#

# **Коди БЧХ. Алгоритми кодування та декодування**

**1 КОДИ БОУЗА-ЧОУДХУРИ-ХОКВИНГЕМА**

Коди Боуза-Чоудхури-Хоквингема (БЧХ) являють собою великий клас кодів, здатних виправляти кілька помилок і займають помітне місце в теорії і практиці кодування. Інтерес до кодів БЧХ визначається щонайменше наступними чотирма обставинами:

1) серед кодів БЧХ при невеликих довжинах існують гарні (але, як правило, не кращі з відомих) коди;

2) відомі відносно прості й конструктивні методи їх кодування і декодування (хоча якщо єдиним критерієм є простота, то перевага варто віддати іншим кодам);

3) коди Ріда-Соломона, що є широко відомим підкласом недвійкових кодів, мають певні оптимальні властивості і прозору вагову структуру;

4) повне розуміння кодів БЧХ, як видно, є найкращою відправною крапкою для вивчення багатьох інших класів кодів.

**2 ВИЗНАЧЕННЯ КОДІВ БЧХ**

Одним із класів циклічних кодів, здатних виправляти багатократні помилки, є коди БЧХ.

Примітивним кодом БЧХ, що виправляє tu помилок, називається код довжиною n=qm-1 над GF(q), для якого елементи є коріннями породжую чого багаточлена. Тут примітивний елемент GF(qm). Породжуючий багаточлен визначається з виразу де f1(x),f2(x)...- мінімальні багаточлени корінь g(x). Число перевірочних елементів коду БЧХ задовольняє співвідношенню

Приклад. Визначити значення породжую чого багаточлена для побудови примітивного коду над GF(2) довжини 31, що виправляє двократні помилки (tu=2). Виходячи з визначення коду БЧХ коріннями багаточлена g(x) є: , де примітивний елемент GF(qm)=GF(25). Породжуючий багаточлен визначається з виразу де f1(x) , f2(x) , f3(x) , f4(x) - мінімальні багаточлени корінь відповідно . Примітка. Мінімальний багаточлен елемента  поля GF(qm) визначається з виразу , де - найменше ціле число, при якому . Значення мінімальних багаточленів будуть наступними:

Тому що f1(x)=f2(x)=f4(x), то

На практиці при визначенні значень породжую чого багаточлена користуються спеціальною таблицею мінімальних багаточленів, і виразом для породжую чого багаточлена . При цьому робота здійснюється в наступній послідовності.

По заданій довжині коду n і кратності помилок tu, що виправляють, визначають:

- з виразу n=2m-1 значення параметра m, що є максимальним ступенем співмножників g(x);

- з виразу j=2tu-1 максимальний порядок мінімального багаточлена, що входить у число співмножників g(x);

* користуючись таблицею мінімальних багаточленів, визначається вираз для g(x) залежно від m і j. Для цього з колонки, що відповідає параметру m, вибираються багаточлени з порядками від 1 до j, які в результаті перемножування дають значення g(x). Примітка. У виразі для g(x) утримуються мінімальні багаточлени тільки для непарних ступенів , тому що звичайно відповідні їм мінімальні багаточлени парних ступенів  мають аналогічні вирази. Наприклад, мінімальні багаточлени елементів відповідають мінімальному багаточлену елемента 1, мінімальні багаточлени елементів відповідають мінімальному багаточлену і т.і.

Приклад. Визначити значення породжуючого багаточлена для побудови примітивного коду над GF(2) довжини 31, що забезпечує tu=3. Визначаємо значення m і j.

Із таблиці мінімальних багаточленів відповідно до m=5 і j=5 одержуємо

Задані вихідні дані: n і tu або k і tu для побудови циклічного коду часто приводять до вибору завищеного значення m і, як наслідок цього, до невиправданого збільшення довжини коду. Таке положення знижує ефективність отриманого коду, тому що частина інформаційних розрядів взагалі не використовується.

Приклад. Побудуємо породжуючий багаточлени для кодів БЧХ у полі GF(16), побудованому як розширення поля GF(2). Коди повинні виправляти помилки кратності 2-7.

У табл. 1 задане подання поля GF(16), як розширення поля GF(2), побудоване по примітивному багаточлену . В неї включені також мінімальні багаточлени GF(2) для всіх елементів з поля GF(16), де — примітивний елемент GF(16). Помітно, що мінімальні багаточлени для будь-якого парного ступеня завжди вже існують в одному з попередніх рядків таблиці. Породжуючий багаточлен для коду БЧХ довжини 15, що виправляє дві помилки:

Оскільки ступінь g(х) дорівнює 8, п — k = 8. Звідси k = 7 і ми одержали породжуючий багаточлен (15, 7)-коду БЧХ, що виправляє 2 помилки. Відзначимо, що коди БЧХ будуються по заданим п и t. Значення k не відомо, поки не знайдений g (х).

**Таблиця 1 – Подання поля GF(24)**

Тим же способом ми можемо побудувати багаточлен, що породжує, для іншого примітивного коду БЧХ довжини 15

Нехай t = 3:

Вийшов породжуючий багаточлен для (15, 5)-коду БЧХ, що виправляє три помилки. Нехай t = 4:

.

Вийшов породжуючий багаточлен для (15,1)-коду БЧХ. Це простий код з повторенням, що виправляє сім помилок.

Нехай t = 5, 6, 7. Кожний із цих випадків приводить до такого ж породжуючого багаточлена, як і при t = 4. При t > 7 код БЧХ не визначений, оскільки ненульових елементів поля GF(16) усього 15.

В табл. 6.2 наведене подання поля GF(16), як розширення поля GF(4), побудоване по примітивному багаточлену . Ця таблиця містить також мінімальні багаточлени над GF(4) для всіх елементів з поля GF(16), де = z — примітивний елемент.

Приклад. Знайдемо породжуючи багаточлени для кодів БЧХ, що виправляють від 1-й до 6 помилок у кодовій комбінації. Код повинен бути побудований у поле GF(16) отриманому як розширення поля GF(4). Породжуючий багаточлен для коду БЧХ над GF(4) довжини 15, що виправляє одиночні помилки:

Цим кодом послідовність 11 чотверичних символів (що еквівалентно 22 бітам)

**Таблиця 2 Подання поля GF (42)**

|  |
| --- |
| GF(4) |
| + | 0 1 2 3 | \* | 0 1 2 3 |
| 0123 | 0 1 2 31 0 3 22 3 0 13 2 1 0 | 0123 | 0 0 0 00 1 2 30 2 3 10 3 1 2 |

кодується в послідовність 15 чотверичних символів. Такий код не є кодом Хемінга.

У такий же спосіб ми можемо знайти породжуючий багаточлени для інших кодів над GF(4) довжини 15.

Нехай t = 2:

Вийшов породжуючий багаточлен для (15, 9)-коду БЧХ над GF(4), що виправляє дві помилки.

Нехай t = 3:

Це дає (15, 6) -код БЧХ над GF(4), що виправляє три помилки.

Нехай t = 4:

Це дає (15, 4) -код БЧХ над GF(4), що виправляє чотири помилки.

Нехай t == 5:

Це дає (15, 3) -код БЧХ над GF (4), що виправляє п'ять помилок.

Нехай t = 6:

Виходить (15, 1) -код БЧХ над GF(4), що виправляє шість помилок. Це простий код з повторенням, що у дійсності виправляє сім помилок.

Тому, що коди БЧХ є циклічними кодами, то при кодуванні використовуються загальні правила кодування інформації циклічними кодами.

# **3 Коди БЧХ. Алгоритми декодування**

Коди БЧХ є циклічними, і, отже, до них застосовні будь-які методи декодування циклічних кодів. Є, однак, істотно кращі алгоритми, розроблені спеціально для декодування кодів БЧХ. Алгоритм, що розглядається, вперше був запропонований Питерсоном для двійкових кодів. Для спрощення рівнянь усюди покладається =1 хоча всі викладення без зміни ідеї можуть бути пророблені для довільного .

Припустимо, що в основі конструкції коду БЧХ лежить елемент поля, можливо не примітивний. Багаточлен помилок дорівнює

,

де не більше t коефіцієнтів відрізняються від нуля. Припустимо, що насправді відбулося v помилок, , і що цим помилкам відповідають невідомі позиції Багаточлен помилок можна записати у вигляді

де — величина l-ї помилки (у двійковому випадку ). Ми не знаємо ні , ні ; у дійсності ми навіть не знаємо числа v. Для виправлення помилок потрібно обчислити всі ці числа. Щоб одержати компонент синдрому S1, треба знайти значення отриманого багаточлена в точці а:

Прийняті тут позначення занадто громіздкі. Для їх спрощення визначимо для всіх , v величини помилок і локатори помилок , де l - дійсне положення l-ї помилки, а - елемент поля, асоційований із цим положенням. Тому що порядок елемента а дорівнює п, то всі локатори розглянутої конфігурації помилок різні.

У цих позначеннях запишеться у вигляді

.

Аналогічно можна обчислити значення прийнятого багаточлена при всіх ступенях , що входять у визначення g(х). Для визначимо синдроми формулами

Тоді одержимо наступну систему з 21 рівнянь відносно v невідомих локаторів і v невідомих величин помилок :

У силу визначення синдрому ця система рівнянь повинна мати хоча б одне рішення. Це рішення єдине. Наше завдання полягає в обчисленні невідомих по заданих компонентах синдрому, тобто в рішенні системи нелінійних рівнянь. Описуваний метод рішення таких систем підходить для довільного поля.

Цю систему нелінійних рівнянь важко вирішувати безпосередньо. Скористаємося штучним прийомом, визначивши деякі проміжні змінні, які можуть бути обчислені по компонентах синдрому і по яких можна обчислити потім локатори помилок.

Розглянемо багаточлен від х:

відомий за назвою багаточлена локаторів помилок і обумовлений як багаточлен, коріннями якого є зворотні до локаторів помилок величини для . Отже,

Якщо коефіцієнти цього багаточлена відомі, то для обчислення локаторів помилок потрібно знайти його корінь. Тому спробуємо спочатку обчислити по заданих компонентах синдрому коефіцієнти .

Помножимо обидві частини рівності, що визначає цей багаточлен, на і покладемо . Тоді ліва частина звернеться в нуль, і ми одержимо

або

.

Ця рівність виконується при кожному l і при кожному j. Підсумуємо ці рівності по l від 1 до v. Для кожного j це дає

Або

Кожна сума в лівій частині останньої рівності є компонентом синдрому, так що рівняння приводиться до виду

Тому що , то для j в інтервалі всі індекси задають відомі компоненти синдрому. Таким чином, одержуємо систему рівнянь

,

тобто систему лінійних рівнянь, що зв'язує компоненти синдрому з коефіцієнтами багаточлена (х). Якщо матриця невироджена, то цю систему можна вирішити шляхом Рисунок 1 - Декодер Питерсона-Горенстейна-Цирлера.

Оскільки число елементів поля обмежено, звичайно найпростішим шляхом знаходження корінь багаточлена є метод проб і помилок, відомий як процедура Ченя. Ця процедура складається просто в послідовному обчисленні для кожного j і перевірки отриманих значень на нуль. Найбільш простим способом обчислення значення в точці є схема Горнера:

.

Для обчислення за схемою Горнера потрібно тільки v множень і v додавань.

Як приклад процедури декодування, розглянемо декодування (15,5)-коду БЧХ, що виправляє три помилки і має породжуючий багаточлен g(х) = х10 + х9 + х6 + х4 + х2 + х + 1.

Алгоритм декодування представлений на рис. 1.

Для приклада будемо вважати прийнятий багаточлен рівним v(х) = x7 + x2. Ясно, що якби відбулося не більше трьох помилок, то кодове слово повинно було б бути нульовим і v(х) = е(х), але декодер не може зробити такого висновку. Виконаємо всі кроки алгоритму декодування. Спочатку обчислимо компоненти синдрому, використовуючи арифметику в полі GF(16):

Нехай v = 3, тоді

Визначник М дорівнює нулю; отже, припускаємо v = 2. Тоді

Визначник не дорівнює нулю; отже, відбулося дві помилки. Далі,

та

отже,

Використовуючи процедуру Ченя, одержуємо розкладання

Багаточлен локаторів помилок має корні й , а локатори помилок дорівнюють елементам, зворотним корінням. Таким чином, помилки відбулися в другій і сьомій позиціях. Оскільки код є двійковим, значення помилок рівні 1 і .

