпаки, потік вхідних даних змінюється в процесі кодування [2]. У більшості випадків необхідне застосування систематичного кодування.

На рис. 2. показано схему процесу приймання-передавання інформації за допомогою РС коду. Кодер РС бере блок цифрових даних і добавляє «надлишкові» біти.

Помилки з'являються під час передачі по каналах зв'язку або при зберіганні з ряду причин (наприклад, через шум і завади, подряпини на CD і т. д.).

Декодер процесів Ріда–Соломона обробляє кожний блок, намагається виправити помилки і відновити вихідні дані.

Кількість і тип помилок, які можуть бути скориговані, залежать від характеристик РС коду.

Рис. 2. Ієрархічна структура процесу приймання-передавання інформації

Виконавши огляд існуючих досліджень у кодуванні інформації та в криптографії, провівши порівняльний аналіз роботи попередників, було проведено синтез алгоритму кодування і декодування інформації РС коду, та виявлено оптимальний, ефективний та раціональний алгоритм для виправлення помилки в блоках даних.

Результати можуть бути використані при проведенні наукових досліджень, у навчальному процесі та в практичній діяльності фахівців галузей кодування та криптографії, а також при подальшому застосуванні РС коду в пристроях зберігання даних (жорсткі диски, компакт-диски, штрих-коди); бездротовому зв'язку (мобільні телефони); цифровому телебаченні; супутниковому зв'язку; широкосмугових модемах.

Реалізація в програмному середовищі C++, Qt

Максимальний об'єм текстового файлу необмежений. Програма здійснює кодування інформації над блоками розміром 256 байт, 236 з яких інформаційні, 20 — перевірні. Тобто програма має змогу відновити в одному блоці 10 пошкоджених байтів.

Інтерфейс такої програми виглядає таким чином, як на рис. 3.

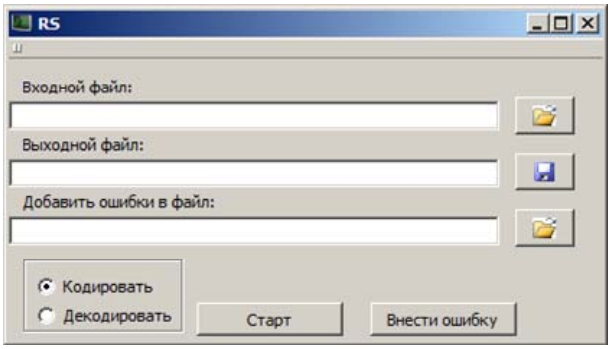

Рис. 3. Інтерфейс програми кодування-декодування текстового файлу

Переконаємось у дієздатності програми RS.Спочатку створимо деякий текстовий файл «test.txt» (рис. 4).

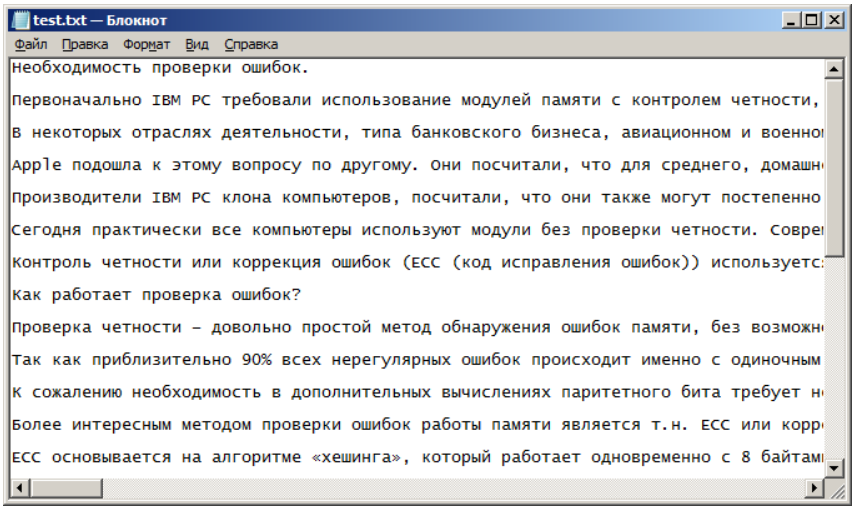

Рис. 4. Програма кодування-декодування текстового файлу

Виберемо та завантажимо вхідний файл (рис. 5), «test.txt», який буде піддаватися кодуванню далі, також визначимо вихідний файл, «testCode.txt», тобто файл в який буде збережено закодований файл:

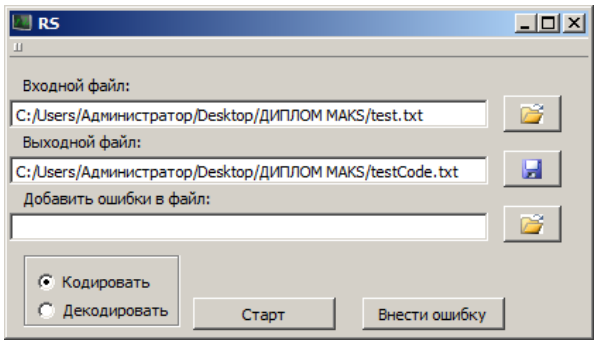

Рис. 5. Програма кодування-декодування текстового файлу

Обираємо «Кодировать» та натискаємо кнопку «Старт». Вигляд закодованого файлу (рис. 6).

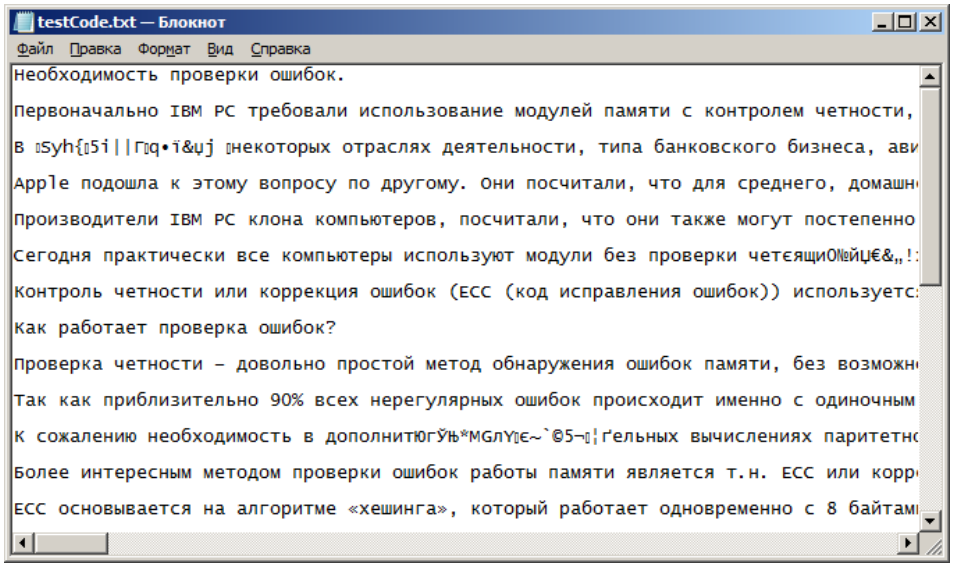

Рис. 6. Програма кодування-декодування текстового файлу

Бачимо, що в тексті з’явилися нові символи, які додались після кодування, це і є перевірні розряди (обведені червоним) (рис. 7).

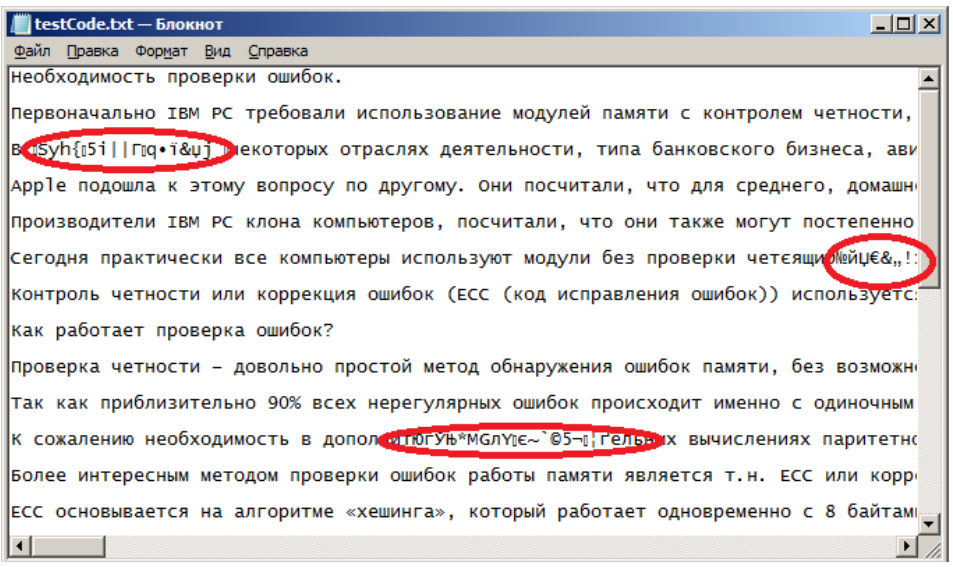

Рис. 7. Програма кодування-декодування текстового файлу

Для внесення помилки у файл потрібно завантажити в поле «Добавить ошибки файл» файл, який був попередньо закодований, тобто «testCode.txt» (рис. 8).

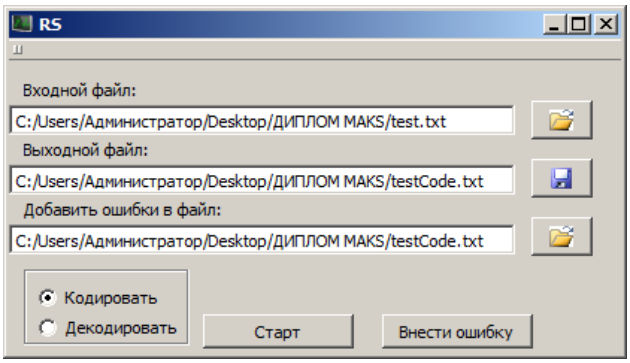

Рис. 8. Програма кодування-декодування текстового файлу

Вигляд файлу після внесення в кожен блок(256 байт) по 10 помилок (рис. 9).

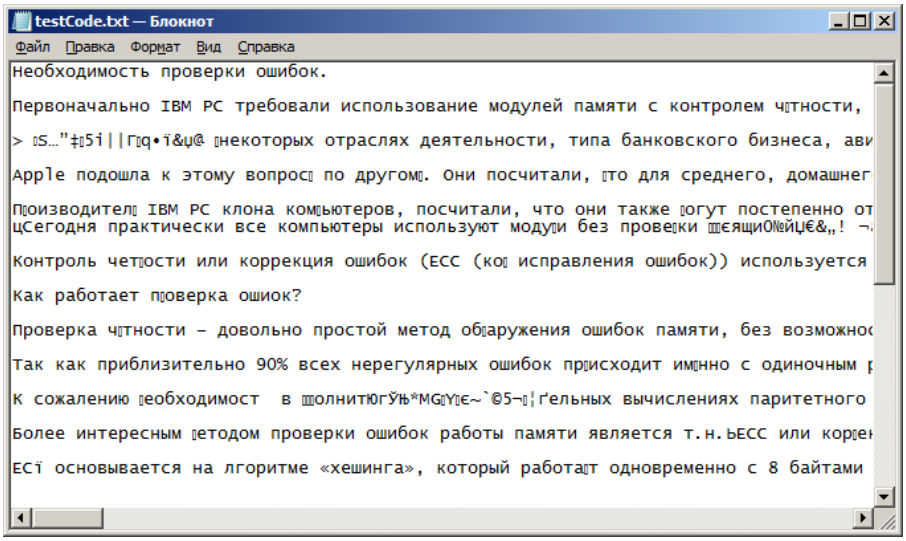

Рис. 9. Програма кодування-декодування текстового файлу

Переглянувши знову файл ми знаходимо, що він був пошкоджений і в ньому хаотично наявні помилки в тексті, які обведені (червоним кольором) (рис. 10).

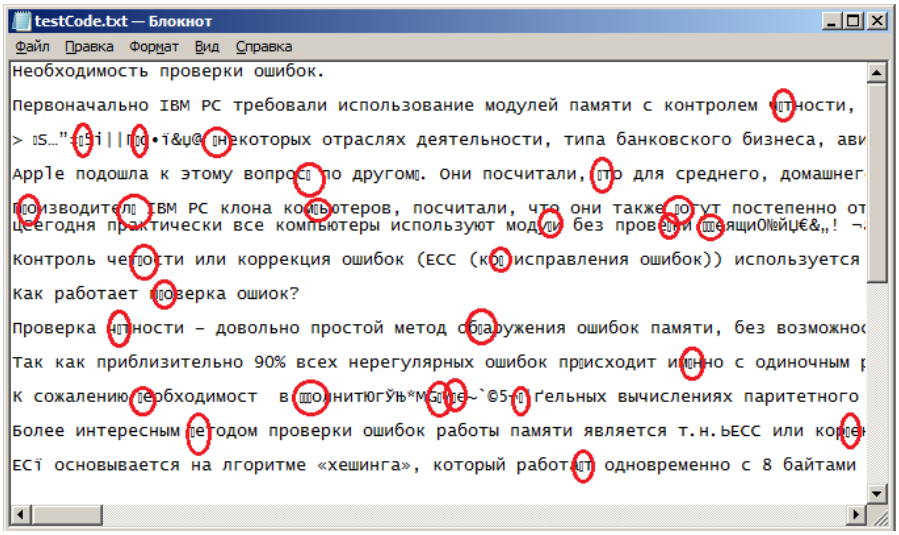

Рис. 10. Програма кодування-декодування текстового файлу

Для того, щоб декодувати файл з помилками, потрібно внести його, як вхідний файл у RS, а вихідний створити інший. Вхідний файл «testCode.txt». Вихідний файл «testdeCode.txt» (рис. 11).

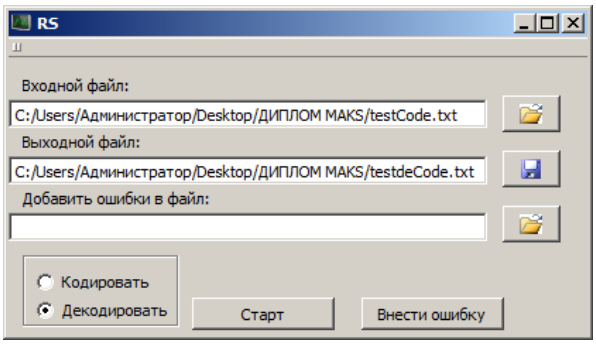

Рис. 11. Програма кодування-декодування текстового файлу

Отримавши файл «testdeCode.txt» та порівнявши його з початковим файлом «test.txt», знайдемо що вони є ідентичними.

Програма, що розроблена, здійснює кодування будь-яких цифрових даних. При цьому під час кодування здійснюється розбиття файлу на блоки, які складають один файл.

Блок складається з 256 байтів 20 з яких є надлишковими (перевірними), вони формуються на стадії кодування і вносяться в кінці кожного 236 символу файлу.

У разі пошкодження файлу та не перевищення кількості помилок у кожному блоці 10-ти інформацію можливо відновити без втрат.

Інтерфейс програми є простим, тому інструкції вгорі достатньо для того, щоб опанувати роботу в програмі.

Висновки

Коди Ріда–Соломона є недвійкові циклічні коди, що дозволяють виправляти помилки в блоках даних. Елементами кодового вектора є не біти, а групи бітів (блоки).

Установлено, що запропонований метод кодування-декодування РС є оптимальним, ефективним та раціональним алгоритмом для виправлення помилок у блоках даних. На основі регістрів зсуву з лінійними зворотними зв'язками будується кодер програми, а використовуючи алгоритми Берлекемпа-Мессі, Ченя, Форне формується декодер РС.

Матеріали даної статті можна використовувати для подальшого розвитку методів кодування-декодування РС, вирішення сучасних проблем кодування інформації, впровадження у виробництво та загальне використання.

ЛІТЕРАТУРА

1. *Золотарев В. В.* Помехоустойчивое кодирование. Методы и алгоритмы: справочник / В. В. Золотарев, Г. В. Овечкин // под ред. чл.-кор. РАН Ю. Б. Зубарева. — М. : Горячая линия–Телеком, 2004. — 126 с.

2. *Скляр Б.* Цифровая связь. Теоретические основы и практическое применение / Б. Скляр. 2-е изд., испр.; пер. с англ. — М. : Вильямс, 2003. — 1104 с.

3. *Reed, Irving S.; Solomon, Gustave* Polyno-mial CodesoverCertainFiniteFields, Journal fthe Society for Industrial and Applied Mathematics (SIAM) 8 (2): 300–304,doi:10.1137/0108018, 1960.

Стаття надійшла до редакції 02.11.2011.