ЛЕКЦІЯ 6

Завадостійке кодування інформації

Від класифікації завад — до побудови та перевірки циклічних кодів.



Еварист Галуа · Évariste Galois

25.10.1811 — 31.05.1832
Французький математик, засновник сучасної алгебри.

ПОВІДОМЛЕННЯ 10

1	0	1	0

↓

ЦИКЛІЧНИЙ КОД

1	0	1	0	0	0	1

Інформаційні біти + перевірні біти

План лекції

01

Класифікація завад

Види завад, їхня фізична природа та способи боротьби з помилками.

02

Принципи завадостійкого кодування

Дозволені комбінації, кодова відстань, лінійні блокові коди.

03

Циклічні коди

Породжувальні поліноми, побудова коду та виправлення одиничної помилки.

Завада та її математична модель

ВИЗНАЧЕННЯ

Завада — сторонній вплив, що діє в системі передачі й заважає правильному прийому сигналів.

$$x = V(s, \xi)$$

ПОЗНАЧЕННЯ

s — повідомлення, яке передається;
ξ — завада;
x — прийняте повідомлення.

Джерела завад

Можуть знаходитися зовні або всередині системи передачі.

Характер впливу

Відомі регулярні завади простіше усувати; випадкові ускладнюють прийом.

Адитивна та мультиплікативна завади

АДИТИВНА ЗАВАДА

$$x = s + \xi$$

Оператор V вироджується в суму. Завада додається до сигналу; адитивну заваду часто називають шумом.

МУЛЬТИПЛІКАТИВНА ЗАВАДА

$$x = \nu \cdot s$$

Оператор V подається як добуток. Випадковий процес v(t) невід'ємний; заваду v називають мультиплікативною.

Завмирання каналу та змішана дія завад

Завмирання каналу

Якщо v змінюється повільно порівняно із s(t), явище, викликане мультиплікативною завадою, називають завмиранням каналу (федінг).

ШУМ І МУЛЬТИПЛІКАТИВНА ЗАВАДА РАЗОМ

$$x = \nu \cdot s + \xi$$

У загальному випадку оператор V не зводиться лише до суми або добутку. За одночасної дії двох завад вводять два випадкові процеси.

Фізична природа випадкових завад

ФЛУКТУАЦІЇ, ДРОБОВИЙ ЕФЕКТ І ТЕПЛОВИЙ ШУМ

Флуктуації — випадкові відхилення фізичних величин від їхніх середніх значень.

Дробовий ефект

У ланцюгах постійного струму виникають флуктуації струму, пов’язані з дискретною природою носіїв заряду — іонів та електронів.

Тепловий шум

Випадковий тепловий рух носіїв заряду створює різницю потенціалів на кінцях провідника. Її середнє дорівнює нулю, а середній квадрат пропорційний абсолютній температурі.

Квантова природа шуму і зміни каналу

ЩЕ ДВА ДЖЕРЕЛА ВИПАДКОВОГО ВПЛИВУ

Дискретне випромінювання

Електромагнітне випромінювання відбувається порціями — квантами, які називають фотонами.

На високих частотах шум, викликаний фотонною структурою випромінювання, може перевищувати інші завади.

Мультиплікативна завада

Її природа полягає у випадкових змінах параметрів каналу передачі.

Такі зміни можуть мати як лінійний, так і нелінійний характер.

Два способи боротьби з помилками

ВЗАЄМОДОПОВНЮВАЛЬНІ МЕТОДИ

Застосування кодів, що контролюють помилки, підвищує надійність передачі й обробки інформації.

Виправлення помилок

Приймач виявляє та виправляє помилки. Такі коди називають коректуючими.

Виявлення помилок

Приймач розпізнає помилки й за потреби запитує повторну передачу помилкового блока.

Повторна передача потребує каналу зворотного зв’язку. Цей підхід застосовують, зокрема, в обчислювальних мережах та інтернеті.

Теорема Шеннона для каналу із завадами

МОЖЛИВІСТЬ ДОСТОВІРНОЇ ПЕРЕДАЧІ

Джерело повільніше за канал

За продуктивності джерела, меншої за пропускну здатність каналу, існує спосіб кодування з як завгодно малою ймовірністю помилки.

Джерело перевищує місткість

Якщо продуктивність джерела більша за пропускну здатність каналу, такого способу кодування не існує.

Теорема встановлює теоретичну межу можливої ефективності системи достовірної передачі інформації.
(ТЕОРЕТИЧНА МЕЖА, А НЕ РЕЦЕПТ ПОБУДОВИ)

Теорема неконструктивна: вона встановлює принципову можливість надійної передачі, але не вказує, як будувати відповідні коди. Це стало основою пошуку конкретних завадостійких кодів.

Дозволені й заборонені комбінації

ОСНОВНА ІДЕЯ ЗАВАДОСТІЙКОГО КОДУВАННЯ

Для передачі використовують не всі можливі комбінації довжини n, а лише частину з них.

$$N_0 = m^n$$

$$N < N_0$$

ВИКОРИСТОВУЮТЬСЯ У КОДІ

Дозволені комбінації

НЕ ВИКОРИСТОВУЮТЬСЯ У КОДІ

Заборонені комбінації

Якщо помилка перетворює дозволене слово на інше дозволене слово, вона не виявляється.

Відстань Хеммінга та кодова відстань

МЕТРИКА

Чим більша відстань між дозволеними кодовими комбінаціями, тим більше помилок може виправляти код.

$$d_{ij} = \sum_{k=1}^{n} |x_{ik} - x_{jk}|$$

Для двійкового коду це кількість позицій, у яких слова відрізняються. Її визначають додаванням за модулем 2 і підрахунком одиниць.

d_{min}

Найменша відстань у коді

Приклад 1: визначення кодової відстані

УМОВА ТА ВСІ ШІСТЬ ПАР КОДОВИХ СЛІВ

$A_1 = 0000;\quad A_2 = 0011;\quad A_3 = 1100;\quad A_4 = 1010.$

Пара	Перше слово	Друге слово	Сума mod 2	Відстань
A_1, A_2	0000	0011	0011	2
A_1, A_3	0000	1100	1100	2
A_1, A_4	0000	1010	1010	2
A_2, A_3	0011	1100	1111	4
A_2, A_4	0011	1010	1001	2
A_3, A_4	1100	1010	0110	2

$$d_{min} = 2$$

Для кожної пари $d_{ij} = d_{ji}$.

Виявлення та виправлення помилок

Кратність помилок — кількість неправильно переданих символів у межах однієї кодової комбінації.

ВИЯВЛЕННЯ ПОМИЛОК

$$d_{min} \geq q_d + 1$$

Для виявлення одиничної помилки мінімальне значення $d_{min} = 2$.

ВИПРАВЛЕННЯ ПОМИЛОК

$$d_{min} \geq 2q_c + 1$$

Для виправлення одиничної помилки мінімальне значення $d_{min} = 3$.

Одночасне виявлення й виправлення

УМОВА

Для одночасного виправлення та виявлення помилок кодова відстань має задовольняти умову:

$$d_{min} \geq q_c + q_d + 1$$

$$q_d \geq q_c$$

Наведені вирази дають змогу будувати прості завадостійкі коди.

Дві спільні властивості завадостійких кодів

РІЗНІ СХЕМИ — СПІЛЬНІ ПРИНЦИПИ

01 Використання надмірності

Закодовані послідовності містять додаткові, або надмірні, символи.

Кількість символів у кодовій послідовності більша, ніж потрібно для однозначного подання повідомлення.

02 Властивість усереднення

Надмірні символи залежать від декількох інформаційних символів.

Інформація, що міститься в кодовій послідовності, перерозподіляється також на надмірні символи.

Імовірнісні та алгебраїчні коди

КЛАСИФІКАЦІЯ ЗА ЗАСАДАМИ ПОБУДОВИ

Імовірнісні

Здатність виявляти й виправляти помилки ґрунтується на визначенні ймовірності появи символів.

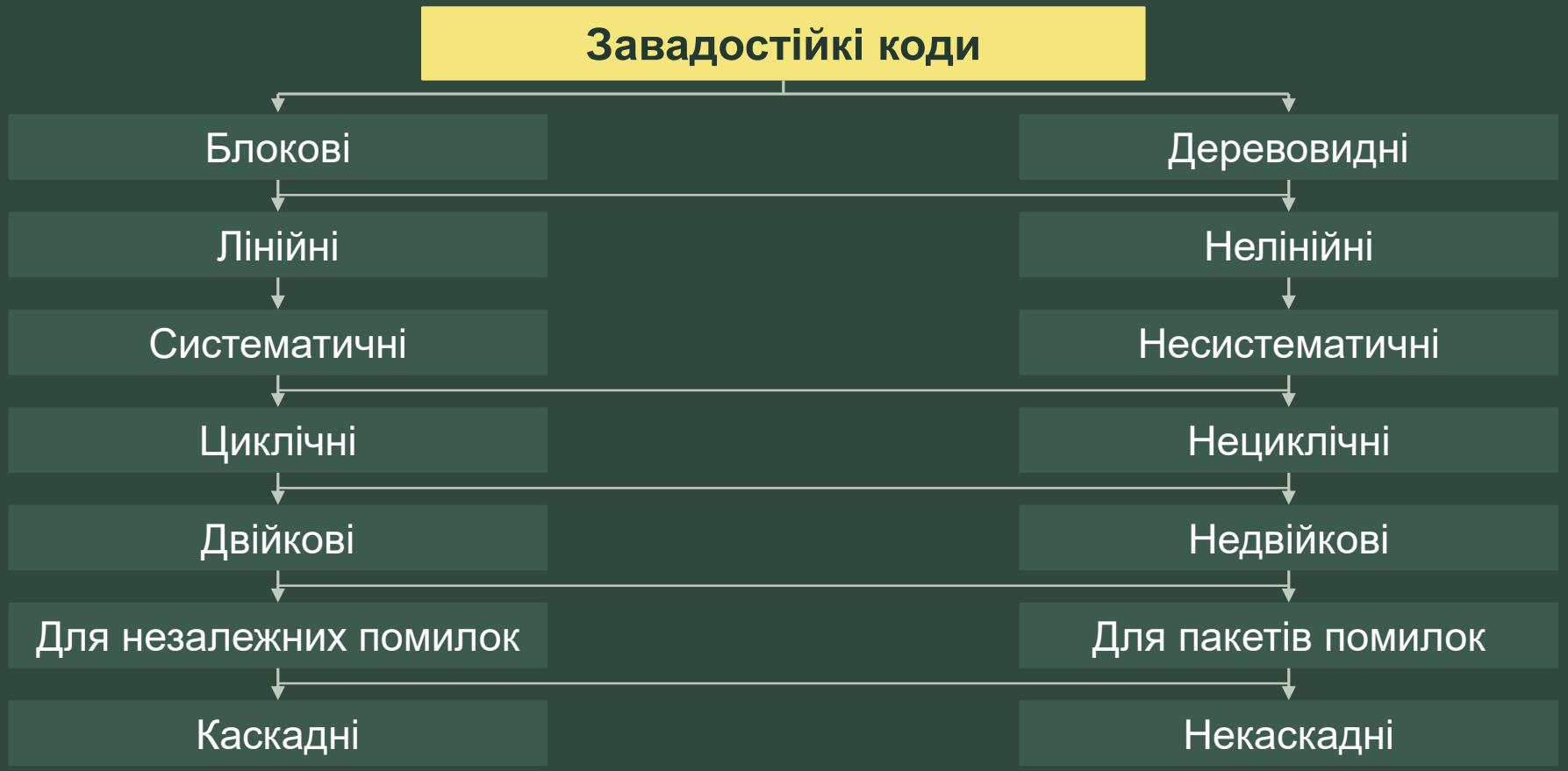
Приклад — коди Вагнера. Вони не знайшли широкого застосування.

Алгебраїчні

Здатність виявляти й виправляти помилки є властивістю алгебраїчної структури коду.

Алгебраїчні завадостійкі коди поділяють на блокові та деревовидні.

Класифікація завадостійких кодів



Основні характеристики завадостійких кодів

Характеристика	Позначення / вираз
Довжина коду	n
Довжина інформаційної послідовності	k
Довжина перевірної послідовності	$m = n - k$
Кодова відстань	d_{min}
Швидкість коду	$v = k / n$
Надмірність коду	$1 / v$
Імовірність виявлення помилки	$p_{вп}$
Імовірність невиявлення помилки (спотворення)	$p_{нв}$

Лінійний блоковий (n, k)-код

БІЛЬШІСТЬ ПРАКТИЧНИХ СХЕМ КОДУВАННЯ ҐРУНТУЮТЬСЯ НА ЛІНІЙНИХ КОДАХ

Інформаційну послідовність розбивають на повідомлення довжини k і відображають у кодові слова довжини n.

$$U = (u_1, u_2, \ldots, u_k) \longrightarrow C = (c_1, c_2, \ldots, c_n)$$

$$C = U \cdot G$$

2^k кодових слів утворюють k-вимірний підпростір V_k у n-вимірному векторному просторі V_n. Його породжує базис із k лінійно незалежних векторів. Ці вектори є рядками породжувальної матриці G.

Породжувальна матриця G

K ЛІНІЙНО НЕЗАЛЕЖНИХ РЯДКІВ • N СТОВПЦІВ

$$G = \begin{bmatrix} g_0 \\ g_1 \\ \vdots \\ g_{k-1} \end{bmatrix} = \begin{bmatrix} g_{0,0} & g_{0,1} & \cdots & g_{0,n-1} \\ g_{1,0} & g_{1,1} & \cdots & g_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k-1,0} & g_{k-1,1} & \cdots & g_{k-1,n-1} \end{bmatrix}$$

Рядки матриці — базисні вектори; множення U·G дає кодове слово C.

Індекси останнього рядка узгоджено з позначенням g_{k-1}.

Матриця циклічного коду

ЗСУНУТІ РЯДКИ

$$G = \begin{bmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_{n-k} \end{bmatrix}$$

Для компактного запису циклічного (n, k)-коду використовують породжувальний, або твірний, поліном g(x) степеня n − k.

Твірний поліном і кодування повідомлення

КОЕФІЦІЄНТИ ПОЛІНОМА — З ПОЛЯ GF(Q)

$$g(x) = g_0 + g_1 x + g_2 x^2 + \ldots + g_{n-k} x^{n-k}$$

Якщо інформаційне повідомлення подати поліномом U(x), кодове слово утворюють множенням на породжувальний поліном:

$$C(x) = U(x)g(x)$$

Три способи записати твірний поліном

ПОЛІНОМ → ДВІЙКОВИЙ / ВІСІМКОВИЙ ЗАПИС → СТЕПЕНІ

$$g(x) = 1 + x + x^4 + x^6$$

КОЕФІЦІЄНТИ ЯК ДВІЙКОВЕ СЛОВО

$$g = 1010011_2 = 123_8$$

СТЕПЕНІ З НЕНУЛЬОВИМИ КОЕФІЦІЄНТАМИ

$$g = (0,1,4,6)$$

Коефіцієнти об’єднують у двійкове слово або перелічують степені при ненульових коефіцієнтах.

Двійкове поле Галуа GF(2)

ОПЕРАЦІЇ ЗА МОДУЛЕМ 2

Поле — множина математичних об’єктів із операціями додавання, віднімання, множення та ділення. Скінченне поле називають полем Галуа.

GF(2) містить два елементи: 0 та 1. Дії у двійкових кодах виконують за модулем 2.

$$1 + 1 = 0, \quad 1 = -1$$

$$1 + 1 = 1 - 1, \quad 1:1 = 1$$

a	b	a + b	a · b
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1

До GF(2) застосовують методи лінійної алгебри, зокрема матричні операції.

Структура систематичного (n, k)-коду

ІНФОРМАЦІЙНА ТА ПЕРЕВІРНА ЧАСТИНИ

Лінійний двійковий блоковий код містить 2^k слів, які утворюють k-вимірний підпростір у просторі n-послідовностей поля GF(2).

НЕЗМІННА ІНФОРМАЦІЙНА ЧАСТИНА + НАДМІРНА ПЕРЕВІРНА ЧАСТИНА



Коди з перевіркою на парність (непарність)

ВИСОКА ШВИДКІСТЬ • ВИЯВЛЕННЯ ОДИНИЧНОЇ ПОМИЛКИ

До k інформаційних бітів додають (k + 1)-й біт так, щоб загальна кількість одиниць у слові була парною.

$$u_{k+1} = u_1 + u_2 + \ldots + u_k$$

Знак «+» тут означає додавання за модулем 2. Це (k + 1, k)-код або (n, n − 1)-код.

Кодова відстань дорівнює 2: одиничні помилки виявляються, але не виправляються.

$$u_1 + u_2 + \ldots + u_k + u_{k+1} = 1$$

За одиничної помилки кількість одиниць стає непарною — перевірна сума дорівнює 1.

Прості коди з повторенням

НИЗЬКА ШВИДКІСТЬ • ВИСОКІ КОРЕГУВАЛЬНІ ХАРАКТЕРИСТИКИ

Інформаційний символ повторюється n разів, зазвичай n непарне. Це (n, 1)-коди.

$$0 \to 000$$

$$1 \to 111$$

ДЛЯ (3, 1)-КОДУ ВІДСТАНЬ ДОРІВНЮЄ 3

$$q_d = \frac{n-1}{2} = \frac{3-1}{2} = 1$$

У цій формулі позначення q_d - кількість виправлюваних помилок.

Приклад: побудова коду з перевіркою на парність

ПОВІДОМЛЕННЯ A_1, A_2, A_3, A_4 • K = 2

Початкові комбінації: 00, 01, 10, 11. Сформуємо перевірний біт.

Символ	Інформаційні біти	Біт парності	Нове кодове слово
A_1	00	$0 \oplus 0 = 0$	000
A_2	01	$0 \oplus 1 = 1$	011
A_3	10	$1 \oplus 0 = 1$	101
A_4	11	$1 \oplus 1 = 0$	110

До двох інформаційних бітів дописано третій — перевірний.

Перевірка відстані для коду парності

УСІ ПОПАРНІ СУМИ ЗА МОДУЛЕМ 2

Перша комбінація	Друга комбінація	Сума mod 2	Кількість одиниць
000	011	011	2
000	101	101	2
000	110	110	2
011	101	110	2
011	110	101	2
101	110	011	2

$$d_{min} = 2$$

Дві помилки можуть перетворити слово на інше дозволене слово з парною кількістю одиниць. Тоді вони не виявляються.

Циклічні коди

ПОЛЯ ГАЛУА, РЕГІСТРИ ЗСУВУ ТА АЛГЕБРАЇЧНА СТРУКТУРА

Циклічні коди були розроблені Хаффманом у середині 1950-х років на основі теорії полів Галуа двійкових багаточленів $GF(2^n)$. Коефіцієнти $c_i \in \{0, 1\}$; додавання виконують за модулем 2.

Просте кодування

Операції виконуються з використанням регістрів зсуву.

Ефективне декодування

Алгебраїчна структура дозволяє знаходити прості способи декодування.

До таких кодів належать коди Боуза–Чоудхурі–Хоквінгема (БЧХ) та Ріда–Соломона (РС).

Циклічний зсув кодової комбінації

ЗСУВ УЛІВО З ПЕРЕНОСОМ СТАРШОГО РОЗРЯДУ В МОЛОДШИЙ

ВИХІДНЕ СЛОВО							ПЕРШИЙ ЗСУВ							ДРУГИЙ ЗСУВ						
1	1	0	0	1	0	1	1	0	0	1	0	1	1	0	0	1	0	1	1	1

Кодову комбінацію можна записати як багаточлен фіктивної змінної x:

$$F(x) = c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \ldots + c_1x^1 + c_0x^0$$

Коефіцієнти c набувають значень 1 або 0 відповідно до символів кодової комбінації

Властивості циклічних (n, k)-кодів

СТЕПІНЬ ПОЛІНОМА ТА ТВІРНИЙ ПОЛІНОМ

Степінь кожного ненульового кодового полінома — від n−k до n−1.

Існує лише один кодовий поліном степеня n − k — породжувальний поліном коду:

$$g(x) = 1 + g_1 x + g_2 x^2 + \ldots + g_{n-k} x^{n-k}$$

КОЖНЕ ЗАКОДОВАНЕ СЛОВО — КРАТНЕ G(X)

$$u(x) = m(x) \cdot g(x)$$

Перевірний поліном h(x)

ВЛАСТИВІСТЬ ПОДІЛЬНОСТІ

Породжувальний поліном циклічного коду ділить двочлен $x^n + 1$ без залишку.

$$x^n + 1 = g(x)h(x) + 0$$

Поліном h(x) — частка від ділення $x^n + 1$ на g(x); його називають перевірним поліномом. Поліноми h(x) і g(x) однозначно пов’язані. За допомогою перевірного полінома також можна проводити кодування, тобто h(x) теж визначає код.

Поліномний запис циклічних зсувів

ДОДАВАННЯ, ВІДНІМАННЯ, МНОЖЕННЯ ТА ДІЛЕННЯ ДВІЙКОВИХ ПОЛІНОМІВ

$$F_1(x) = x^6 + x^5 + x^2 + 1 \leftrightarrow 1100101$$

$$F_2(x) = F_1(x) \cdot x = x^6 + x^3 + x + 1$$

$$F_3(x) = x^4 + x^2 + x + 1$$

$$F_1(x) + F_2(x) = x^5 + x^3 + x^2 + x \leftrightarrow 0101110$$

При зсуві враховується перенесення старшого розряду: $x^{n-1} \cdot x = x^0 = 1$.

Побудова систематичного циклічного коду

ПОВІДОМЛЕННЯ G(X) • ПОРОДЖУВАЛЬНИЙ ПОЛІНОМ P(X) СТЕПЕНЯ R

01 ДОПИСУЄМО R РОЗРЯДІВ І ДІЛИМО НА P(X)

$$[G(x) \cdot x^r] : P(x)$$

ЧАСТКА

$Q(x)$

ЗАЛИШОК

$R(x)$

02 ДОДАЄМО ЗАЛИШОК ЗА МОДУЛЕМ 2

$$F(x) = G(x) \cdot x^r \oplus R(x)$$

Частку та залишок показано окремо; в оригіналі цей крок записано як Q(x) + R(x).

Таблиця поліномів: степені 1–4

«ПОЛІНОМИ, ЩО НЕ ПРИВОДЯТЬСЯ» • ЧАСТИНА 1/2

Степінь r	Поліном P(x)	$n = l = 2^r - 1$
1	$x + 1$	1
2	$x^2 + x + 1$	3
3	$x^3 + x^2 + 1$ $x^3 + x + 1$	7
4	$x^4 + x + 1$ $x^4 + x^3 + 1$ $x^4 + x^3 + x^2 + x + 1$	15

Степінь твірного полінома визначає кількість перевірних розрядів r.

Таблиця поліномів: степінь 5

«ПОЛІНОМИ, ЩО НЕ ПРИВОДЯТЬСЯ» • ЧАСТИНА 2/2

r	Поліном P(x)	$n = l = 2^r - 1$
5	$x^5 + x^2 + 1$	31
5	$x^5 + x^3 + 1$	31
5	$x^5 + x^4 + x^2 + 1$	31
5	$x^5 + x^3 + x^2 + x + 1$	31
5	$x^5 + x^4 + x^2 + x + 1$	31
5	$x^5 + x^4 + x^3 + x + 1$	31
5	$x^5 + x^4 + x^3 + x^2 + 1$	31

Кодовий запис породжувальних поліномів

ДВІЙКОВІ КОМБІНАЦІЇ ТА ЇХНІ ПОЛІНОМИ

Код	Поліном
11	$x + 1$
101	$x^2 + 1$
111	$x^2 + x + 1$
1001	$x^3 + 1$
1011	$x^3 + x + 1$
1101	$x^3 + x^2 + 1$
1111	$x^3 + x^2 + x + 1$

Код	Поліном
10001	$x^4 + 1$
10011	$x^4 + x + 1$
10101	$x^4 + x^2 + 1$
10111	$x^4 + x^2 + x + 1$
11001	$x^4 + x^3 + 1$
11011	$x^4 + x^3 + x + 1$
11111	$x^4 + x^3 + x^2 + x + 1$

Перевірка прийнятої комбінації

ДЕКОДЕР • ПЕРЕВІРКА ЗАЛИШКУ

Прийняту кодову комбінацію $\hat{F}(x)$ ділять на породжувальний поліном $P(x)$.

$$\hat{F}(x) : P(x) \rightarrow Q^{*}(x), R^{*}(x)$$

$R^{*}(x) = 0$

Комбінація прийнята правильно або помилка не виявляється, якщо кількість спотворених символів перевищує $g = 1$.

$R^{*}(x) \neq 0$

Виявлено помилку. Необхідно визначити спотворений розряд і виправити комбінацію.

У джерелі результати ділення записано як $Q^{*}(x) + R^{*}(x)$; тут їх подано як частку та залишок.

Приклад 1: кодова комбінація повідомлення

ЦИКЛІЧНИЙ КОД, ЩО ВИПРАВЛЯЄ ОДИНИЧНІ ПОМИЛКИ

У радіосистемі передають M елементарних повідомлень. Потрібно визначити кодову комбінацію для повідомлення за номером 10, якщо M = 16.

КІЛЬКІСТЬ ІНФОРМАЦІЙНИХ СИМВОЛІВ

$$k = \log_2 16 = 4$$

КІЛЬКІСТЬ КОНТРОЛЬНИХ СИМВОЛІВ

$$2^r - 1 \geq 4 + r, \quad r = 3$$

Використовуємо чотири інформаційні та три контрольні символи.

Приклад 1: підготовка до кодування

G(X), P(X) ТА ЗАЛИШОК R(X)

ПОВІДОМЛЕННЯ ЗА НОМЕРОМ 10

1	0	1	0

$$G(x) = x^3 + x$$

ДЛЯ R = 3 ОБИРАЄМО ПОРОДЖУВАЛЬНИЙ ПОЛІНОМ

$$P(x) = x^3 + x^2 + 1$$

$$F(x) = G(x) \cdot x^r \oplus R(x)$$

R(x) — залишок від ділення $G(x)\cdot x^r$ на P(x).

Приклад 1: ділення за модулем 2

ПОЛІНОМНЕ ДІЛЕННЯ • УСІ ПРОМІЖНІ КРОКИ

$$G(x) \cdot x^r = (x^3 + x) \cdot x^3 = x^6 + x^4$$

$$\begin{array}{l|l}
x^6 + x^4 & x^3 + x^2 + 1 \\
\oplus\ x^6 + x^5 + x^3 & \hline
\quad x^5 + x^4 + x^3 & x^3 + x^2 + 1 \\
\quad \oplus\ x^5 + x^4 + x^2 & \\
\hline
\qquad x^3 + x^2 & \\
\qquad \oplus\ x^3 + x^2 + 1 & \\
\hline
R(x) = 1 &
\end{array}$$

РЕЗУЛЬТАТ

$$R(x) = 1$$

Усі додавання та віднімання виконуються за модулем 2.

Приклад 1: готове кодове слово

ПІДСУМОК КОДУВАННЯ

$$F(x) = x^6 + x^4 + 1$$

ІНФОРМАЦІЙНІ БІТИ / ПЕРЕВІРНІ БІТИ

1	0	1	0	0	0	1

1010 001

Для повідомлення 10 отримано комбінацію 1010001.

Приклад 2: перевірка прийнятого повідомлення

N = 7 • ВИЯВЛЕННЯ ТА ВИПРАВЛЕННЯ ОДИНИЧНОЇ ПОМИЛКИ

Прийнято кодову комбінацію 1110001. Перевірити правильність прийому і за необхідності виправити її.

ПРИЙНЯТА КОМБІНАЦІЯ

1	1	1	0	0	0	1

ПОРОДЖУВАЛЬНИЙ ПОЛІНОМ

$$P(x) = x^3 + x^2 + 1$$

$$\widehat{F}(x) = x^6 + x^5 + x^4 + 1$$

Приклад 2: виявлення помилки

ДІЛЕННЯ ПРИЙНЯТОГО ПОЛІНОМА НА P(X)

$$
\begin{array}{rl|l}
 & x^6 + x^5 + x^4 \quad + 1 & x^3 + x^2 + 1 \\
\oplus & x^6 + x^5 \quad + x^3 & x^3 + x \\
\hline
 & x^4 + x^3 \quad + 1 & \\
\oplus & x^4 + x^3 \quad + x & \\
\hline
 & R^*(x) = x + 1 &
\end{array}
$$

ЗАЛИШОК

$$x + 1$$

Залишок ненульовий: у слові є помилка.

$$R^*(x) = x + 1 \neq 0$$

Приклад 2: вектор помилки

ПОШУК СПОТВОРЕНОГО РОЗРЯДУ

Щоб виправити помилку, необхідно знайти вектор помилки та додати його до прийнятої комбінації за модулем 2.

$$E(x) = x^i, \quad i = 0,\ldots,n-1$$

$$\hat{F}(x) \oplus E(x) = F(x)$$

ПОРІВНЯННЯ З ЕТАЛОННИМ ЗАЛИШКОМ

Знаходимо еталонний залишок, що відповідає помилці в першому — старшому — розряді кодової комбінації. Для цього ділимо відповідний вектор помилки E(x) на P(x).

Приклад 2: еталонний залишок

Оцінка помилки в першому (старшому) розряді • $E(X) = X^6$

$$
\begin{array}{l|l}
x^6 & x^3 + x^2 + 1 \\
\oplus\ x^6 + x^5 + x^3 & x^3 + x^2 + x \\
\hline
x^5 + x^3 & \\
\oplus\ x^5 + x^4 + x^2 & \\
\hline
x^4 + x^3 + x^2 & \\
\oplus\ x^4 + x^3 + x & \\
\hline
\end{array}
$$

$$R_{ет}(x) = x^2 + x$$

ЕТАЛОН

$$x^2 + x$$

Цей залишок фіксуємо для подальшого порівняння.

Приклад 2: порівняння та перший зсув

ПОМИЛКА НЕ В ПЕРШОМУ РОЗРЯДІ

$$R_1^*(x) \oplus R_{ет}(x) = (x + 1) \oplus (x^2 + x) = x^2 + 1$$

Залишок не збігається. Зсуваємо прийняте слово на один розряд справа наліво і знову ділимо на P(x).



$$\hat{F}(x) \cdot x = x^6 + x^5 + x + 1$$

Приклад 2: перевірка після зсуву

ЗАЛИШОК ЗІСТАВЛЯЄМО З ЕТАЛОННИМ

$$
\begin{array}{rl|l}
 & x^6 + x^5 + x + 1 & x^3 + x^2 + 1 \\
\hline
\oplus & x^6 + x^5 + x^3 & x^3 + 1 \\
\hline
 & x^3 + x + 1 & \\
\oplus & x^3 + x^2 + 1 & \\
\hline
 & x^2 + x &
\end{array}
$$

$$R_2^*(x) = x^2 + x$$

ЗБІГ

$$x^2 + x$$

Отриманий залишок дорівнює еталонному.

$$R_2^*(x) \oplus R_{ет}(x) = (x^2 + x) \oplus (x^2 + x) = 0$$

Приклад 2: локалізація помилки

КІЛЬКІСТЬ ЗСУВІВ + 1 = НОМЕР СПОТВОРЕНОГО РОЗРЯДУ

ПРИЙНЯТЕ СЛОВО • ВІДЛІК ЗЛІВА

1	1	1	0	0	0	1

Помилка у другому розряді

Рівність еталонного й одержаного залишків досягнута після одного зсуву. Якщо рівність не досягнута, зсув і ділення продовжують до збігу.

Висновки:

Завади поділяють на адитивні та мультиплікативні.
Один зі способів боротьби з ними — застосування завадостійких кодів.

принципи завадостійкого кодування:

Надмірність

Додаткові символи у складі кодової комбінації.

Дозволені комбінації

Використання дозволених і заборонених кодових слів.

Кодова відстань

Спеціальна метрика Хеммінга для оцінювання відмінностей.

Висновки: параметри та циклічні коди

КОДОВЕ СЛОВО = ІНФОРМАЦІЙНА ЧАСТИНА + КОНТРОЛЬНА ЧАСТИНА

Параметр	Позначення
Довжина коду	n
Інформаційна послідовність	k
Перевірна послідовність	m = n − k
Кодова відстань	d_{min}
Швидкість коду	v = k/n
Надмірність коду	1/v

Кодові слова містять інформаційну та контрольну складові.

Комбінації циклічного коду утворюються за допомогою твірних поліномів.

$$F(x) = G(x)x^r \oplus R(x)$$