**Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»**

**Факультет Программной Инженерии и Компьютерной техники**

**Лабораторная работа №2**

**Синтез помехоустойчивого кода**

**Вариант 78**

**Выполнила:**

**Фонарева Виктория Сергеевна**

**Группа P3110**

**Проверил:**

**Рыбаков Степан Дмитриевич**

Оглавление

[Task 3](#_Toc183432968)

[Task I 3](#_Toc183432969)

[Task II 4](#_Toc183432970)

[Task III 5](#_Toc183432971)

[Task IV 6](#_Toc183432972)

[Task V 7](#_Toc183432973)

[Task VI 7](#_Toc183432974)

[Ответы 8](#_Toc183432975)

[Заключение 8](#_Toc183432976)

[Список использованных источников 8](#_Toc183432977)

# Task

1. Построить схему декодирования классического кода Хэмминга (7;4), которую представить в отчёте в виде изображения.
2. На основании номера варианта задания выбрать набор из 4 полученных сообщений в виде последовательности 7-символьного кода. Показать, исходя из выбранных вариантов сообщений (по 4 у каждого – часть №1 в варианте), имеются ли в принятом сообщении ошибки, и если имеются, то какие. Подробно прокомментировать и записать правильное сообщение.
3. Построить схему декодирования классического кода Хэмминга (15;11), которую представить в отчёте в виде изображения.
4. На основании номера варианта задания выбрать 1 полученное сообщение в виде последовательности 11-символьного кода. Показать, исходя из выбранного варианта сообщений (по 1 у каждого – часть №2 в варианте), имеются ли в принятом сообщении ошибки, и если имеются, то какие. Подробно прокомментировать и записать правильное сообщение.
5. Сложить номера всех 5 вариантов заданий. Умножить полученное число на 4. Принять данное число как число информационных разрядов в передаваемом сообщении. Вычислить для данного числа минимальное число проверочных разрядов и коэффициент избыточности.
6. Написать программу на любом языке программирования, которая на вход получает набор из 7 цифр «0» и «1», записанных подряд, анализирует это сообщение на основе классического кода Хэмминга (7,4), а затем выдает правильное сообщение (только информационные биты) и указывает бит с ошибкой при его наличии.

# Task I

Схема декодирования классического кода Хэмминга (7;4) представлена на рисунке 1.

Изображение выглядит как текст, диаграмма, линия, План

Автоматически созданное описание

Рисунок 1 – «Схема декодирования кода Хэмминга (7;4)»

# Task II

Построим таблицу кода Хэмминга (7;4) для каждого из 4 сообщений.

Сообщение 1

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 |  |
| Сообщение | 0 | 0 | 0 | 0 | 1 | 1 | 0 |  |
| 2x | *r1* | *r2* | *i1* | *r3* | *i2* | *i3* | *i4* | *s* |
| 1 |  |  |  |  |  |  |  | s1 |
| 2 |  |  |  |  |  |  |  | s2 |
| 4 |  |  |  |  |  |  |  | s3 |

Таблица 1 – «Схема декодирования кода Хэмминга (7;4)»

Проверим синдромы *s1, s2* и *s3:*

*s1 =* r1^i1^i2^i4 = 0^0^1^0 = 1

*s2 =* r2^i1^i3^i4 = 0^0^1^0 = 1

*s3 =* r3^i2^i3^i4 = 0^1^1^0 = 0

Имеем синдром (1;1;0)

Посмотрим, за какой бит отвечает только s1 и s2: за i1. Следовательно, ошибка в бите i1.

Исправленное сообщение: 0010110

Сообщение 2

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 |  |
| Сообщение | 1 | 1 | 1 | 0 | 1 | 1 | 0 |  |
| 2x | *r1* | *r2* | *i1* | *r3* | *i2* | *i3* | *i4* | *s* |
| 1 |  |  |  |  |  |  |  | s1 |
| 2 |  |  |  |  |  |  |  | s2 |
| 4 |  |  |  |  |  |  |  | s3 |

Таблица 2 – «Схема декодирования кода Хэмминга (7;4)»

Проверим синдромы *s1, s2* и *s3:*

*s1 =* r1^i1^i2^i4 = 1^1^1^0 = 1

*s2 =* r2^i1^i3^i4 = 1^1^1^0 = 1

*s3 =* r3^i2^i3^i4 = 0^1^1^0 = 0

Имеем синдром (1;1;0)

Посмотрим, за какой бит отвечает только s1 и s2: за i1. Следовательно, ошибка в бите i1.

Исправленное сообщение: 1100110

Сообщение 3

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 |  |
| Сообщение | 1 | 0 | 0 | 0 | 0 | 0 | 1 |  |
| 2x | *r1* | *r2* | *i1* | *r3* | *i2* | *i3* | *i4* | *s* |
| 1 |  |  |  |  |  |  |  | s1 |
| 2 |  |  |  |  |  |  |  | s2 |
| 4 |  |  |  |  |  |  |  | s3 |

Таблица 3 – «Схема декодирования кода Хэмминга (7;4)»

Проверим синдромы *s1, s2* и *s3:*

*s1 =* r1^i1^i2^i4 = 1^0^0^1 = 0

*s2 =* r2^i1^i3^i4 = 0^0^0^1 = 1

*s3 =* r3^i2^i3^i4 = 0^0^0^1 = 1

Имеем синдром (0;1;1)

Посмотрим, за какой бит отвечает только s2 и s3: за i3. Следовательно, ошибка в бите i3.

Исправленное сообщение: 1000011

Сообщение 4

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 |  |
| Сообщение | 1 | 0 | 1 | 0 | 0 | 0 | 0 |  |
| 2x | *r1* | *r2* | *i1* | *r3* | *i2* | *i3* | *i4* | *s* |
| 1 |  |  |  |  |  |  |  | s1 |
| 2 |  |  |  |  |  |  |  | s2 |
| 4 |  |  |  |  |  |  |  | s3 |

Таблица 4 – «Схема декодирования кода Хэмминга (7;4)»

Проверим синдромы *s1, s2* и *s3:*

*s1 =* r1^i1^i2^i4 = 1^1^0^0 = 0

*s2 =* r2^i1^i3^i4 = 0^1^0^0 = 1

*s3 =* r3^i2^i3^i4 = 0^0^0^0 = 0

Имеем синдром (0;1;0)

Посмотрим, за какой бит отвечает только s2: за r2. Следовательно, ошибка в бите r2.

Исправленное сообщение: 1110000

# Task III

Схема декодирования кода Хэмминга (15;11) представлена на рисунке 2.

Изображение выглядит как текст, диаграмма, линия, Параллельный

Автоматически созданное описание

Рисунок 2 – «Схема декодирования кода Хэмминга (15;11)»

# Task IV

Было получено сообщение: 010101011110010. Построим таблицу кода Хэмминга (15;11).

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |  |
| Сообщение | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 |  |
| 2x | *r1* | *r2* | *i1* | *r3* | *i2* | *i3* | *i4* | *r4* | *i5* | *i6* | *i7* | *i8* | *i9* | *i10* | *i11* | s |
| 1 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | s1 |
| 2 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | s2 |
| 4 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | s3 |
| 8 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | s4 |

Таблица 6 – «Схема декодирования кода Хэмминга (15;11)»

Проверим синдромы *s1, s2, s3* и *s4:*

*s1 =* r1^i1^i2^i4^i5^i7^i9^i11 = 0^1^1^0^1^1^1^0 = 1

*s2 =* r2^i1^i3^i4^i6^i7^i10^i11 = 0^1^0^0^0^1^0^0 = 0

*s3 =* r3^i2^i3^i4^i8^i9^i10^i11 = 1^1^0^0^0^1^0^0 = 1

*s4 =* r4^i5^i6^i7^i8^i9^i10^i11 = 1^1^0^1^0^1^0^0 = 0

Имеем синдром (1;0;1;0)

Посмотрим, за какой бит отвечает только s1 и s3: за i2. Следовательно, ошибка в бите i2.

Исправленное сообщение: 001100011010100

# Task V

Вычислим рассматриваемое число: c = 4\*(32+64+96+16+47) = 1020.

Число разрядов в передаваемом сообщении 1020. Найдем минимальное число проверочных разрядов.

Воспользуемся формулой

2*r* ≥ *r + i* + 1, где *r* – количество проверочных разрядов, а *i* – количество информационных разрядов.

2*r* ≥ *r +* 1020 + 1

2*r* ≥ *r +* 1021

Подставим 10

210 ≥ 10 *+* 1021

1024 ≥ 1031

Неверно

Подставим 11

211 ≥ 11 *+* 1021

2048 ≥ 1032

Верно. Минимальное количество проверочных разрядов для сообщения с 1020ю информационными разрядами = 11

Найдем коэффицент избыточности:

k = = = = 0.01066925315

Ответ: 11; 0.01066925315

# Task VI

Код решения представлен в Листинге 1

Листинг 1 – Решение дополнительного задания

|  |
| --- |
| **def** f**(**s**):**  s1 **=** s**[**0**]^**s**[**2**]^**s**[**4**]^**s**[**6**]**  s2 **=** s**[**1**]^**s**[**2**]^**s**[**5**]^**s**[**6**]**  s3 **=** s**[**3**]^**s**[**4**]^**s**[**5**]^**s**[**6**]**  s **=** **str(**s3**)+str(**s2**)+str(**s1**)**  bit\_number **=** **int(**s**,**2**)**  **return** bit\_number  s **=** **[int(**x**)** **for** x **in** **input()]**  **bit\_dict** **=** **{**1**:** 'r1'**,** 2**:** 'r2'**,** 3**:** 'i1'**,** 4**:** 'r3'**,** 5**:** 'i2'**,** 6**:** 'i3'**,** 7**:** 'i4'**}**  b **=** f**(**s**)**  **if(**b **==** 0**):**  **print(**'correct'**)**  **else:**  **print(bit\_dict[**b**])** |

# Ответы

Задание 1 – i1

Задание 2 – i1

Задание 3 – i3

Задание 4 – r2

Задание 5 – i2

# Ответы

Задание 1 – i1

Задание 2 – i1

Задание 3 – i3

Задание 4 – r2

Задание 5 – i2

# Ответы

Задание 1 – i1

Задание 2 – i1

Задание 3 – i3

Задание 4 – r2

Задание 5 – i2

# Ответы

Задание 1 – i1

Задание 2 – i1

Задание 3 – i3

Задание 4 – r2

Задание 5 – i2

# Ответы

Задание 1 – i1

Задание 2 – i1

Задание 3 – i3

Задание 4 – r2

Задание 5 – i2

# Ответы

Задание 1 – i1

Задание 2 – i1

Задание 3 – i3

Задание 4 – r2

Задание 5 – i2

# Ответы

Задание 1 – i1

Задание 2 – i1

Задание 3 – i3

Задание 4 – r2

Задание 5 – i2

# Заключение

В ходе лабораторной работы я получила знания о коде Хэмминга и научилась его применять.

# Список использованных источников

1. Самокорректирующиеся коды и их применения в криптографии / Ю. В. Таранников. — М.: Ленанд, 2023. — 256 с. — (Классический учебник МГУ, Основы защиты информации).
2. Заметки по теории кодирования / А. Е. Ромащенко, А. Ю. Румянцев, А. Шень. — 2-е изд., испр. и доп. — М.: МЦНМО, 2017. — 88 с.