Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

МЕТОДИЧНІ ВКАЗІВКИ
до практичних занять з дисципліни
«ТЕОРІЯ ІНФОРМАЦІЇ ТА КОДУВАННЯ»
для студентів денної форми навчання
спеціалізації «Системи, технології та комп'ютерні засоби створення мультимедіа»

ЗАТВЕРДЖЕНО
кафедрою…МІРЕС
Протокол №5
від “5” 12.2017

Харків 2017

Методичні вказівки до практичних занять з дисципліни “Теорія інформації та кодування” для студентів денної форми навчання спеціалізації «Системи, технології та комп’ютерні засоби створення мультимедіа»/ Упоряд. Зубков О.В. – Харків: ХНУРЕ, 2017. – 29 с.

Упорядник: О.В. Зубков

Рецензенти: І.В. Савченко, к.т.н., доц. каф. МІРЕС ХНУРЕ

ЗМІСТ

ВСТУП

Дисципліна “Теорія інформації та кодування” входить до циклу професійно-орієнтованих дисциплін спеціальності «Апаратура радіозв’язку, радіомовлення та телебачення» при підготовці магістрів та спеціалістів. Успішне засвоєння цієї дисципліни забезпечує майбутньому фахівцю можливість розуміти методи стиснення інформації, завадостійкого кодування та шифрування в сучасних системах зв’язку.

Мета методичних вказівок – допомогти студентам підготуватися до практичних занять з різних розділів дисципліни, засвоїти основні алгоритми стиснення інформації, завадостійкого кодування та декодування, а також сучасний математичний апарат обробки інформації, що є складовою частиною вивчаємих алгоритмів.

Кількість розділів в методичних вказівках обумовлена кількістю практичних занять згідно з діючим навчальним планом.

У кожному розділі наведено основні розрахункові співвідношення, методичні вказівки та приклади розв’язання основних типів задач. Подано також достатню кількість задач для самостійного розв’язання.

Практичне заняття №1. Коди Хафмана та арифметичний.

При підготовці до практичного заняття слід вивчити [2, с.879-887]. Усю інформацію можна поділити на декілька основних груп: відео- та фото, звукова інформація, текстова чи двійкові файли. Стиснення фото, відео чи звуку базується на особливостях людського зору та слуху, тобто на нечутливості цих органів сприйняття інформації до незначних втрат у зображенні та сприйнятті слабких частотних складових звуку на фоні потужних. Для цих видів інформації використовують у більшості випадків стиснення з втратами, коли частина інформації безповоротно втрачається. Але для стиснення текстової інформації чи, наприклад, *.exe файлів втрати недопустимі. Розглянемо у цьому практичному занятті деякі сучасні методи стиснення без втрат, такі як: метод Хаффмана та арифметичне стиснення. Стиснення інформації за цими методами можливо, коли різні символи у деякому об'ємі інформації з'являються частіше за інших. Тобто коли символи мають різні імовірності появи. Знайти ці імовірності можна підрахував кількість появ кожного з символів у файлі. Для текстових файлів різних мов також існують таблиці середньостатистичної появи символів алфавіту. На практичному занятті будемо вважати, що аналіз ймовірностей появи символів вже виконано. Розглянемо безпосередньо стиснення інформації за методом Хаффмана і арифметичне стиснення. Суть метода Хаффмана полягає у кодуванні символів, що з'являються часто – короткими кодовими комбінаціями, а символи що з'являються рідкіше кодують більш довгими комбінаціями.

Стиснення за методом Хаффмана виконується за наступним алгоритмом:

1) записуємо усі символи та ймовірності їх появи p_i у стовбець у порядку зменшення ймовірностей;

2) об'єднуємо (складаємо) дві найменші ймовірності у стовбці та записуємо праворуч новий стовбець ймовірностей у порядку зменшення їх значень. У цей стовбець увійде результат об'єднання та усі інші ще не об'єднанні ймовірності;

3) повторюємо другий шаг алгоритму, доки процес об'єднання не закінчиться і ми отримаємо повну ймовірність, що дорівнює 1;

4) на попередніх кроках ми отримали таблицю об'єднання ймовірностей. Тепер, використовуючи її, починаємо побудову дерева ймовірностей. Починаємо рух від повної ймовірності в зворотному напрямку. При кожному розпаданні ймовірності маємо дві гілки дерева. Гілку з більшою

ймовірність позначаємо умовною логічною «1», а гілку з меншою ймовірністю – умовним логічним «0». Побудова дерева продовжується доки не отримаємо гілки с усіма початковими ймовірностями;

5) рухаючись від повної ймовірності до ймовірностей кожного з символів записуємо відповідні символам кодові комбінації. Для оцінювання ефективності стиснення розрахуємо середню довжину кодової комбінації $\overline{n}$ за формулою

$$\overline{n} = \sum_{i=0}^{m} p_i \cdot n_i, \tag{1.1}$$

де m – загальна кількість символів джерела інформації;

n_i – довжини отриманих кодових комбінацій.

Приклад 1. Нехай джерело інформації генерує 5 символів Z1…Z5 з наступними ймовірностями появи p(Z1)=0.17, p(Z2)=0.25, p(Z3)=0.35, p(Z4)=0.08, p(Z5)=0.15. Закодувати методом Хаффмана символи, розрахувати середню довжину кодової комбінації.

Таблиця 1.1 – Кодування за методом Хаффмана

Z_i	P_i	Кроки об'єднання			
		1	2	3	4
Z_3	0.35	0.35	0.40	0.60	1.00
Z_2	0.25	0.25	0.35	0.40	
Z_1	0.17	0.23	0.25		
Z_5	0.15	0.17			
Z_4	0.08				

Використовуючи таблицю 1.1 побудуємо дерево ймовірностей.

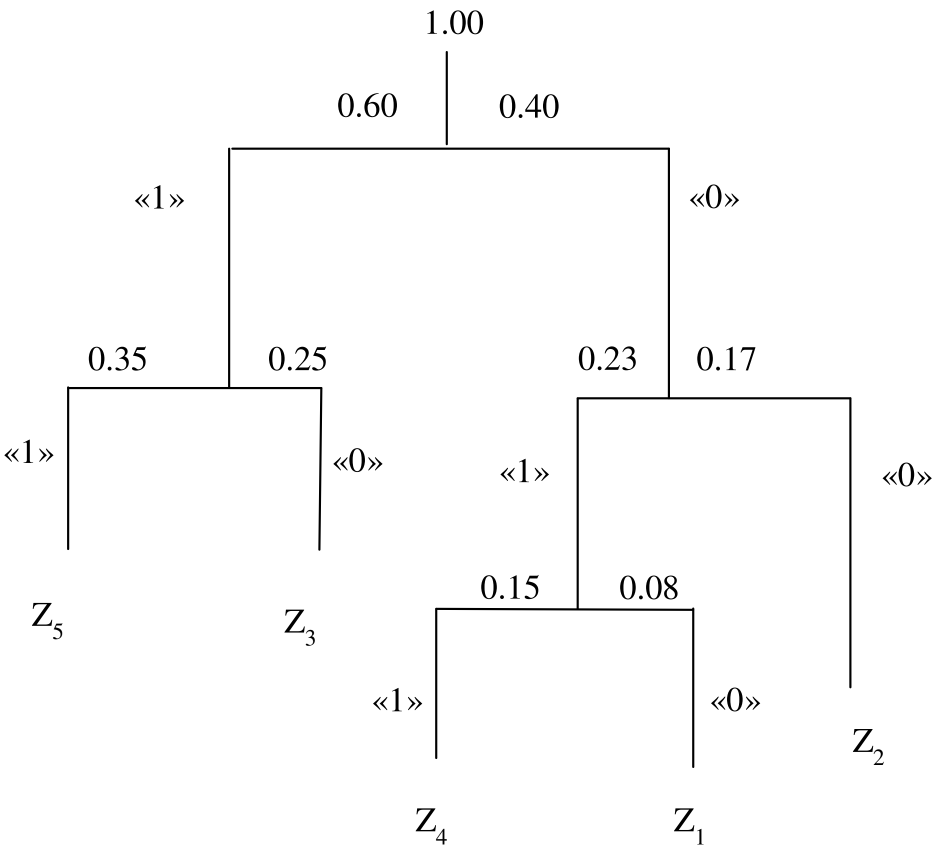


Рисунок 1.1 – Дерево ймовірностей

Використовуючи дерево визначимо кодові комбінації, що будуть відповідати символам.

Z_1 – 010; Z_2 – 00; Z_3 – 10; Z_4 – 011; Z_5 – 11.

Середня довжина кодової комбінації складе

$$\overline{\mathrm{n}} = \sum_{i=0}^{5} p_i \cdot n_i = 0.17 \cdot 2 + 0.25 \cdot 2 + 0.35 \cdot 2 + 0.15 \cdot 3 + 0.08 \cdot 3 =$$

$$= 2.23 \text{ біт/символ}$$

Арифметичне стиснення, як і метод Хаффмана, також використовує ймовірності появи символів у файлу, але кодуються не окремі символи тексту, а ланцюжки символів. При кодуванні арифметичним методом використовується наступний алгоритм:

1) використовуючи ймовірності появи символів будуємо інтервал ймовірностей від 0 до 1, на якому розміщуємо існуючи символи. Це необхідно, щоб визначити для кожного символу підінтервал;

2) починаємо кодувати символи ланцюжка, починаючи з першого символу за допомогою формул

$$l_i = l_{i-1} + (h_{i-1} - l_{i-1}) \cdot l_x$$
$$h_i = l_{i-1} + (h_{i-1} - l_{i-1}) \cdot h_x \qquad (1.2)$$

де l_i, h_i – нижня та верхня межа інтервалу ймовірності на поточному кроку кодування;

l_{i-1}, h_{i-1} – нижня та верхня межа інтервалу ймовірності на попередньому кроку кодування;

l_x, h_x – нижня та верхня межа інтервалу ймовірності символу, що кодується. Ці значення беруться з інтервалу, що побудован на першому кроку кодування.

На початку кодування вважають, що верхня та нижня межі інтервалу кодування дорівнюють відповідно l_0=0 та h_0=1. При розрахунках за формулами (1.2) не допускається будь-яке округлення отриманих значень.

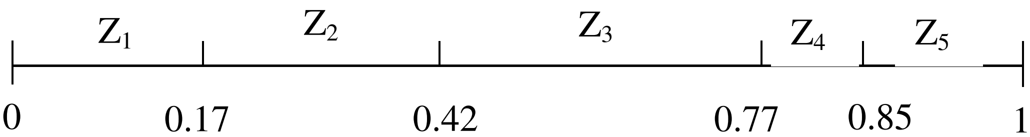
Кількість кроків кодування відповідає кількості символів у ланцюжку. З кожним кроком інтервал кодування буде звужуватися.

3) Результатом кодування є будь-яке число з кінцевого інтервалу кодування, що має найменшу кількість знаків після коми.

Приклад 2. Закодуємо послідовність символів Z2Z3Z5, якщо ймовірності появи символів задані у попередньому прикладі.

Розв’язок

Побудуємо інтервал ймовірностей



Кодування послідовності буде складатися з трьох кроків.

1) Крок перший. Кодуємо символ Z2 *l_0=0, h_0=1, l_x,=0.17, h_x=0.42;*

$$l_1 = l_0 + (h_0 - l_0) \cdot l_x = 0 + (1 - 0) \cdot 0.17 = 0.17,$$
$$h_1 = l_0 + (h_0 - l_0) \cdot h_x = 0 + (1 - 0) \cdot 0.42 = 0.42.$$

2) Крок другий. Кодуємо символ Z3 *l_1=0, h_1=1, l_x,=0.42, h_x=0.77;*

$$l_2 = l_1 + (h_1 - l_1) \cdot l_x = 0.17 + (0.42 - 0.17) \cdot 0.42 = 0.275,$$
$$h_2 = l_1 + (h_1 - l_1) \cdot h_x = 0.17 + (0.42 - 0.17) \cdot 0.77 = 0.3625.$$

3) Крок третій. Кодуємо символ Z5 *l_2=0.275, h_2=0.3625, l_x,=0.85, h_x=1;*

$$l_3 = l_2 + (h_2 - l_2) \cdot l_x = 0.275 + (0.3625 - 0.275) \cdot 0.85 = 0.349375,$$
$$h_3 = l_2 + (h_2 - l_2) \cdot h_x = 0.275 + (0.3625 - 0.275) \cdot 1 = 0.3625.$$

Результатом кодування буде число 0.36, що належить інтервалу 0.349375…0.3625 та має найменшу кількість знаків після коми.

Завдання для самостійного виконання

Завдання 1. Джерело інформації генерує 6 символів X1…X6 з наступними ймовірностями появи p(X1)=0.12, p(X2)=0.03, p(X3)=0.4, p(X4)=0.26, p(X5)=0.09, p(X6)=0.1. Закодувати методом Хаффмана символи, розрахувати середню довжину кодової комбінації.

Завдання 2. Закодувати послідовність символів X4X3X6, якщо ймовірності появи символів задані у попередньому прикладі.

Практичне заняття №2. Поля Галуа. Кодування та декодування двійковим кодом БЧХ

При підготовці до практичного заняття слід вивчити [1, с.84-110, 187-201]. Поля Галуа – це спеціалізований розділ математики, що покладений у основу сучасних завадостійких кодів та шифрування інформації. Кінцеве поле Галуа позначають, як GF(q), де q розмірність поля, тобто кількість елементів у полі. Якщо $q=p^m$, тоді говорять, що поле GF(q) є розширенням поля $GF(p^m)$. Поля Галуа мають декілька важливих властивостей для практичного використання у завадостійких кодах. Кожне поле має один нульовий елемент та q-1 ненульових. Поля є кінцевими та кільцевими, тобто якщо при математичних операціях над елементами поля ми отримаємо елемент, що не входить до поля, то йому обов'язково є відповідний серед елементів поля. Елементи поля позначаються як α^0, α^1, α^2… Ці елементи розраховуються за допомогою примітивного многочлена. Максимальний ступень примітивного многочлена дорівнює m. Для знаходження елементів поля необхідно виконати ділення z^i, i=0,1,2… на примітивний многочлен. Залишки від ділення *R* є елементами поля. У таблиці 2.1 наведені примітивні многочлени.

Таблиця 2.1 – Примітивні многочлени для побудови полів Галуа

m	Многочлен
2	z^2+z+1
3	z^3+z+1
4	z^4+z+1

Приклад 1. Знайдемо 6 перших елементів поля $GF(16)= GF(2^4)$.

Розв'язок

Поле GF(16) повинно мати 16 елементів: 0 та α^0, α^1, α^2… α^{14}. При m=4 обираємо примітивний многочлен z^4+z+1. Знайдемо елементи поля

$$\alpha^0 = R(z^0/(z^4+z+1)).$$

z^0 не можна розділити на примітивний многочлен, тому залишок від ділення є z^0. Тобто $\alpha^0 = z^0$

$$\alpha^1 = R(z^1/(z^4+z+1)) = z^1;$$
$$\alpha^2 = R(z^2/(z^4+z+1)) = z^2;$$
$$\alpha^3 = R(z^3/(z^4+z+1)) = z^3;$$
$$\alpha^4 = R(z^4/(z^4+z+1));$$

$$\begin{array}{l|l} z^4 & \underline{z^4+z+1} \\ \underline{z^4+z+1} & 1 \end{array}$$

$$R = z+1$$
$$\alpha^4 = z+1;$$
$$\alpha^5 = R(z^5/(z^4+z+1));$$

$$\begin{array}{l|l} z^5 & \underline{z^4+z+1} \\ \underline{z^5+z^2+z} & z \end{array}$$

$$R = z^2+z$$
$$\alpha^5 = z^2+z;$$
$$\alpha^6 = R(z^6/(z^4+z+1));$$

$$\begin{array}{l|l} z^6 & \underline{z^4+z+1} \\ \underline{z^6+z^3+z^2} & z^2 \end{array}$$

$$R = z^3+z^2$$
$$\alpha^6 = z^3+z^2;$$

Над елементами поля Галуа можливо виконувати математичні дії:

- додавання, при якому необхідно складати по модуля 2 поліноміальні еквіваленти елементів поля;
- вирахування по модулю 2, що еквівалентно додаванню;
- множення та ділення, які виконуються за загальними математичними правилами.

Приклад 2. Використовуючи таблицю елементів поля Галуа GF(2^4) (Додаток А) виконати наступні математичні дії з його елементами $\alpha^5+\alpha^9$, $\alpha^6 \cdot \alpha^5$, $\alpha^9 \cdot \alpha^7$, α^8/α^3, α^7/α^9

Розв’язок

$$\alpha^5 + \alpha^9 = z^2 + z + z^2 + 1 = z + 1 = \alpha^4;$$
$$\alpha^6 \cdot \alpha^5 = \alpha^{11};$$
$$\alpha^9 \cdot \alpha^7 = \alpha^{16} = \alpha;$$
$$\frac{\alpha^8}{\alpha^3} = \alpha^5;$$
$$\frac{\alpha^7}{\alpha^9} = \alpha^{-2} = \alpha^{13}.$$

Завадостійкі коди БЧХ є різновидом циклічних кодів та мають найменшу надлишковість у порівнянні з іншими кодами. Ці коди дозволяють виправляти 2 або більше помилок. При кодуванні інформації використовується класичний алгоритм кодування циклічними кодами. Класичний алгоритм кодування двійкових кодів складається з наступних дій:

1) Відповідно до заданого завадостійкого коду представляємо інформацію, що треба закодувати, у двійковому виді та у вигляді двійкового полінома

$$V(x) = b_{k-1} \cdot x^{k-1} + \ldots + b_1 \cdot x + b_0, \tag{2.1}$$

де b_{k-1},...b_1, b_0 відповідають значенням біт у двійковому вигляді інформації, а k – кількість інформаційних біт у кодовій комбінації.

2) Помножуємо $V(x)$ на x^r, де r – кількість контрольних біт у кодовій комбінації.

3) З довідкових таблиць (Додаток Б) обираємо утворюючий поліном g(x) та виконуємо ділення $V(x) \cdot x^r / g(x)$. У результаті ділення отримаємо остаток $R(x)$. Тоді повна кодова комбінація буде мати вигляд

$$F(x) = V(x) \cdot x^r + R(x). \tag{2.2}$$

Приклад 3. Закодувати з використання коду БЧХ $(15,7)$ число 43. Код побудований у поле $GF(2^4)$, яке є розширенням поля $GF(2)$ за поліномом $P(z) = z^4 + z + 1$.

Розв'язок. Визначимо кількість інформаційних і контрольних символів у кодовій комбінації: $k = 7$; $r = n - k = 15 - 7 = 8$.

Кодова комбінація для числа 43 має вигляд 101011, або представлена у вигляді двійкового полінома $\mathrm{V(x) = x^5 + x^3 + x + 1}$.

Код БЧХ$(15,7)$, побудований у поле $GF(2^4)$, що є розширенням поля $GF(2)$ за поліномом $P(z) = z^4 + z + 1$, є двійковим кодом. Він виправляє дві помилки та має утворюючий поліном $\mathrm{g(x) = x^8 + x^7 + x^6 + x^4 + 1}$. Визначаємо комбінацію коду за формулою (2.2)

$$
\begin{array}{l|l}
x^{13}+x^{11}+x^{9}+x^{8} & \underline{x^{8}+x^{7}+x^{6}+x^{4}+1} \\
\underline{x^{13}+x^{12}+x^{11}+x^{9}+x^{5}} & x^{5}+x^{4}+x^{3}+x+1
\end{array}
$$

$x^{12}+x^{8}+x^{5}$

$\underline{x^{12}+x^{11}+x^{10}+x^{8}+x^{4}}$

$x^{11}+x^{10}+x^{5}+x^{4}$

$\underline{x^{11}+x^{10}+x^{9}+x^{7}+x^{3}}$

$x^{9}+x^{7}+x^{5}+x^{4}+x^{3}$

$\underline{x^{9}+x^{8}+x^{7}+x^{5}+x}$

$x^{8}+x^{4}+x^{3}+x$

$\underline{x^{8}+x^{7}+x^{6}+x^{4}+1}$

$R(x)=x^{7}+x^{6}+x^{3}+x+1.$

Залишок $R(x)=x^{7}+x^{6}+x^{3}+x+1$. Отже, кодова комбінація має вигляд $F(x)=x^{13}+x^{11}+x^{9}+x^{8}+x^{7}+x^{6}+x^{3}+x+1$.

При декодуванні двійкових кодових комбінацій кодів БЧХ використовується алгоритм Пітерсона-Горенстейна-Цилліра. Відповідно до цього алгоритму виконуються наступні кроки:

1) Робимо припущення, що у прийнятій кодовій комбінації $F^{*}(x)$ виникла максимальна кількість помилок υ=t, що може виправити код. Розраховуємо 2υ компонентів синдрому за правилами

$$S_1 = F^{*}(\alpha), S_2 = F^{*}(\alpha^2) \ldots S_{2\upsilon} = F^{*}(\alpha^{2\upsilon}).$$

2) Записуємо матрицю Вандемара M та знаходимо її визначник detM

$$M = \begin{bmatrix} S_1 S_2 \ldots S_\upsilon \\ S_2 S_3 \ldots S_{\upsilon+1} \\ \ldots \\ S_{\upsilon+1} S_{\upsilon+2} \ldots S_{2\upsilon} \end{bmatrix}.$$

Якщо $det\mathrm{M} = 0$, то припущення о кількості помилок невірне (їх менше). Тоді вважають, що υ=υ-1 і розмір матриці Вандемара зменшується на 1. Другий пункт алгоритму повторюють доки detM не стане ненульовим, або розмір матриці не зменшиться до 0. Якщо υ стає рівним 0, то помилок немає.

3) Якщо $det\mathrm{M} \neq 0$ та υ=1, то помилка одна і її номер у кодовій комбінації однозначно визначається $S_1 = \alpha^i$, тобто номером елементу поля α^i. При υ>1, необхідно обчислити зворотну матрицю M^{-1} та вектор-стовбець локаторів помилок за формулою

$$\begin{bmatrix} \Lambda_\upsilon \\ \dots \\ \Lambda_1 \end{bmatrix} = M^{-1} \begin{bmatrix} S_{\upsilon+1} \\ \dots \\ S_{2\upsilon} \end{bmatrix}.$$

4) За визначеними значеннями елементів вектор-стовбця локаторів помилок записуємо многочлен локаторів помилок

$$\Lambda(x) = \Lambda_\upsilon \cdot x^\upsilon + \ldots + \Lambda_1 \cdot x + 1.$$

5) Знаходимо корні рівняння $\Lambda(x) = 0$, якими, відповідно до теорії полей Галуа, можуть бути елементи поля. Для цього використовуємо процедуру Ченя. За цією процедурою у $\Lambda(x)$ замість x підставляємо елементи поля. Коли $\Lambda(\alpha^i) = 0$, це корінь рівняння, а номер спотвореного символу визначається номером елемента поля

$$\frac{1}{\alpha^i} = \alpha^j.$$

Приклад 4. Внесемо помилки в третій і восьмий розряди отриманої у прикладі 3 кодової комбінації та покажемо процес їх виправлення.

Розв'язок

Прийнята кодова комбінація у вигляді двійкового полінома буде мати вигляд $F^*(x) = x^{13} + x^{11} + x^9 + x^7 + x^6 + x + 1$.

Для виявлення спотворених позицій у кодовій комбінації скористаємося методом Пітерсона – Горенстейна – Цирліра. Обчислимо компоненти синдрому, використовуючи арифметику у полі $GF(16)$:

$$S_1 = F^*(\alpha) = \alpha^{13} + \alpha^{11} + \alpha^9 + \alpha^7 + \alpha^6 + \alpha + 1 = z^3 + z^2 + 1 + z^3 + z^2 + z + z^3 + z +$$
$$+ z^3 + z + 1 + z^3 + z^2 + z + 1 = z^3 + z^2 + 1 = \alpha^{13};$$
$$S_2 = F^*(\alpha^2) = \alpha^{26} + \alpha^{22} + \alpha^{18} + \alpha^{14} + \alpha^{12} + \alpha^2 + 1 = z^3 + z^2 + z + z^3 + z + 1 + z^3 + z^3 + 1 +$$
$$+ z^3 + z^2 + z + 1 + z^2 + 1 = z^3 + z^2 + z = \alpha^{11};$$
$$S_3 = F^*(\alpha^3) = \alpha^{39} + \alpha^{33} + \alpha^{27} + \alpha^{21} + \alpha^{18} + \alpha^3 + 1 = z^3 + z + z^3 + z^3 + z^2 + z + 1 +$$
$$+ z^3 + z^2 + z^3 + z^3 + 1 = 0;$$
$$S_4 = F^*(\alpha^4) = \alpha^{52} + \alpha^{44} + \alpha^{36} + \alpha^{28} + \alpha^{24} + \alpha^4 + 1 = z^3 + z + 1 + z^3 + 1 + z^3 + z^2 + z^3 +$$
$$+ z^2 + 1 + z^3 + z + z + 1 + 1 = z^3 + z + 1 = \alpha^7.$$

Припустимо, що у прийнятій кодовій комбінації відбулися $\upsilon = 2$ помилки. Складемо матрицю Вандемара, елементами якої є компоненти синдрому

$$M = \begin{bmatrix} S_1 & S_2 \\ S_2 & S_3 \end{bmatrix} = \begin{bmatrix} \alpha^{13} & \alpha^{11} \\ \alpha^{11} & 0 \end{bmatrix}.$$

Знайдемо визначник отриманої матриці

$$\det M = \alpha^{13} \cdot 0 + \alpha^{11}\alpha^{11} = \alpha^{22} = \alpha^{7}.$$

Визначник не дорівнює нулю. Отже, відбулися дві помилки.

Визначимо вектор локаторів помилок

$$\begin{bmatrix} \Lambda_2 \\ \Lambda_1 \end{bmatrix} = M^{-1} \begin{bmatrix} S_3 \\ S_4 \end{bmatrix}.$$

Знайдемо зворотну матрицю

$$M^{-1} = \frac{1}{\det M} \begin{bmatrix} A_{11} & A_{21} \\ A_{12} & A_{22} \end{bmatrix} = \frac{1}{\alpha^7} \begin{bmatrix} 0 & \alpha^{11} \\ \alpha^{11} & \alpha^{13} \end{bmatrix} = \begin{bmatrix} 0 & \alpha^{4} \\ \alpha^{4} & \alpha^{6} \end{bmatrix}.$$

Тоді

$$\begin{bmatrix} \Lambda_2 \\ \Lambda_1 \end{bmatrix} = \begin{bmatrix} 0 & \alpha^{4} \\ \alpha^{4} & \alpha^{6} \end{bmatrix} \begin{bmatrix} 0 \\ \alpha^{7} \end{bmatrix} = \begin{bmatrix} 0 \cdot 0 + \alpha^4\alpha^7 \\ \alpha^4 \cdot 0 + \alpha^6\alpha^7 \end{bmatrix} = \begin{bmatrix} \alpha^{11} \\ \alpha^{13} \end{bmatrix}.$$

Тоді рівняння локаторів помилок буде мати вигляд

$$\Lambda(x) = \Lambda_2 x^2 + \Lambda_1 x + 1 = \alpha^{11}x^2 + \alpha^{13}x + 1.$$

Знайдемо корні рівняння $\Lambda(x) = 0$, підставляючи замість x елементи поля. Маємо

$\Lambda(\alpha^0) = \alpha^{11}\alpha^0 + \alpha^{13}\alpha^0 + 1 = \alpha^{11} + \alpha^{13} + 1 = z^3 + z^2 + z + z^3 + z^2 + 1 + 1 = z = \alpha;$

$\Lambda(\alpha) = \alpha^{11}\alpha^2 + \alpha^{13}\alpha + 1 = \alpha^{13} + \alpha^{14} + 1 = z^3 + z^2 + 1 + z^3 + 1 + 1 = z^2 + 1 = \alpha^8;$

$\Lambda(\alpha^2) = \alpha^{11}\alpha^4 + \alpha^{13}\alpha^2 + 1 = \alpha^{15} + \alpha^{15} + 1 = 1 = \alpha^0;$

$\Lambda(\alpha^3) = \alpha^{11}\alpha^6 + \alpha^{13}\alpha^3 + 1 = \alpha^{17} + \alpha^{16} + 1 = \alpha^2 + \alpha + 1 = z^2 + z + 1 = \alpha^{10};$

$\Lambda(\alpha^4) = \alpha^{11}\alpha^8 + \alpha^{13}\alpha^4 + 1 = \alpha^{19} + \alpha^{17} + 1 = \alpha^4 + \alpha^2 + 1 = z + 1 + z^2 + 1 = z^2 + z = \alpha;$

$\Lambda(\alpha^5) = \alpha^{11}\alpha^{10} + \alpha^{13}\alpha^5 + 1 = \alpha^{21} + \alpha^{18} + 1 = \alpha^6 + \alpha^3 + 1 = z^3 + z^2 + z^3 + 1 = z^2 + 1 =$
$= \alpha;$

$\Lambda(\alpha^6) = \alpha^{11}\alpha^{12} + \alpha^{13}\alpha^6 + 1 = \alpha^{23} + \alpha^{19} + 1 = \alpha^8 + \alpha^4 + 1 = z^2 + 1 + z + 1 + 1 =$
$= z^2 + z + 1 = \alpha^{10};$

$\Lambda(\alpha^7) = \alpha^{11}\alpha^{14} + \alpha^{13}\alpha^7 + 1 = \alpha^{25} + \alpha^{20} + 1 = \alpha^{10} + \alpha^5 + 1 = z^2 + z + 1 + z^2 + z + 1 = 0;$

$\Lambda(\alpha^8) = \alpha^{11}\alpha^{16} + \alpha^{13}\alpha^8 + 1 = \alpha^{27} + \alpha^{21} + 1 = \alpha^{12} + \alpha^6 + 1 = z^3 + z^2 + z + 1 + z^3 +$
$+ z^2 + 1 = z = \alpha;$

$\Lambda(\alpha^9) = \alpha^{11}\alpha^{18} + \alpha^{13}\alpha^9 + 1 = \alpha^{29} + \alpha^{22} + 1 = \alpha^{14} + \alpha^7 + 1 = z^3 + 1 + z^3 + z +$
$+ 1 + 1 = z + 1 = \alpha^4;$

$\Lambda(\alpha^{10}) = \alpha^{11}\alpha^{20} + \alpha^{13}\alpha^{10} + 1 = \alpha^{31} + \alpha^{23} + 1 = \alpha + \alpha^{8} + 1 = z + z^{2} + 1 + 1 =$
$= z^{2} + z = \alpha^{5};$
$\Lambda(\alpha^{11}) = \alpha^{11}\alpha^{22} + \alpha^{13}\alpha^{11} + 1 = \alpha^{33} + \alpha^{24} + 1 = \alpha^{3} + \alpha^{9} + 1 = z^{3} + z^{3} + z +$
$+ 1 = z + 1 = \alpha;$
$\Lambda(\alpha^{12}) = \alpha^{11}\alpha^{24} + \alpha^{13}\alpha^{12} + 1 = \alpha^{35} + \alpha^{25} + 1 = \alpha^{5} + \alpha^{10} + 1 = z^{2} + z + z^{2} +$
$+ z + 1 + 1 = 0;$
$\Lambda(\alpha^{13}) = \alpha^{11}\alpha^{26} + \alpha^{13}\alpha^{13} + 1 = \alpha^{37} + \alpha^{26} + 1 = \alpha^{7} + \alpha^{11} + 1 = z^{3} + z + 1 +$
$+ z^{3} + z^{2} + z + 1 = x^{2} = \alpha^{2};$
$\Lambda(\alpha^{14}) = \alpha^{11}\alpha^{28} + \alpha^{13}\alpha^{14} + 1 = \alpha^{39} + \alpha^{27} + 1 = \alpha^{9} + \alpha^{12} + 1 = z^{3} + z + z^{3} +$
$+ z^{2} + z + 1 + 1 = z^{2} = \alpha^{2}.$

Таким чином, елементи α^7 та α^{12} визначають місця розташування помилок. Тоді помилки знаходяться у $\frac{1}{\alpha^7} = \alpha^{-7} = \alpha^8$ та $\frac{1}{\alpha^{12}} = \alpha^{-12} = \alpha^3$, тобто у восьмому та третьому розрядах кодової комбінації, тому що код двійковий. Значення помилок дорівнюють 1, а багаточлен помилок має вигляд $e(x) = x^8 + x^3$. Тоді кодова комбінація буде мати вигляд

$F(x) = F^*(x) + e(x) = x^{13} + + x^{11} + x^{9} + x^{7} + x^{6} + x + 1 + x^{8} + x^{3} = x^{13} + x^{11} + x^{9} +$
$+ x^{8} + x^{7} + x^{6} + x^{3} + x + 1,$

що відповідає переданій кодовій комбінації.

Задачі для самостійного виконання.

Задача 1. Розрахувати елементи поля Галуа GF(8)=GF(2^3).

Задача 2. Використовуючи знайдені у задачі №1 елементи поля, виконати наступні арифметичні операції з цими елементами $\alpha^4 + \alpha^6$, $\alpha^1 \cdot \alpha^4$, $\alpha^4 \cdot \alpha^6$, α^2/α^4, α^5/α^2

Задача 3. Закодувати завадостійким кодом БЧХ (15,5) у полі GF(16)=GF(2^4) число 20. Код виправляє 3 помилки на кодову комбінацію. Внести помилки у 6-й та 12-й біт отриманої кодової комбінації. Показати їх виправлення.

Практичне заняття №3. Кодування та декодування завадостійким кодом Ріда-Соломона

При підготовці до практичного заняття слід вивчити [1, с.201-221]. Коди Ріда-Соломона це недвійкові коди, що будуються у полях Галуа типу GF(p^1).

Серед існуючих кодів вони найбільш ефективні з точки зору надлишковості у порівнянні з виправляючою спроможністю коду. У цих кодах породжуючий поліном формується за наступним математичним правилом

$$g(x) = \prod_{i=1}^{2t}\left(x - \alpha^{i+j_0}\right) \tag{3.1}$$

де t – кількість помилок, що може виправити код;
j_0 – параметр, що не впливає на виправлячі можливості коду, а лише дозволяє збудувати схемну реалізацію коду з мінімальною кількістю математичних операцій, j_0=0,1,2...

Приклад 1. Розрахуємо породжуючий поліном для коду Ріда-Соломона GF(16), що виправляє 2 помилки на кодову комбінацію.

Розв'язок

Використаємо формулу (3.1) при t=2, j_0=0

$$g(x) = \prod_{i=1}^{4}\left(x - \alpha^{i}\right) = (x+\alpha)(x+\alpha^2)(x+\alpha^3)(x+\alpha^4) =$$

$$= (x^2 + \alpha x + \alpha^2 x + \alpha^3)(x^2 + \alpha^3 x + \alpha^4 x + \alpha^7) = (x^2 + \alpha^5 x + \alpha^3)(x^2 + \alpha^7 x + \alpha^7) =$$

$$= x^4 + \alpha^7 x^3 + \alpha^7 x^2 + \alpha^5 x^3 + \alpha^{12} x^2 + \alpha^{12} x + \alpha^3 x^2 + \alpha^{10} x + \alpha^{10} =$$

$$= x^4 + \alpha^{13} x^3 + \alpha^6 x^2 + \alpha^3 x + \alpha^{10}$$

Ми отримали код Ріда-Соломона (15,11), у якому 15 символів усього, з них 11 інформаційні. Кожен з символів чотирьохрозрядне число.

Коди Ріда-Соломона є циклічними. Тому при кодуванні інформації цими кодами використовується загальний алгоритм кодування з врахуванням того, що код недвійковий. Особливістю кодування є перетворення інформаційних груп бітів у відповідні їм елементи поля Галуа. Тобто коефіцієнти b_{k-1},...b_1, b_0 у формулі (2.1) є недвійковими та відповідають елементам поля.

Приклад 2. Закодувати число 21 кодом Ріда-Соломона (15,11), що виправляє 2 помилки на кодову комбінацію у полі GF(16).

Розв'язок

Представимо число 21 у двійковому вигляді

21=0001 0101

Використання поля GF(16) означає, що кожен з символів – 4 біта. Розділяючи інформаційну послідовність на групи по 4 біта та користуючись таблицею додатка Б запишемо інформаційний поліном

$$V(x) = x + \alpha^5.$$

Помножаємо інформаційний поліном на $x^r = x^4$

$$v(x) \cdot x^r = (x + \alpha^8)x^4 = x^5 + \alpha^8 x^4.$$

Розділимо отриманий поліном на породжуючий

$$\begin{array}{l|l} x^5 + \alpha^8 x^4 & \underline{x^4 + \alpha^{13}x^3 + \alpha^6 x^2 + \alpha^3 x + \alpha^{10}} \\ \underline{x^5 + \alpha^{13}x^4 + \alpha^6 x^3 + \alpha^3 x^2 + \alpha^{10}x} & x + \alpha^3 \end{array}$$

$$\alpha^3 x^4 + \alpha^6 x^3 + \alpha^3 x^2 + \alpha^{10} x$$
$$\underline{\alpha^3 x^4 + \alpha x^3 + \alpha^9 x^2 + \alpha^6 x + \alpha^{13}}$$
$$R(x) = \alpha^{11}x^3 + \alpha x^2 + \alpha^7 x + \alpha^{13}.$$

Тоді повна кодова комбінація має вигляд

$$F(x) = x^5 + \alpha^8 x^4 + \alpha^{11}x^3 + \alpha x^2 + \alpha^7 x + \alpha^{13}.$$

Декодування кодів Ріда-Соломона складається з двох частин:

1) знаходження номерів спотворених символів;
2) знаходження вагових коефіцієнтів помилок.

Перша частина декодування виконується за розглянутим раніше алгоритмом Пітерсона-Горенстейна-Цилліра.

Друга частина декодування виконується за алгоритмом Форні. Розглянемо детально цей алгоритм:

1) Знаходимо похідну многочлена локаторів помилок ;
$$\Lambda'(x) = \upsilon \cdot \Lambda_\upsilon \cdot x^{\upsilon-1} + \ldots + \Lambda_1.$$
2) Записуємо синдромний многочлен у вигляді
$$S(x) = \sum_{i=1}^{2\upsilon} S_i \cdot x^{i-1}$$
3) Знаходимо многочлен помилок
$$\Omega(x) = S(x) \cdot \Lambda'^{(x)} mod\ x^{2\upsilon}.$$

Операція по $mod\ x^{2\upsilon}$ означає, що в отриманому многочлені усі доданки з показниками 2υ та більше відкидаються.

4) Знаходимо вагові коефіцієнти помилок за формулою
$$Y_l = \frac{\Omega(\alpha_l)}{\Lambda'(\alpha_l)},$$

де α_l – корні многочлена локаторів помилок.

5) Записуємо многочлен помилок

$$e(x) = \sum Y_l \cdot x^j ,$$

де j – спотворені номера символів у кодовій комбінації.

Додаючи многочлен помилок до спотвореної комбінації отримаємо неспотворену комбінацію

$$F^*(x) + e(x) = F(x).$$

Приклад 3. Внесемо помилки у 7-й та 12-й біт отриманої у другому прикладі кодової комбінації та покажемо процес виправлення помилок

Розв’язок

Спотворення 7-го біта відповідає помилці у коефіцієнті при x в комбінації $F(x)$, а спотворення у 12-му біті відповідає помилці у коефіцієнті при x^3. Тоді

$$\left(\alpha^7 + z^3\right)x = \left(z^3 + z + 1 + z^3\right)x = (z+1)x = \alpha^4 x ,$$

$$\left(\alpha^{11} + 1\right)x^3 = \left(z^3 + z^2 + z + 1\right)x^3 = \alpha^{12} x^3 .$$

Тоді прийнята кодова комбінація має вигляд

$$F^*(x) = x^5 + \alpha^8 x^4 + \alpha^{12} x^3 + \alpha x^2 + \alpha^4 x + \alpha^{13}.$$

Знайдемо компоненти синдрома, використовуючи додаток А

$$S_1 = F^*(\alpha) = \alpha^5 + \alpha^8\alpha^4 + \alpha^{12}\alpha^3 + \alpha\alpha^2 + \alpha^4\alpha + \alpha^{13} = \alpha^5 + \alpha^{12} + \alpha^{15} + \alpha^3 + \alpha^5 + \alpha^{13} =$$

$$= z^2 + z + z^3 + z^2 + z + 1 + 1 + z^3 + z^2 + z + z^3 + z^2 + 1 = z^3 + z + 1 = \alpha^7;$$

$$S_2 = F^*(\alpha^2) = \alpha^{10} + \alpha^8\alpha^8 + \alpha^{12}\alpha^6 + \alpha\alpha^4 + \alpha^4\alpha^2 + \alpha^{13} = \alpha^{10} + \alpha^{16} + \alpha^{18} + \alpha^5 +$$

$$+ \alpha^6 + \alpha^{13} = z^2 + z + 1 + z + z^3 + z^2 + z + z^3 + z^2 + z^3 + z^2 + 1 = z^3 + z = \alpha^9;$$

$$S_3 = F^*(\alpha^3) = \alpha^{15} + \alpha^8\alpha^{12} + \alpha^{12}\alpha^9 + \alpha\alpha^6 + \alpha^4\alpha^3 + \alpha^{13} = \alpha^{15} + \alpha^{20} + \alpha^{21} + \alpha^7 +$$

$$+ \alpha^7 + \alpha^{13} = 1 + z^2 + z + z^3 + z^2 + z^3 + z^2 + 1 = z^2 + z = \alpha^5;$$

$$S_4 = F^*(\alpha^4) = \alpha^{20} + \alpha^8\alpha^{16} + \alpha^{12}\alpha^{12} + \alpha\alpha^8 + \alpha^4\alpha^4 + \alpha^{13} = \alpha^{20} + \alpha^{24} + \alpha^{24} + \alpha^9 +$$

$$+ \alpha^8 + \alpha^{13} = z^2 + z + z^3 + z + z^2 + 1 + z^3 + z^2 + 1 = z^2 = \alpha^2.$$

Припустимо, що у кодовій комбінації виникло 2 помилки та запишемо матрицю Вандемара

$$M = \begin{bmatrix} S_1 & S_2 \\ S_2 & S_3 \end{bmatrix} = \begin{bmatrix} \alpha^7 & \alpha^9 \\ \alpha^9 & \alpha^5 \end{bmatrix}.$$

Знайдемо визначник матриці

$$\det M = \alpha^7\alpha^5 + \alpha^9\alpha^9 = \alpha^{12} + \alpha^{18} = \alpha^{12} + \alpha^3 = x^3 + x^2 + x + 1 + x^3 = x^2 + x + 1 = \alpha^{10}.$$

Визначник не дорівнює нулю, тобто припущення про дві помилки вірно.

Знайдемо зворотну матрицю та вектор локаторів помилок

$$M^{-1} = \frac{1}{\det M}\begin{bmatrix} A_{11} & A_{21} \\ A_{12} & A_{22} \end{bmatrix} = \frac{1}{\alpha^{10}}\begin{bmatrix} \alpha^5 & \alpha^9 \\ \alpha^9 & \alpha^7 \end{bmatrix} = \begin{bmatrix} \alpha^{-5} & \alpha^{-1} \\ \alpha^{-1} & \alpha^{-3} \end{bmatrix} = \begin{bmatrix} \alpha^{10} & \alpha^{14} \\ \alpha^{14} & \alpha^{12} \end{bmatrix},$$

$$\begin{bmatrix} \Lambda_2 \\ \Lambda_1 \end{bmatrix} = M^{-1}\begin{bmatrix} S_3 \\ S_4 \end{bmatrix},$$

$$\begin{bmatrix} \Lambda_2 \\ \Lambda_1 \end{bmatrix} = \begin{bmatrix} \alpha^{10} & \alpha^{14} \\ \alpha^{14} & \alpha^{12} \end{bmatrix}\begin{bmatrix} \alpha^5 \\ \alpha^2 \end{bmatrix} = \begin{bmatrix} \alpha^{10}\alpha^5 + \alpha^{14}\alpha^2 \\ \alpha^{14}\alpha^5 + \alpha^{12}\alpha^2 \end{bmatrix} = \begin{bmatrix} \alpha^{15} + \alpha^{16} \\ \alpha^{19} + \alpha^{14} \end{bmatrix} = \begin{bmatrix} \alpha^0 + \alpha \\ \alpha^4 + \alpha^{14} \end{bmatrix} =$$

$$= \begin{bmatrix} 1 + x \\ x + 1 + x^3 + 1 \end{bmatrix} = \begin{bmatrix} x + 1 \\ x^3 + x \end{bmatrix} = \begin{bmatrix} \alpha^4 \\ \alpha^9 \end{bmatrix}.$$

Тоді поліном локаторів помилок буде мати вигляд

$$\Lambda(x) = \Lambda_2 x^2 + \Lambda_1 x + 1 = \alpha^4 x^2 + \alpha^9 x + 1.$$

Знайдемо корні рівняння $\Lambda(x) = 0$, використовуючи процедуру Ченя.

$$\Lambda(\alpha^0) = \alpha^4\alpha^{00} + \alpha^9\alpha^0 + 1 = \alpha^4 + \alpha^9 + 1 = x + 1 + x^3 + x + 1 = x^3 = \alpha^3;$$

$$\Lambda(\alpha) = \alpha^4\alpha^2 + \alpha^9\alpha + 1 = \alpha^6 + \alpha^{10} + 1 = x^3 + x^2 + x^2 + x + 1 + 1 = x^3 + x = \alpha^9;$$

$$\Lambda(\alpha^2) = \alpha^4\alpha^4 + \alpha^9\alpha^2 + 1 = \alpha^8 + \alpha^{11} + 1 = x^2 + 1 + x^3 + x^2 + x + 1 = x^3 + x = \alpha^9;$$

$$\Lambda(\alpha^3) = \alpha^4\alpha^6 + \alpha^9\alpha^3 + 1 = \alpha^{10} + \alpha^{12} + 1 = x^2 + x + 1 + x^3 + x^2 + x + 1 + 1 =$$
$$= x^3 + 1 = \alpha^{14};$$

$$\Lambda(\alpha^4) = \alpha^4\alpha^8 + \alpha^9\alpha^4 + 1 = \alpha^{12} + \alpha^{13} + 1 = x^3 + x^2 + x + 1 + x^3 + x^2 + 1 + 1 =$$
$$= x + 1 = \alpha^4;$$

$$\Lambda(\alpha^5) = \alpha^4\alpha^{10} + \alpha^9\alpha^5 + 1 = \alpha^{14} + \alpha^{14} + 1 = 1 = \alpha^0;$$

$$\Lambda(\alpha^6) = \alpha^4\alpha^{12} + \alpha^9\alpha^6 + 1 = \alpha^{16} + \alpha^{15} + 1 = \alpha + 1 + 1 = \alpha;$$

$$\Lambda(\alpha^7) = \alpha^4\alpha^{14} + \alpha^9\alpha^7 + 1 = \alpha^{18} + \alpha^{16} + 1 = \alpha^3 + \alpha + 1 = x^3 + x + 1 = \alpha^7;$$

$$\Lambda(\alpha^8) = \alpha^4\alpha^{16} + \alpha^9\alpha^8 + 1 = \alpha^{20} + \alpha^{17} + 1 = \alpha^5 + \alpha^2 + 1 = x^2 + x + x^2 + 1 =$$
$$= x + 1 = \alpha^4;$$

$$\Lambda(\alpha^9) = \alpha^4\alpha^{18} + \alpha^9\alpha^9 + 1 = \alpha^{22} + \alpha^{18} + 1 = \alpha^7 + \alpha^3 + 1 = x^3 + x + 1 + x^3 + 1 =$$
$$= x = \alpha;$$

$$\Lambda(\alpha^{10}) = \alpha^4\alpha^{20} + \alpha^9\alpha^{10} + 1 = \alpha^{24} + \alpha^{19} + 1 = \alpha^9 + \alpha^4 + 1 = x^3 + x + x + 1 + 1 =$$
$$= x^3 = \alpha^3;$$

$$\Lambda(\alpha^{11}) = \alpha^4\alpha^{22} + \alpha^9\alpha^{11} + 1 = \alpha^{26} + \alpha^{20} + 1 = \alpha^{11} + \alpha^5 + 1 = x^3 + x^2 + x +$$
$$+ x^2 + x + 1 = x^3 + 1 = \alpha^{14};$$

$$\Lambda(\alpha^{12}) = \alpha^4\alpha^{24} + \alpha^9\alpha^{12} + 1 = \alpha^{28} + \alpha^{21} + 1 = \alpha^{13} + \alpha^6 + 1 = x^3 + x^2 + 1 + x^3 +$$
$$+ x^2 + 1 = 0;$$
$$\Lambda(\alpha^{13}) = \alpha^4\alpha^{26} + \alpha^9\alpha^{13} + 1 = \alpha^{30} + \alpha^{22} + 1 = 1 + \alpha^7 + 1 = \alpha^7;$$
$$\Lambda(\alpha^{14}) = \alpha^4\alpha^{28} + \alpha^9\alpha^{14} + 1 = \alpha^{32} + \alpha^{23} + 1 = \alpha^2 + \alpha^8 + 1 = x^2 + x^2 + 1 + 1 = 0.$$

Таким чином елементи α^{12} та α^{14} визначають номера спотворених символів

$$\frac{1}{\alpha^{12}} = \alpha^{-12} = \alpha^3,$$
$$\frac{1}{\alpha^{14}} = \alpha^{-14} = \alpha.$$

Спотворені перший та третій символи.

Для знаходження вагових коефіцієнтів вектора помилок використаємо алгоритм Форні. Запишемо синдромний многочлен

$$S(x) = S_1 + S_2x + S_3x^2 + S_4x^3 = \alpha^7 + \alpha^9x + \alpha^5x^2 + \alpha^2x^3.$$

Обчислимо многочлен помилок

$$\Omega(x) = S(x)\Lambda(x)(\mathrm{mod}\, x^{2t}) = \left(\alpha^7 + \alpha^9x + \alpha^5x^2 + \alpha^2x^3\right)\times\left(\alpha^4x^2 + \alpha^9x +\right.$$
$$\left.+1\right)(\mathrm{mod}\, x^4) = \left(\alpha^7\alpha^4x^2 + \alpha^7\alpha^9x + \alpha^7 + \alpha^9x\alpha^4x^2 + \alpha^9x\alpha^9x + \alpha^9x +\right.$$
$$\left.+\alpha^5x^2\alpha^4x^2 + \alpha^5x^2\alpha^9x + \alpha^5x^2 + \alpha^2x^3\alpha^4x^2 + \alpha^2x^3\alpha^9x + \alpha^2x^3\right)(\mathrm{mod}\, x^4) =$$
$$= \left(\alpha^{11}x^2 + \alpha^{16}x + \alpha^7 + \alpha^{13}x^3 + \alpha^{18}x^2 + \alpha^9x + \alpha^9x^4 + \alpha^{14}x^3 + \alpha^5x^2 +\right.$$
$$\left.+\alpha^6x^5 + \alpha^{11}x^4 + \alpha^2x^3\right)(\mathrm{mod}\, x^4) = \left(\alpha^6x^5 + \left(\alpha^9 + \alpha^{11}\right)x^4 + \left(\alpha^{13} + \alpha^{14} +\right.\right.$$
$$\left.\left.+\alpha^2\right)x^3 + \left(\alpha^{11} + \alpha^3 + \alpha^5\right)x^2 + \left(\alpha + \alpha^9\right)x + \alpha^7\right)(\mathrm{mod}\, x^4) = \alpha^3x + \alpha^7.$$

Знайдемо похідну многочлена локаторів помилок

$$\Lambda'(x) = \left(\alpha^4x^2 + \alpha^9x + 1\right)' = 2\alpha^4x + \alpha^9 = \alpha^9.$$

Обчислимо вагові коефіцієнти помилок

$$Y_1 = \frac{\Omega(\alpha^{12})}{\Lambda'(\alpha^{12})} = \frac{\alpha^3\alpha^{12} + \alpha^7}{\alpha^9} = \frac{\alpha^{15} + \alpha^7}{\alpha^9} = \frac{\alpha^9}{\alpha^9} = \alpha^0 = 1;$$
$$Y_2 = \frac{\Omega(\alpha^{14})}{\Lambda'(\alpha^{14})} = \frac{\alpha^3\alpha^{14} + \alpha^7}{\alpha^9} = \frac{\alpha^{17} + \alpha^7}{\alpha^9} = \frac{\alpha^2 + \alpha^7}{\alpha^9} = \frac{\alpha^{12}}{\alpha^9} = \alpha^3.$$

Тоді многочлен помилок має вигляд

$$e(x) = x^3 + \alpha^3x$$

Виправляємо спотворену комбінацію

$$F(x)=F^*(x)+e(x)=x^5+\alpha^8x^4+\alpha^{12}x^3+\alpha x^2+\alpha^4x+\alpha^{13}+x^3+\alpha^3x=$$
$$=x^5+\alpha^8x^4+\alpha^{11}x^3+\alpha x^2+\alpha^7x+\alpha^{13}.$$

Задачі для самостійного виконання

Задача1. Розрахувати породжуючий поліном для завадостійкого коду Ріда-Соломона у полі Галуа GF(8). Код повинен виправляти дві помилки на кодову комбінацію.

Задача 2. Закодувати число 10 завадостійким кодом Ріда-Соломона, що виправляє 2 помилки у полі GF(8). Внести помилки у 6,7,13 біти повної кодової комбінації завадостійкого кода.

Практичне заняття №4. Дослідження методів кодування та декодування згортковим кодом

При підготовці до практичного заняття слід вивчити [2, с.406-435]. Згорткові коди – це коди, які використовують безперервну, або послідовну, обробку інформації короткими фрагментами (блоками) для виправлення помилок. Згортковий кодер має пам'ять у тому розумінні, що символи на його виході залежать не тільки від (чергового фрагмента) інформаційних символів на вході, але й попередніх символів на його вході. Інакше кажучи, кодер являє собою послідовну машину або автомат з кінцевим числом станів. Стан кодера визначається вмістом його пам'яті.

Згорткові коди характеризуються кодовим обмеженням K, відповідно до якого кодер має K елементів пам'яті $S_1, S_2, \dots S_k$. Кодер, що використовує K елементів пам'яті, називається надалі кодер пам'яті K. Під швидкістю коду в теорії кодування визначається відношення $R = k/n$. Більш точне найменування параметра R – відносна швидкість коду, оскільки за одиницю часу кодер приймає на вхід k інформаційних розрядів і трансформує їх в n розрядів надлишкового коду. Кодер пам'яті K і швидкості R двійкового згорткового коду можна розглядати також як дискретну лінійну інваріантну в часі систему. Це означає, що відгук кодера на нульову послідовність, у якій є єдина одиниця, тобто вихід кодера, отриманий для вхідної послідовності, повністю визначає код. Розглянемо один з найбільш відомих загорткових кодів (рисунок 4.1).

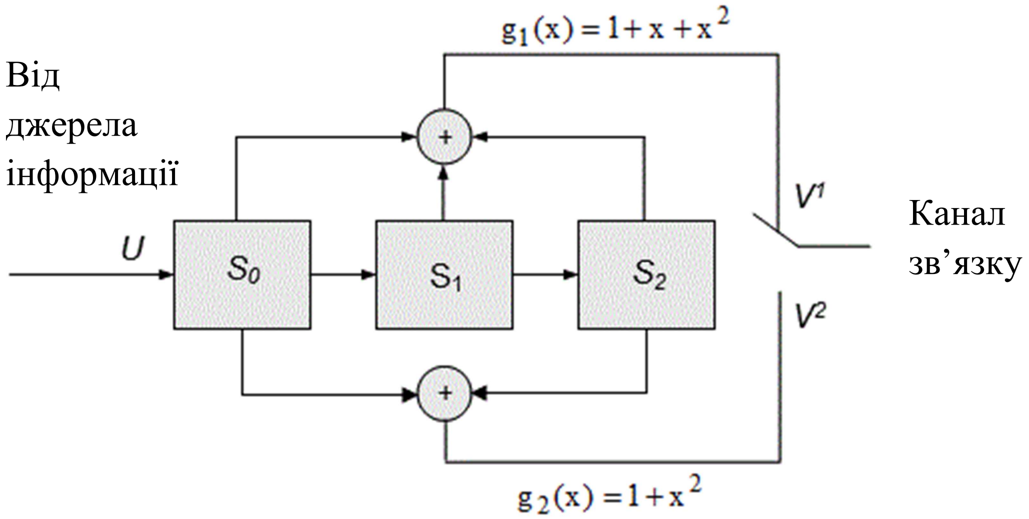


Рисунок 4.1 – Згортковий кодер

Цей кодер характеризується фізичними зв'язками у схемі, які математично описуються векторами зв'язку $g_1(x) = 1 + x + x^2$ та $g_2(x) = 1 + x^2$. На кожен вхідний біт у канал зв'язку відправляється 2 біта, що реалізується перемиканням вихідного ключа з положення V^1 у V^2 та навпаки. Розглянемо процес кодування інформації на прикладі

Приклад 1. Закодуємо послідовність інформаційних двійкових біт 10101 згортковим кодом з ступенем кодування 1/2. Використати кодер з кодовим обмеженням $K = 3$ (вектори зв'язку 111, 101) и нульовим початков станом кодера. Результат кодування представимо у вигляді таблиці 4.1.

Таблиця 4.1 – Процес кодування інформації загортковим кодом

Такт кодування	Інформаційний біт на вході кодера	Стан кодера	Кодове слово на виході кодера
1	1	100	11
2	0	010	10
3	1	101	00
4	0	010	10
5	1	101	00
6	0	010	10
7	0	001	11

Закодована комбінація буде мати вигляд 11010001000111.

Найбільш відомий алгоритм декодування – алгоритм по максимуму правдоподібності (Вітербі). Цей алгоритм використовує решітку, що зображена на рисунку 4.2

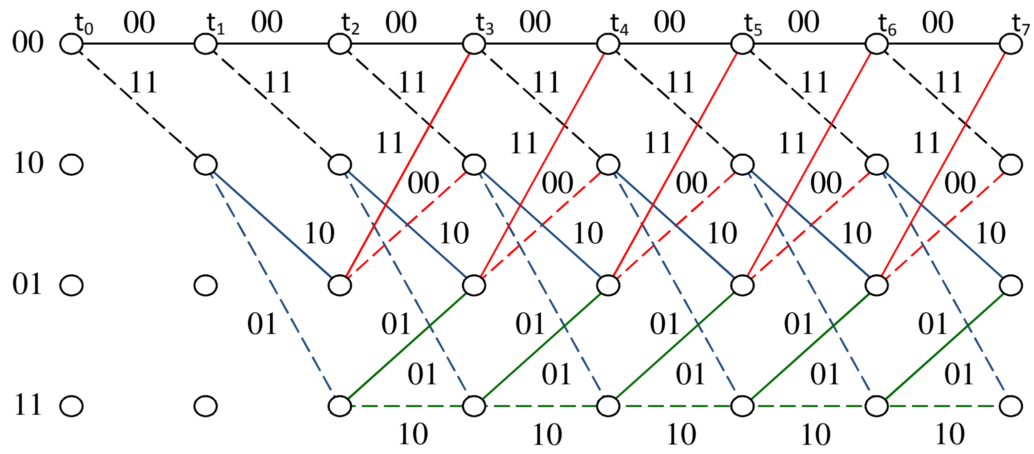


Рисунок 4.2 – Решітка Вітербі

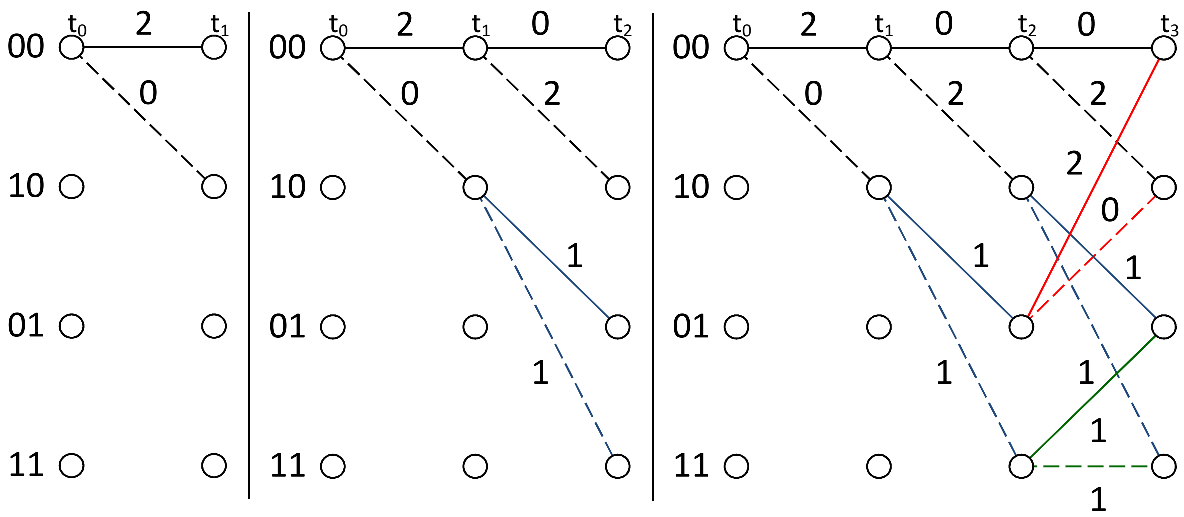
Декодер обчислює відстань Хеммінга між прийнятою послідовністю біт і всіма можливими кодовими векторами U_i і виносить рішення на користь того вектора, який виявляється ближче до прийнятого. Кодова решітка ілюструє можливі стани на виході кодера у різні моменти часу від початку кодування. Безперервні лінії у решітці відповідають стану на виході кодера, коли на вхід поданий «0», а пунктирні лінії – коли на вхід подана «1».

На вхід декодера надходить сегмент вхідної послідовності біт довжиною 2 біта. Він порівнюється з усіма ребрами решітки і для кожного з них обчислюється вага, як кількість біт, якою відрізняється вхідний сегмент від ребра. Так у момент часу t_1 вхідний сегмент порівнюється лише з двома ребрами, а в момент часу t_3 вже з вісьма. Починаючи з моменту часу t_3 у кожний з вузлів решітки входять два шляхи. З них необхідно залишати лише один. Для цього, по кожному з двох шляхів розраховується сума ваг. Залишають шлях з найменшою сумою ваг. Якщо по кожному з шляхів сума ваг однакова, то залишають або верхній, або нижній шлях. При цьому, якщо залишили, наприклад, верхній шлях, то у подальшому у таких випадках завжди треба залишати верхній шлях. Для деякого моменту часу процес декодування слід вважати закінченим, якщо на цей момент часу залишився лише один шлях з усіх можливих. При декодуванні за алгоритмом Вітербі для однозначного прийняття рішення, його приймають з запізненням на 3-5К. Таким чином, декодер Вітербі у кожний момент часу не знає, у якому вузлі перебуває кодер, і не намагається його декодувати. Замість цього декодер по прийнятій послідовності визначає найбільш правдоподібний шлях до кожного вузла й визначає відстань між кожним таким шляхом і прийнятою послідовністю.

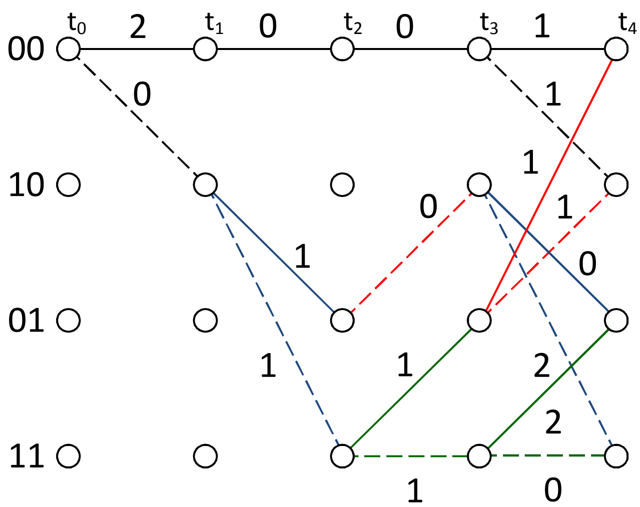
Приклад 2. Спотворимо отриману у прикладі 1 кодову комбінацію (2-й біт). Тоді спотворена кодова комбінація буде мати вигляд 11010001000011. Простежимо процес виправлення помилки за допомогою алгоритму Вітербі. Для виявлення єдиного шляху, що вижив, доповнимо задану інформаційну послідовність декількома нульовими бітами, тобто кодова комбінація буде мати вигляд 0000000011010001000011.

Розв’язок

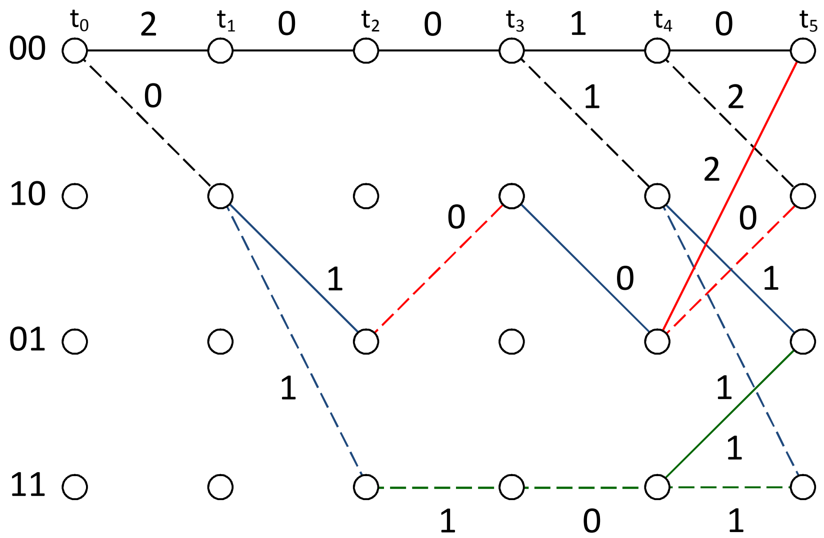
Зобразимо декодувальну решітку для кожного кроку декодування.



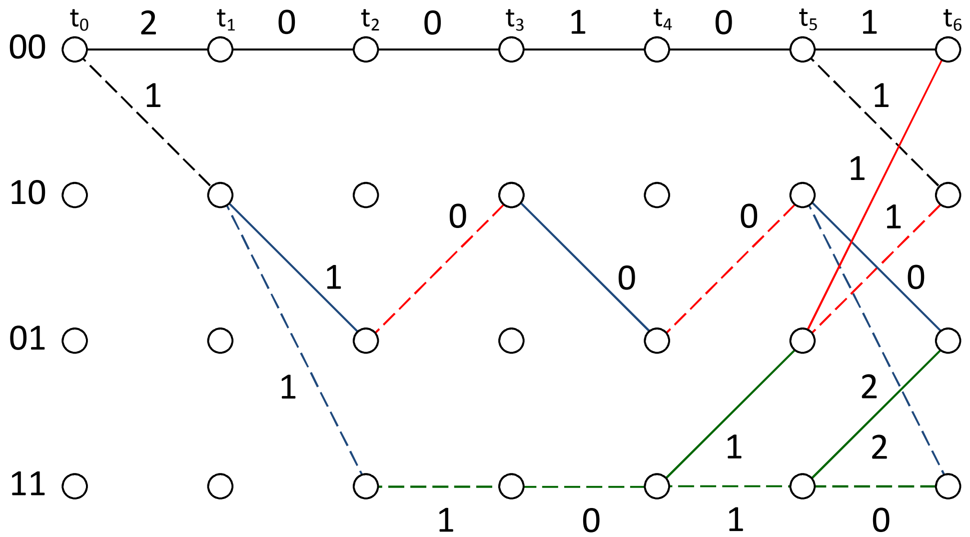
Крок 1 Крок 2 Крок 3



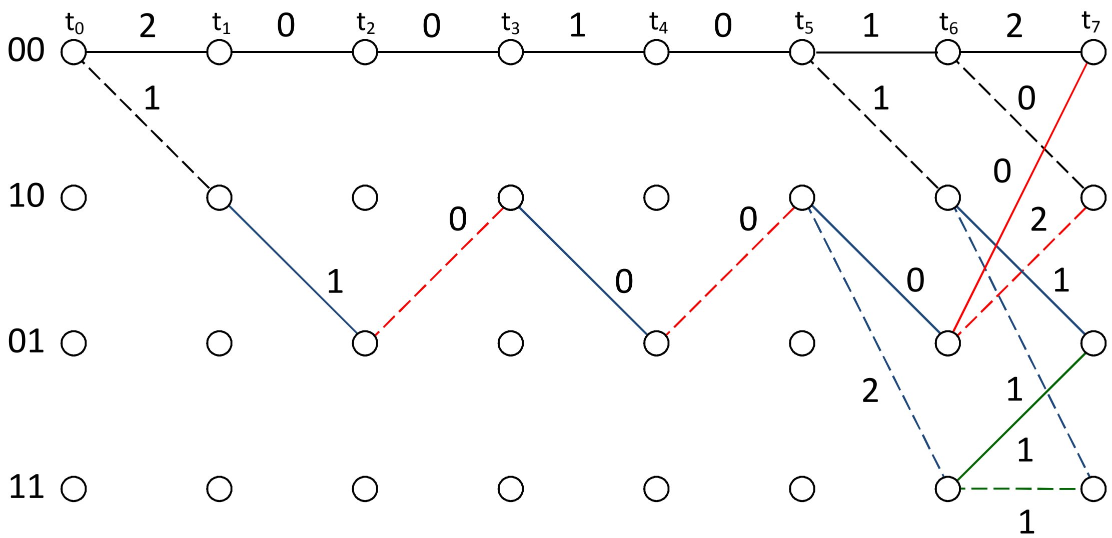
Крок 4



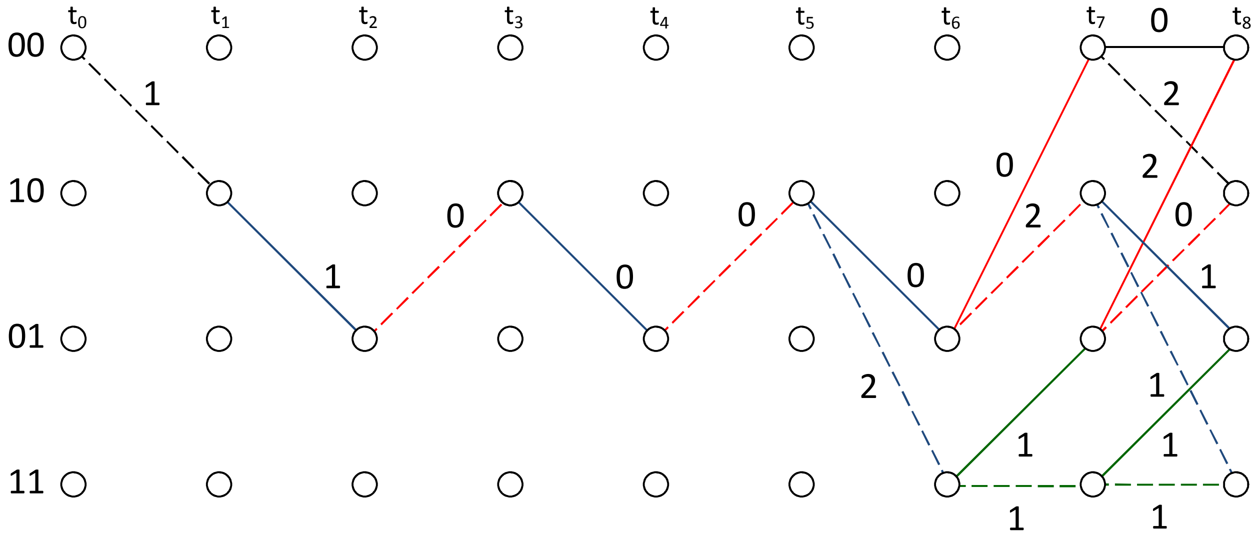
Крок 5



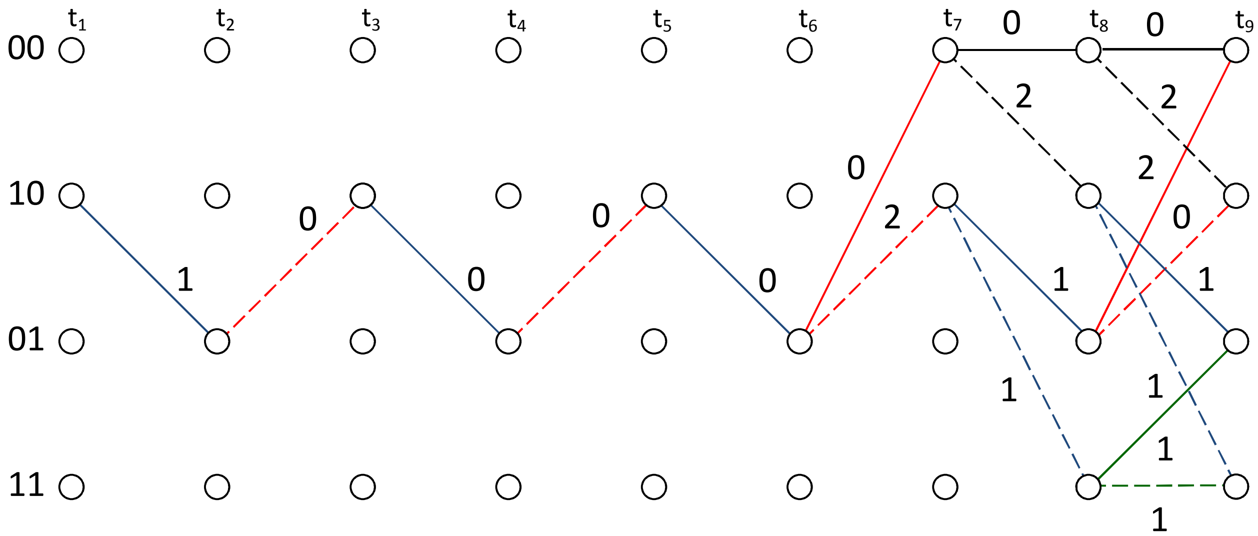
Крок 6



Крок 7

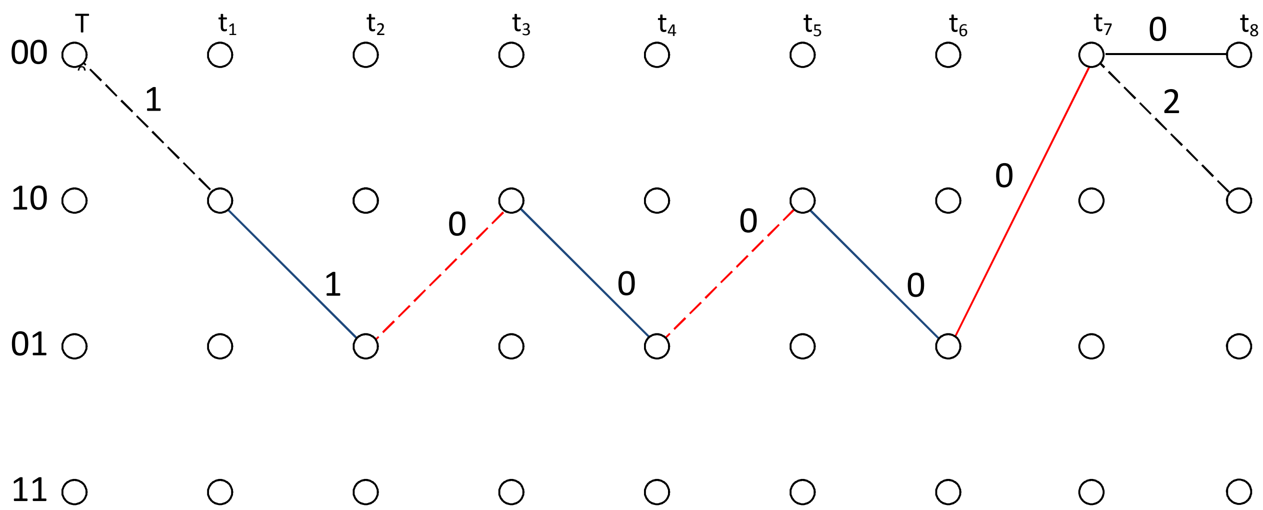


Крок 8



Крок 9

У результаті декодування отримаємо один шлях, що вижив



Виконуючи декодування відповідно решітці та шляху, що вижив отримаємо послідовність інформаційних біт на виході декодера

1010100….

Порівнюючи її з переданою послідовністю – бачимо, що помилка виправлена.

Задачі для самостійного виконання

Задача 1. Закодувати послідовність інформаційних біт 100111010111 завадостійким загортковим кодом з кодовим обмеженням К=3 та векторами зв’язку 111, 101.

Задача 2. Внести помилку у 4-й біт отриманої в результаті виконання задачі №1 кодової послідовності. Показати процес виправлення помилки.

Задача 3. Внести помилки у 2-й та 5-й біти отриманої в результаті виконання задачі №1 кодової послідовності. Показати процес виправлення помилок.

Перелік посилань

1. Блейхут Р. Теория и практика кодов, контролирующих ошибки.: Пер. С англ. – М.: Мир, 1986. – 576 с.

2. Скляр Бернард. Цифровая связь. Теоретические основы и практическое применение.: Пер. с англ. – М.: Издательский дом «Вильямс», 2003. – 1104 с.

Додаток А Елементи поля Галуа GF(2^4)

Елементи поля	Поліноміальне подання	У двійковому вигляді
0	0	0000
$a^0\ a^{15}\ a^{30}\ a^{45}$	1	0001
$a^1\ a^{16}\ a^{31}\ a^{46}$	z	0010
$a^2\ a^{17}\ a^{32}\ a^{47}$	z^2	0100
$a^3\ a^{18}\ a^{33}\ a^{48}$	z^3	1000
$a^4\ a^{19}\ a^{34}\ a^{49}$	z+1	0011
$a^5\ a^{20}\ a^{35}\ a^{50}$	z^2+z	0110
$a^6\ a^{21}\ a^{36}\ a^{51}$	z^3+z^2	1100
$a^7\ a^{22}\ a^{37}\ a^{52}$	z^3+z+1	1011
$a^8\ a^{23}\ a^{38}\ a^{53}$	z^2+1	0101
$a^9\ a^{24}\ a^{39}\ a^{54}$	z^3+z	1010
$a^{10}\ a^{25}\ a^{40}\ a^{55}$	z^2+z+1	0111
$a^{11}\ a^{26}\ a^{41}\ a^{56}$	z^3+z^2+z	1110
$a^{12}\ a^{27}\ a^{42}\ a^{57}$	z^3+z^2+z+1	1111
$a^{13}\ a^{28}\ a^{43}\ a^{58}$	z^3+z^2+1	1101
$a^{14}\ a^{29}\ a^{44}\ a^{59}$	z^3+1	1001

Додаток Б Породжуючі многочлени кодів БЧХ та Ріда-Соломона

Кількість помилок, що виправляє код	Породжуючий поліном
Коди БЧХ у полі GF(16)=GF(2^4)	
2	$g(x) = x^8 + x^7 + x^6 + x^4 + 1$
3	$g(x) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$
Код Ріда-Соломона у полі GF(16)	
2	$g(x) = x^4 + \alpha^{13}x^3 + \alpha^6 x^2 + \alpha^3 x + \alpha^{10}$

Електронне видання

МЕТОДИЧНІ ВКАЗІВКИ
до практичних занять з дисципліни
«ТЕОРІЯ ІНФОРМАЦІЇ ТА КОДУВАННЯ»

для студентів денної форми навчання спеціалізації
«Системи, технології та комп'ютерні засоби створення мультимедіа»

Упорядник: Зубков Олег Вікторович

Відповідальний випусковий В.М. Карташов

Авторська редакція