

МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«Санкт-Петербургский государственный технологический институт (технический университет)»

СПбГТИ(ТУ)

|  |  |  |
| --- | --- | --- |
| УГНС | 09.00.00 | Информатика и вычислительная  техника |
| Направление подготовки | 09.03.01 | Информатика и вычислительная техника |
| Направленность (профиль) |  | Системы автоматизированного проектирования |
| Факультет |  | Информационных технологий и управления |
| Кафедра |  | Систем автоматизированного проектирования и управления |
| Учебная дисциплина |  | **ВЫЧИСЛИТЕЛЬНЫЕ СИСТЕМЫ, СЕТИ И ТЕЛЕКОММУНИКАЦИИ** |

Курс 3 Группа 494

# Отчет по лабораторной работе №3

## Тема: «Изучение алгоритмов обнаружения и исправления ошибок при передаче данных по каналам связи»

Студент А.А. Гусев

Преподаватель Р.В. Макарук

Отметка о зачете

(подпись преподавателя)

Санкт-Петербург 2021

Цель работы

Целью данной лабораторной работы является изучение алгоритмов обнаружения и исправления ошибок при передаче данных по каналам связи.

Задачи лабораторной работы

* аналитический обзор алгоритмов обнаружения и исправления ошибок при передаче данных по каналам связи;
* практическое знакомство с алгоритмами «контроль по паритету», «вертикальный и горизонтальный контроль по паритету», «циклический избыточный контроль» путём выполнения практического задания без применения вычислительной техники;
* закрепление полученных в ходе выполнения первой части лабораторной работы знаний, умений и навыков.
* практическое знакомство с алгоритмами «контроль по паритету», «вертикальный и горизонтальный контроль по паритету», «циклический избыточный контроль» путём написания программных функций, которые реализуют изучаемые алгоритмы на выбранном языке программирования;
* реализация программного обеспечения, для подсчёта контрольных сумм файлов с применением ранее написанных функций; программное обеспечение должно обеспечивать подсчёт и проверку контрольных сумм;
* закрепление полученных в ходе выполнения второй части лабораторной работы знаний, умений и навыков.

Аналитическая часть

Методы обнаружения ошибок

Контроль по паритету является наиболее простым и в то же время наименее мощным методом контроля. Он предназначен для обнаружения битовых ошибок данных. Его суть заключается в следующем. К информационным данным добавляется один контрольный бит, который дополняет количество единичных бит до четного или нечетного значения. В первом случае говорят о контроле четности данных, во втором - о контроле нечетности. Соглашение о выборе вида контроля принимается заранее.

Для обнаружения ошибки все передаваемые биты блока (как информационные, так и контрольный) суммируются по модулю 2. При наличии ошибки в передаваемом блоке (как исходных, так и контрольном) результат суммирования будет отличаться от контрольного разряда, который был принят. Это свидетельствует о наличии ошибки. Однако, если ошибок было четное количество (две, четыре и т. д.), то такое искажение останется незамеченным. Из-за этой особенности данный метод контроля применяется к небольшим блокам данных, обычно байтам. В этом случае избыточность кода составляет 1/8, что является довольно значительным, поэтому в компьютерных сетях контроль по паритету используется редко.

Вертикальный и горизонтальный контроль по паритету во многом похож на рассмотренный выше метод с тем отличием, что информационные данные представляются (располагаются) в виде матрицы. Строками этой матрицы являются отдельные байты данных. Контрольные биты данных добавляются как для каждой строки, так и для каждого столбца (рисунок 1).

Бит паритета «р» (горизонтальный контроль) добавляется к каждому передаваемому символу. Бит паритета вертикального контроля рассчитывается для каждой позиции бита в символе. Вертикальные контрольные биты собираются в отдельный контрольный символ (байт).

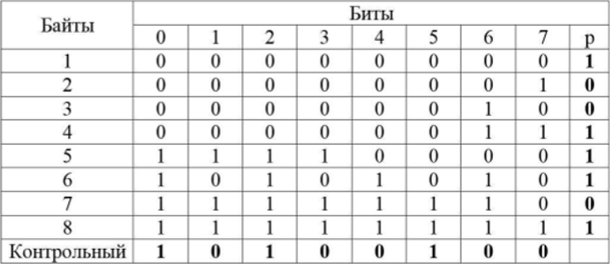


Рисунок 1 — Вертикальный и горизонтальный контроль по паритету

Данный метод позволяет обнаружить большую часть ошибок кратности 2. В то же время он обладает еще большей избыточностью, но сравнению с обычным контролем по паритету, поэтому в реальных СПД вертикальный и горизонтальный контроль по паритету почти не применяется.

Циклический избыточный контроль (Cyclic Redundancy Check, CRC) является популярным методом обнаружения ошибок в СПД и других задачах, где не требуется исправление пакетных ошибок, например, при записи данных на жесткие и оптические носители.

Суть метода CRC заключается в следующем. На передатчике формируется n-бит кодовое слово, состоящее из k информационных и r проверочных бит (поле FCS). До передачи кадра все проверочные биты имеют значение 0. Кадр целиком (все n бит, включая и обнуленные проверочные) в виде двоичного числа делится за некоторый делитель R. Остаток от деления по модулю 2 помещается в иоле FCS. На стороне приемника принятый кадр целиком делится на тот же делитель R. Если остаток от деления на приемнике равен 0, то принимается решение, что ошибок при передаче данных не произошло, иначе данные считаются искаженными.

Число бит в кадре может быть достаточно большим. Например, стандартный кадр Ethernet имеет длину 1024 байт, т. о. число будет содержать 8096 бит.

В циклических кодах передаваемые кадры имеют определенную структуру, т. е. информационные и проверочные биты всегда располагаются на определенных местах. С целью упрощения кодирования и декодирования проверочные биты обычно располагают в конце блока. Каждый блок данных кодируется и декодируется независимо от других блоков.

При практической реализации CRC значения бит представляются в виде многочленов от некоторой фиксированной переменной х. Коэффициентами многочленов являются двоичные числа, которые соответствуют передаваемым битам. Например, блок данных 10011010 представляется в виде многочлена 7-й степени с коэффициентами 1, 0, 0, 1, 1, 0, 1, 0 соответственно, т. е. х7 + х4 + х2 + х.

Операции в циклических кодах можно рассматривать как с точки зрения операций над двоичными числами, так и с точки зрения операций над полиномами. При вычислениях используют операции сложения и деления полиномов.

В циклических кодах разрешенные комбинации имеют два важных с точки зрения реализации свойства:

* Для разрешенной комбинации циклический побитовый сдвиг приводит к разрешенной комбинации. Именно этот факт и послужил основой для названия метода.
* Все разрешенные комбинации (в полиномиальном представлении) делятся без остатка на некоторый полином Р(х).

Избыточность метода считается невысокой. Например, кадр в 1024 бит может иметь контрольные данные размером в 4 бита, что составляет 0,4%.

Практическая часть

Для закрепления материала по теме лабораторной работы, необходимо посчитать вручную контрольные суммы алгоритмами «контроль по паритету» (каждая буква передаётся отдельно), «вертикальный и горизонтальный контроль по паритету» (все буквы передаются одним пакетом), «циклический избыточный контроль» (все буквы передаются одним пакетом). В качестве исходного сообщения, подлежащего передаче, использована фамилия Гусев.

Получившееся для передачи сообщение представлено в шестнадцатеричном и двоичном кодах в таблице ниже:

Таблица 1 — Создание исходного сообщения

|  |  |
| --- | --- |
| Фамилия в виде текста: | Гусев |
| Фамилия в виде шестнадцатеричного кода: | 83 E3 E1 A5 A2 |
| Фамилия в виде двоичного кода: | 10000011 11100011 11100001 10100101 10100010 |

Далее была посчитана контрольная сумма алгоритмом «контроль по паритету». Результат записан в таблицах ниже.

Таблица 2 — Контроль по паритету буквы Г

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Биты** | | | | | | | | **КС** |
| 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |

Таблица 3 — Контроль по паритету буквы У

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Биты** | | | | | | | | **КС** |
| 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 |

Таблица 4 — Контроль по паритету буквы С

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Биты** | | | | | | | | **КС** |
| 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 |

Таблица 5 — Контроль по паритету буквы Е

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Биты** | | | | | | | | **КС** |
| 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 |

Таблица 6 — Контроль по паритету буквы В

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Биты** | | | | | | | | **КС** |
| 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 |

Далее была посчитана контрольная сумма алгоритмом «вертикальный и горизонтальный контроль по паритету». Результат записан в таблице ниже.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Байты** | **Биты** | | | | | | | | |
| **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **КС** |
| **Г** | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| **У** | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 |
| **С** | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 |
| **Е** | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 |
| **В** | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 |
| **КС** | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 |  |

Далее была посчитана контрольная сумма алгоритмом «циклический избыточный контроль». Результат представлен ниже.

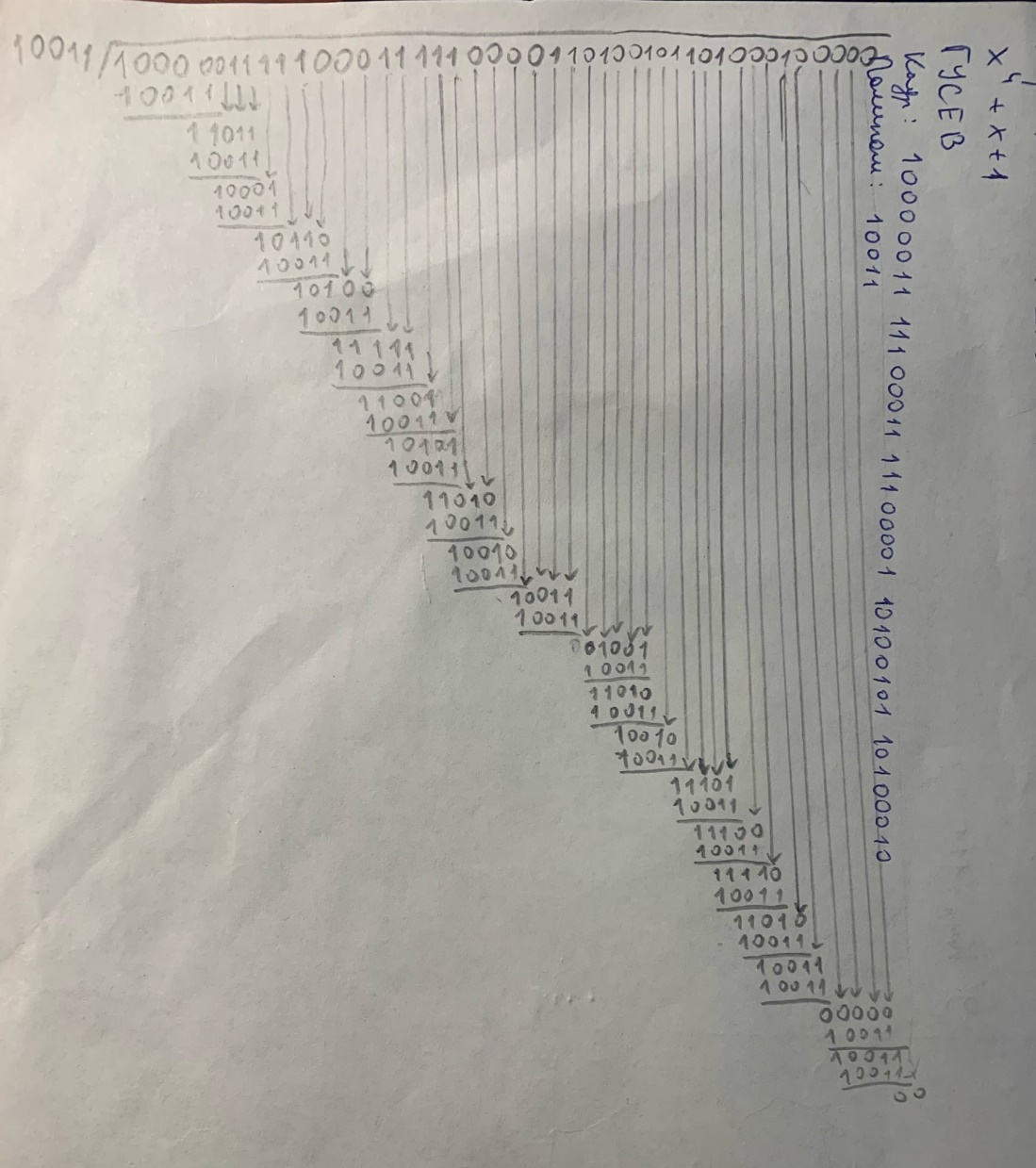


Рисунок 2 — Расчет контрольной суммы фамилии алгоритмом циклического избыточного контроля

Следующим шагом было создание программного продукта для подсчета контрольной суммы файла тремя изученными алгоритмами поиска ошибок.

В качестве алгоритма CRC выбран CRC-32Q с полиномом 814141ABh, начальное состояние регистра равно нулю, инверсия входных и выходных данных не производится, результат складывается по модулю 2 с нулем, т.е. не изменяется. Тестовый вектор выбран из таблицы спецификаций алгоритмов CRC для проверки корректности работы алгоритма, файл содержит строку 123456789. На рисунке ниже представлен пример работы программы.

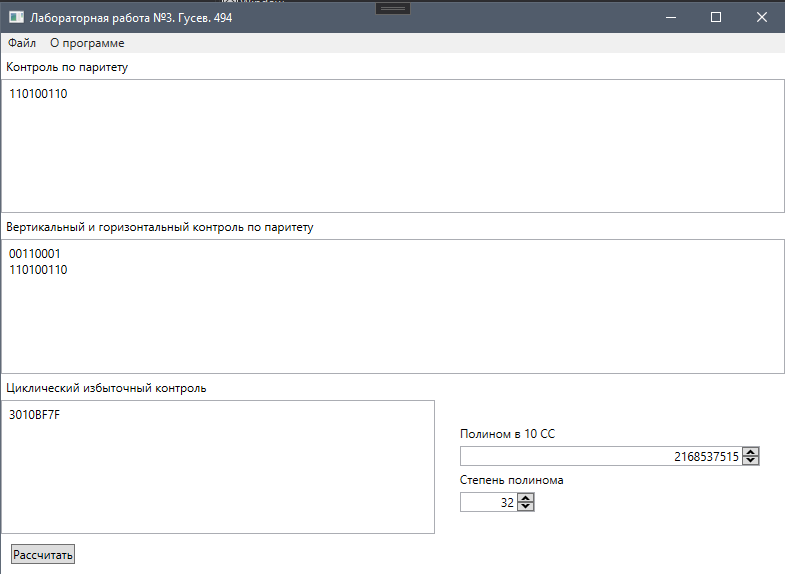


Рисунок 3 — Пример работы приложения

Пользователь может указать другой полином, а также степень полинома в диапазоне от 8 до 64 с шагом в 8. Для того же файла, но с другим полиномом и степенью программа также выдает корректный результат в соответствии с таблицей спецификаций алгоритмов CRC (рисунок 4).

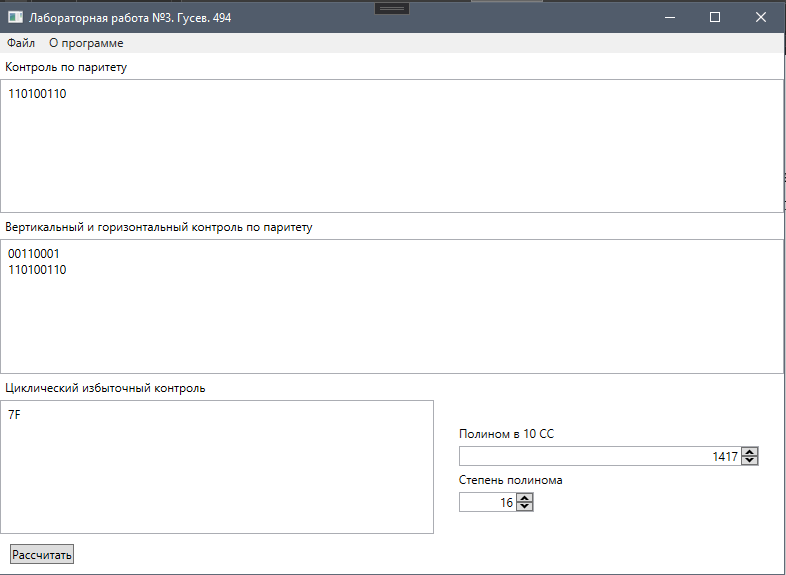


Рисунок 4 — Пример работы приложения

Выводы

В процессе выполнения лабораторной работы были изучены различные алгоритмы подсчета контрольных сумм. На примерах были изучены алгоритмы: контроль по паритету, вертикальный и горизонтальный контроль по паритету, циклический избыточный контроль. Была написана программа для нахождения контрольных сумм файла.