

Міністерство освіти і науки, молоді та спорту України
Українська інженерно – педагогічна академія,
Полтавський національний технічний університет
імені Юрія Кондратюка

Теорія інформації та кодування

*Підручник для студентів вищих навчальних
закладів*

Під загальною редакцією
В. І. Барсова

Полтава – 2011

ББК 32.973.2
УДК 621.391
0-75

Затверджено
Міністерством освіти і науки України як підручник для студентів
вищих навчальних закладів. Лист № 1.4/18-Г-1394 від
11.06.2008 року.

Рецензенти:

О. Ю. Соколов, доктор техн. наук, професор, зав. кафедри інформатики Національного аерокосмічного університету ім. М. С. Жуковського ("ХАІ");

І. О. Фурман, доктор техн. наук, професор, зав. кафедри автоматизації та комп'ютерних технологій Харківського національного технічного університету сільського господарства ім. Петра Василенка.

0-75 В. І. Барсов, В. А. Краснобаєв,

З. В. Барсова, О. І. Тиртишніков, І. В. Авдєєв.

Теорія інформації та кодування / Під загальною редакцією В. І. Барсова:
Підручник для студентів ВНЗ. - Полтава: 2011. – 320 с.

Наведено теоретичні відомості з теорії інформації та кодування щодо систем обробки інформації та управління. Розглянуто основні математичні моделі сигналів та перешкод, моделі каналів зв'язку. Окремо розглянуте перешкодостійке кодування даних у системах обробки інформації та управління. Також розглянуто кодування даних у модулярній системі числення. Дано перелік контрольних питань. Також наведено завдання для самостійного розв'язання.

Підручник призначений для студентів та аспірантів інженерних, інженерно - педагогічних спеціальностей вищих навчальних закладів України і наукових працівників в галузі управління та зв'язку.

ISBN

© Барсов В. І., Краснобаєв В. А., Барсова З. В., Тиртишніков О. І.,
Авдєєв І. В. 2011

© Українська інженерно – педагогічна академія 2011

© Полтавський національний технічний університет
імені Юрія Кондратюка 2011

Зміст

Передмова	6
Розділ 1.	
Загальні поняття теорії інформації	12
1.1. Загальні поняття та визначення теорії ймовірностей.....	12
1.2. Поняття інформації, ентропії, повідомлення та сигналу.....	16
1.3. Системи передачі інформації.....	26
1.3.1. Класифікація систем передачі інформації. Модель системи передачі інформації.....	26
1.3.2. Основні характеристики систем передачі інформації.....	29
1.3.3. Статистичне трактування процесу передачі інформації.....	32
1.3.4. Спотворення та перешкоди у каналах зв'язку.....	34
1.4. Контрольні питання.....	36
Розділ 2.	
Ентропія та інформація джерел повідомлень	38
2.1. Кількісна міра оцінки інформації, що передається по каналу зв'язку.....	38
2.2. Міра оцінки кількості інформації за Р. Хартлі.....	42
2.3. Міра оцінки кількості інформації за К. Шенноном (Бернуллі).....	46
2.4. Міра оцінки кількості інформації за А. А. Марковим.....	48
2.5. Основні властивості інформації та ентропії.....	58
2.6. Інформаційні характеристики джерел дискретних повідомлень.....	63
2.7. Приклади кількісної оцінки ентропії та інформації у повідомленні.....	67
2.8. Ентропія джерел неперервних повідомлень.....	69
2.9. Контрольні питання.....	76
Розділ 3.	
Види сигналів, що використовуються у системах обробки інформації та управління	78
3.1. Основні математичні моделі сигналів та перешкод.....	78
3.2. Форми представлення сигналів.....	90
3.3. Дискретизація сигналів за часом і за рівнем. Теорема В. О. Котельникова.....	96
3.4. Основні види випадкових процесів, що протікають у СОГУ.....	107
3.5. Енергетичний спектр сигналу.....	111

3.6. Спектральне подання дискретизованих сигналів.....	118
3.7. Особливості процесу дискретизації сигналів.....	120
3.8. Контрольні питання.....	126

Розділ 4.

Види та моделі каналів зв'язку у системах обробки інформації та управління

4.1. Моделі каналів зв'язку.....	127
4.1.1. Класифікація каналів зв'язку	127
4.1.2. Модель дискретного каналу зв'язку.....	130
4.1.3. Модель неперервного каналу зв'язку.....	133
4.1.4. Канали передачі інформації зі змінними параметрами.....	137
4.2. Пропускна здатність каналів зв'язку.....	139
4.2.1. Оцінка кількості інформації та пропускна здатність дискретного каналу зв'язку.....	139
4.2.2. Оцінка кількості інформації та пропускна здатність неперервного каналу зв'язку.....	150
4.3. Методи ефективного кодування інформації у каналах зв'язку... ..	157
4.3.1. Узгодження джерел інформації з каналами зв'язку.....	157
4.3.2. Ефективне кодування Шеннона – Фано.....	159
4.3.3. Ефективне кодування Хаффмана.....	161
4.4. Контрольні питання.....	163

Розділ 5.

Перешкодостійке кодування даних у системах обробки інформації та управління.....

5.1. Основні поняття та визначення перешкодостійкого кодування. Класифікація перешкодостійких кодів.....	164
5.2. Основні принципи та характеристики перешкодостійкого кодування.....	167
5.3. Лінійні групові перешкодостійкі коди.....	176
5.4. Коди Хеммінга.....	186
5.5. Лінійні циклічні перешкодостійкі коди.....	190
5.6. Згортувальні перешкодостійкі коди	215
5.7. Підвищення достовірності передачі та обробки інформації в СОІУ з безнадмірним кодуванням.....	225
5.8. Контрольні питання	235

Розділ 6.

Кодування даних у модулярній системі числення.....	237
6.1. Загальні відомості про МСЧ.....	237
6.2. Основні властивості порівнянь.....	244
6.3. Реалізація модульних операцій у МСЧ.....	251
6.4. Реалізація немодульних операцій у МСЧ.....	260
6.5. Модулярні обчислення.....	263
6.6. Функціональне кодування.....	268
6.7. Контрольні питання.....	271
Додатки.....	272
Додаток А. Приклади розв'язання завдань. Задачі для самостійного розв'язання.....	272
Додаток Б. Двійкові логарифми чисел від 1 до 128.....	306
Додаток В. Значення двійкових логарифмів чисел виду $-p \log_2 p$	307
Додаток Д. Розподіл ймовірностей появи літер російського алфавіту.....	312
Додаток Е. Розподіл ймовірностей появи літер українського алфавіту.....	313
Додаток Ж. Розподіл ймовірностей появи літер англійського алфавіту.....	314
Додаток К. Загальнонаукові поняття та визначення теорії інформації.....	315
Література.....	319

Передмова

Взаємодія людини з зовнішнім середовищем відбувається на основі процесів передачі, прийому, переробки, представлення, зберігання та використання інформації. Саме тому сучасний стан і подальший розвиток промисловості України в значній мірі залежить від розвитку та впровадження інформаційних технологій інформаційно-управляючих систем (ІУС), засобів та пристроїв обробки та передачі інформації.

Під поняттям інформації будемо розуміти сукупність відомостей про будь які явища природи, процеси, системи, об'єкти та ін., тобто, те, що людина отримує у результаті взаємодії з навколишнім світом. У подальшому ми будемо розглядати тільки технічні аспекти інформаційних процесів, що протікають у ІУС.

Теорія і практика обробки та передачі інформації склалися протягом багатьох років. Спроби кількісного виміру інформації здійснювалися неодноразово. Перші виразні пропозиції про загальні способи виміру кількості інформації були зроблені Р. Фішером (1921 р.) у процесі рішення питань математичної статистики.

Проблемами зберігання інформації, передачі її по каналах зв'язку й завданнями визначення кількості інформації займалися Р. Хартлі (1928 р.) і Х. Найквіст (1924 р.).

В 1928 р. Р. Хартлі зв'язав кількість інформації із числом станів фізичної системи. Оскільки він працював інженером у телеграфній компанії, він міркував про кількість інформації, що міститься в телеграфному тексті. Р. Хартлі заклав основи теорії інформації, визначивши логарифмічну міру кількості інформації.

Для того, щоб застосувати математичні засоби для вивчення інформації, у статистичному підході, на відміну від семантичного, треба було відволіктися від змісту інформації. Цей підхід був загальним для згаданих дослідників, тому що чиста математика оперує з кількісними співвідношеннями, не вдаючись у фізичну природу тих об'єктів, за якими стоять відповідні співвідношення.

Значний вклад у розробку загальної теорії інформації було зроблено роботою знаменитого радянського вченого академіка В. О. Котельникова "Про пропускну здібність «ефіру» і дроту" (1933 р.). В 1947 році ним була розроблена фундаментальна теорія потенційної завадостійкості. Ця теорія дала інженерам інструмент для синтезу оптимальних пристроїв обробки прийнятих сигналів на фоні шумів і перешкод, на її основі були розроблені методи оцінки якості прийому аналогових і цифрових сигналів у різних каналах зв'язку. З виникненням цієї теорії з'явилася можливість створення

оптимальних систем зв'язку на твердій теоретичній основі, а не на невизначених інтуїтивних поданнях, як це було до її створення.

У загальному випадку теорія інформації, як наука, що вивчає поняття інформації, її передачу, прийом, обробку, представлення, зберігання та використання, складає один з головних розділів кібернетики. Книга Н. Вінера "Кібернетика", що вийшла в 1947 році дала ім'я відповідній науці. У книзі автор звернув увагу читачів на те, що в загальному значенні доцільно розглядати наступні цеглини світобудови - елементи, пристрої, системи, зв'язки, управління й інформацію. Перші три "цеглини" утворюють довільну структуру, четверта характеризує її цілісність, п'ята - функції, що виконуються, а шоста - призначення. Норберт Вінер визначив кібернетику, як математичну науку про процеси управління у технічних системах, у суспільстві та у живій природі.

Датою народження теорії інформації вважається 1948 рік - рік появи основної статті Клода Шеннона "Математична теорія зв'язку". Його роботи "Математична теорія зв'язку" і "Теорія зв'язку в секретних системах" поклали початок теорії інформації й криптографії в її сучасному розумінні. Шеннон у цих роботах увів поняття, що описують довільні системи зв'язку. Серед них найбільш важливі поняття схеми зв'язку, у тому числі й секретної, і її компонентів (джерела інформації й шуму, повідомлення, сигнали канали й ін.) разом з їхніми характеристиками (пропускна здатність, ентропія, як міра невизначеності джерела повідомлень, кількість інформації в повідомленні, надійність шифрування й ін.). Він ввів в розгляд статистичну структуру повідомлень, довів ряд важливих теорем, зокрема, з оптимальних методів кодування, при яких забезпечується гранично досяжна швидкість передачі інформації по каналу зв'язку.

На основі теорії розробленої вченими Н. Вінером та К. Шенноном склалося розуміння поняття інформації як повідомлення чи сигналу, що формуються у результаті взаємодії джерела повідомлень (інформації) (ДП), каналу зв'язку (КЗ) та приймача повідомлень (ПП). У цьому випадку цінність інформації (як однієї з її характеристик) не залежить від її сенсу, а залежить тільки від таких факторів, як, наприклад, вірогідність та час її доставки від ДП до ПП, ймовірність перекручення повідомлення при його передачі по КЗ та ін.

Великий внесок у розвиток теорії інформації внесли також видатні радянські математики А. М. Колмогоров і О. Я. Хінчін. До середини 50 - х р.р. саме Андрій Миколайович Колмогоров запропонував найбільш загальне визначення кількості інформації в імовірнісному змісті, а надалі розвив і інший підхід, так звану алгоритмічну теорію інформації, де під ентропією розумілася складність об'єкта, яка дорівнює складності

алгоритму, що описує об'єкт. А. М. Колмогоров запропонував ідею виміру порядку й хаосу. Послідовність нехаотична, якщо існує її простий опис, а якщо такого не існує, тобто вона досить складна, то вона несе в собі всі ознаки випадкової послідовності. У цій концепції А. М. Колмогорова зв'язалися в єдине теорія функцій і теорія ймовірностей, конструкції математичної логіки й теорії алгоритмів, поняття й методи теорії інформації, опису багатьох явищ динамічних систем (у тому числі - класичної механіки), досвід вивчення явищ природи.

Самим захоплюючим при створенні основ теорії інформації було вивчення того, що ж таке інформація. Зрозуміло, і в роботах Шеннона і в книзі Вінера давалися тлумачення поняттю "інформація", однак потрібні були додаткові зусилля О. Я. Хінчіна, щоб кількісні характеристики інформації - ентропія й кількість інформації - знайшли статус математичних понять. Дослідженню взаємодії окремих компонентів інформаційних систем за допомогою каналів зв'язку була присвячена книга О. Я. Хінчіна "Математичні методи теорії масового обслуговування".

Специфіка різних областей застосування і конкретні умови, в яких працюють системи обробки та передачі інформації, накладають особливості на їх склад, параметри, технічне виконання. Проте, можна виділити коло питань, загальних для всіх систем обробки та передачі інформації. Саме такі питання і вивчаються в теорії інформації – науки, що пов'язана з вивченням понять кількості інформації, її передачею, сприйняттям, обробкою (переробкою), представленням та зберіганням. Теоретичною основою теорії інформації є теорія ймовірностей.

Базовими в теорії інформації є терміни "інформація", "повідомлення", "сигнал". Ці терміни широко використовуються і в інших областях науки і техніки, у зв'язку з чим є безліч їх визначень – від найзагальніших філософських, до найвужчих, зручніших для використання в конкретних практичних додатках. Так під інформацією звичайно розуміють всі відомості, що є об'єктом зберігання, перетворення і передачі. Інформація міститься в повідомленнях, які є сукупністю деяких символів, знаків, образів тощо. Послідовність, що складається з n розрядів, кожен з котрих може приймати довільне значення букви даного алфавіту (який у свою чергу складається з m символів), називається **повідомленням** (текстом). Число n називають **довжиною повідомлення**. При $n = 1$ повідомлення (довжина повідомлення) складається лише з одного символу, який може приймати m різних значень у відповідності з об'ємом алфавіту ДП. Якщо довжина слова (повідомлення) дорівнює $n = 5$, тоді при використанні, наприклад, українського алфавіту, об'єм якого дорівнює $m = 33$, можна

скласти сукупність різних повідомлень, число яких дорівнює $N = m^n = 33^5$.

Джерело повідомлень може бути дискретним чи неперервним.

Дискретне джерело повідомлень (ДДП) має кінцеву множину елементів $\{x_i\}$ алфавіту m . При цьому на виході ДДП формується дискретне повідомлення X з елементів x_i алфавіту послідовно у часі. У загальному випадку ДДП характеризується ймовірностями $p(x_i)$, $i = \overline{1, m}$ появи елементів x_i алфавіту m на його виході.

Джерело неперервних повідомлень (ДНП) формує на своєму виході повідомлення (та відповідні йому сигнали) у вигляді неперервних функцій часу. Неперервне повідомлення $X(t)$ у загальному випадку приймає нескінченне число значень як за часом, так і за рівнем (величиною), тому кількість інформації ДНП нескінченна. З метою кількісної оцінки інформації неперервне повідомлення представляється у дискретному (цифровому) вигляді у відповідності з результатами теореми В. О. Котельнікова, тобто неперервне повідомлення представляється дискретним і таким чином передається у КЗ. Тому у подальшому будемо розглядати в основному ДДП, що зумовлено перевагами дискретних (цифрових) засобів передачі та обробки інформації.

Ключем до нового розуміння сутності феномена інформації й механізму інформаційних процесів послужив встановлений Л. Бріллюеном взаємозв'язок інформації й фізичної ентропії. Цей взаємозв'язок був спочатку закладений у самий фундамент теорії інформації, оскільки для обчислення кількості інформації К. Шенон запропонував використати запозичену зі статистичної термодинаміки ймовірнісну функцію ентропії:

$$H = - p * \log p$$

Завдяки теорії інформації стало очевидно, що за допомогою тієї ж самої функції можна досліджувати й такі далекі від стану максимальної ентропії системи, як, наприклад, письмовий текст.

Для того, щоб повідомлення можна було передати на відстань, необхідний деякий “посередник”, який міг би виконати функцію переносника інформації. З цією метою можна використати будь-який матеріальний процес, здатний розповсюджуватися в просторі, наприклад звукові або електромагнітні хвилі, електричний струм тощо. Для передачі інформації переносник повинен змінюватися за часом так, щоб між його характеристиками і повідомленнях існувала однозначна, наперед встановлена залежність. Фізичний процес, параметри якого змінюються відповідно до повідомлення, називається *сигналом*.

Класична схема інформаційної системи була запропонована К. Шенноном. У сучасних системах зв'язку і управління найчастіше всього використовуються електричні сигнали. Для передачі повідомлень ДП і ПП

з'єднуються лінією зв'язку (ЛЗ). Сукупність технічних засобів, що необхідні для організації процесу передачі інформації, та ЛЗ називають каналом зв'язку. Засоби кодування призначені для представлення повідомлення у вигляді сигналів (первісне кодування). Передавач призначено для передачі сформованих сигналів у ЛЗ, а приймач інформації виконує функції прийому сигналів. Засоби декодування призначені для перетворення сигналів у повідомлення.

У реальних умовах на корисний сигнал неминуче накладаються перешкоди, що виникають в системах передачі інформації з багатьох причин. У результаті порушується однозначна відповідність між сигналами, що передаються та приймаються, і, як наслідок, зменшується достовірність передачі. У інформаційному аспекті зменшення достовірності передачі еквівалентне втраті деякої кількості інформації. Задача створення систем, стійких до дії перешкод, є однією з центральних в сучасній теорії інформації. Для досягнення цього застосовуються різні методи, як правило, пов'язані з ускладненнями сигналів, апаратури, способів передачі і приймання.

Отже, в дисципліні "Теорія інформації" вивчаються такі основні питання:

- математичний опис повідомлень, сигналів, перешкод і їх перетворення в системах передачі інформації;
- інформаційний підхід до аналізу характеристик систем передачі інформації;
- методи підвищення достовірності передачі дискретної інформації.

Підручник містить шість розділів. У першому даються загальні поняття та визначення теорії ймовірностей; поняття інформації, ентропії та сигналу; модель, класифікація та основні характеристики системи передачі інформації; властивості інформації та ентропії; кількісна міра інформації, що передається по каналу зв'язку. Також наведені приклади якісної оцінки ентропії та інформації у повідомленні. У другому розділі розглянуто інформаційні характеристики джерел повідомлень; оцінку кількості ентропії та інформації у повідомленні; ентропію та інформація джерел дискретних та неперервних повідомлень. Також наведені приклади кількісної оцінки ентропії та інформації у повідомленні. У третьому розділі розглядається сигнал, як носій інформації. Приводяться характеристики основних типів детермінованих і випадкових сигналів, способи їх математичного опису і перетворення. Висловлені основні положення теорії квантування сигналів за часом і рівнем. У четвертому розділі розглянуті основні характеристики каналів передачі інформації, способи оцінки швидкості передачі інформації і пропускну здатності

інформаційного каналу, основи теорії ефективного кодування і способи узгодження сигналів з каналом зв'язку. П'ятий розділ присвячений методам підвищення достовірності інформації на основі перешкодостійкого кодування. У шостому розділі розглядаються питання підвищення достовірності інформації на основі перешкодостійкого кодування у модулярній системі числення.

Також у підручнику приведено перелік контрольних запитань. Приведено докладне рішення типових задач, що повинно істотно полегшити виконання студентами контрольних завдань та розуміння теоретичних питань дисципліни у цілому. У даному підручнику також приведено задачі та вправи для самостійного рішення. Мета приведених типових задач і контрольних питань з дисципліни «Теорія інформації і кодування» це придбання і закріплення студентами навичок практичного розрахунку ентропії джерел (систем) та повідомлень, кількості інформації в них, основних інформаційних характеристик телекомунікаційних каналів (головним чином цифрових) з перешкодами, а також розрахунків основних характеристик каналних кодів (перешкодостійких) кодів, способів і методів кодування і декодування інформаційних повідомлень у цифрових каналах зв'язку. Розглянуто обчислення реальних та потенційних інформаційних характеристик систем передачі інформації, питання перешкодостійкості; елементи синтезу деяких простих, але ефективних декодерів кодів, що коректують.

У додатках приведені приклади вирішення практичних завдань, містяться дані, за допомогою яких спрощується процес виконання та перевірки розрахунків при рішенні задач та вправ на практичних заняттях, а також дано сучасні поняття та визначення, що використовуються в області практичного застосування інформаційних технологій.

При самостійній роботі над підручником бажано скласти короткий конспект проробленого матеріалу, після вивчення кожної теми необхідно дати відповіді на контрольні запитання.

Розділ 1

Загальні поняття теорії інформації

Розглянуті загальні поняття та визначення теорії ймовірностей, що використовуються при вивченні теорії інформації, поняття інформації, ентропії та сигналу, наведена та описана загальна структура системи передачі інформації. Також наведено контрольні питання.

1.1. Загальні поняття та визначення теорії ймовірностей

Події – всі можливі явища: природи, суспільства, науки, техніки та ін. Ситуація, при якій подія може настати, називається **випробуванням**.

Події поділяються наступним чином:

- **випадкові** - це такі події, які у результаті випробувань можуть статися або ні;
- **вірогідні** - це такі події, які обов'язково відбудуться в результаті випробувань, позначаються літерою E ;
- **неможливі** – це такі події, які в результаті випробувань ніколи не відбудуться, позначаються літерою V .

Приклад 1.1.

При підкиданні однієї монети можливі наступні події:

A_1 – випав герб; A_2 – випала цифра; A_3 – не випав ні герб, ні цифра; A_4 – одноразово випав герб та цифра; A_5 – випав герб або цифра. В цьому випадку події: A_1, A_2 – випадкові; A_3, A_4 – неможливі (V); A_5 – вірогідна (E).

Приклад 1.2

Випробування складається у підкиданні шестигранного грального куба з цифрами 1, 2, 3, 4, 5 та 6 на його гранях. Розглянемо деякі можливі при цьому події:

- поява наступної кількості очок: 1 – подія A_1 ; 2 – A_2 ; 3 – A_3 ; 4 – A_4 ; 5 – A_5 , 6 – A_6 ;
- поява на гранях значень простих чисел A_{np} ;
- поява на гранях значень парних чисел A_n ;
- поява на гранях значень непарних чисел A_n ;

- поява на гранях числа очок, що діляться на три A_{03} ;
- поява на гранях числа очок, що діляться на шість A_{06} .

Дві події називають **несумісними**, якщо в результаті випробування вони одночасно не можуть відбутися (для приклада 1.2. – це події A_1, A_2, A_3, A_4, A_5 та A_6).

Події називають **сумісними**, якщо при випробуванні вони можуть одночасно настати (для приклада 1.2 – це події A_{03} та A_{06}).

Подія \bar{A} називається **протилежною** події A , якщо вона полягає в тому, що подія A не відбулася (для приклада 1.2 – це події A_n та A_n).

Видно, що подія A та її протилежна подія \bar{A} – несумісні.

Події A_i ($i = \overline{1, n}$) утворюють **повну групу подій**, якщо при випробуванні одне з них обов'язково відбудеться (для приклада 1.2 – це події A_i ($i = \overline{1, 6}$)).

Події бувають елементарні та складні. **Елементарна подія** – яка при випробуванні обов'язково відбудеться. **Складна подія** – це подія, яку можливо представити через сукупність елементарних подій. Для приклада 1.2:

- елементарні події це $A_1 \div A_6$;
- складна подія, наприклад, $A_n = A_2 \vee A_4 \vee A_6$.

Елементарні події називають **рівноможливими** при умові однаковості шансів їх появи при випробуванні. Для приклада 1.2:

- події A_3 та A_5 є рівноможливі;

➤ події A_6 та \bar{A}_6 (не поява на грані куба шести очок) не рівноможливі, так як шість очок (подія A_6) на грані куба мають шанс з'явитися значно менше, ніж шанс не з'явитися (\bar{A}_6).

Дамо визначення ймовірності $P(A)$ появи події A . Ступінь можливості появи події в майбутньому випробуванні має назву ймовірність цієї події і позначається як $P(A)$. **Ймовірність** $P(A)$ є чисельна міра можливості появи даної події у даному випробуванні і в загальному випадку визнається як відношення числа m елементарних подій, що сприяють появі події A , до загального числа n елементарних подій, що виникли в результаті випробування, тобто

$$P(A) = \frac{m}{n}. \quad (1.1)$$

Формула (1.1) є класичне визначення ймовірності випадкової події (статистична ймовірність, апіорна ймовірність або частота появи події A). В цьому випадку $0 \leq P(A) \leq 1$.

Користуючись визначенням ймовірності (1.1) для двох протилежних подій A та \bar{A} можна записати $P(A) + P(\bar{A}) = 1$, а для повної групи подій $-\sum_{i=1}^n P(A_i) = 1$ (для прикладу 1.2 $-\sum_{i=1}^6 P(A_i) = 1$).

Приклад 1.3

З урни, яка містить 6 білих та 4 чорних кулі, навмання взяли одну з цих куль. Знайти ймовірність $P(A)$ події A того, що витягнута куля буде білою $P(A_b)$ (чорною $P(A_q)$).

Розв'язання. Для нашого випадку $n = 6 + 4 = 10$. Згідно з формулою (1.1) для білої кулі маємо ($m = 6$) $- P(A_b) = \frac{m}{n} = \frac{6}{10} = \frac{3}{5}$, а для чорної кулі

($m = 4$) $- P(A_q) = \frac{m}{n} = \frac{4}{10} = \frac{2}{5}$. Відзначимо, що події A_b та A_q $-$ несумісні, тобто $P(A_b) + P(A_q) = 1$.

Приклад 1.4

За умови прикладу 1.3 навмання одноразово беруть 2 кулі. Знайти ймовірність $P(A)$ того, що обидві кулі будуть білі.

Розв'язання. Для нашого випадку загальна кількість варіантів подій витягнення одноразово двох куль дорівнює $n = C_{10}^2 = \frac{10!}{2!8!} = 45$, а кількість сприятливих подій витягнення одноразово двох білих куль дорівнює $m = C_6^2 = \frac{6!}{2!4!} = 15$. Згідно з формулою (1.1) маємо

$$P(A) = \frac{m}{n} = \frac{15}{45} = \frac{1}{3}$$

Приклад 1.5

За умови прикладу 1.3 навмання одноразово беруть 5 куль.

Яка ймовірність того, що серед 5 навмання взятих куль буде знаходитися 3 білі та 2 чорні кулі.

Розв'язання. Загальна кількість варіантів, подій вибору п'яти куль буде дорівнювати

$$n = C_{10}^5 = \frac{10!}{5!5!} = 2 \cdot 3 \cdot 7 \cdot 6, \quad \text{а} \quad m = C_6^3 \cdot C_4^2 = 5 \cdot 4 \cdot 3 \cdot 2$$

по формулі (1.1) маємо

$$P(A) = \frac{m}{n} = \frac{5 \cdot 4 \cdot 3 \cdot 2}{7 \cdot 6 \cdot 2 \cdot 3} = \frac{10}{21}$$

Відзначимо, що формула (1.1) для знаходження чисельного значення ймовірності випадкової величини A застосовується у випадку, коли події $\{A_i\}$ мають слідуєчі властивості: рівноможливі, несумісні та складають повну групу подій.

Властивості ймовірності $P(A)$ випадкової події A .

1. $0 \leq P(A) \leq 1$.
2. Ймовірність вірогідної події E дорівнює $P(E) = 1$ ($m = n$).
3. Ймовірність неможливої події $V - P(V) = 0$ ($m = 0$).

Приведемо декілька важливих теорем для визначення ймовірностей суми та добутку подій:

- ймовірність суми несумісних подій

$$P(A + B + D) = P(A) + P(B) + P(D);$$

- ймовірність суми сумісних подій

$$P(A + B + D) = P(A) + P(B) + P(C) - P(AB) - P(AC) - P(BC) + P(ABC);$$

- ймовірність добутку незалежних подій

$$P(AB) = P(A) \cdot P(B); \quad P(ABC) = P(A) \cdot P(B) \cdot P(C);$$

- ймовірність добутку двох залежних подій

$$P(AB) = P(A) \cdot P_A(B) = P(B) \cdot P_B(A),$$

де: $P_A(B) = P(B/A)$ – ймовірність події B при умові, що подія A відбулась;

$P_B(A) = P(A/B)$ – ймовірність події A при умові, що подія B відбулась.

Формула повної ймовірності

Нехай подія A може настати при умові появи однієї із попарно несумісних подій (гіпотез) H_i , $i = \overline{1, n}$, що утворюють повну групу подій

$(\sum_{i=1}^n P(H_i) = 1)$. Відомі значення $P(H_i)$, а також умовні ймовірності

$P(A/H_i)$, $i = \overline{1, n}$, події A .

Треба знайти безумовну ймовірність $P(A)$ події A .

Для цього випадку (без доведення) маємо

$$P(A) = \sum_{i=1}^n P(H_i) \cdot P(A/H_i). \tag{1.2}$$

Формула Байеса (формула гіпотез)

Нехай маємо повну групу попарно несумісних подій (гіпотез) H_i , $i = \overline{1, n}$. Ймовірність $P(H_i)$ гіпотез відомі до випробування (априорно).

Проводимо випробування, в результаті якого відбулась подія A .

Треба знайти умовні ймовірності $P(H_i/A)$ гіпотез після випробування (апостеріорні ймовірності).

Звісна тотожність $P(A) \cdot P(H_i/A) = P(H_i) \cdot P(A/H_i)$.

$$\text{Відкіля маємо, що } P(H_i/A) = \frac{P(H_i) \cdot P(A/H_i)}{P(A)},$$

або з урахуванням (1.2) маємо

$$P(H_i/A) = \frac{P(H_i) \cdot P(A/H_i)}{\sum_{i=1}^n P(H_i) \cdot P(A/H_i)}. \quad (1.3)$$

1.2. Поняття інформації, ентропії, повідомлення та сигналу

Будь-яке відображення матеріального миру, яке може бути зафіксоване живою істотою або приладом, несе в собі інформацію.

Інформація (від латинського *information* – роз'яснення, викладення) в загальноприйнятому значенні пов'язана зі змістовою стороною інформаційного процесу та означає деякі відомості, сукупність яких-небудь даних, знань. Існує багато різних визначень інформації. Звичайно під інформацією розуміють нові відомості про світ, що нас оточує, відомості, що ми отримуємо в результаті взаємодії з ним, пристосування до нього та його зміни.

Існує багато визначень для поняття інформації, що відносяться до різних аспектів життєдіяльності людини. Аналіз цих понять та визначень дозволяє зробити висновок, що під інформацією слід розуміти не самі дійсні речі та процеси, а їх суттєві характеристики. Тобто маються на увазі не самі речі та процеси, а тільки їх відбиття чи відображення у вигляді чисел, формул, опису, схем, креслень, символів та інших абстрактних (формалізованих) характеристик. Таким чином, інформація відноситься до області абстрактних категорій, однак, вона завжди виявляється у матеріально-енергетичній формі, тобто, у вигляді сигналів.

Віддзеркалення результатів людської діяльності або осмислення навколишнього світу може бути надано у формалізованому вигляді, наприклад, у вигляді наборів букв або цифр. Такі формалізовані набори називають **даними**. Дані, отримані від джерела інформації, називають **повідомленнями**. Інформацією стають ті повідомлення, що знімають невизначеність, існуючу до їхнього надходження.

Теорія інформації займається вивченням кількості інформації в повідомленнях без урахування конкретного їхнього змісту. Предметом вивчення теорії інформації є ймовірнісні характеристики досліджуваних об'єктів і явищ, оскільки ймовірність є найзручнішою чисельною мірою невизначеності, зі зменшенням якої і пов'язаний процес отримання

інформації. Невизначеність появи явища, невизначеність знаходження в тому або іншому стані деякої фізичної системи або її окремих елементів, невизначеність появи тієї або іншої букви в текстовому повідомленні можна подати за допомогою характеристик ймовірності символів деякого абстрактного алфавіту і вивчати його інформаційні характеристики без урахування того фізичного змісту, який криється за тим або іншим символом. За допомогою такого абстрактного алфавіту в теорії інформації моделюються всі джерела інформації.

Теорія інформація – це основа для рішення багатьох теоретичних проблем і практичних задач у галузі науки та техніці. Найважливіше питання теорії інформації - оцінка кількості та якості інформації. Інформаційні міри відповідають трьом основним теоретичним напрямкам: структурному, статистичному та семантичному. Розглянемо кожен з цих напрямків окремо.

Структурна теорія - розглядає дискретну побудову масивів інформації та її вимір простим розрахунком елементарних інформаційних елементів (квантів) чи комбінаторним методом кодування масивів інформації. У структурній теорії розрізняють три види оцінки міри інформації: геометрична, комбінаторна та адитивна. Найбільше розповсюдження одержала двійкова адитивна міра (міра Р. Хартлі), яка вимірює кількість інформації у двійкових одиницях, так званих бітах.

Статистична теорія - розглядає поняття ентропії, як міру невизначеності, що у свою чергу визначає інформативність повідомлень на основі ймовірнісних характеристик. При цьому кількість інформації залежить від апріорних (до дослідних) ймовірностей випадкових подій, функцій, величин та ін. (міра визначення інформації по К. Шеннону).

Семантична теорія - визначає цінність, корисність або сутність інформації. Під семантикою розуміють смисл та зміст інформації. У загальному випадку семантика міститься у семіотиці (семіотика (грец.) - наука про знаки, слова та мови).

У теорії інформації на семантичному рівні аналізуються відношення між знаками та позначеними ними предметами, діями та якістю, тобто аналізується смисловий зміст (змістовність) тексту по відношенню до джерела повідомлень (інформації) (ДП).

При інженерних розрахунках кількості інформації прагматичні оцінки співпадають з семантичними, оскільки відомості, що не мають сенсу, не потрібні, а непотрібні відомості - безглузді.

Оцінка ефективності логічного виводу, ступеню наближення до істини потребує формалізації, а у даному випадку - формалізації смислу.

Один з таких шляхів формалізації є застосування семантичної теорії інформації.

Кожен з розглянутих трьох напрямків має свою область застосування. Так структурна теорія застосовується для оцінки інформаційних можливостей засобів складових інформаційних систем (ІС), каналу зв'язку (КЗ) та ін., незалежно від умов їх застосування. Статистична теорія дає можливість оцінки якості ІС у конкретних випадках її застосування, наприклад, при передачі інформації (повідомлення) по КЗ. Семантична теорія дає змогу оцінювати ефективність логічного досліду.

Використання інформації неможливо без її передачі та збереження. Передача інформації може здійснюватися як у просторі, так і у часі. По призначенню, інформацію, що передається по КЗ, можна розділити на пізнавальну та управляючу.

Сприйняття інформації - це процес цілеспрямованого отримання та аналізу інформації про будь-які явища природи, процеси, системи та ін. Найважливіші етапи сприйняття інформації наступні:

- первинне сприйняття інформації та вибір необхідних для вимірювання величин (задачі пошуку, локалізації та вибору інформації);
- аналіз об'єкту дослідження;
- виявлення та розпізнавання (процеси контролю та діагностики, розпізнавання образів);
- прогнозування ситуацій.

Зазначимо, що у теорії та практиці сприйняття інформації широке застосування знайшли різноманітні методи досліджень: аналітичні, статистичні, логічні, евристичні та ін.

У загальному випадку під **обробкою інформації** розуміють такий процес перетворення інформації, який представляється у знаках чи сигналах, у наслідок якого її зміст стає максимально підготовленим до реалізації наступного етапу її спрямування, котрим може бути, наприклад, сприйняття інформації людиною чи технічними засобами.

Поняття переробки інформації є поняття більш широке, ніж поняття обробки інформації.

Переробка інформації - це логічне, аналітичне або евристичне перетворення інформації людиною чи засобами ІС, що пов'язано з процесами та формами діяльності систем, подібних до систем штучного інтелекту.

Представлення інформації - це процес перетворення її у форму, що сприятлива та придатна до сприйняття та переробки її людиною. Для цього інформація представляється у вигляді наочних сигналів, що легко сприймаються та символів, що формуються з урахуванням психофізичних

та психофізіологічних можливостей людини. В наш час у ІС використовують три найбільш розповсюдженні форми представлення інформації: сигналізація, індикація та реєстрація.

Поняття інформації пов'язане з моделями дійсних речей, що відображають їх сутність у той мірі, в якій це необхідно для практичних цілей дослідження. У подальшому під інформацією $I(X)$ у техніці будемо розуміти сукупність відомостей про будь які події, явища, процеси, об'єкти, системи та ін.

Інформація виникає тоді, коли встановлюються деякі загальні властивості конкретизованих речей та явищ природи, тому під поняттям "інформація" можна розуміти сутність, характеристику цих речей та явищ.

Близьким до поняття інформації є поняття ентропії, що позначається $H(X)$. Якісно *ентропія* визначається як міра невизначеності (незнання, сумніву та ін.) явища, події, повідомлення, процесу функціонування системи та тощо. В цьому випадку кількість інформації $I(X)$, яку одержуємо після досліду, дорівнює

$$I(X) = H_{\text{анр}}(X) - H_{\text{аносм}}(X),$$

де: $H_{\text{анр}}(X)$ – ентропія, яка визначається апріорно, тобто до проведення досліду (випробування);

$H_{\text{аносм}}(X)$ – ентропія, яка залишилась про об'єкт дослідження після проведення досліду (випробування), тобто після дослідна або апостеріорна ентропія.

Поняття "ентропія" запозичено з термодинаміки, де аналогічний термін характеризує середню невизначеність стану системи молекул речовини. Так, дійсно, у відповідності з другим законом термодинаміки ентропія замкненого простору визначається виразом

$$H = -\frac{1}{M_n} \sum_{i=1}^n m_i \cdot \ln \frac{m_i}{M_n},$$

де: M_n - кількість молекул у даному просторі;

m_i - кількість молекул, що мають швидкість руху $V_i + \Delta V$.

Так, як значення m_i/M_n - це ймовірність P_i того, що молекула має швидкість $V_i + \Delta V$, тоді формула для визначеності ентропії буде мати наступний вигляд

$$H = -\sum_{i=1}^n P_i \cdot \ln P_i.$$

Таким чином, термін "ентропія", буде використовуватися надалі як синонім поняття невизначеності (кількості невизначеності), пов'язаний з результатом деякого випадкового експерименту.

Наведемо приклад якісної оцінки поняття ентропії $H(X)$.

Приклад 1.6.

Нехай на початку нового семестру перед вивченням дисципліни, що складається з N лекцій, ентропія $H_{анр}(X)$ (міра невизначеності, незнання матеріалу даної дисципліни) максимальна $H_{анр}(X) = H_N(X) = H_{max}(X)$, тобто студент нічого не знає за даною дисципліною, не вивчено ні однієї лекції. Тоді кількість інформації $I_i(X)$, що одержав студент після вивчення матеріалу i -х лекцій дорівнює

$$I_i(X) = H_{max}(X) - H_j(X),$$

де: $H_{max}(X)$ – початкова (максимальна) ентропія, що є у студента відносно даної дисципліни, яку він зовсім не вивчав;

$H_j(X)$ – ентропія, що залишилася у студента після вивчення i -х лекцій;

$H_0(X)$ – ентропія, що залишилася у студента після вивчення всіх N лекцій даної дисципліни.

Тобто, якщо все вивчено ентропія дорівнює нулю - $H_j(X) = H_0(X) = 0$. При цьому очевидно, що $(i + j) = N$, тоді $I_i(X) = H_{max}(X) - H_{N-i}(X)$.

Розглянемо співвідношення між величинами $I_i(X)$ та $H_{N-i}(X)$, що поступово складаються при вивченні студентами даної дисципліни, яка складається, наприклад, з $N = 8$ лекцій, а також дамо геометричну інтерпретацію кожному такому випадку.

Випадок 1. Не вивчено ні однієї з $N = 8$ лекцій ($i = 0, j = 8, N - i = 8 - 0 = 8$) тоді маємо $I_0(X) = H_{max}(X) - H_8(X) = H_{max}(X) - H_{max}(X) = 0$, тобто інформації студент не отримав. Вихідна ентропія $H(X)$ залишилася максимальною (рис. 1.1).

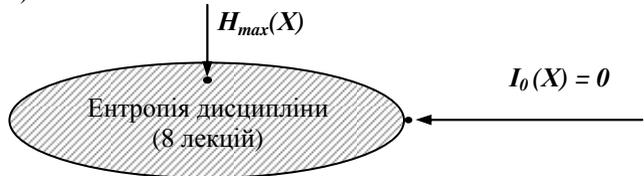


Рис. 1.1 - Геометрична інтерпретація випадку 1

Випадок 2. Вивчено 2 лекції із 8 ($i = 2, j = 6$) $I_2(X) = H_{max}(X) - H_6(X)$

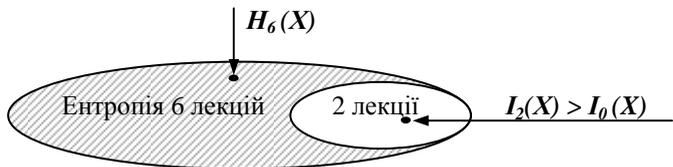


Рис. 1.2 - Геометрична інтерпретація випадку 2

Випадок 3. Вивчено 7 лекцій із 8 ($i = 7, j = 1$) $I_7(X) = H_{max}(X) - H_1(X)$

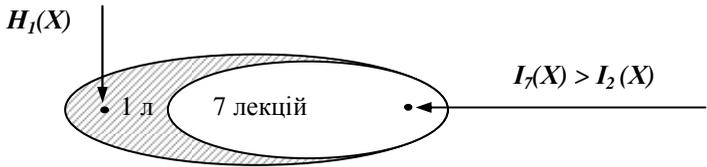


Рис. 1.3 - Геометрична інтерпретація випадку 3

Випадок 4. Вивчено матеріал всієї дисципліни, що складається з $N = 8$ лекцій ($i = 8, j = 0, N - N = 0, H_0(X) = 0$). У цьому випадку маємо

$$I_{max}(X) = I_8(X) = H_{max}(X) - H_0(X) = H_0(X) - 0 = H_0(X) = H_{max}(X).$$

Тобто кількість інформації буде максимальна і дорівнює початковій ентропії $I_{max}(X) = H_{max}(X)$. Відзначимо, що при вивченні всього матеріалу дисципліни ($N = 8$ лекцій) вихідна ентропія $H_0(X)$ (невизначеність, незнання дисципліни) не існує, тобто $H_0(X) = 0$.

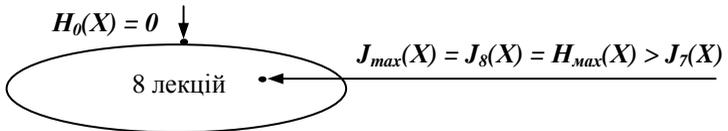


Рис. 1.4 - Геометрична інтерпретація випадку 4

При цьому $I_0(X) = 0 < I_2(X) < I_7(X) < I_8(X) = I_{max}(X)$.

Випадок 5. До слідуючого семестру студент забув частину $I'(X)$ матеріалу дисципліни. В цьому випадку у студента з'являється частина невизначеності (незнання) відносно матеріалу вивченої дисципліни у формі ентропії $H'(X)$, тобто частина $I'(X)$ загальної $I_{max}(X)$ інформації втрачається. Кількість інформації $I_{зали}(X)$, яка залишилася у студента, буде дорівнювати $I_{зали}(X) = I_{max}(X) - I'(X) = H_{max}(X) - H'(X)$.

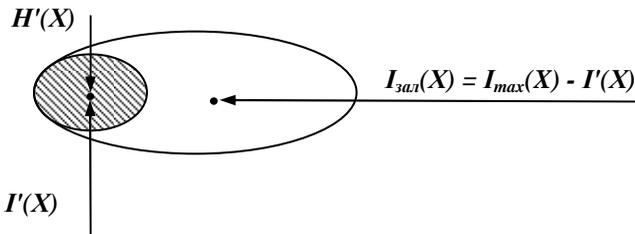


Рис. 1.5 - Геометрична інтерпретація випадку 5

З поняттям інформації пов'язано також поняття повідомлення X . Потрібно розрізнити поняття “інформація” і “повідомлення”. **Повідомлення** – це форма подання інформації, це результат відзеркалення джерелом на кінцевому інтервалі часу кінцевої кількості інформації, поданої у формі, що може бути сприйнята одержувачем.

Передавати інформацію, тобто які-небудь відомості або повідомлення з одного пункту в інший або від одних людей до інших, можна різними засобами і способами. Інформацію (повідомлення, відомості) передають за допомогою листів, газет, книг тощо. Можна передавати інформацію по дротових і оптичних лініях зв'язку. Врешті, по системах зв'язку інформацію можна передавати за допомогою радіо. В цьому випадку переносником інформації є електромагнітні хвилі. Загальним для всіх перерахованих способів є те, що в них від відправника до одержувача передається не який-небудь вид енергії (механічної, електричної), а повідомлення, інформація.

Повідомлення завжди надається у матеріально-енергетичній формі, тобто у вигляді сигналів (змінна фізична величина). **Сигнал** – це матеріальний, технічний носій повідомлення. У загальному випадку сигналом може бути будь-яка зміна початкового стану об'єкта, який здатний викликати реакцію людини або приладу. Будемо позначати повідомлення, що передаються і відповідні їм первинні сигнали, тобто напруги або струми, символом $\lambda(t)$.

Сучасне визначення сигналу зводиться до його уявлення у вигляді фізичного явища або процесу, як функції часу, що несе повідомлення (інформацію) про яку-небудь подію, стан об'єкта спостереження, команди управління тощо.

Сигнали є складними фізичними об'єктами з великою кількістю їх класифікаційних характеристик. Розрізняють сигнали зорові (телевізійне зображення), звукові (дзвінок), електричні (послідовність імпульсів), радіосигнали тощо. Одні сигнали можуть викликати інші. Так, наприклад, електричний сигнал може викликати звуковий (у електричному дзвінку), світловий сигнал – електричний (у фотоелементі). Сигнали можуть бути взаємозв'язані в просторі і за часом. У техніці застосовуються наступні види сигналів: електричні; електромагнітні; акустичні; світлові; механічні; звукові; оптичні та ін.

Сигнали, як функції часу, можна класифікувати за такими признаками.

Детерміновані сигнали - коливання, значення яких можна передбачити у будь-який час. Тобто значення детермінованих сигналів задаються конкретними функціями часу. Класичний приклад

детермінованого сигналу – гармонійне коливання

$$U(t) = U_m \sin(\omega t + \varphi),$$

графік якого зображений на рис. 1.6, а

Таким чином, знаючи амплітуду сигналу U_m , частоту ω , фазу φ гармонійного коливання можна визначити $U(t)$ в будь-який момент часу.

Випадкові сигнали – це коливання, значення яких не можуть бути передбачені точно у будь-який час. З математичної точки зору випадкове коливання описується випадковою функцією. Типовим прикладом є функція перешкоди, що зображена на рис. 1.6, б.

У сучасній теорії інформації джерело повідомлень є пристроєм, який здійснює вибір повідомлення, що підлягає передачі у канал зв'язку, з дискретної множини можливих повідомлень. При цьому повідомлення передається у вигляді сигналу. Передача детермінованих сигналів не має сенсу, тому що такі сигнали не містять у собі ніякої інформації. Але такі інформація широко використовуються у техніці зв'язку як переносники інформації.

За характеристиками області значень і області визначень прийнято розрізняти неперервні (аналогові) і дискретні (квантовані) сигнали. При цьому остання ознака додається, як до часової структури сигналу – до аргументу t , так і до значень функції $\lambda(t)$. Відповідно можна визначити чотири види сигналів.

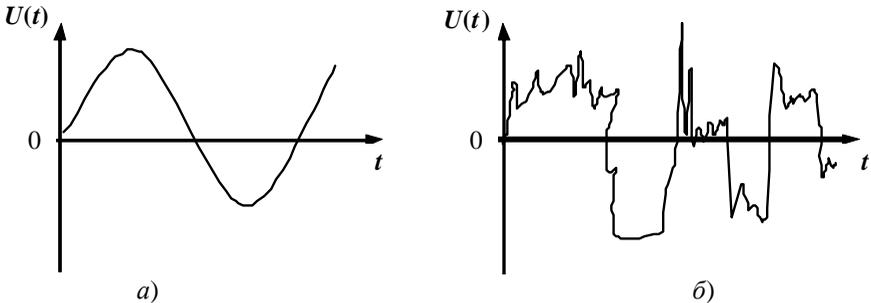


Рис. 1.6. Детермінований (а) та випадковий (б) сигнали

1. **Неперервні сигнали** описуються функцією $\lambda(t)$, що задана на деякому кінцевому або на нескінченному інтервалі часу і може приймати будь-які значення. Приклад неперервного повідомлення, заданого на інтервалі $t \in (0, T)$, зображений на рис. 1.7. До неперервних сигналів належать звукові коливання на виході мікрофона, телевізійні сигнали на

виході передавальної трубки, сигнали, що знімаються з різних датчиків неперервної дії в телеметричних системах.

2. **Імпульсні аналогові сигнали** – коливання, дискретні за часом і неперервні по шкалі рівнів. Повідомлення, дискретне за часом, означає, що функція $\lambda(t)$ задана або визначена тільки на рахунковій множині моментів часу t_1, t_2, \dots, t_n . Інтервал між сусідніми відліковими точками t_i і t_{i+1} звичайно має постійне значення $T_0 = t_{i+1} - t_i$ і називається інтервалом або кроком дискретності.



Рис. 1.7. Неперервний сигнал (повідомлення)

По шкалі рівнів функція $\lambda(t_i)$ неперервна і може приймати будь-які значення з інтервалу $\lambda(t_i) \in (\lambda_{min}, \lambda_{max})$. Значення $\lambda(t)$ повідомлення $\lambda(t)$ у відлікові моменти будемо називати відліками. Приклад імпульсного аналогового повідомлення зображений на рис. 1.8.

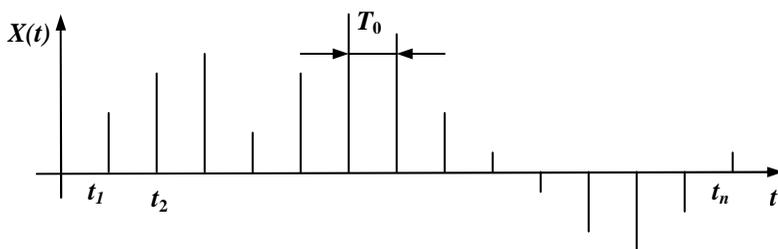


Рис. 1.8. Імпульсний аналоговий сигнал (повідомлення)

Такі повідомлення можуть формуватися в системах передачі інформації (СПП) безпосередньо, а також в результаті дискретизації за часом неперервних повідомлень.

3. **Дискретно - неперервні повідомлення** – повідомлення, дискретні

по шкалі рівнів і неперервні за часом. Повідомлення, дискретне по шкалі рівнів, означає, що функція $\lambda(t)$ приймає значення тільки на множині, яку можна порахувати $\lambda_1, \lambda_2, \dots, \lambda_m$. По шкалі часу функція $\lambda(t)$ неперервна. Приклад дискретно-неперервного повідомлення зображений на рис. 1.9.

4. **Дискретні або цифрові повідомлення** – повідомлення, дискретні, як за часом, так і по шкалі рівнів. Відповідно відліку $\lambda(t_i)$ можуть приймати значення, що належать до кінцевої множини наперед заданих рівнів $\lambda_1, \lambda_2, \dots, \lambda_m$.

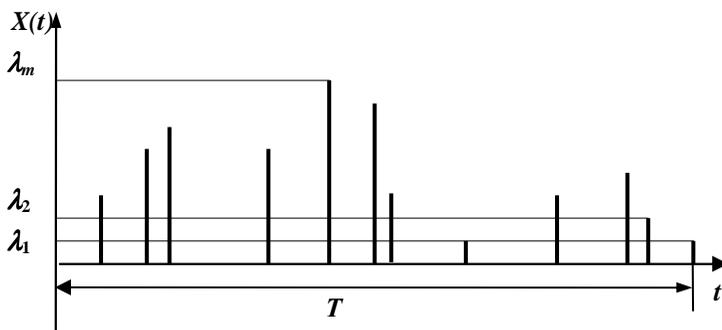


Рис. 1.9. Дискретно-неперервний сигнал (повідомлення)

Звичайно дозволені рівні відстоять один від одного на одну і ту ж саму відстань $\Delta\lambda = \lambda(i+1) - \lambda(i)$, яка називається **кроком квантування**. На рис. 1.10 зображене таке дискретне повідомлення.

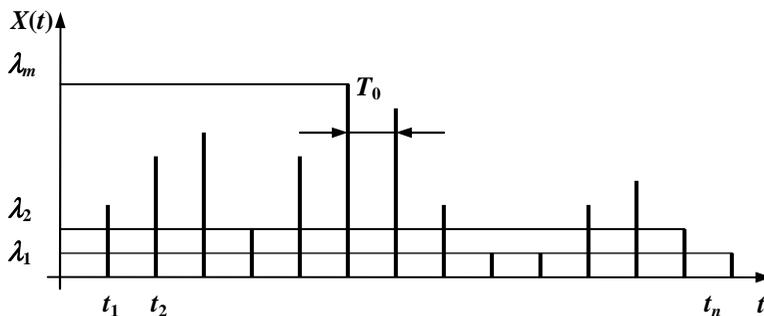


Рис. 1.10. Дискретний сигнал (повідомлення)

Дозволенним рівням можна поставити у відповідність натуральний ряд чисел $0, 1, \dots, m-1$. Відліки при цьому будуть мати цілочисельні значення, а повідомлення буде являти собою послідовність цілих чисел, що настають одне за одним з інтервалом дискретності T_0 . Дискретні сигнали мають ряд практичних переваг. Крім того, для них простіше встановити загальні закономірності, ніж для неперервних сигналів.

У зв'язку з цим має інтерес той факт, що будь-які повідомлення з точністю, достатньою для практичного застосування, можуть бути замінені імпульсними аналоговими і навіть цифровими сигналами.

1.3. Системи передачі інформації

1.3.1. Класифікація систем передачі інформації. Модель системи передачі інформації

Під *системою передачі інформації* (СПІ) розуміють цілісний комплекс взаємозв'язаних об'єктів, здатних обмінватися інформацією. До СПІ належать:

- системи радіозв'язку і радіомовлення;
- системи телебачення;
- фототелеграф – передача по радіо нерухомих зображень (фотографій);
- системи телеграфії і передачі даних – для передачі друкованих текстів і цифрових даних;
- командні лінії радіоуправління – призначені для передачі команд, формалізованих повідомлень, наказів, управління літальними апаратами;
- системи радіотелеметрії – передача по радіо даних вимірювань параметрів деяких фізичних систем, наприклад, дані про об'єкти, що рухаються;
- системи радіолокації;
- системи радіонавігації тощо.

Розглянемо узагальнену структурну схему системи передачі інформації, яка зображена на рис. 1.11.

Джерело повідомлень (відправник) – це пристрій для формування повідомлення, що передається. Конкретний вид повідомлень, що передаються (позначених на рис. 1.11 символом λ), залежить від виду СПІ і може являти собою мову, музику, зображення, результати вимірювань параметрів системи (телеметрія), знакові або цифрові пакети, сигнали (команди, накази) тощо.

Багато повідомлень, наприклад, мова, зображення, телеметрична інформація являють собою деякі функції часу $\lambda(t)$. Проте, надалі буде показано, що будь-яке повідомлення може бути подане у вигляді послідовності елементарних повідомлень – чисел λ , які передаються через деякий інтервал часу T_0 . В цьому випадку кожне елементарне повідомлення λ може приймати одне з m значень $\lambda_1, \lambda_2, \dots, \lambda_m$. На математичній мові говориться, що λ є елементом множини (або належить множині) $\{\lambda_1, \lambda_2, \dots, \lambda_m\}$ і позначається $\lambda \in \{\lambda_1, \lambda_2, \dots, \lambda_m\}$.



Рис. 1.11. Узагальнена структурна схема СПІ

Так, наприклад, у телеграфії елементарними повідомленнями λ є букви тексту. Відповідно, множина $\{\lambda_1, \lambda_2, \dots, \lambda_m\}$ являє собою множину букв алфавіту *а, б, ..., я*.

Передавач – це пристрій, що в загальному випадку в СПІ виконує такі функції.

1. **Перетворення** повідомлення в потрібний (електричний) сигнал, тобто в електричний струм або напругу, зміна параметрів яких у часі відтворює повідомлення, що передається $\lambda(t)$ або послідовність повідомлень $\lambda(t_1), \lambda(t_2), \dots, \lambda(t_m)$.

Прикладом перетворення повідомлення в електричний сигнал є робота мікрофона або телевізійної камери, що перетворюють в електричний струм відповідно мову (або музику) і зображення. Умовимося електричні сигнали, так само як і повідомлення, позначати символом $\lambda(t)$ або λ , оскільки з математичної точки зору вони співпадають з точністю до постійного коефіцієнта.

2. **Кодування** повідомлень або сигналів, під яким розуміється таке перетворення множини елементарних повідомлень (або сигналів), при якому кожному елементарному повідомленню $\lambda_i, i = 1, 2, \dots, m$ ставиться у відповідність кодова комбінація $\alpha_1, \alpha_2, \dots, \alpha_l$, яка складається з декількох більш простих символів $\alpha_k, k = 1, 2, \dots, l$. Переважно, але не обов'язково, в коді використовуються двійкові цифри $\alpha_k \in \{0, 1\}$. Кодування при цьому зводиться до подання елементарних повідомлень у вигляді l -значних двійкових чисел. Наприклад, при телеграфії первинне повідомлення, надруковане на бланку у вигляді тексту, перетворюється у форму п'ятизначних чисел в двійковій системі числення (код Бодо). В цьому випадку кожній букві ставиться у відповідність послідовність (кодова комбінація) з п'яти двійкових цифр (0 або 1). Аналогічно може бути закодована будь-яка множина елементарних сигналів $\lambda_1, \lambda_2, \dots, \lambda_m$. Кодування сигналів широко використовується для перешкодостійкості зв'язку і збільшення кількості інформації, що передається, по каналах зв'язку.

3. **Модуляція** – формування радіосигналу (або високочастотного сигналу) за допомогою накладання низькочастотного первинного сигналу на переносник інформації. Переважно в СПІ переносником інформації є високочастотне гармонійне коливання. Як переносник може бути вибрана і більш складна функція часу. Таким чином, на виході передавача формується високочастотний сигнал $S(t, \lambda)$, який є деякою функцією $S(\bullet)$ часу t і повідомлення λ , що передається.

Лінія зв'язку – це фізичне середовище, в якому розповсюджується сигнал – переносник. Коливання на виході лінії зв'язку, яке будемо називати коливанням, що приймається, і позначати символом $U(t)$, істотно відрізняється від сигналу $S(t, \lambda)$ на вході лінії зв'язку з таких причин: по-перше, при розповсюдженні сигнал слабшає і зазнає деяке запізнення τ , внаслідок чого приймає вигляд $\varepsilon S(t - \tau, \lambda)$, де ε – параметр інтенсивності, що характеризує ослаблення, і τ – час затримки; по-друге, в лінії зв'язку до сигналу добавляються перешкоди різного походження: промислові, атмосферні, космічні, перешкоди від сторонніх радіостанцій, внутрішні шуми апаратури. Останні з міркувань зручності різних досліджень відносять (перераховують) до виходу лінії зв'язку. Перешкоди будемо позначати символом $n(t)$. В результаті коливання, що приймається, має вигляд

$$U(t) = \varepsilon S(t - \tau, \lambda) + n(t).$$

Приймач – пристрій, призначення якого з максимально можливою точністю по прийнятому коливанню $U(t)$ відновити послане повідомлення λ . Прийняте повідомлення, тобто повідомлення, яке було відтвореним на виході приймача, через наявність перешкод в загальному випадку може відрізнятись від переданого. Назвемо прийняте повідомлення оцінкою (ϵ на увазі оцінка повідомлення) і позначимо тим же символом, що і повідомлення, але тільки із зірочкою: λ^* або $\lambda^*(t)$.

Одержувач (адресат) – це людина, ЕОМ, який-небудь виконуючий або інший пристрій, якому призначені повідомлення, що передаються.

Сукупність передавача, лінії зв'язку і приймача називається **каналом передачі інформації** (зв'язку). Канал зв'язку сумісно з джерелом та отримувачем повідомлень складають **систему передачі інформації** (зв'язку).

Загальна схема передачі інформації по КЗ за допомогою різноманітних видів сигналів представлена на рис. 1.12.

1.3.2. Основні характеристики систем передачі інформації

Основне призначення СПІ – передати повідомлення від джерела повідомлень до одержувача. При цьому йдеться не просто про передачу деякої кількості інформації, а оскільки інформація має очевидну властивість старіння, то необхідно говорити про передачу деякого заданого об'єму інформації по каналу зв'язку з перешкодами за заданий (допустимий) час. Тому при оцінці СПІ перш за все виходять з того, яку точність передачі повідомлень вона забезпечує при заданій швидкості передачі інформації.

Точність передачі повідомлень визначається ступенем відповідності прийнятого повідомлення переданому. Цей показник називають **достовірністю**. При передачі дискретних повідомлень цю відповідність можна оцінити відношенням числа помилково прийнятих елементарних повідомлень до загального числа переданих. При достатньо великій довжині повідомлення і незмінних умовах передачі це відношення є ймовірністю помилкового прийняття елементарного повідомлення (або відповідного йому елементарного сигналу) – $P_{ном}$

При передачі безперервних повідомлень ступінь відповідності прийнятого повідомлення переданому характеризують середньквдратичним відхиленням одного від іншого.

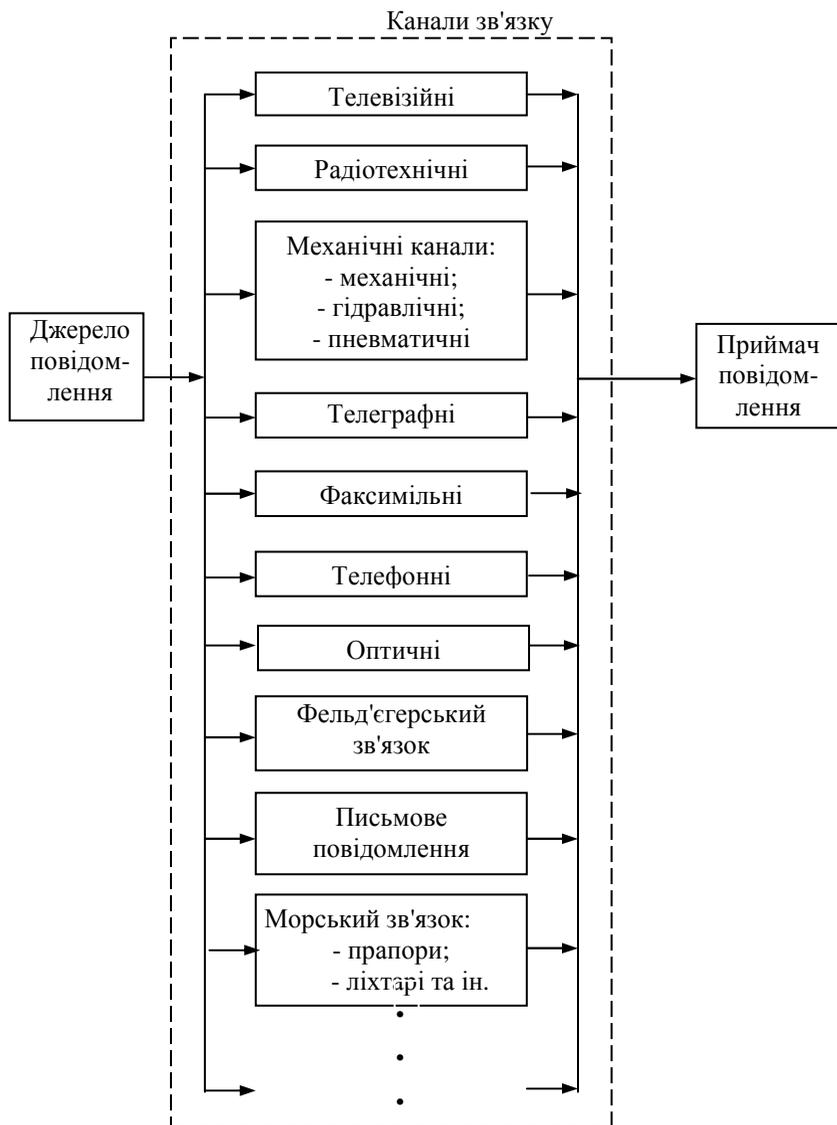


Рис. 1.12 - Схема передачі інформації (повідомлення) за допомогою різних видів сигналів

Характеристикою тісно пов'язаною з достовірністю є **перешкодостійкість**, під якою розуміється здатність системи зв'язку протистояти дії різних перешкод і спотворень, що заважають.

Якщо хочуть підкреслити здатність СПІ протистояти навмисним перешкодам, то використовують термін **перешкодозахищеність**.

Для кількісної оцінки перешкодостійкості використовують різні показники. Найбільше поширення набув показник, відповідно до якого перешкодостійкість оцінюється відношенням середньої потужності сигналу до середньої потужності перешкоди на вході приймача, при якому забезпечується задана достовірність. Чим менше величина цього відношення, тим вище перешкодостійкість системи.

Різні системи зв'язку дозволяють передавати одні й ті ж повідомлення з різною швидкістю. Чисельно швидкість передачі інформації визначається кількістю інформації, що поступила від відправника до одержувача за одну секунду. Кількість інформації вимірюють в спеціальних одиницях – так званих двійкових одиницях або бітах.

Швидкість передачі інформації випадковим чином залежить від ряду чинників: статистичних властивостей повідомлень, що передаються, перешкод, характеристик каналу зв'язку. Гранична швидкість передачі інформації по каналу зв'язку визначається його **пропускною здатністю**, що характеризує максимальну кількість інформації, яка може бути передана по каналу в одиницю часу і є одним з фундаментальних понять, що характеризують потенційні можливості системи передачі інформації.

При передачі дискретних повідомлень для характеристики швидкодії апаратури користуються поняттям технічної швидкості передачі. Вона визначається кількістю посилок дискретного повідомлення (числом змін сигналу), сформованих за секунду і вимірюється в бодах.

Але завжди виникає питання: а якою ціною ці показники досягнуті? Необхідно мати таку систему зв'язку, яка забезпечувала б задану достовірність і швидкість передачі інформації найбільш економічно, тобто з якнайменшими витратами, під якими можна розуміти потужність сигналу, смугу частот, вартість апаратури тощо. Сукупність властивостей (показників), що характеризують економічність системи з погляду вказаних витрат, називають **ефективністю системи**.

Важливою характеристикою деяких систем зв'язку є **скритність**, під якою розуміється здатність системи працювати в режимі, що утрудняє виявлення повідомлень, які передаються, і оцінку їх параметрів спеціальною розвідувальною апаратурою зловмисника. Розрізняють енергетичну, просторову, часову і частотну скритність. Енергетична

скритність досягається зниженням середньої потужності сигналу; просторова – застосуванням гостроспрямованих антен; часова – зменшенням тривалості сеансу зв'язку за рахунок підвищення швидкості передачі; частотна – зміною робочих частот. Іноді для підвищення скритності використовується криптографічне кодування, що полягає в спеціальному перетворенні сигналів при передачі, яке утруднює розшифровку повідомлень зловмисником.

Існують багато інших параметрів, що характеризують системи зв'язку з різних точок зору. До них, зокрема, належать надійність, габарити, маса, вартість, потужність тощо.

1.3.3. Статистичне трактування процесу передачі інформації

У найзагальнішому вигляді процес передачі інформації виглядає так. Повідомлення, що видається джерелом інформації, перетворюється на сигнал, який за допомогою певних технічних засобів передається одержувачеві. Приймаючи сигнал і знаючи закон відповідності сигналів і повідомлень, одержувач може вилучити інформацію, що міститься в повідомленні.

У реальних умовах, в результаті дії перешкод порушується взаємно-однозначна відповідність між сигналами, що передаються та приймаються, і, як наслідок, зменшується вірність передачі, що еквівалентно втраті деякої кількості інформації.

Розглянемо передачу і приймання одного елементарного повідомлення λ . В процесі передачі – приймання повідомлень розрізняють два стани: апіорний (до приймання повідомлення) і апостеріорний (після приймання повідомлення). **Апіорним** називається стан, в якому знаходиться одержувач до того, як буде послане повідомлення λ .

Апостеріорний називається стан, в якому знаходиться одержувач після того, як буде послане повідомлення λ , а на приймальній стороні сформульована відповідна оцінка λ' . Відомості, які має в своєму розпорядженні одержувач в апіорному і апостеріорному станах, називають відповідно апіорними і апостеріорними.

У апіорному стані одержувач знає, що буде створене повідомлення λ , яке може прийняти одне з m наперед відомих значень $\lambda_1, \lambda_2, \dots, \lambda_m$. Яке саме значення з множини $\{\lambda_1, \lambda_2, \dots, \lambda_m\}$ прийме повідомлення λ , спостерігач (одержувач) не знає. Останнє положення є принциповим. Дійсно, якби одержувач наперед знав, яке повідомлення буде передане, не

мало б сенсу передавати це повідомлення по каналу зв'язку: нічого нового, одержавши повідомлення, він би не дізнався. Інакше кажучи, передача інформації була б відсутня.

Створення повідомлень джерелом повідомлень є типовим випадковим експериментом, множиною результатів якого є множина елементарних повідомлень $\{\lambda_1, \lambda_2, \dots, \lambda_m\}$. Ймовірність різних результатів $P(\lambda_i)$ звичайно можна вважати відомими одержувачеві в апіорному стані. Так, наприклад, якщо елементарні повідомлення – це букви тексту, то $P(\lambda_i)$ – ймовірність того, що довільно вибрана з тексту (або створена джерелом) буква буде λ_i . Таку ймовірність неважко підрахувати: потрібно взяти достатньо довгий текст і підрахувати кількість $\lambda_i - N_i$ у цьому тексті. Якщо в тексті загальне число букв N , то $P(\lambda_i) = N_i / N$.

Таким чином, робота джерела повідомлень є випадковим експериментом, а одержувачеві в апіорному стані відомий закон розподілу ймовірності різних результатів в цьому експерименті. Якщо розглядати повідомлення, сформоване на тривалішому інтервалі часу, то це буде послідовність результатів випадкових експериментів або послідовність випадкових величин, яка відповідно до визначень теорії ймовірності є випадковим процесом.

Нехай було послане повідомлення λ і одержана оцінка λ^* . У апостеріорному стані одержувач не може бути впевнений, що одержана їм оцінка λ^* співпадає з посланим повідомленням λ через випадковий (ймовірнісний) характер перешкод. Коливання, що приймається, а, отже, і сформована по ньому оцінка λ^* також носять випадковий характер. У цілому передача – приймання повідомлення в системі зв'язку є випадковим експериментом з двома статистично пов'язаними результатами λ і λ^* . Останні вказують на статистичний характер проблеми організації ефективного зв'язку і роблять доцільним вивчення цієї проблеми статистичними методами. Відповідно основним апаратом теорії інформації є теорія ймовірності, математична статистика та теорія випадкових процесів.

Практично основна трудність, що виникає при передачі повідомлень або при організації зв'язку, полягає у тому, що перешкоди, які завжди присутні в каналі зв'язку, істотно утрудняють, а іноді роблять нездійсненним відтворення повідомлень, що передаються, на приймальній стороні.

1.3.4. Спотворення та перешкоди у каналах зв'язку

Всю сукупність чинників, що негативно впливають на електричний сигнал в каналах зв'язку, залежно від характеру взаємозв'язку з сигналом, поділяють на спотворення і перешкоди.

Спотворенням називають всяке детерміноване (невипадкове) перетворення сигналу, не передбачене алгоритмом інформаційного обміну.

Під **перешкодами** розуміються будь-які збурення в каналі передачі інформації, що викликають випадкові відхилення прийнятого повідомлення від переданого.

На відміну від перешкод, спотворення сигналів при виявленні джерел їх виникнення можуть бути усунені (скоректовані).

Частіше за все спотворення виявляються або в зміні масштабу сигналу, або в появі затримки з часом (так звані лінійні спотворення).

Перешкоди, як випадкові дії, що заважають, класифікують за різними групами ознак:

- за місцем виникнення;
- за характером взаємодії з сигналом;
- за спектральним складом (широкосмугові, вузькосмугові);
- за часовими характеристиками (повільні, швидкі);
- за властивостями ймовірності (статистичні).

В основі класифікації перешкод за місцем виникнення лежать фізичні причини виникнення чинників, що заважають. За місцем виникнення перешкоди можна розділити на зовнішні та внутрішні.

До **зовнішніх перешкод** належать перешкоди, джерела яких знаходяться поза системою передачі інформації. До них можна віднести:

- атмосферні перешкоди, що породжуються природними електромагнітними процесами в земній атмосфері (грозовими розрядами, електризацією антен тощо), радіовипромінюванням атмосфери, тепловими шумами Землі;
- космічні перешкоди, що викликаються позаземними джерелами – радіовипромінюваннями Сонця, Місяця, планет і космічними радіовипромінюваннями;
- промислові (індустріальні) перешкоди, що обумовлені роботою різних електричних пристроїв і агрегатів, пов'язані з замиканням і розмиканням електричних ланцюгів, розрядами в лініях електропередач тощо;
- станційні перешкоди, що можуть створюватися як навмисно (з метою радіоелектронної боротьби), так і ненавмисно (при

випадковому перекритті спектрів сигналів сусідніх за частотою станцій).

Внутрішні перешкоди безпосередньо пов'язані з фізичними особливостями пристроїв і виникають в самій апаратурі, що входить в структуру системи передачі даних. Вони викликаються випадковими флуктуаціями фізичних властивостей елементів цих пристроїв. До них можна віднести:

- перешкоди у вигляді теплових шумів напівпровідникових приладів, опорів і інших елементів (*шумові перешкоди*);
- перешкоди, викликані змінами параметрів у лініях зв'язку, впливом ліній однієї на іншу, а також неоднорідностями в лініях зв'язку;
- перешкоди, що виникають при перетворенні сигналу в окремих елементах системи. Алгоритмічні перешкоди характерні для аналого-цифрових систем передачі даних (шуми квантування і дискретизації);
- перешкоди, обумовлені нестабільністю елементів апаратури, а також апаратурні спотворення, викликані технічною несправністю або недостатньо точною настройкою апаратури.

За своїми властивостями перешкоди можуть бути детермінованими (регулярними) і випадковими. Захист від детермінованих перешкод не викликає особливих труднощів. Випадкові перешкоди довільно міняють свій рівень за часом і в просторі.

За характером взаємодії з сигналом перешкоди розділяють на два великі класи: адитивні і мультиплікативні. *Адитивною* називається перешкода, яка підсумовується до сигналу. Вона існує незалежно від сигналу і може спостерігатися як за наявності сигналу, так і при його відсутності. Для адитивних перешкод оператором взаємодії з сигналом є співвідношення

$$y(t) = S(t) + n(t) .$$

Залежно від форми, адитивні перешкода поділяються на:

- *флуктуаційні* – перешкоди з нульовим середнім значенням. Це, як правило, теплові шуми, перехідні перешкоди і цілий ряд перешкод зовнішнього походження (космічні). Найчастіше це перешкоди з симетричними функціями щільності ймовірності (наприклад, гаусові, рівномірні тощо);
- *імпульсні* (зосереджені за часом) перешкоди, що є випадковою послідовністю короткочасних (мають вид поодиноких імпульсів) дій, які заважають (грозових розрядів, комутації каналів тощо);

- **гармонійні** (зосереджені за частотою) – перешкоди, енергія яких зосереджена у вузькій смузі частот (мають спектр менший, ніж частотна смуга приймача).

Мультиплікативною називається перешкода, що перемножується з сигналом і впливає на сигнал $S(t)$ згідно з співвідношенням

$$y(t) = \mu S(t) .$$

Вони обумовлені такими діями, що можуть інтерпретуватися як випадкова зміна коефіцієнта передачі каналу зв'язку (випадковими змінами залишкового загасання, несправностями автоматичного регулювання підсилення, випадковими перемиканнями і порушеннями контактів). Мультиплікативні перешкоди з'являються тільки при передачі сигналів і їх дія полягає в багатократному підсиленні або ослабленні сигналів.

1.4. Контрольні питання

1. Перелічіть всі можливі методи представлення повідомлень.
2. Що розуміється під інформаційними системами?
3. Дайте визначення поняттям: ентропія, інформація, повідомлення, сигнал.
4. У якому випадку кількість інформації $I(X)$ буде максимальною?
5. У чому полягає процес перетворення повідомлення у сигнал?
6. Назвіть та поясніть основні елементи (об'єкти), що складають узагальнену інформаційну систему будь-якого (загального) призначення.
7. Дайте визначення лінії та каналу зв'язку інформаційної системи.
8. Пояснити логічний зв'язок між поняттями: «інформація», «повідомлення» та «сигнал».
9. Поясніть вибір значення a основи логарифма у виразі для оцінки кількості інформації.
10. Представте загальну структурну схему інформаційної системи. Поясніть її складові.
11. Які способи представлення сигналів Вам відомі?
12. Перелічіть основні елементарні сигнали та поясніть їхні властивості.
13. Поясніть сутність поняття «ентропія». У яких одиницях вона може вимірюватися?
14. Сформулюйте та поясніть всі основні властивості ентропії.
15. Як кількісно визначається ентропія дискретних систем з рівноймовірними та нерівноймовірними станами?

16. Поясніть якісний та кількісний зв'язок між ентропією та інформацією повідомлення (події).

17. Дайте визначення поняттю «інформація». Перелічіть та поясніть які основні вимоги пред'являються до міри визначення кількості інформації.

18. Перелічіть та поясніть основні властивості інформації.

19. Перелічіть та поясніть всі основні властивості ентропії дискретних повідомлень.

20. Охарактеризуйте сутність поняття ентропії та інформації. Яким чином вони кількісно оцінюються?

21. Показати, що ентропія джерела інформації, що має m станів, максимальна при $p = 1/m$.

22. У яких одиницях можна вимірювати кількість інформації $I(X)$ та ентропію $H(X)$ та чому?

23. Визначте основні переваги та недоліки дискретних (цифрових) методів передачі інформації у порівнянні з неперервними.

24. Перелічіть та поясніть можливі види сигналів, що використовуються в інформаційних системах.

25. Дайте визначення поняттям “обробка інформації” та “переробка інформації”. У чому полягає зміст розходжень даних понять?

26. Сформулюйте та поясніть математичні моделі основних елементарних сигналів.

27. Дайте визначення наступним поняттям: «подія», «ймовірність», «здійснення події», «залежні, незалежні, спільні і неспільні події», повна група подій.

Розділ 2

Ентропія та інформація джерел повідомлень

Розглянуто міри оцінки кількості інформації, ентропію та інформацію джерел дискретних повідомлень, розкриті методи оцінки інформації та ентропії, інформаційні характеристики джерел дискретних повідомлень, ентропію джерел неперервних повідомлень, властивості інформації та ентропії, властивості інформації та ентропії складних дискретних повідомлень. Також наведено контрольні питання.

2.1. Кількісна міра оцінки інформації, що передається по каналу зв'язку

З визначенням інформації пов'язані наступні важливі поняття:

- кількість інформації;
- цінність інформації;
- вірогідність інформації;
- оперативність інформації ;
- корисність інформації;
- ефективність використання інформації;
- об'єм інформації;
- ціль використання інформації;
- смисловий зміст інформації;
- тезаурус (словник, що використовується; запас знання);
- доцільність інформації;
- якість інформації ;
- сенс інформації;
- своєчасність інформації та ін.

Поняття інформації пов'язане насамперед з моделями реальних речей, які відображають їх сутність у тій мірі, в якій це необхідно для практичних цілей дослідника. Тобто, під інформацією слід розуміти не самі предмети, символи, явища чи процеси, а їх характеристики або відображення. Як зазначалось вище, інформація може бути представлена у вигляді: звуків, зображень, чисел, формул, знаків, вербального опису, креслень, символів,

образів, букв та інших абстрактних (формалізованих) характеристик, сукупність яких ми будемо називати повідомленням.

Найважливішим питанням теорії інформації є визначення кількісної міри оцінки інформації. Ця міра повинна визначатися наступним чином: по-перше, щоб вона відповідала інтуїтивним представленням про склад та поняття інформації, а по-друге, щоб вона була зручною при її розрахунку.

Природно рахувати, що інформації одержують більше тоді, коли подія заздалегідь не була визначена, або визначена з малим значенням ймовірності її появи. З другого боку, чим більш ймовірна подія, тим менше інформації одержує спостерігач від повідомлення про те, що вона відбулась. Тобто, ми можемо зробити первісний висновок: кількість інформації у повідомленні залежить від ймовірності появи події, про яку говориться у цьому повідомленні.

За основу визначення кількості інформації (чи просто інформації) покладено ймовірнісні характеристики повідомлення, які відображають ступінь їх невизначеності (несподіваності) при появі їх у одержувача інформації (приймача повідомлення).

Приведемо приклад. Нехай у буфеті продають пиріжки. Заходить студент у буфет та очікує повідомлення продавця про наявність пиріжків різних видів з наступною ймовірністю (табл. 2.1).

Природно, чим менше ймовірність $p(x_i)$ повідомлення про наявність необхідних видів пиріжків, тим більше інформації $I(x_i)$ одержує студент від продавця про види існуючих пиріжків (більше несподіваність повідомлення). Так у даному прикладі (табл. 2.1) найбільшу кількість інформації студент одержує у випадку 4, а найменшу – у випадках 1 та 2.

Таблиця 2.1

Таблиця ймовірностей очікування повідомлення

x_i $i = \overline{1,4}$	<i>Пиріжки</i>			
	x_1	x_2	x_3	x_4
	<i>Картопля</i>	<i>М'ясо</i>	<i>Вишня</i>	<i>Ананас</i>
$p(x_i)$	0,4	0,4	0,19999	0,00001

Таким чином можна зробити висновок що кількість інформації $I(x_i)$ у повідомленні x_i обернено пропорційно ймовірності $p(x_i)$ появи цього повідомлення, тобто

$$I(x_i) \sim \frac{1}{p(x_i)} \cdot$$

Введемо кількісну міру інформації, що передається по каналу зв'язку. Це деяка формалізована кількість інформації, що міститься в повідомлен-

ні, яка в першу чергу характеризує завантаження каналу зв'язку.

Поняття джерела інформації є найважливішим поняттям теорії інформації. Як вже говорилося, джерело інформації може бути представлено ансамблем повідомлень. Дискретним джерелом інформації вважається джерело, безліч значень якого є дискретним. Неперервним джерелом інформації вважається джерело, безліч значень якого є неперервним.

З погляду теорії інформації джерело вважається заданим повністю, якщо є деяка ймовірнісна модель, що описує процес появи сигналів на виході джерела. Для опису послідовності станів джерела використовуються математичні моделі у вигляді дискретних або неперервних випадкових процесів. Основу цього опису складає ймовірнісна міра ансамблю джерела. При цьому, в загальному випадку, вважається, що ймовірнісна міра визначається станом джерела і може змінюватися під час переходу його з одного стану в інший. Для побудови дискретного джерела необхідно знати алфавіт джерела. Основною інформаційною характеристикою джерел інформації є ентропія.

Почнемо розгляд з простих повідомлень – дискретних. Виділимо один інтервал дискретності $t \in (0, T_0)$. Джерело повідомлень на цьому інтервалі створює елементарне повідомлення X , яке може прийняти одне з M значень символів: x_1, x_2, \dots, x_M . Загальне число символів алфавіту M називають *основою (потужністю) алфавіту* джерела повідомлень. Одержувач після обробки коливання, що приймається, приймає рішення про те, яке саме повідомлення з множини $\{x_i\}$ було передано. Відповідно до позначень, прийнятих в теорії інформації, це рішення (оцінку повідомлення, що приймається) позначимо через Y . Рішень взагалі може бути M , тобто $Y \in \{y_1, y_2, \dots, y_M\}$, і y_1 означає рішення про те, що передано повідомлення x_1 і т.д.

Нагадаємо характеристику двох основних станів: апіорного і апостеріорного, в яких знаходиться одержувач в процесі приймання кожного елементарного повідомлення.

Відповідно до реальних умов роботи більшості СПП в теорії інформації приймається, що в апіорному стані одержувачеві відомий набір можливих елементарних повідомлень x_1, x_2, \dots, x_M і ймовірність посилки кожного повідомлення $p(x_1), p(x_2), \dots, p(x_M)$. Характерним є стан невизначеності у одержувача: він знає, що йому послано одне з M наперед відомих йому повідомлень, але яке саме послане, він не знає. Цю невизначеність одержувача в апіорному стані називають апіорною невизначеністю. Кількісно ця невизначеність може характеризуватися апіорним законом розподілу ймовірності посилки різних повідомлень $p(x_i)$, $i = 1, 2, \dots, M$.

Апостеріорний стан одержувача характеризується тим, що на вхід приймальної системи (приймача) надійшло коливання (що приймається) і по ньому сформовано рішення (оцінка) Y .

Припустимо, що одержувач, діючи за наказаним йому алгоритмом обробки, прийняв деяке конкретне рішення, скажімо, y_j . Якщо перешкод у каналі немає, то одержувач в цьому випадку точно знає, що було послане повідомлення x_j . Ніякої невизначеності у нього не залишається. Але основним інтересом є урахування явищ, пов'язаних з обов'язковою наявністю різних перешкод в каналі зв'язку. Якщо перешкоди є, то після отримання оцінки y_j в адресата ще залишається деяка невизначеність відносно того, яке повідомлення з множини x_1, x_2, \dots, x_M насправді було послане. Ця невизначеність, називається апостеріорною невизначеністю адресата (одержувача) і характеризується апостеріорним розподілом $p(x_i/x_j)$, тобто розподілом імовірності посилки різних повідомлень x_i за умови, що прийняте повідомлення (оцінка) x_j . В окремому випадку, коли дію перешкод можна не враховувати, апостеріорний розподіл вироджується в розподіл вигляду $p(x_i/x_j) = p(x_i)$, що характеризує детермінованість результату.

Отримання інформації тотожне усуненню незнання чогось або усуненню невизначеності чогось. Тому, розумно визначити кількість інформації, яку одержує адресат або яку передають йому по каналу зв'язку, як кількість невизначеності, що знімається в адресата при отриманні ним повідомлення. Відповідно кількість інформації, що передана по каналу зв'язку, ми можемо визначити за допомогою наступної, поки що словесної, формули, що показана на рис. 2.1.

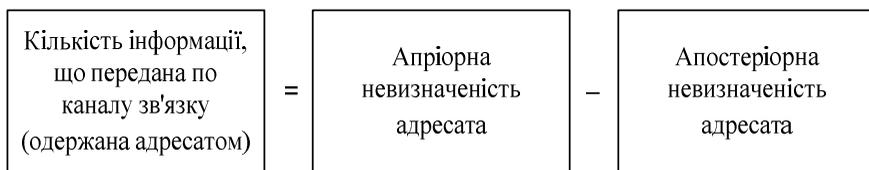


Рис. 2.1. Формула визначення кількості інформації, що передана по каналу зв'язку з перешкодами

В ідеалізованому каналі зв'язку без перешкод, апостеріорна невизначеність відсутня, тобто дорівнює нулю. При цьому кількість інформації визначається згідно формули, що показана на рис. 2.2.

Таким чином, кількість інформації виражається через кількість невизначеності в адресата в апіорному і апостеріорному стані. Інакше кажучи, необхідність визначення кількісної міри інформації зводиться до необхідності визначення кількісної міри невизначеності.

Кількість інформації, що передана по каналу зв'язку (одержана адресатом)	=	Апіорна невизначеність адресата
---	---	---------------------------------------

Рис. 2.2. Формула визначення кількості інформації, що передана по каналу зв'язку без перешкод

Апіорна і апостеріорна невизначеності адресата є окремим випадком загальної невизначеності – невизначеності довільного апіорного експерименту, або невизначеності закону розподілу ймовірності $p(x_i)$, що описує довільний випадковий експеримент X з результатами x_1, x_2, \dots, x_M . Кількісно міру невизначеності випадкового експерименту в теорії інформації, як було зазначено раніше називають ентропією H .

2.2. Міра оцінки кількості інформації за Р. Хартлі

Будь-який випадковий експеримент, зокрема робота джерел повідомлень, описується законом розподілу ймовірності різних результатів і має деяку невизначеність в тому значенні, що результат експерименту точно передбачити неможливо. Невизначеність тим більша, чим менше шансів (менша ймовірність) передбачити результат експерименту. І також, чим менша апіорна ймовірність окремої події, тим більшу кількість інформації вона несе. Ці твердження будуть лежати в основі визначення кількісної міри невизначеності (ентропії) випадкового експерименту і кількості інформації, що міститься в одному результаті.

Припустимо, що кількісною мірою невизначеності може бути величина, зворотня його апіорній ймовірності $1/p(x_i)$. Однак при визначенні кількісної міри невизначеності необхідно, щоб ентропія випадкового експерименту задовольняла таким умовам.

1. Ентропія H випадкового експерименту з рівноймовірними результатами повинна монотонно зростати зі збільшенням кількості результатів (потужності алфавіту) M .

Дійсно, при киданні монети $M=2$, ймовірність передбачити результат експерименту дорівнює $1/2$ (шанси передбачити результат 50 %). При киданні гральної кості $M=6$, ймовірність передбачити результат експерименту дорівнює $1/6$.

До першої умови приєднаємо ще дві очевидні умови, яким повинна задовольняти кількісна міра невизначеності будь-яких випадкових експериментів (не тільки з рівноймовірними результатами).

2. Якщо число результатів експерименту дорівнює одиниці ($M=1$), то результат експерименту відомий наперед і невизначеності немає ($H=0$).

3. Якщо відбуваються два незалежних експерименти A і B , то повна невизначеність експерименту AB дорівнює сумі невизначеностей експерименту A й експерименту B (властивість адитивності)

$$H(AB) = H(A) + H(B) \quad (2.1)$$

Остання умова еквівалентна наступній очевидній вимозі, яку необхідно пред'явити до кількісної міри невизначеності.

Невизначеність $H(AA)$ двічі незалежно повтореного експерименту A в два рази більша невизначеності $H(A)$ одного експерименту, $H(AA)=2H(A)$. Якщо експеримент A незалежним чином повторюється n разів, то повна невизначеність n -кратного експерименту повинна дорівнювати $nH(A)$.

Виразимо тепер сформульовані умови або вимоги до кількісної міри невизначеності H в аналітичному вигляді. На підставі першої умови можна записати наступне.

Якщо експеримент має M рівноймовірних результатів, то

$$H = f(M),$$

де $f(\bullet)$ – деяка монотонно зростаюча функція, яку належить визначити.

Друга умова дає

$$f(1) = 0. \quad (2.2)$$

Для того, щоб скористатися третьою умовою, припустимо, що експеримент A має M_A рівноймовірних результатів і відповідно ентропію $H(A) = f(M_A)$, а експеримент B має M_B рівноймовірних результатів і ентропію $H(B) = f(M_B)$.

Тоді експеримент AB , що є сукупністю експерименту A і експерименту B (які в цьому випадку вважаються незалежними), має $M_A M_B$ рівноймовірних результатів і його ентропія повинна мати вираз $H(A) = f(M_A M_B)$. На підставі третьої умови для функції $f(\bullet)$ повинна виконуватися рівність

$$f(M_A M_B) = f(M_A) + f(M_B). \quad (2.3)$$

Співвідношенням (2.2) і (2.3) при довільних значеннях M_A і M_B задо-

вольняє логарифмічна функція. Отже,

$$f(\bullet) = \log_a(\bullet). \quad (2.4)$$

Вибір основи логарифму принципового значення не має. Основа логарифму визначає величину одиниці вимірювання невизначеності. Вибір тієї або іншої одиниці є питанням зручності. Найчастіше всього приймають основу логарифма в (2.4) рівною 2.

Тоді кількість інформації $I(x_i)$, що міститься в символі x_i , вибраному з множини $\{x_i\}$ ($i = 1, 2, \dots, M$; M – об'єм алфавіту джерела повідомлень), з імовірністю $p(x_i)$, причому $\sum_{i=1}^M p(x_i) = 1$, визначається як

$$I(x_i) = \log \frac{1}{p(x_i)} = -\log p(x_i). \quad (2.5)$$

Цю аналітичну залежність для визначення кількості інформації у вигляді логарифмічного виразу запропонував у 1928 році американець Р. Хартлі. Логарифмічна міра оцінки кількості інформації як це буде показано нижче, найбільш повно відповідає вимогам, що пред'являються до неї. Значення основи логарифму може бути довільне. Воно визначає лише систему одиниць вимірювання кількості інформації (масштаб). При використанні десяткових логарифмів кількість інформації та ентропія визначаються в десяткових одиницях – дитах. У разі використання двійкових логарифмів кількість інформації та ентропія визначаються в двійкових одиницях – бітах. Нарешті, при використуванні натуральних логарифмів одиницею вимірювання є натуральна одиниця – ніт. При аналізі інформаційних процесів в пристроях, що функціонують на основі двійкової системи числення, зручно користуватися двійковими одиницями. У математичних викладеннях зручно користуватися натуральними одиницями.

У випадку рівної імовірності повідомлень $p(x_1) = p(x_2) = \dots = p(x_M) = 1/M$ вираз (2.5) для кількості інформації має вигляд

$$I(x_i) = -\log p(x_i) = \log M. \quad (2.6)$$

Таким чином один **біт інформації** – це така кількість інформації, що міститься в одній із двох рівноймовірних, незалежних та несумісних подій.

Такі джерела називаються джерелами нульового типу або джерелами Хартлі, а величини їх інформаційних мір відзначаються підрядковим індексом "0". Ентропія джерела Хартлі H_0 є максимальною.

У виразі (2.6) і в подальшому, відповідно до символіки, прийнятої в теорії інформації, основа логарифма a не ставиться, якщо $a=2$.

Визначимо ентропію випадкового експерименту з рівноймовірними

результатами, як середню кількість інформації, що припадає на один символ

$$\begin{aligned}
 H &= \frac{1}{M} \sum_{i=1}^M I(x_i) = \frac{1}{M} \left[- \sum_{i=1}^M \log p(x_i) \right] = \\
 &= \frac{1}{M} \sum_{i=1}^M \log M = \frac{1}{M} M \log M = \log M
 \end{aligned}
 \tag{2.7}$$

У виразі (2.7) за одиницю невизначеності прийнята невизначеність, яку має випадковий процес з двома рівноймовірними результатами ($M=2$). Прикладами такого експерименту є кидання монети, посилка двійкового повідомлення “0” або “1” (при рівності ймовірностей “0” і “1”).

Дійсно, підставлення в (2.7) $M=2$ дає $H=1$. Цю величину називають “двійкова одиниця” (дв. од.), або “біт”, що є скороченням англійського терміну “binary digit”. Отже для двійкового ДП ($m = 2$) кількість інформації, що передається одним символом (бітом), дорівнює

$$I(x_i) = - \log_2 p(x_i) = - \log_2 \frac{1}{2} = 1 \text{ (біт), так як } p(x_i) = \frac{1}{2}.$$

Розглянемо приклад. Нехай джерело повідомлень створює одне з 32-х рівноймовірних повідомлень, тоді ентропія джерела повідомлень або апіорна ентропія адресата дорівнює $H = \log_2 32 = 5$ дв. од.

Кожне повідомлення при роботі такого джерела можна надати п’ятизначним двійковим числом і звести до послідовного проведення п’яти простих незалежних експериментів з двома рівноймовірними результатами {0, 1}.

Не дивлячись на збіг залежностей (2.6) та (2.7), ентропія H і кількість інформації $I(x_i)$ принципово різні.

Ентропія H виражає середню невизначеність стану джерела повідомлень. Якщо відома статистика повідомлень, то H може бути обчислена апіорно, тобто до отримання повідомлення.

Кількість інформації $I(x_i)$ є апостеріорною характеристикою і визначає кількість інформації, що одержана з надходженням повідомлення x_i .

Збіг виражень для ентропії та кількості інформації свідчить лише про те, що кількість одержаної інформації чисельно дорівнює ентропії джерела у випадку рівної ймовірності його повідомлень.

Необхідно визначити, що запроваджена логарифмічна міра оцінки кількості інформації (міра Р. Хартлі) не враховує такі властивості інформації, як цінність, важливість та корисність.

2.3. Міра оцінки кількості інформації за К. Шенноном (Бернуллі)

Нехай дана загальна схема передачі інформації (повідомлень) у технічних системах (рис. 2.3.).

Нехай з виходу ДП передається дискретне повідомлення, що сформовано за допомогою кінцевої множини елементів $\{x_j\}$, $i = \overline{1, m}$ (алфавіту повідомлень). Сукупність усіх можливих символів $\{x_j\}$ алфавіту та ймовірності їх появи на виході ДП представляється у вигляді матриці, яку у теорії інформації називають **ансамблем повідомлень** або кінцевою схемою

$$X = \begin{pmatrix} x_1 & x_2 & \dots & x_i & \dots & x_m \\ p(x_1) & p(x_2) & \dots & p(x_i) & \dots & p(x_m) \end{pmatrix}, \quad (2.8)$$

при цьому $\sum_{i=1}^m p(x_i) = 1$.



Рис. 2.3 - Схема передачі повідомлення X

У цьому випадку (рис. 2.3) невизначеність передачі повідомлення розуміється у тому сенсі, що заздалегідь невідомо який саме символ x_i з m можливих алфавіту $\{x_j\}$, $i = \overline{1, m}$, може з'явитися на виході ДП, тобто це невизначеність $H(X)$ стану ДП. Тому середня кількість інформації, яку несе один символ дискретного повідомлення, дорівнює загальній (середньої) ентропії ДП.

Математичною моделлю таких повідомлень буде дискретна випадкова послідовність, елементи в якій нерівноймовірні, але вибір елементу здійснюється в незалежних від попередніх виборів умовах. Такі послідовності в математиці відомі як послідовності Бернуллі, а джерело, що формує такі послідовності називається дискретним джерелом без пам'яті (джерелом Шеннона (Бернуллі)), а величини їх інформаційних мір будемо відзначати підрядковим індексом "1". Зрозуміло, що кількість різних по-

відомлень, яка може бути створена джерелом Шеннона (Бернулі) буде декілька меншою ніж у джерел Хартлі.

Поняття ентропії та інформації близькі і пов'язані між собою, однак вони принципово відрізняються одне від одного.

Так ентропія $H(X)$ інформаційно характеризує ДП і якщо ми знаємо статистику повідомлення X (ансамбль повідомлення), то значення ентропії $H(X)$ може бути визначено апіорно (до проведення випробування, тобто до передачі повідомлення).

Інформація являє собою апостеріорну (після отримання ПП повідомлення) характеристику та на відміну від ентропії характеризує ПП. Кількість інформації $I(X)$, яку приймає ПП, визначається формулою, яка в даному випадку представляється у вигляді

$$I(X) = H(X) - H(X/Y), \quad (2.9)$$

де значення $H(X/Y)$ є апостеріорна ентропія повідомлення, тобто невизначеність того, що при передачі від ДП повідомлення X одержуємо на вході ПП повідомлення Y .

З урахування, що кількісно ентропія $H(X)$ дискретного джерела повідомлень є середня кількість інформації, яку несе один символ дискретного повідомлення, а також з урахуванням (2.8) маємо вираз для визначення загальної (середньої) ентропії ДДП:

$$H(X) = - \sum_{i=1}^m p(x_i) \cdot \log_2 p(x_i), \quad (2.10)$$

Вираз (2.10) являє собою повну (середню) безумовну ентропію (по К. Шеннону) для нерівноймовірних та незалежних символів алфавіту (подій). При цьому кількість інформації $I(X)$ в повідомленні X , що складається з n символів (тобто довжина повідомлення дорівнює n), дорівнює

$$I(X) = n \cdot H(X), \quad (2.11)$$

де n – кількість взаємозалежних (у цьому випадку у формулі (2.9) умовна ентропія дорівнює $H(X/Y) = 0$) символів у повідомленні.

У реальних умовах символи алфавіту $\{x_i\}$, $i = \overline{1, m}$, ДДП як правило мають різну ймовірність появи. Наприклад, літери російського алфавіту **О**, **Е** та **А** зустрічаються у тексті книжок частіше, ніж літери **Щ**, **Ы**, **Ф**. Так як ймовірності появи літер (символів) неоднакові, то кожна з них несе (містить) різну кількість інформації $I(x_i) = - \log_2 p(x_i)$. Малоімовірні повідомлення несуть більшу кількість інформації. Таким чином, середня кількість інформації на один символ x_i алфавіту визначається як математичне очікування дискретної випадкової величини $I(x_i)$.

Розглянемо випадок, коли символи на виході ДДП нерівноймовірні та незалежні.

Нехай маємо текстову X інформацію, що містить достатню кількість S символів x_i ($i = \overline{1, m}$) алфавіту. При цьому символ x_1 у тексті зустрічається n_1 раз, символ x_2 - n_2 раз, символ x_3 - n_3 раз і т.д., де символ x_m зустрічається n_m раз. У відповідності з цим кількість інформації, яка міститься у всіх символах тексту виду x_1 дорівнює $n_1 \cdot I(x_1)$, у символах x_2 - $n_2 \cdot I(x_2)$ і т.д., у всіх символах x_m - $n_m \cdot I(x_m)$. В цьому випадку загальна кількість інформації $I(X)$, що міститься у тексті, дорівнює значенню

$$I(X) = n_1 \cdot I(x_1) + n_2 \cdot I(x_2) + \dots + n_m \cdot I(x_m),$$

а середня кількість інформації, що приходить на один символ x_i алфавіту, дорівнює

$$I(X) = \frac{n_1 \cdot I(x_1) + n_2 \cdot I(x_2) + \dots + n_m \cdot I(x_m)}{S}.$$

Відношення n_i/S становить частоти повторення i -х символів і при великому значенні S будуть мати значення відповідних ймовірностей, тобто

$$\lim_{S \rightarrow \infty} n_i / S = p(x_i).$$

Якщо мати на увазі, що $I(x_i) = -\log_2 p(x_i)$, тоді маємо загальну формулу для визначення середньої (повної) безумовної ентропії у вигляді

$$\begin{aligned} \lim_{S \rightarrow \infty} \left[\frac{n_1 \cdot I(x_1) + n_2 \cdot I(x_2) + \dots + n_m \cdot I(x_m)}{S} \right] &= \\ = \lim_{S \rightarrow \infty} \left[\frac{n_1}{S} \cdot I(x_1) + \frac{n_2}{S} \cdot I(x_2) + \dots + \frac{n_m}{S} \cdot I(x_m) \right] &= \\ = - p(x_1) \cdot \log_2 p(x_1) - p(x_2) \cdot \log_2 p(x_2) - \dots - p(x_m) \cdot \log_2 p(x_m) &= \\ = - \sum_{i=1}^m p(x_i) \cdot \log_2 p(x_i). \end{aligned}$$

Розглянемо ще декілька визначень безумовної ентропії для нерівномірних, взаємозалежних символів $\{x_i\}$, алфавіту ДДП:

- $H(x_i) = -\log_2 p(x_i)$ – особистісна, безумовна ентропія ДДП (невизначеність на один конкретний x_i символ алфавіту $\{x_i\}$, $i = \overline{1, m}$, повідомлення ДДП);
- $H_i(x) = -p(x_i) \log_2 p(x_i)$ – особистісна, безумовна ентропія ДДП (характеризує лише i -й стан ДДП).

2.4. Міра оцінки кількості інформації за А. А. Марковим

Раніше розглядалося два варіанти функціонування джерел дискретних повідомлень. Перший варіант (міра Р. Хартлі), коли символи алфавіту

ДДП рівноймовірні та незалежні, та другий варіант (міра К. Шеннона) - символи алфавіту нерівноймовірні та незалежні. Всі розглянуті варіанти декілька спрощені та не зовсім відповідають реальним моделям побудови ДДП.

Коли виникає потреба кількісної оцінки ентропії одного ДДП з взаємозалежними повідомленнями (символами), або має місце об'єднання декількох ДДП в одну загальну систему, що виробляє загальне повідомлення, то такі повідомлення називаються **складними повідомленнями**.

Розглянемо кількісну оцінку ентропії та інформації складних дискретних повідомлень, що базується на поняттях особистісної та загальної умовних ентропій. Для складних дискретних повідомлень символи алфавіту ДДП - нерівноймовірні та залежні (джерело Маркова). Дискретним джерелом Маркова називається дискретне джерело з пам'яттю. Це джерело, що створює послідовності, у яких ймовірність формування чергового знака залежить від того, які знаки були вибрані до цього. Дискретні джерела Маркова є найзагальнішими моделями джерел дискретних повідомлень. Одномірні (джерела Шеннона) і нульмірні (джерела Хартлі) є їх окремими випадками.

Для математичного опису джерел Маркова необхідно окрім означення параметрів M і n повністю задати ансамбль імовірності, як при описі джерел Шеннона, і матрицю переходів кожного попереднього стану джерела в подальше.

При визначенні ентропії та інформації для повідомлень одного ДДП зі статичною залежністю елементів необхідно враховувати кореляційні зв'язки між ними. Такі зв'язки можуть бути як між окремими елементами, так і між різними групами елементів. Якщо кореляційний зв'язок охоплює тільки два сусідніх елементи, то ймовірність передачі будь-якого з цих двох елементів повідомлення залежатиме тільки від того, який з них був попереднім.

Наприклад, для елементів x_i та y_l ($l = \overline{1, m}$) можливі тільки два варіанти їх передачі: $x_i y_l$ або $y_l x_i$ з відповідними умовними ймовірностями $p(x_i/y_l)$ та $p(y_l/x_i)$. Такий зв'язок двох елементів x_i та y_l називають **однозв'язним простим ланцюгом Маркова**.

Так дійсно, у смислових повідомленнях одні літери зустрічаються частіше ніж інші, одні літери та слова частіше слідує за іншими та ін. Наприклад, у англійській мові найбільш часто зустрічаються літери e та t , на французькій мові після літери q частіше буде літера u , в українській та російських мовах ніколи не розміщуються поряд два м'яких знаки **ьь**.

Причини, що призводять до появи нерівноймовірності елементів алфавіту в повідомленні наступні. В російській мові, письмовий текст якого

є характерним прикладом джерела Маркова, залежність елементів в словах обумовлена обмеженнями, що накладаються російською граматикою на правила формування повідомлень. Так, в граматиці російської мови виключене написання букви “**Ъ**” після букви “**Ь**” і не допускається написання, наприклад, після букви “**Ч**” букв “**ЬГ**”, “**Я**”, “**Ю**”.

Обмеження такого вигляду можуть інтерпретуватися як двомірна пов’язаність в послідовності Маркова (або ланцюги, які іноді називають послідовностями). Обмеження можуть розповсюджуватися на три і більше символів повідомлень дискретного джерела. У цих випадках математичними моделями повідомлень будуть двозв’язні, тривз’язні і більшої зв’язності ланцюги Маркова. Зрозуміло, що при цьому ускладнюються методи визначення інформаційних характеристик повідомлень в порівнянні з джерелами Хартлі і Шеннона.

Для математичного опису джерел Маркова необхідно окрім вказівки параметрів M і n повністю задати ансамбль імовірності, як при описі джерел Шеннона, і матрицю переходів кожного попереднього стану джерела у подальшому.

Дискретні джерела Маркова є найзагальнішими моделями джерел дискретних повідомлень. Одномірні (джерела Шеннона) і нульмірні (джерела Хартлі) є їх окремими випадками.

Поняття умовної ентропії у теорії інформації використовується у слідуючих випадках:

- при визначенні взаємозалежності між символами алфавіту, що передаються по каналам зв’язку;
- для визначенні інформаційних втрат при передачі повідомлення;
- при необхідності обчислення ентропії об’єднання.

Розглянемо ці три випадки окремо.

1. Необхідність визначення взаємозалежності між різними символами алфавіту одного (рис. 2.4), чи декількох одноразово (рис. 2.5) ДДП.

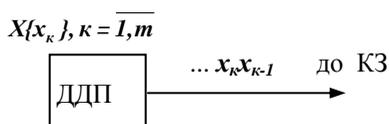


Рис. 2.4 Схема статистичних зв’язків символів алфавіту одного ДДП

2. При визначенні втрат інформації при передачі повідомлень по каналу зв’язку (рис. 2.6).

3. При обчисленні ентропії $H(X, Y)$ об’єднання, що використовується для знаходження ентропії спільної появи статистично залежних повідом-

лень (елементів повідомлення).

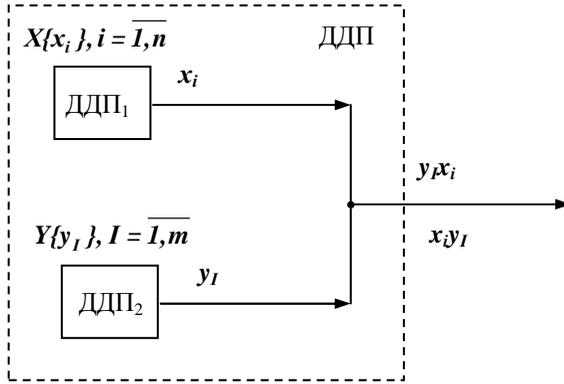


Рис. 2.5 - Схема статистичних зв'язків символів двох ДДП

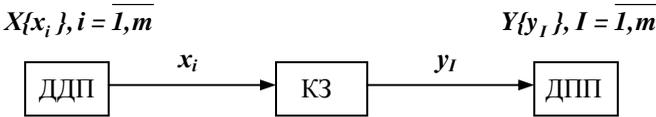


Рис. 2.6 - Схема передачі інформації по КЗ

Нехай об'єднання двох ДДП X та Y задані двома ансамблями повідомлень

$$X = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ p(x_1) & p(x_2) & \dots & p(x_n) \end{pmatrix} \quad \text{та} \quad Y = \begin{pmatrix} y_1 & y_2 & \dots & y_m \\ p(y_1) & p(y_2) & \dots & p(y_m) \end{pmatrix},$$

що є сукупністю цих взаємозалежних ансамблів, яка характеризує загальну ентропію $H(X, Y)$ об'єднання повідомлень X та Y .

Необхідно визначити наступні інформаційні характеристики об'єданого ДДП.

1. Особистісні умовні ентропії $H(x_i/y_i) = H(X/y_i)$ та $H(y_i/x_i) = H(Y/x_i)$.
2. Загальні умовні ентропії $H(X/Y)$ та $H(Y/X)$.
3. Ентропію об'єднання $H(X, Y)$, яка використовується для обчислення ентропії спільної появи статично залежних повідомлень (об'єднанням звать сукупність двох і більше взаємозалежних ансамблів дискретних повідомлень).

4. Середня кількість інформації, що одержує ДПП:

$$I(X, Y) = I(Y, X) = I(X) = H(X) - H(X/Y).$$

5. Взаємну ентропію $H(X \cdot Y)$.

Схема об'єднання двох ДДП в одно ДДП задана матрицею $P(X, Y)$ (табл. 2.2) об'єднання двох джерел X та Y (так звана канална матриця).

Визначимо особистісні умовні ентропії $H(x_i/y_j) = H(X/y_j)$ та $H(y_j/x_i) = H(Y/x_i)$.

Таблиця 2.2

Матриця об'єднання $P(X, Y)$

$X \backslash Y$	x_1	x_2	...	x_i	...	x_n	$p_I = p(y_I)$
y_1	$p(x_1, y_1)$	$p(x_2, y_1)$		$p(x_i, y_1)$		$p(x_n, y_1)$	$p_I = p(y_1)$
y_2	$p(x_1, y_2)$	$p(x_2, y_2)$		$p(x_i, y_2)$		$p(x_n, y_2)$	$p_2 = p(y_2)$
.							.
							.
y_j	$p(x_1, y_j)$	$p(x_2, y_j)$...	$p(x_i, y_j)$...	$p(x_n, y_j)$	$p(y_j) = \sum_{i=1}^n p(x_i, y_j),$ $j = \overline{1, m}.$
							.
							.
							.
y_m	$p(x_1, y_m)$	$p(x_2, y_m)$...	$p(x_i, y_m)$...	$p(x_n, y_m)$	$p_m = p(y_m)$
$P_i = p(x_i)$	P_1	P_2		P_i		$P_n = p(x_n)$	I I
$P_i = p(x_i) = \sum_{j=1}^m p(x_i, y_j), \quad i = \overline{1, n}.$							

Нехай поява події X залежить від появи події Y і навпаки. Нехай $p(x_i)$ - ймовірність появи i -ої ознаки події X , а $p(y_j)$ - ймовірність появи j -ої ознаки події Y ; $p(x_i/y_j)$ - умовна ймовірність появи i -ої ознаки x_i події X , відносно j -ої ознаки y_j події Y (наприклад: поява i -го символу повідомлення X після появи j -го символу повідомлення Y); $p(y_j/x_i)$ - умовна ймовірність появи j -ої ознаки події Y , відносно i -ої ознаки події X .

З теорії ймовірності відомо, що для взаємозалежних подій X та Y ма-

єМО

$$P(X, Y) = P(Y, X) = P(X) \cdot P(Y/X) = P(Y) \cdot P(X/Y).$$

Визначимо особистісну умовну ентропію $H(Y/x_i)$. Згідно з загальною схемою передачі інформації (рис. 2.6) особистісна умовна ентропія визначається підстановкою замість значення $p(y_j)$ значення ймовірності $p(y_j/x_i)$. Тоді маємо

$$H(y_i/x_i) = H(Y/x_i) = \sum_{j=1}^m p(y_j/x_i) \log_2 p(y_j/x_i). \quad (2.12)$$

Таким чином частинна умовна ентропія $H(Y/x_i)$ - це невизначеність того, що відправив із ДДП символ x_i на вході ДПП одержимо символ y_j (рис. 2.7)

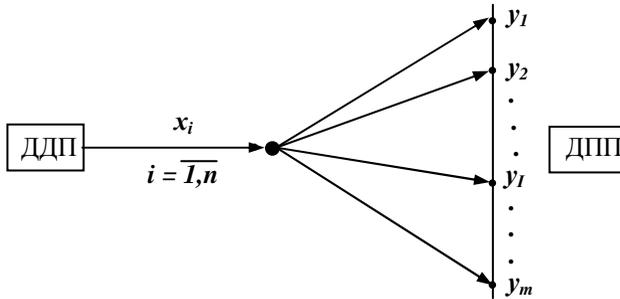


Рис. 2.7 - Схема статистичної залежності символів x_i та y_j при передачі повідомлення X

Особистісна умовна ентропія $H(X/y_j)$ кількісно визначається за формулою загальної безумовної ентропії $H(X)$ підстановкою замість $p(x_i)$ значення $p(x_i/y_j)$. Тоді маємо

$$H(x_i/y_j) = H(X/y_j) = \sum_{i=1}^n p(x_i/y_j) \log_2 p(x_i/y_j), \quad (2.13)$$

де $j = \text{const}$; $I = \text{const}$; $i = \overline{1, n}$.

На рис. 2.8 представлена схема статистичної залежності символів при прийомі повідомлення.

Таким чином особистісна умовна ентропія $H(X/y_j)$ - це невизначеність, яка залишилася після отримання ДПП символу y_j у тому, що ДДП пердало символ x_i .

Визначимо загальні умовні ентропії $H(X/Y)$ та $H(Y/X)$. Загальна умовна ентропія повідомлення Y відносно повідомлення X характеризує кількість інформації, що міститься у будь якому символі алфавіту. Загальна

умовна ентропія $H(Y/X)$ або $H(X/Y)$ може змінюватися у таких межах $0 \leq H(Y/X) \leq H(Y)$ та відповідно $0 \leq H(X/Y) \leq H(X)$.

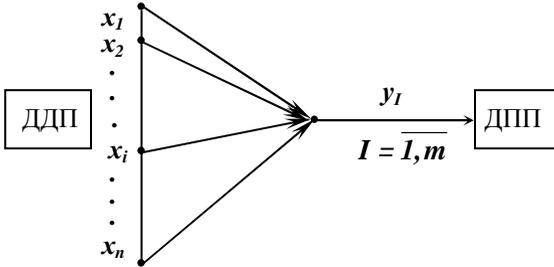


Рис. 2.8 - Схема статичної залежності символів x_i та y_i при прийомі повідомлення Y

При повній статистичній залежності між елементами повідомлення $H(Y/X) = 0$ та $H(X/Y) = 0$. При незалежних між собою повідомленнях X та Y маємо $H(Y/X) = H(Y)$ та $H(X/Y) = H(X)$.

Для об'єднаної ентропії $H(X, Y)$ виконується наступна нерівність $H(X, Y) \leq H(X) + H(Y)$.

Для незалежних повідомлень X та Y буде виконуватися рівність $H(X, Y) = H(X) + H(Y)$.

Загальна умовна ентропія повідомлення Y відносно повідомлення X визначається усередненням за всіма символами, тобто за всіма станами з обліком ймовірностей появи кожного зі станів, та чисельно дорівнює сумі ймовірностей появи символів алфавіту, помноженої на невизначеність, яка залишається після того, як адресат прийняв повідомлення

$$H(Y/X) = + \sum_{i=1}^n p(x_i) H(Y/x_i) = - \sum_{i=1}^n p(x_i) \sum_{j=1}^m p(y_j / x_i) \log_2 p(y_j / x_i). \quad (2.14)$$

Аналогічно можна отримати вираз для визначення $H(X/Y)$, тобто,

$$H(X/Y) = + \sum_{j=1}^m p(y_j) H(X/y_j) = - \sum_{j=1}^m p(y_j) \sum_{i=1}^n p(x_i / y_j) \log_2 p(x_i / y_j). \quad (2.15)$$

Визначимо ентропію об'єднання $H(X, Y)$, яка використовується для обчислення ентропії спільної появи статистично залежних повідомлень, тобто це міра невизначеності того, що якщо буде відправлено повідомлення X , а прийнято повідомлення Y .

У цьому випадку ентропія об'єднання $H(X, Y)$ кількісно оцінюється наступним чином

$$H(X, Y) = - \sum_{i=1}^n \sum_{j=1}^m p(x_i, y_j) \cdot \log_2 p(x_i, y_j) \text{ [біт/два символи]}. \quad (2.16)$$

Таким чином ентропія об'єднання $H(X, Y)$ - це середня кількість інформації на пару (переданого та прийнятого) символів x_i та y_j алфавіту.

З теорії ймовірностей для залежних подій x_i та y_j маємо

$$p(x_i, y_j) = p(y_j, x_i) = p(x_i) \cdot p(y_j / x_i) = p(y_j) \cdot p(x_i / y_j). \quad (2.17)$$

Тоді з урахуванням (2.17) вираз (2.16) приймає наступний вигляд

$$\begin{aligned} H(X, Y) &= - \sum_{i=1}^n \sum_{j=1}^m p(x_i, y_j) \cdot \log_2 p(x_i, y_j) = \\ &= - \sum_{i=1}^n \sum_{j=1}^m p(x_i) p(y_j / x_i) \log_2 [p(x_i) p(y_j / x_i)] = \\ &= - \left\{ \sum_{i=1}^n \sum_{j=1}^m p(x_i) p(y_j / x_i) \left[\log_2 p(x_i) + \log_2 p(y_j / x_i) \right] \right\} = \\ &= - \left\{ \sum_{i=1}^n \sum_{j=1}^m p(x_i) \cdot p(y_j / x_i) \cdot \log_2 p(x_i) + \right. \\ &\quad \left. + \sum_{i=1}^n \sum_{j=1}^m p(x_i) p(y_j / x_i) \log_2 p(y_j / x_i) \right\} = \\ &= - \sum_{i=1}^n p(x_i) \log_2 p(x_i) \sum_{j=1}^m p(y_j / x_i) - \sum_{j=1}^m p(y_j / x_i) \log_2 p(y_j / x_i) \sum_{i=1}^n p(x_i). \end{aligned} \quad (2.18)$$

З формули (2.18) маємо:

$$\sum_{j=1}^m p(y_j / x_i) = p(y_1 / x_i) + p(y_2 / x_i) + \dots + p(y_m / x_i) = 1,$$

так як i -й стан залишається постійним (повна група подій $\sum_{i=1}^n p(x_i) = 1$), а

$$H(X) = - \sum_{i=1}^n p(x_i) \log_2 p(x_i) \quad \text{і} \quad H(Y/X) = - \sum_{j=1}^m p(y_j / x_i) \log_2 p(y_j / x_i),$$

хуванням вищеозначеного формула (2.18) приймає вигляд

$$H(X, Y) = H(X) + H(Y/X). \quad (2.19)$$

Нескладно показати, що у загальному випадку

$$H(X, Y) = H(Y, X) = H(X) + H(Y/X) = H(Y) + H(X/Y). \quad (2.20)$$

Формула (2.20) є співвідношенням для визначення ентропії об'єднання за рахунок використання аналітичних залежностей для безумовної та умовної ентропій.

Тепер визначимо середню кількість інформації $I(X)$. Середня кіль-

кість інформації $I(X)$ – це кількість інформації на один символ повідомлення, переданого по КЗ під впливом перешкод. Визначимо значення $I(X)$ за допомогою ентропії об'єднання $H(X, Y)$.

У загальному випадку середня кількість інформації визначається відомим співвідношенням

$$I(X, Y) = I(Y, X) = H(X) - H(X/Y), \quad (2.21)$$

де: $H(X)$ - безумовна апіорна (додослідна) ентропія ДДП;

$H(X/Y)$ - загальна умовна апостеріорна (після дослідна) ентропія ДДП;

$I(X)$ - кількість інформації, що одержує ДПП.

Визначимо значення $I(X)$. Для цього підставимо значення ймовірностей у формулу (2.21). Маємо

$$I(X) = H(X) - H(X/Y) = -\sum_{i=1}^n p(x_i) \cdot \log_2 p(x_i) + \sum_{i=1}^n \sum_{j=1}^n p(y_j) \times \\ \times p(x_i/y_j) \cdot \log_2 p(x_i/y_j). \quad (2.22)$$

У формулі (2.22) зробимо правомірну заміну $p(y_j) p(x_i/y_j) = p(x_i, y_j)$, а також помножимо першу частину формули (2.22) на значення

$\sum_{j=1}^n p(y_j/x_i) = 1$. У цьому випадку маємо

$$I(X) = -\sum_{i=1}^n p(x_i) \log_2 p(x_i) \sum_{j=1}^n p(y_j/x_i) + \sum_{i=1}^n \sum_{j=1}^n p(x_i, y_j) \log_2 p(x_i/y_j) = \\ = -\sum_{i=1}^n \sum_{j=1}^n p(x_i, y_j) \log_2 p(x_i) + \sum_{i=1}^n \sum_{j=1}^n p(x_i, y_j) \log_2 \frac{p(x_i, y_j)}{p(y_j)}, \quad (2.23)$$

тому, що $p(x_i, y_j) = p(x_i) \cdot p(y_j/x_i)$ та $p(x_i/y_j) = \frac{p(x_i, y_j)}{p(y_j)}$.

Після перетворення вираз (2.23) приймає такий вигляд

$$I(X) = \sum_{i=1}^n \sum_{j=1}^n p(x_i, y_j) \cdot \log_2 \frac{p(x_i, y_j)}{p(x_i) \cdot p(y_j)}. \quad (2.24)$$

Таким чином формула (2.24) визначає кількість інформації на один символ повідомлення, переданого КЗ (середню кількість інформації) шляхом застосування відомої ентропії $P(x_i, y_j)$ об'єднання.

Визначимо взаємну ентропію. Взаємна ентропія $H(X, Y)$ системи передачі та прийому у цілому, або середня кількість інформації на одну пару (переданого та прийнятого) символів алфавіту, визначається таким чином

$$H(XY) = -\sum_{i=1}^n \sum_{j=1}^m p(x_i \cdot y_j) \cdot \log_2 p(x_i \cdot y_j). \quad (2.25)$$

Формула (2.25) визначається шляхом підстановки замість значення $p(x_i)$ ймовірності $p(x_i y_j)$.

З теорії ймовірностей відомо, що

$$p(x_i y_j) = p(x_i) \cdot p(y_j/x_i) = p(y_j) \cdot p(x_i/y_j). \quad (2.26)$$

Тоді вираз (2.25) приймає наступний вигляд

$$\begin{aligned} H(XY) &= -\sum_{i=1}^n \sum_{j=1}^m p(x_i y_j) \cdot \log_2 [p(x_i) p(x_i/y_j)] = \\ &= -\sum_{i=1}^n \sum_{j=1}^m p(x_i y_j) \cdot \log_2 p(x_i) - \sum_{i=1}^n \sum_{j=1}^m p(x_i y_j) \cdot \log_2 p(x_i/y_j). \end{aligned}$$

З урахуванням співвідношення (2.26) маємо

$$\begin{aligned} H(XY) &= -\sum_{i=1}^n \sum_{j=1}^m p(x_i) p(y_j/x_i) \log_2 p(x_i) - \\ &\quad - \sum_{i=1}^n \sum_{j=1}^m p(y_j) p(x_i/y_j) \log_2 p(y_j/x_i) = \\ &= \sum_{j=1}^m p(y_j/x_i) \sum_{i=1}^n p(x_i) \log_2 p(x_i) - \\ &\quad - \sum_{j=1}^m p(y_j) \sum_{i=1}^n p(x_i/y_j) \log_2 [p(y_j/x_i)^{-1}]. \end{aligned} \quad (2.27)$$

Тоді вираз (2.27) представиться у наступному вигляді

$$\begin{aligned} H(XY) &= -\sum_{j=1}^m p(y_j/x_i) \sum_{i=1}^n p(x_i) \log_2 p(x_i) - \\ &\quad - \left\{ -\sum_{j=1}^m p(y_j) \sum_{i=1}^n p(x_i/y_j) \log_2 p(x_i/y_j) \right\}. \end{aligned}$$

Так, як $\sum_{j=1}^m p(y_j/x_i) = 1$, а $-\sum_{i=1}^n p(x_i) \log_2 p(x_i) = H(X)$ та

$-\sum_{j=1}^m p(y_j) \sum_{i=1}^n p(x_i/y_j) \log_2 (x_i/y_j) = H(X/Y)$, вираз (2.27) буде мати такий

вигляд

$$H(XY) = H(X) - H(X/Y). \quad (2.28)$$

Аналогічно можна вивести наступне співвідношення

$$H(XY) = H(Y) - H(Y/X). \quad (2.29)$$

2.5. Основні властивості інформації та ентропії

Можна виділити наступні основні властивості інформації.

1. Інформація $I(x_i)$ є величина нескінченна, тобто $0 \leq I(x_i) \leq \infty$. Дійсно, при $P(x_i) = 1$ (відоме повідомлення) кількість інформації дорівнює $I(x_i) = 0$, а при $P(x_i) \rightarrow 0$, $I(x_i) \rightarrow \infty$ (рис. 2.9).

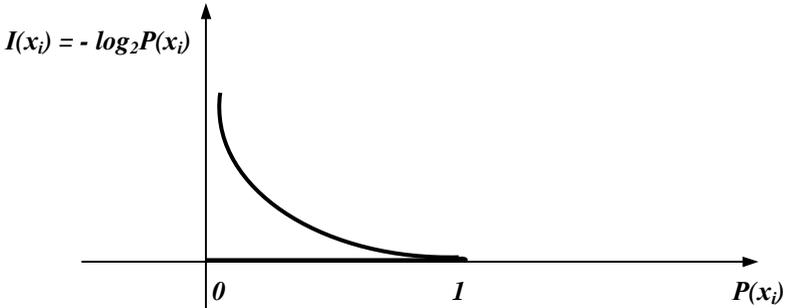


Рис. 2.9 - Графік залежності $I(x_i) = -\log_2 P(x_i)$

2. Кількість інформації $I(x_i)$ від n незалежних ДП дорівнює сумі інформації $I(x_i)$ від кожного з даних джерел, тобто

$$I(X) = \sum_{i=1}^n I(x_i). \quad (2.30)$$

Покажемо це на прикладі двох ($n = 2$) незалежних ДП. Дійсно,

$$I(X) = I(x_1, x_2) = \log_2 \frac{1}{P(x_1, x_2)}.$$

Так, як події x_1 та x_2 незалежні, то $P(x_1, x_2) = P(x_1) \cdot P(x_2)$. У цьому разі

$$\begin{aligned} I(X) &= \log_2 \frac{1}{P(x_1, x_2)} = \log_2 \frac{1}{P(x_1) \cdot P(x_2)} = \log_2 \left[\frac{1}{P(x_1)} \cdot \frac{1}{P(x_2)} \right] = \\ &= \log_2 \frac{1}{P(x_1)} + \log_2 \frac{1}{P(x_2)} = I(x_1) + I(x_2). \end{aligned}$$

Не складно показати, що для загального випадку, якщо маємо n незалежних ДП формула (2.30) також дійсна.

У випадку, коли повідомлення складається з $n > 1$ елементів (літер

повідомлення) маємо

$$I(X) = H(X) = \log_2 N = \log_2 m^n = n \log_2 m,$$

де: $N = m^n$ – загальна кількість повідомлень, що можна отримати, комбінує m символів алфавіту по n елементів в кожному повідомленні, тобто кількість елементів в повідомленні (довжина повідомлення) дорівнює n .

З метою подальшої кількісної оцінки ентропії та інформації розглянемо основні властивості ентропії.

1. Ентропія $H(X)$ невід'ємна величина, яка лежить у діапазоні

$$0 \leq H(X) = - \sum_{i=1}^m p(x_i) \cdot \log_2 p(x_i) \leq \log_2 m. \quad (2.31)$$

2. При рівноймовірних та незалежних символах алфавіту $\{x_i\}$, $i = 1, m$, значення ентропії $H(X)$ дорівнює $\log_2 m$. Дійсно, для рівноймовірних подій (рівно ймовірних символів алфавіту) маємо

$$p(x_1) = p(x_2) = \dots = p(x_m) = \frac{1}{m}.$$

Ентропії визначається, як

$$H(X) = - \sum_{i=1}^m p(x_i) \cdot \log_2 p(x_i) = m \cdot \frac{1}{m} \cdot \log_2 m = \log_2 m. \quad (2.32)$$

3. Ентропія детермінованих станів ДДП (означених: $p(x_i) = 1$ (вірогідний), або $p(x_i) = 0$ (неможливий)) дорівнює нулю. Розглянемо ці два випадки.

3.1. Нехай $m = 1$ та $p(x_i) = 1$ (подія вірогідна). Тоді

$$H(X) = - p(x_1) \cdot \log_2 p(x_1) = -1 \cdot \log_2 1 = 0$$

3.2. Якщо $p(x_i) = 0$ (подія неможлива), тоді

$$[- p(x_i) \cdot \log_2 p(x_i)] = p(x_i) \cdot \log_2 \frac{1}{p(x_i)} = 0 \cdot \log_2 \infty = 0 \cdot \infty.$$

Розкриваємо невизначеність виду $0/\infty$ по правилу Лопітала, тобто приводимо цю невизначеність до невизначеності виду ∞/∞ , тобто

$$\lim_{p(x_i) \rightarrow 0} [- p(x_i) \cdot \log_2 p(x_i)] = \lim_{p(x_i) \rightarrow 0} \left[\frac{\log_2 \frac{1}{p(x_i)}}{\frac{1}{p(x_i)}} \right].$$

Позначимо $K = \frac{1}{p(x_i)}$. В цьому випадку маємо $\lim_{k \rightarrow \infty} \frac{\log_2 k}{k} = \frac{\infty}{\infty}$. Далі

по правилу Лопітала беремо першу похідну для значень чисельника та знаменника і отриманий вираз прирівнюємо до нуля

$$\lim_{k \rightarrow \infty} \frac{(\log_2 K)'}{K'} = \lim_{k \rightarrow \infty} \frac{\frac{1}{k} \cdot \log_2 e}{\frac{1}{k}} = \log_2 \frac{1}{k} \cdot \log_2 e = 0.$$

Тоді у загальному випадку отримуємо, що

$$H(X) = - \sum_{i=1}^m p(x_i) \cdot \log_2 p(x_i) \equiv 0.$$

4. Ентропія $H(X)$ має екстремум.

Спочатку зробимо дослідження на екстремум особистісної $H_i(x)$ ентропії. Для цього беремо першу похідну від $H_i(x)$ по $p(x_i)$ і прирівнюємо її до нуля, тобто

$$\frac{dH_i(x)}{dp(x_i)} = \frac{d[-p(x_i) \cdot \log_2 p(x_i)]}{dp(x_i)} = 0.$$

Маємо

$$\begin{aligned} [-p(x_i) \cdot \log_2 p(x_i)]' &= -1 \cdot \log_2 p(x_i) - p(x_i) \cdot \frac{1}{p(x_i)} \cdot \log_2 e = \\ &= -\log_2 p(x_i) - \log_2 e = 0. \end{aligned}$$

Тоді, якщо $-\log_2 [p(x_i) \cdot e] = 0$, і відповідно $\log_2 [p(x_i) \cdot e] = 0$, а $p(x_i) \cdot e = 1$, отримуємо, що $p(x_i) = \frac{1}{e} \approx \frac{1}{2,7} \approx 0,36$.

Таким чином ентропія $H_i(x)$ максимальна при $p(x_i) \approx 0,36$. В цьому випадку $H_i(x) = -p(x_i) \cdot \log_2 p(x_i) = 0,36 \cdot \log_2 0,36 \approx 0,531 = \max$. На рис. 2.10 представлений графік залежності $H_i(x) = F[p(x_i)]$, де показано зміну значень ентропії $H_i(x)$ при $0 \leq p(x_i) \leq 1$.

5. Прийmemo без доведення, що загальна ентропія $H(X)$ ДДП максимальна для рівномірних подій (див. другу властивість ентропії $H(X)$), тобто

$$H(X) = - \sum_{i=1}^m p(x_i) \cdot \log_2 p(x_i) = \log_2 m = \max,$$

при $p(x_1) = p(x_2) = \dots = p(x_m) = \frac{1}{m}$.

Нехай $m = 2$ ($p(x_1) = p(x_2) = \frac{1}{2}$), тобто, маємо двійкове ДДП. Тоді

$$H(X) = - \sum_{i=1}^2 p(x_i) \cdot \log_2 p(x_i) = -2 \cdot \frac{1}{2} \cdot \log_2 \frac{1}{2} = \log_2 2 = 1 \text{ (біт)}.$$

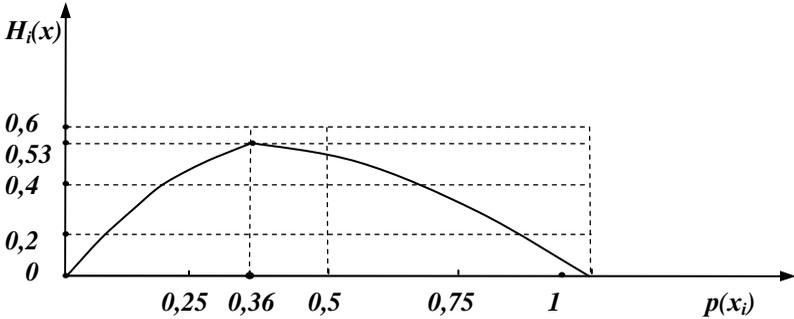


Рис. 2.10 - Графік функції $H_i(x) = F[p(x_i)]$

Таким чином загальна безумовна ентропія $H(X)$ максимальна і дорівнює одному біту інформації (рис. 2.11)

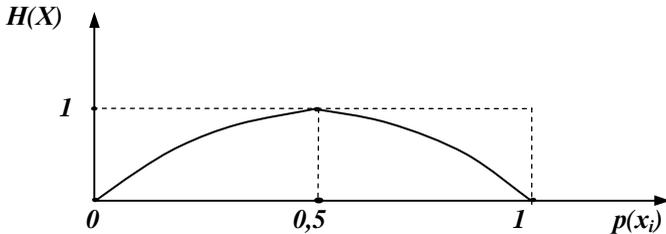


Рис. 2.11 - Графік залежності $H(X) = F[p(x_i)]$ при $m = 2$

6. Властивість адитивності ентропії

Повна ентропія $H(A, B)$ повідомлення, що складається з двох окремих незалежних повідомлень A та B , дорівнює сумі ентропій $H(A)$ та $H(B)$ цих повідомлень. У загальному випадку

$$H(A_1, A_2, \dots, A_k) = H(A_1) + H(A_2) + \dots + H(A_k) \quad (2.33)$$

Для випадку $m = 2$ (рис. 2.12)

Розглянемо можливі випадки станів сумісного ДДП. Нехай:

$P_i(A)$ – ймовірність появи події A (ДДП₁);

$P_j(B)$ – ймовірність появи події B (ДДП₂);

$P_{ij}(A, B)$ – ймовірність появи сумісної події A і B .

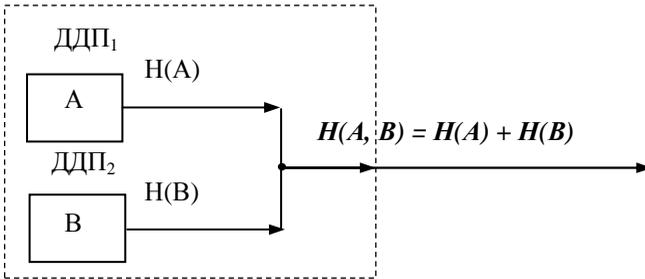


Рис. 2.12 - Схема об'єднання двох ДДП

З теорії ймовірностей відомо, що для незалежних подій A та B виконується умова $P_{ij}(A, B) = P_i(A) \cdot P_j(B)$. В цьому випадку визначимо повну сумісну ентропію $H(X)$ двох повідомлень

$$\begin{aligned} H(A, B) &= - \sum_{i=1}^m \sum_{j=1}^m P_{ij}(A, B) \cdot \log_2 P_{ij}(A, B) = - \sum_{i=1}^m \sum_{j=1}^m P_i(A) \cdot P_j(B) \cdot \log_2 [P_i(A) \cdot P_j(B)] = \\ &= - \sum_{i=1}^m \sum_{j=1}^m P_i(A) \cdot P_j(B) \cdot [\log_2 P_i(A) + \log_2 P_j(B)] = \\ &= - \sum_{i=1}^m P_i(A) \cdot \log_2 P_i(A) \cdot \sum_{j=1}^m P_j(B) - \sum_{j=1}^m P_j(B) \cdot \log_2 P_j(B) \cdot \sum_{i=1}^m P_i(A). \quad (2.34) \end{aligned}$$

У разі того, що $\sum_{j=1}^m P_j(B) = 1$ та $\sum_{i=1}^m P_i(A) = 1$ (повна група подій) вираз

(2.34) набуває вигляд

$$H(A, B) = - \sum_{i=1}^m P_i(A) \cdot \log_2 P_i(A) - \sum_{j=1}^m P_j(B) \cdot \log_2 P_j(B),$$

тобто маємо

$$H(A, B) = H(A) + H(B). \quad (2.35)$$

Формула (2.35) підтверджує інтуїтивний висновок, що повна ентропія повідомлення, яка складається з декількох незалежних повідомлень, дорівнює сумі ентропій цих повідомлень, тобто

$$H(A_1, A_2, \dots, A_k) = \sum_{i=1}^k H(A_i).$$

2.6. Інформаційні характеристики джерел дискретних повідомлень

Середня ентропія повідомлень при однаковій кількості m елементів алфавіту джерела дискретних повідомлень (ДДП) може бути різною залежно від статистичних характеристик повідомлень. Відомо, що ентропія приймає максимальне значення, якщо елементи повідомлення рівномірні та незалежні. В цьому випадку $H_0 = \log_2 m$. Природно, що повідомлення, ентропія яких максимальна, є оптимальними з точки зору найбільшої кількості інформації, яка міститься в одному розряді повідомлення (довжина повідомлення може дорівнювати S_n розрядів).

Таким чином можна виділити такі важливими інформаційними характеристиками джерела дискретних повідомлень:

- ентропія;
- інформація;
- абсолютна інформаційна недовантаженість на один символ повідомлення $\Delta H(X)$;
- коефіцієнт інформаційної надмірності K_n ;
- коефіцієнт стиску інформації K_c ;
- продуктивність ДДП $H'(X)$.

Абсолютна інформаційна недовантаженість на один символ повідомлення ДДП $\Delta H(X)$ визначається таким чином

$$\Delta H(X) = H_0(X) - H_n(X), \quad (2.36)$$

де: $H_0(X)$ – максимальна можлива ентропія на один символ алфавіту повідомлення, що складається з S_0 елементів (довжина повідомлення складається з S_0 елементів);

$H_n(X)$ – ентропія даного ДДП для реальних повідомлень, що складаються з S_n елементів (середня ентропія на один символ алфавіту $X\{x_i\}$, $i = \overline{1, m}$, повідомлення, що складається з S_n елементів).

На рисунку 2.13 представлено пояснення до формули (2.36).

Більшість реальних джерел повідомлень мають надмірність, яка визначається відмінністю закону розподілу ймовірності появи символів від рівномірного і наявністю зв'язків між ними. Ентропія таких джерел менша за максимальну – кожен символ в середньому несе меншу кількість інформації, ніж він міг би нести.

Надмірність дискретного M -ічного джерела обчислюється за формулою

$$\rho = \frac{H_{\max}(X) - H(X)}{H_{\max}(X)} = 1 - \frac{H(X)}{H_{\max}(X)} = 1 - \frac{H(X)}{\log_2 M}.$$

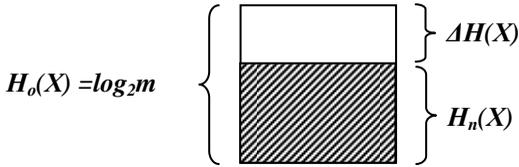


Рис. 2.13 - Середня ентропія на один символ повідомлення

Вона характеризує ступінь використання інформаційної ємності алфавіту джерела. Якщо $\rho=0$, то ємність алфавіту використовується повністю, якщо $\rho>0$, то, в принципі, існує інший, більш стислий спосіб подання повідомлень джерела.

Надмірність повідомлень джерела призводить до надмірності кодових комбінацій, що призводить до зменшення швидкості передачі інформації. Припустимо, що необхідно закодувати 32 букви російського алфавіту. При двійковому коді їх можна кодувати послідовностями з п'яти двійкових символів, оскільки таких послідовностей теж 32. Якщо вважати алфавіт рівномірним, то кожна буква і кожна кодова комбінація переносять 5 біт інформації, а кожен кодовий символ 1 біт.

Але насправді через нерівномірність і залежність кожна буква несе в середньому меншу кількість інформації. Так, ентропія джерела при урахуванні статистичних зв'язків всього лише між трьома буквами дорівнює 3 біт і на частину кожного кодового символу доводиться в середньому 0,6 біт. При цьому швидкість передачі інформації буде менша, ніж пропускна здібність каналу, тобто символ коду при одній і тій же тривалості τ міг би доставити за секунду $1/\tau$ біт інформації, а доставляє лише $0,6/\tau$ біт. Отже, канал використовується неефективно. Швидкість передачі інформації в ньому менша, ніж пропускна здатність.

Велика надмірність повідомлень, з одного боку, перешкоджає інформаційному обміну, вимагаючи зайвих витрат енергії і часу на передачу повідомлень. З іншого боку, повідомлення з малою інформаційною надмірністю виявляються дуже чутливими до дії перешкод, а це, в свою чергу, перешкоджає забезпеченню достовірності їх передачі по реальних каналах зв'язку.

Коефіцієнт інформаційної надмірності (інформаційна надмірність) K_n на один символ алфавіту $X\{x_i\}$, $i = \overline{1, m}$, знаходиться за формулою

$$K_n = \frac{\Delta H(X)}{H_0(X)} = \frac{H_0(X) - H_n(X)}{H_0(X)} = 1 - \frac{H_n(X)}{H_0(X)} \quad (2.37)$$

Відзначимо, що $H_o(X)$ може бути досягнута підбором розподілу ймовірностей появи символів x_i алфавіту та усуненням взаємної залежності між ними, тобто їх кореляції.

Коефіцієнт стиску інформації K_c визначається таким чином

$$K_c = \frac{H_n(X)}{H_o(X)}, \quad (2.38)$$

де $0 \leq K_c \leq 1$.

Співвідношення (2.37) та (2.38) зв'язані між собою таким чином

$$K_n + K_c = 1. \quad (2.39)$$

Кількість $I(X)$ інформації у повідомленні, що містить S_o елементів, і кожен з яких містить $H_o(X)$ ентропії, дорівнює $I(X) = S_o \cdot H_o(X)$.

В той же час кількість $I(X)$ інформації у повідомленні, що містить S_n елементів і кожен з яких містить $H_n(X)$ ентропії, дорівнює $I(X) = S_n \cdot H_n(X)$. Таким чином

$$I(X) = S_o \cdot H_o(X) = S_n \cdot H_n(X) \quad (2.40)$$

На рис. 2.14 представлені структурні схеми повідомлень для S_o , $H_o(X)$ (а) та для S_n , $H_n(X)$ (б)

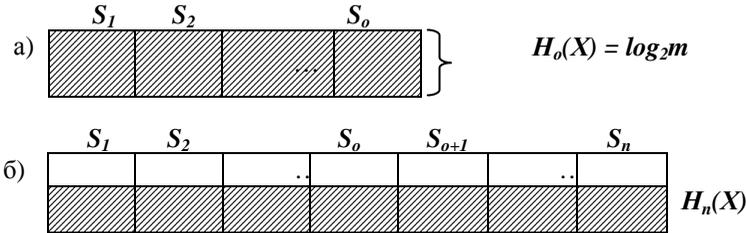


Рис. 2.14 - Структури повідомлень

Розглянемо ще одну важливу інформаційну характеристику джерела дискретних повідомлень – **продуктивність** $H'(X)$. Під продуктивністю ДДП будемо розуміти середню кількість інформації, що створюється джерелом в одиницю часу. Ця величина визначається наступним виразом

$$H'(X) = V_{сер} \cdot H_n(X) = \frac{H_n(X)}{T_{сер}} [\text{біт/сек}], \quad (2.41)$$

де: $V_{сер}$ – середня швидкість формування символів x_i алфавіту ДДП на його виході (кількість символів, що у середньому видає ДДП за 1 сек);

$T_{сер}$ – середня тривалість одного елемента повідомлення.

Джерело дискретних повідомлень називається **стаціонарним** (ергодичним), якщо його ймовірнісні характеристики не змінюються у часі.

У теорії інформації ДДП вважається повністю заданим, якщо відомі всі його інформаційні характеристики.

Продуктивність $H'(X)$ характеризує динамічні властивості ДДП. Так вираз (2.41) характеризує продуктивність, при умові, що символи алфавіту посилаються у канал зв'язку рівномірно.

Розглянемо приклад визначення інформаційних характеристик ДДП.

Приклад 2.1

Нехай задано ДДП таким ансамблем повідомлень

$$X = \begin{bmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 \\ 0,01 & 0,02 & 0,03 & 0,04 & 0,1 & 0,2 & 0,25 & 0,35 \end{bmatrix},$$

де $m = 8$ та $\sum_{i=1}^8 p(x_i) = 1$.

Необхідно визначити наступні інформаційні характеристики ДДП при $V_{сеп} = 10^3$ [симв./сек]:

1. Ентропію $H_n(X)$ ДДП.
2. Кількість інформації $I(X)$, що містить повідомлення, що складається з $S_n = 10^6$ (довжина повідомлення дорівнює 10^6 розрядів (елементів)).
3. Кількість S_o елементів повідомлення, що необхідна для передачі тієї ж кількості $I(X)$ інформації шляхом передачі безнадмірного повідомлення.
4. Абсолютну інформаційну недовантаженість $\Delta H(X)$.
5. Коефіцієнт інформаційної надмірності K_n .
6. Коефіцієнт інформаційного стиску K_c .
7. Продуктивність ДДП $H'(X)$.

Розв'язання:

1. Ентропія $H_n(X)$ повідомлення визначається як:

$$\begin{aligned} H_n(X) &= - \sum_{i=1}^m p(x_i) \cdot \log_2 p(x_i) = - \sum_{i=1}^8 p(x_i) \cdot \log_2 p(x_i) = \\ &= - p(x_1) \cdot \log_2 p(x_1) - p(x_2) \cdot \log_2 p(x_2) - p(x_3) \cdot \log_2 p(x_3) - p(x_4) \cdot \log_2 p(x_4) - \\ &- p(x_5) \cdot \log_2 p(x_5) - p(x_6) \cdot \log_2 p(x_6) - p(x_7) \cdot \log_2 p(x_7) - p(x_8) \cdot \log_2 p(x_8) = \\ &= - 0,01 \cdot \log_2 0,01 - 0,02 \cdot \log_2 0,02 - 0,03 \cdot \log_2 0,03 - 0,04 \cdot \log_2 0,04 - \\ &- 0,1 \cdot \log_2 0,1 - 0,2 \cdot \log_2 0,2 - 0,25 \cdot \log_2 0,25 - 0,35 \cdot \log_2 0,35 \approx \\ &\approx 0,0664 + 0,1129 + 0,1518 + 0,1858 + 0,3222 + 0,4644 + 0,5 + 0,5301 = \\ &= 2,334517 \text{ (біт)}. \end{aligned}$$

2. Кількість інформації визначається таким чином

$$I(X) = S_n \cdot H_n(X) = 10^6 \cdot 2,334517 = 2334517 \text{ (біт)}.$$

3. Як було вище зазначено, $I(X) = S_o \cdot H_o(X) = S_n \cdot H_n(X)$. Тоді маємо

$$S_o = \frac{J(X)}{H_o(X)}.$$

Ентропія $H_o(X)$ безнадлишкового повідомлення, тобто при рівномірних символах алфавіту

$$p(x_1) = p(x_2) = p(x_3) = p(x_4) = p(x_5) = p(x_6) = p(x_7) = p(x_8) = \frac{1}{8},$$

дорівнює $H_o(X) = -\log_2 p(x_i) = \log_2 \frac{1}{8} = 3$ (біт).

Таким чином

$$S_o = \frac{J(X)}{H_o(X)} = \frac{2334517}{3} \approx 778172,33 \text{ (розрядів)}.$$

Так як кількість S_o розрядів ціле число, то результат округляється до найближчого цілого у більшу сторону, тобто $S_o = 778173$.

4. Тоді маємо $\Delta H(X) = H_o(X) - H_n(X) = 3 - 2,334517 \approx 0,665$ (біт).

5. Коефіцієнт інформаційної надмірності визначається наступним чином:

$$K_n = \frac{\Delta H(X)}{H_o(X)} = \frac{0,665}{3} \approx 0,22.$$

6. Коефіцієнт інформаційного стиску $K_c = 1 - K_n = 1 - 0,22 = 0,78$.

7. Згідно з вихідними даними продуктивність ДДП $H'(X)$ визначається

$$H'(X) = V_{cep} \cdot H_n(X) \approx 10^3 \cdot 2,335 \approx 2335 \text{ [біт/сек]}.$$

Таким чином визначені всі інформаційні характеристики ДДП.

З розглянутого прикладу видно, що реальне повідомлення при однаковій інформативності має надмірність розрядів S_n порівняно з кількістю S_o розрядів оптимального повідомлення. Таким чином, з одного боку надмірність завжди приводить до збільшення часу передачі повідомлень, тобто надмірного завантаження КЗ. З другого боку, надмірність може бути застосована для підвищення перешкодостійкості передачі та обробки повідомлень (перешкодостійке кодування).

Так, результати розрахунків ентропії різних мов показали, що ентропії російської, англійської та української мов відповідно дорівнюють приблизно $H_{op} = 5,04$ [біт], $H_{oa} = 4,75$ [біт] та $H_{oy} = 5,13$ [біт].

2.7. Приклади кількісної оцінки ентропії та інформації у повідомленні

Розглянемо приклади кількісної оцінки ентропії та інформації у повідомленні.

Приклад 2.2.

Нехай алфавіт повідомлення складається з чотирьох літер x_1, x_2, x_3 та x_4 . Ймовірності появи цих літер дорівнюють відповідно $p(x_1) = 0,16$, $p(x_2) = 0,34$ та $p(x_3) = p(x_4) = 0,25$.

Треба визначити середню кількість інформації, що приходить на символ повідомлення даного алфавіту.

Розв'язання. Кількість інформації, що приходить у середньому на один символ повідомлення є його ентропія. Для взаємозалежних та нерівномірних символів $x_i, i = 1, m$, ентропія дорівнює

$$\begin{aligned}
 I(X) = H(X) &= - \sum_{i=1}^4 p(x_i) \log_2 p(x_i) = \\
 &= - (2 \cdot 0,25 \cdot \log_2 0,25 + 0,34 \cdot \log_2 0,34 + 0,16 \cdot \log_2 0,16) = \\
 &= 2 \cdot 0,5 + 0,5292 + 0,4230 = 1,9522 \text{ (біт)}.
 \end{aligned}$$

Приклад 2.3.

Число символів алфавіту дорівнює $m = 5$. Треба визначити ентропію повідомлення для даного алфавіту у випадках, якщо:

а) символи алфавіту взаємозалежні та рівномірні;

б) символи алфавіту взаємозалежні та нерівномірні для $p(x_1) = 0,8$; $p(x_2) = 0,15$; $p(x_3) = 0,03$; $p(x_4) = 0,015$; $p(x_5) = 0,005$.

Розв'язання. Випадає:

а). Для цього випадку використовується джерело Р. Хартлі

$$H(X) = \log_2 m = \log_2 5 \approx 2,3220 \text{ (біт)}.$$

б). В цьому разі маємо джерело К. Шеннона

$$\begin{aligned}
 H(X) &= - \sum_{i=1}^5 p(x_i) \log_2 p(x_i) = -(0,8 \cdot \log_2 0,8 + 0,15 \cdot \log_2 0,15 + \\
 &+ 0,03 \cdot \log_2 0,03 + 0,015 \cdot \log_2 0,015 + 0,005 \cdot \log_2 0,005) \approx 0,9490 \text{ (біт)}.
 \end{aligned}$$

Приклад 2.4.

У тексті переданої телеграми міститься 50 літер. Літери російського алфавіту друкуються взаємозалежно.

Треба визначити ентропію $H(X)$ переданого повідомлення враховуючи пробіли між словами, а також кількість інформації, що міститься у тексті телеграми.

Рішення. Користуючись ймовірностями появи літер російського алфавіту маємо

$$H(X) = - \sum_{i=1}^{34} p(x_i) \log_2 p(x_i) = 0,249 + 0,086 + 0,179 + 0,440 \approx 4,35 \text{ (біт)}.$$

Так, як кількість інформації, що у середньому приходить на одну з 50 літер телеграми, дорівнює $H(X) = 4,35$ (біт), то загальна кількість інфо-

рмачі у телеграмі дорівнює $I(X) = 50 \cdot H(X) = 50 \cdot 4,35 = 217,5$ (біт)

Приклад 2.5.

Дискретне джерело повідомлень виробляє ансамбль символів $X\{x_i\}$, $i = \overline{1,4}$ зі слідуючими ймовірностями їх появи на виході: $p(x_1) = 0,2$; $p(x_2) = 0,3$; $p(x_3) = 0,4$ та $p(x_4) = 0,1$. Кореляційні зв'язки між символами алфавіту відсутні.

Треба обчислити $H(X)$ ентропію даного джерела повідомлень

Розв'язання.

$$H(X) = - \sum_{i=1}^4 p(x_i) \log_2 p(x_i) = - [p(x_1) \log_2 p(x_1) + p(x_2) \log_2 p(x_2) + p(x_3) \log_2 p(x_3) + p(x_4) \log_2 p(x_4)] = - [0,2 \log_2 0,2 + 0,3 \log_2 0,3 + 0,4 \log_2 0,4 + 0,1 \log_2 0,1] \approx 0,4643 + 0,5210 + 0,5287 + 0,3321 = 1,8461 \text{ (біт)}$$

Приклад 2.6.

Двійкове джерело повідомлень виробляє символ x_1 алфавіту $X\{x_1, x_2\}$ з ймовірністю $p(x_1) = 0,1$.

Визначити кількість інформації у кожному з символів x_1 та x_2 алфавіту X , а також ентропію джерела повідомлень.

Розв'язання. Так, як для двійкового ДП $p(x_1) + p(x_2) = 1$, тоді $p(x_2) = 0,9$. Кількість інформації $I(x_i)$ визначиться наступним чином:

$$I(x_1) = H(x_1) = \log_2 \frac{1}{p(x_1)} = \log_2 \frac{1}{0,1} \approx 3,322 \text{ (біт)}$$

$$I(x_2) = H(x_2) = \log_2 \frac{1}{p(x_2)} = \log_2 \frac{1}{0,9} \approx 0,152 \text{ (біт)}$$

Тоді маємо

$$H(X) = - \sum_{i=1}^2 p(x_i) \log_2 p(x_i) = - p(x_1) \log_2 p(x_1) - p(x_2) \log_2 p(x_2) = - 0,1 \cdot \log_2 0,1 - 0,9 \cdot \log_2 0,9 \approx 0,469 \text{ (біт)}$$

Наведені приклади пояснюють правила визначення ентропії та інформації.

2.8. Ентропія джерел неперервних повідомлень

У загальному випадку неперервне повідомлення $X(t)$ приймає нескінченну множину значень як у часі, так і за рівнем (величиною). В цьому випадку кількість ентропії та інформації джерела неперервного повідомлення (ДНП) нескінченна за рахунок нескінченно великої кількості значень повідомлення (сигналу). До неперервних повідомлень відносяться неперервні значення напруги, струму, тиску, температури, усна мова, му-

зика тощо.

Тому, на відміну від дискретних повідомлень, утворених рахованою множиною елементів (символів) x_i , що задані ймовірностями появи $p(x_i)$, символи алфавіту неперервних повідомлень пронумерувати не можна. Неперервне повідомлення як випадкова величина характеризується диференціальним законом розподілу ймовірностей $W(x)$. Ймовірність кожного окремого значення неперервного повідомлення дорівнює нулю, а розподіл ймовірностей характеризується щільністю ймовірності $W(x)$.

Узагальнимо на випадок неперервних повідомлень маємо наступний вираз

$$H = - \sum_{i=1}^M p(x_i) \log p(x_i) \cdot$$

Для цього було здійснено квантування за рівнем, тобто заміна неперервного значення повідомлень дискретними відліками x_1, x_2, \dots, x_M , як зображено на рис. 2.15. Ймовірності появи дискретних відліків можна записати так: $p(x_k) = W(x_k) \Delta x$.

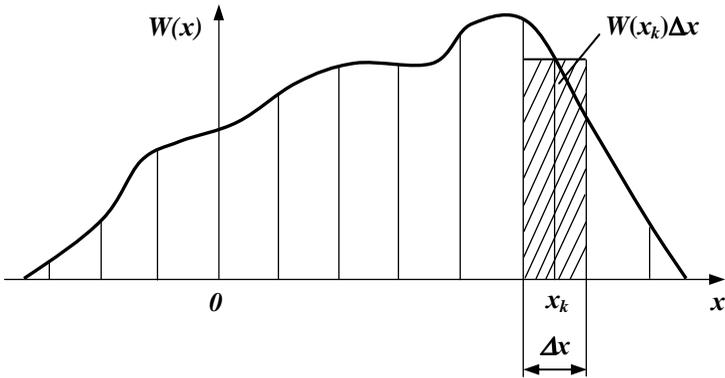


Рис. 2.15. Щільність ймовірності неперервних повідомлень

Така заміна буде більш точною, чим менший інтервал Δx . Одержимо ентропію квантованого неперервного повідомлення, підставивши значення $p(x_k)$:

$$H^*(X) \approx - \sum_{k=1}^M W(x_k) \Delta x \log [W(x_k) \Delta x] = \quad (2.42)$$

$$- \sum_{k=1}^M [W(x_k) \log W(x_k)] \Delta x - \sum_{k=1}^M \log \Delta x [W(x_k)] \Delta x.$$

При граничному переході ($\Delta x \rightarrow 0, \Delta m \rightarrow \infty$) перша сума виразу (2.42) переходить до інтеграла $\int_{-\infty}^{\infty} W(x) \log W(x) dx$, а друга сума – до величини $\lim_{\Delta x \rightarrow 0} \log \Delta x$, тому що $\int_{-\infty}^{\infty} W(x) dx = 1$.

Тоді вираз (2.42) приймає такий вигляд:

$$H(X) = - \int_{-\infty}^{\infty} W(x) \log W(x) dx - \lim_{\Delta x \rightarrow 0} \log \Delta x. \quad (2.43)$$

Вираз (2.43) називається абсолютною ентропією неперервного повідомлення і дорівнює нескінченності, тому що дорівнює нескінченності $\lim_{\Delta x \rightarrow 0} \log \Delta x$.

У цьому немає нічого несподіваного, тому що ентропія джерела повідомлення з нескінченною кількістю можливих станів також нескінченна. Однак ця обставина не є нездоланною задачею для визначення ентропії неперервних джерел. Дійсно, у реальних системах крок квантування Δx не може дорівнювати нулю, тому що неперервне повідомлення не можна відтворити з абсолютною точністю, – цьому заважають погрішності виміру і перешкоди в каналі зв'язку. Тому інтервал Δx завжди кінцева величина і абсолютна ентропія неперервного повідомлення має вигляд:

$$H(X) = - \int_{-\infty}^{\infty} W(x) \log W(x) dx - \log \Delta x.$$

При порівнянні ентропії різних неперервних повідомлень, відтворених з однаковою точністю Δx , доданок $\log \Delta x$ нехай являє собою дуже велику, але кінцеву постійну величину, однаковою для функцій, що порівнюються. Тому його звичайно опускають, а розглядають вираз для ентропії неперервних повідомлень у такому вигляді:

$$h(X) = - \int_{-\infty}^{\infty} W(x) \log W(x) dx \quad (2.44)$$

Визначену в такий спосіб ентропію неперервного повідомлення називають *диференціальною* (оскільки вона пов'язана з диференціальним за-

коном розподілу ймовірностей). Диференціальна ентропія не має абсолютного характеру, властивого ентропії дискретних повідомлень, і не може бути мірою невизначеності джерела повідомлень, оскільки залежить від масштабу і навіть здатна приймати негативні значення. Однак вона відіграє важливу роль при розгляді інформаційних характеристик систем передачі, оскільки ці характеристики в основному залежать від різниці ентропії різних джерел повідомлень.

Визначимо диференціальну ентропію повідомлення, значення якого розподілені за нормальним законом:

$$W(x) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left\{-\frac{(x - \bar{x})^2}{2\sigma^2}\right\},$$

де \bar{x} – математичне очікування;

σ^2 – дисперсія.

З виразу (2.44) отримаємо

$$\begin{aligned} h(X) &= - \int_{-\infty}^{\infty} W(x) \log W(x) dx = - \int_{-\infty}^{\infty} W(x) \left[\log \sqrt{\pi\sigma^2} + \frac{\log e}{2\sigma^2} (x - \bar{x})^2 \right] dx = \\ &= \log \sqrt{2\pi\sigma^2} \int_{-\infty}^{\infty} W(x) dx + \frac{\log e}{2\sigma^2} \int_{-\infty}^{\infty} (x - \bar{x})^2 W(x) dx. \end{aligned}$$

Перший інтеграл за загальною властивістю щільності ймовірності дорівнює одиниці, а другий інтеграл дорівнює дисперсії σ^2 . Тоді

$$h(X) = \log \sqrt{2\pi\sigma^2} + \frac{1}{2} \log e = \log \sqrt{2\pi\sigma^2} + \log \sqrt{e} = \log \sqrt{2e\pi\sigma^2}.$$

Таким чином, диференціальна ентропія гауссовської випадкової величини не залежить від її математичного очікування і монотонно зростає зі збільшенням дисперсії.

Визначимо диференціальну ентропію процесу, рівномірно розподіленого на інтервалі $(-\alpha, \alpha)$.

З виразу (2.44) отримаємо

$$h(x_2) = - \int_{-\alpha}^{\alpha} \frac{1}{2\alpha} \log \frac{1}{2\alpha} dx = \log 2\alpha.$$

Дисперсія процесу з рівномірним розподілом дорівнює σ^2 при $\alpha = \sigma\sqrt{3}$. Таким чином, диференціальна ентропія процесу з рівномірним розподілом дорівнює

$$h(x_2) = \log \sqrt{12\sigma^2}.$$

При заданій дисперсії σ^2 диференціальна ентропія нормального процесу більша диференціальної ентропії процесу з рівномірним розподілом на

$$\Delta h = \log \sqrt{2\pi\sigma^2} - \log \sqrt{12\sigma^2} = \log \sqrt{\frac{\pi e}{6}} \approx 0,3 \text{ біт/відлік}.$$

Раніше було доведено, що ентропія дискретного джерела максимальна при рівній імовірності появи його символів. При цьому виникає питання, а при якому розподілі ймовірностей ентропія неперервних повідомлень максимальна. Дослідження показали, що повідомлення з нормальним розподілом мають максимальну ентропію в порівнянні з будь-якими іншими випадковими повідомленнями з тією же дисперсією. З висновку формули диференціальної ентропії нормального закону розподілу виходить, що

$$-\int_{-\infty}^{\infty} W(x) \log \left[\frac{1}{\sqrt{2\pi\sigma^2}} \exp \left(-\frac{(x-\bar{x})^2}{2\sigma^2} \right) \right] dx = \log \sqrt{2e\pi\sigma^2}$$

для будь-якого закону розподілу.

Для знаходження максимальної ентропії визначимо різницю диференціальної ентропії довільного закону розподілу $W(x)$ і нормального закону

$$\begin{aligned} h(X) - h_n(X) &= -\int_{-\infty}^{\infty} W(x) \log W(x) dx + \int_{-\infty}^{\infty} W(x) \log \left[\frac{1}{\sqrt{2\pi\sigma^2}} \exp \left(-\frac{(x-\bar{x})^2}{2\sigma^2} \right) \right] dx = \\ &= \int_{-\infty}^{\infty} W(x) \log \frac{1}{W(x)} dx + \int_{-\infty}^{\infty} W(x) \log \left[\frac{1}{\sqrt{2\pi\sigma^2}} \exp \left(-\frac{(x-\bar{x})^2}{2\sigma^2} \right) \right] dx = \\ &= \int_{-\infty}^{\infty} W(x) \log \left[\frac{1}{W(x)\sqrt{2\pi\sigma^2}} \exp \left(-\frac{(x-\bar{x})^2}{2\sigma^2} \right) \right] dx. \end{aligned}$$

Враховуючи, що $\log(x) \leq x - 1$, одержимо

$$\begin{aligned} h(X) - h_n(X) &= \int_{-\infty}^{\infty} W(x) \log \left[\frac{1}{W(x)\sqrt{2\pi\sigma^2}} \exp \left(-\frac{(x-\bar{x})^2}{2\sigma^2} \right) \right] dx \leq \\ &\leq \int_{-\infty}^{\infty} W(x) \left[\frac{1}{W(x)\sqrt{2\pi\sigma^2}} \exp \left(-\frac{(x-\bar{x})^2}{2\sigma^2} \right) - 1 \right] dx = \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi\sigma^2}} \exp \left(-\frac{(x-\bar{x})^2}{2\sigma^2} \right) dx - \\ &- \int_{-\infty}^{\infty} W(x) dx = 1 - 1 = 0 \end{aligned}$$

Отже, максимальна диференціальна ентропія досягається при норма-

льному законі розподілу.

За аналогією з формулами для дискретного джерела кількість інформації, що міститься в одному неперервному відліку процесу $Y(t)$ відносно відліку процесу $X(t)$, визначається за формулою

$$I(X, Y) = - \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} W(x, y) \log \frac{W(x, y)}{W(x)W(y)} dx dy,$$

де $W(x, y)$ – сумісна щільність імовірності процесів $X(t)$ і $Y(t)$.

Величину $I(X, Y)$ можна записати так:

$$I(X, Y) = h(X) - h(X/Y) = h(Y) - h(Y/X),$$

де $h(X)$, $h(Y)$ – диференціальна ентропія на відлік процесів $X(t)$ і $Y(t)$;

$h(X/Y) = - \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} W(x, y) \log W(x/y) dx dy$ – умовна диференціальна ентропія відліку $X(t)$ при відомому відліку $Y(t)$;

$h(Y/X) = - \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} W(x, y) \log W(y/x) dx dy$ – умовна диференціальна ентропія відліку $Y(t)$ при відомому відліку $X(t)$.

Приклад 2.7.

Розглянемо приклад. По каналу зв'язку передається сигнал $X(t)$, який являє собою нормальний випадковий процес з нульовим середнім значенням і дисперсією $\sigma_x^2 = 4 \text{ МВТ}$. У каналі діє незалежний до сигналу нормальний шум $n(t)$ з нульовим середнім значенням і дисперсією $\sigma_n^2 = 1 \text{ МВТ}$. Знайти диференціальні ентропії вхідного та вихідного сигналів, а також умовні диференціальні ентропії $h(X/Y)$ та $h(Y/X)$. Сигнал на виході $Y(t) = X(t) + n(t)$.

Розв'язання. Так як $X(t)$ і $n(t)$ незалежні та мають нормальний розподіл, $Y(t)$ також буде мати нормальний розподіл з дисперсією $\sigma_y^2 = \sigma_x^2 + \sigma_n^2$. Диференціальні ентропії вхідного та вихідного сигналів будуть дорівнювати

$$h(X) = \log \sqrt{2\pi\sigma_x^2} = 3,05 \text{ біт/відлік};$$

$$h(Y) = \log \sqrt{2\pi(\sigma_x^2 + \sigma_n^2)} = 3,21 \text{ біт/відлік.}$$

Умовна диференціальна ентропія відліку $Y(t)$ при відомому $X(t)$ визначається ентропією шуму у каналі. Отже,

$$h(Y / X) = \log \sqrt{2\pi\sigma_n^2} = 2,05 \text{ біт/відлік.}$$

Найдемо умовну диференціальну ентропію відліку $X(t)$ при відомому $Y(t)$:

$$\begin{aligned} h(X/Y) &= - \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} W(x, y) \log W(x/y) dx dy = \\ &= - \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} W(x)W(y/x) \log \frac{W(x)W(y/x)}{W(y)} dx dy. \end{aligned}$$

Так як $\int_{-\infty}^{\infty} W(x)W(y/x) dx = W(y)$, отримуємо:

$$h(X/Y) = h(X) + h(Y/X) - h(Y) = \log \sqrt{2\pi e \frac{\sigma_x^2 \sigma_n^2}{\sigma_x^2 + \sigma_n^2}} = 1,89 \text{ біт/відлік.}$$

Приклад 2.8.

Треба визначити диференційну ентропію $h(x)$ нормального закону розподілу випадкової неперервної величини x , тобто закону

$$W(x) = \frac{1}{\sigma \cdot \sqrt{2\pi}} \cdot e^{-\frac{(x-\bar{x})^2}{2\sigma^2}},$$

де: \bar{x} - математичне очікування;
 σ^2 - дисперсія.

Розв'язання. З формули (2.44) маємо

$$\begin{aligned} h(x) &= - \int_{-\infty}^{+\infty} W(x) \cdot \log_2 W(x) dx = - \int_{-\infty}^{+\infty} W(x) \cdot \log_2 \left[\frac{1}{\sigma \cdot \sqrt{2\pi}} \cdot e^{-\frac{(x-\bar{x})^2}{2\sigma^2}} \right] dx = \\ &= - \left\{ \int_{-\infty}^{+\infty} W(x) \cdot \log_2 \frac{1}{\sigma \cdot \sqrt{2\pi}} dx + \int_{-\infty}^{+\infty} W(x) \cdot \log_2 e^{-\frac{(x-\bar{x})^2}{2\sigma^2}} dx \right\} = \\ &= - \left\{ - \int_{-\infty}^{+\infty} W(x) \cdot \log_2 \sigma \cdot \sqrt{2\pi} dx - \int_{-\infty}^{+\infty} W(x) \cdot \log_2 e^{-\frac{(x-\bar{x})^2}{2\sigma^2}} dx \right\} = \end{aligned}$$

$$\begin{aligned}
 &= \int_{-\infty}^{+\infty} W(x) \cdot \log_2 \sigma \cdot \sqrt{2\pi} dx + \int_{-\infty}^{+\infty} W(x) \cdot \frac{(x - \bar{x})^2}{\sigma^2} \cdot \log_2 e dx = \\
 &= \log_2 \sigma \cdot \sqrt{2\pi} \cdot \int_{-\infty}^{+\infty} W(x) dx + \frac{\log_2 e}{\sigma^2} \int_{-\infty}^{+\infty} W(x) \cdot (x - \bar{x})^2 dx. \quad (2.45)
 \end{aligned}$$

Перший інтеграл у виразі (2.45) дорівнює 1 (за властивістю функції $W(x)$ щільності ймовірності), тобто $\int_{-\infty}^{+\infty} W(x) dx = 1$, а другий інтеграл дорівнює дисперсії σ^2 . Таким чином вираз (2.45.) буде мати наступний вигляд

$$\begin{aligned}
 h(x) &= \log_2 \sigma \sqrt{2\pi} + \frac{\log_2 e}{2\sigma^2} \cdot \sigma^2 = \log_2 \sigma \sqrt{2\pi} + \log_2 \sqrt{e} = \\
 &= \log_2 \sqrt{2\pi \cdot e \cdot \sigma^2} \quad (\text{біт/повідомлення}). \quad (2.46)
 \end{aligned}$$

Таким чином видно, що диференційна ентропія гауссовської випадкової величини не залежить від її математичного очікування і підвищується разом з підвищенням значення σ^2 дисперсії. Для неперервного ДП (як показано в літературі) повідомлення з нормальним розподілом має максимальну ентропію у порівнянні з іншими випадковими повідомленнями з однаковим значенням величини дисперсії σ^2 .

Приклад 2.9.

Визначити диференційну ентропію вимірів величини X у межах $[a, a+b]$, якщо її значення розподілено за рівномірним законом.

Розв'язання. Представимо умови прикладу 2.6 у наступному вигляді

$$W(x) = \begin{cases} \frac{1}{b}, & \text{якщо } a \leq x \leq a+b \\ 0, & \text{якщо } a > x \text{ та } x > a+b \end{cases}$$

Використовуючи формулу (2.44) одержимо

$$\begin{aligned}
 h(x) &= - \int_{-\infty}^{+\infty} w(x) \cdot \log w(x) dx = - \int_a^{a+b} \frac{1}{b} \cdot \log_2 \frac{1}{b} dx = \\
 &= - \left[(a+b) \cdot \frac{1}{b} \cdot \log_2 b - a \cdot \frac{1}{b} \log_2 \frac{1}{b} \right] = (a+b-a) \frac{1}{b} \log_2 b = \log_2 b \quad (\text{біт/повідом.}).
 \end{aligned}$$

2.9. Контрольні питання

1. Дайте визначення кількості інформації. Як вона розраховується?
2. Дайте визначення ентропії.
3. Яким умовам задовольняє ентропія випадкового експерименту?

4. Поясніть порядок розрахунку ентропії випадкового експерименту з рівноймовірними наслідками.
5. Дайте визначення одиниці виміру невизначеності.
6. Поясніть порядок розрахунку ентропії випадкового експерименту з нерівноймовірними наслідками.
7. Поясніть умови максимізації ентропії джерел повідомлень.
8. Поясніть порядок обчислення ентропії експерименту при взаємозалежності подій.
9. Поясніть порядок обчислення ентропії об'єднання.
10. Поясніть суть надмірності джерел повідомлень.
11. Дайте визначення диференціальної ентропії джерел неперервних повідомлень.
12. Поясніть порядок обчислення диференціальної ентропії джерел з нормальним законом розподілу.
13. Поясніть порядок обчислення диференціальної ентропії процесу з рівномірним розподіленням.
14. Сформулюйте міру невизначеності за Р. Хартлі. Назвіть основний недолік даної міри.
15. Сформулюйте міру невизначеності за Маркова.
16. Як визначити ентропію одночасно декількох взаємозалежних ансамблів повідомлень?
17. Довести, що безумовна ентропія $H(X)$ детермінованих станів дорівнює нулю.
18. Навести формулу для визначення середньої кількості інформації $J(X)$, що міститься у будь-якому прийнятому елементі x_j повідомлення щодо реалізованого (переданого) x_i .
19. Наведіть та поясніть формулу для визначення кількості інформації за Р. Хартлі.
20. Навести загальний вираз для визначення кількості інформації $I(X)$. У якому випадку кількість інформації $I(X)$ буде максимальною?
21. Наведіть та поясніть формулу для визначення кількості інформації за К. Шенноном.
22. У чому суть відмінностей в оцінці кількості інформації за критеріями Р. Хартлі та К. Шеннона?
23. Дайте визначення та приведіть формулу диференційної ентропії неперервних повідомлень. В яких одиницях вона вимірюється?
24. Перелічіть та поясніть властивості ентропії складних дискретних повідомлень. Приведіть їх геометричну інтерпретацію.
25. Приведіть формулу для визначення ентропії ДДП при повній статистичній залежності його елементів.

Розділ 3

Види сигналів, що використовуються у системах обробки інформації та управління

Розглянуто основні математичні моделі сигналів та перешкод, форми представлення сигналів, методи дискретизації сигналів за часом і за рівнем, основні види випадкових процесів, що протікають у СОІУ та енергетичний спектр сигналу. Також наведено контрольні питання.

3.1. Основні математичні моделі сигналів та перешкод

В системах передачі інформації кожному повідомленню, що створене джерелом інформації, відповідає деякий електричний сигнал. Як вже було відзначено, всі сигнали діляться на дві групи. По-перше, це детерміновані сигнали; по-друге, – випадкові. Перші описуються і аналізуються за допомогою апарату класичної математики, а другі – за допомогою апарату теорії випадкових функцій. Під **детермінованими** (невипадковими) **сигналами** або функціями розуміються звичайні функції, в яких ставиться в однозначну відповідність кожному значенню аргументу відповідне значення функції.

Приведемо приклад аналітичного представлення детермінованої функції на нескінченному інтервалі часу

$$S(t) = A \cos(\omega t + \varphi).$$

Передача детермінованих сигналів не має сенсу, тому що такі сигнали не містять у собі будь-якої інформації. Але такі коливання широко використовуються як переносники інформації (несучі коливання) при формуванні сигналів.

Прийнято розрізняти неперервні (аналогові) і дискретні (квантовані) сигнали. При цьому остання ознака додається як до часової структури повідомлення – до аргументу t , так і до шкали рівнів функції $\lambda(t)$. Відповідно можна визначити чотири види повідомлення:

- неперервні;

- імпульсні аналогові (дискретні за часом і неперервні за шкалою рівнів);
- дискретно – неперервні (дискретні за шкалою рівнів і неперервні за часом);
- дискретні або цифрові повідомлення.

Для характеристики сигналу, з погляду витрат енергії, вводять поняття енергії сигналу, що обчислюється за формулою

$$E_c = \int_{t_n}^{t_k} S^2(t) dt,$$

де t_n – час початку сигналу;

t_k – час закінчення сигналу.

Функцію $p(t) = S^2(t)$ називають *миттєвою потужністю сигналу*.

Це потужність, що виділяється на опорі навантаження в 1 Ом.

На інтервалі тривалості сигналу $T_c = t_k - t_n$ вводиться поняття *середньої потужності сигналу*

$$P_c = \frac{1}{T_c} \int_{t_n}^{t_k} p(t) dt = \frac{1}{T_c} \int_{t_n}^{t_k} S^2(t) dt.$$

Якщо є сімейство сигналів $S_1(t), S_2(t), \dots, S_N(t)$ з рівними енергіями

$$E_k = \int_{t_n}^{t_k} S_k^2(t) dt, \quad k = 1, \dots, N$$

і для кожної пари виконується умова

$$\int_{t_n}^{t_k} S_i(t) S_j(t) dt = 0, \quad i \neq j,$$

то *сигнали ортогональні*.

Випадкові сигнали класифікуються так само, як і детерміновані. При цьому випадкові функції дискретного аргументу прийнято називати послідовностями.

Для аналізу і порівняння випадкових сигналів використовують ймовірнісні характеристики. Випадковий процес $X(t)$ може бути охарактеризований одномірною або багатомірною функцією щільності ймовірності. При цьому, якщо значення випадкової функції при довільних значеннях аргументу є незалежними випадковими величинами, то n -мірна функція щільності ймовірності буде дорівнювати добутку одновимірних функцій.

Для багатьох практичних випадків достатньо описати випадковий сигнал $X(t)$ за допомогою невинуватливих характеристик: математичного очі-

кування $m_X(t)$, дисперсії $D[X(t)]$ і кореляційної функції $R_X(t, \tau)$.

Математичним очікуванням випадкової функції $X(t)$ називають не випадкову функцію $m_X(t) = M[X(t)]$, миттєві значення якої в кожній відліковій точці t_i аргументу t дорівнюють математичному сподіванню випадкової величини $M[X(t_i)]$, яка відповідає цій відліковій точці t_i . Математичне очікування є деякою середньою функцією, біля якої групуються і навколо якої коливаються всі можливі реалізації $X(t)$.

Дисперсією випадкової функції $X(t)$ називають не випадкову функцію $D[X(t)]$, миттєві значення якої в кожній відліковій точці t_i аргументу t дорівнюють дисперсії випадкової величини, яка відповідає цій відліковій точці t_i . Часто також використовується числова характеристика $\sigma_X(t) = \sqrt{D[X(t)]}$, яка називається *середньоквадратичним відхиленням*. Дисперсія і середньоквадратичне відхилення характеризують величину розсіювання значень процесу щодо його математичного очікування. Фізично дисперсію часто трактують як середню енергетичну характеристику процесу $X(t)$.

Кореляційною (автокореляційною) функцією випадкового процесу $R_X(t, \tau)$ називають не випадкову функцію двох незалежних між собою часових аргументів: t і τ .

Термін “процес” означає функцію часу. Це поняття достатньо загальне і охоплює повідомлення, сигнали і перешкоди.

Випадкова функція є результатом випадкового експерименту і передбаченим чином приймає вигляд конкретної функції $X^{(\omega)}(t)$ з сукупності можливих значень $\{X^{(\omega)}(t)\}$, $\omega \in \Omega$.

Якщо за своєю природою випадкові функції і випадкові величини схожі, то в цьому випадку вводиться поняття множини (простір) Ω можливих результатів ω випадкового експерименту. Для випадкових величин кожному результату ω ставиться у відповідність конкретна реалізація випадкової величини X – число X^ω . Аналогічно, коли результатами є не величини, а функції часу, то кожній точці ω безлічі можливих результатів Ω ставиться у відповідність одержана реалізація випадкового процесу $X(t)$ – функція часу $X^{(\omega)}(t)$. Приклади реалізацій випадкового процесу зображені на рис. 3.1.

Множина можливих результатів в цьому випадку (рис. 3.1) складається з трьох точок $\Omega \in (1, 2, 3)$. При проведенні випадкового експерименту

випадковий процес $X(t)$ може прийняти непередбачуваним чином вигляд однієї з трьох функцій $X^{(1)}(t)$, $X^{(2)}(t)$, $X^{(3)}(t)$, зображених на рис. 3.1.

Необхідно відзначити, що графічне зображення випадкового процесу $X(t)$ – виключення, а не правило. Звичайно множина можливих результатів Ω нескінченна. Тому потрібний спеціальний математичний апарат для подання і аналізу випадкових процесів.

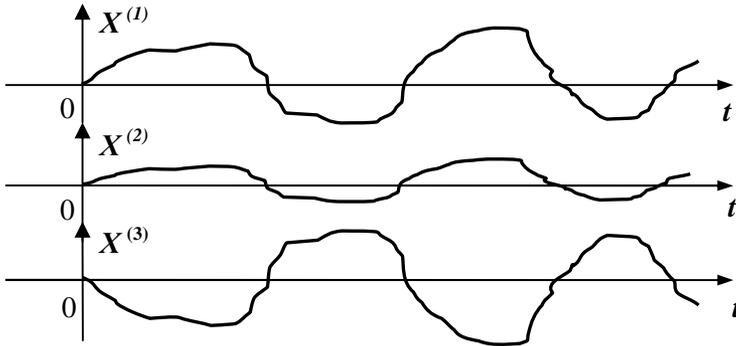


Рис. 3.1. Приклади реалізацій випадкового процесу

Неперервні сигнали є випадковими функціями, оскільки в процесі роботи джерела повідомлень непередбачуваним чином приймають вигляд конкретних функцій $S^{(\omega)}(t)$ з сукупності можливих функцій $\{S^{(\omega)}(t)\}$, $\omega \in \Omega$. Якби можна було передбачити, який конкретно вигляд $S^{(\omega)}(t)$ прийме повідомлення, то необхідність в його передачі відпала би. Крім того, випадковими функціями є перешкоди, природа яких по суті випадкова.

З другого боку, конкретні реалізації повідомлень, що передаються, $S^{(\omega)}(t)$ або в загальному випадку конкретні реалізації $X^{(\omega)}(t)$ випадкових процесів є детермінованими процесами, які можуть бути подані звичайними методами.

Найпоширенішими моделями випадкових сигналів і перешкод є телеграфний сигнал, гауссів білий шум і вузькосмуговий випадковий процес. Розглянемо кореляційні і спектральні характеристики процесів, що описуються цими моделями.

Телеграфний сигнал. Узагальненим телеграфним сигналом назива-

ють випадкову послідовність знакозмінних прямокутних відеоімпульсів однакової амплітуди U (рис. 3.2).

Ця послідовність характеризується тим, що у будь-який момент часу значення U і $-U$ рівномірні, переходи від U до $-U$ і навпаки – незалежні, а ймовірність того, що на достатньо великому інтервалі ΔT відбувається рівно k переходів, визначається законом Пуассона

$$P(k, \Delta T) = \frac{(\lambda \Delta T)^k}{k!} e^{-\lambda \Delta T},$$

де λ – середнє число переходів за одиницю часу.

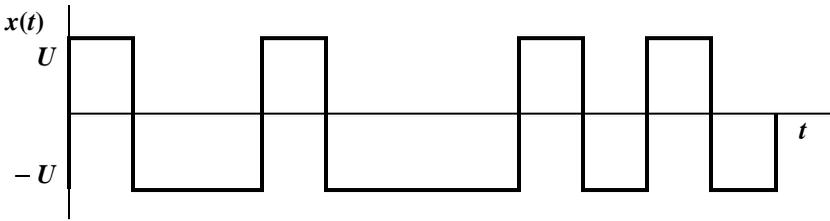


Рис. 3.2. Узагальнений телеграфний сигнал

Автокореляційна функція такого процесу має експоненціальну форму

$$R_x(\tau) = U^2 e^{-2\lambda|\tau|},$$

а спектральна щільність потужності має вигляд

$$G(f) = \frac{8U^2 \lambda}{4\lambda^2 + (2\pi f)^2}.$$

Інтервал кореляції і ширина спектра узагальненого телеграфного сигналу дорівнюють

$$\tau_{\text{кор}} = \int_0^{\infty} e^{-2\lambda\tau} d\tau = \frac{1}{2} \lambda^{-1}; \quad (3.1)$$

$$F_c = \frac{\lambda}{2U^2} \int_0^{\infty} \frac{8U^2 \lambda}{4\lambda^2 + (2\pi f)^2} df = \lambda. \quad (3.2)$$

З формул (3.1) і (3.2) витікає, що чим більше середнє число переходів за одиницю часу λ , тим менше час кореляції процесу і ширший його спектр. При $\lambda \rightarrow \infty$ даний процес перетворюється в такий, у якого всі перетини, у тому числі і сусідні, некорельовані, а спектральна щільність постійна у всьому діапазоні частот. При $\lambda \rightarrow 0$ процес перетворюється в детермінований (у постійну складову).

Разом з випадковим узагальненим телеграфним сигналом часто роз-

глядають випадковий синхронний телеграфний сигнал, який також приймає з рівною ймовірністю значення U і $-U$, але зміна цих значень відбувається тільки в ті моменти часу, що розділені проміжком кратним тактовому інтервалу T (рис. 3.3).

Межі тактових інтервалів у різних реалізацій не співпадають, тому в будь-який момент часу на інтервалі існування сигналу може з рівною ймовірністю виявитися моментом початку такту.

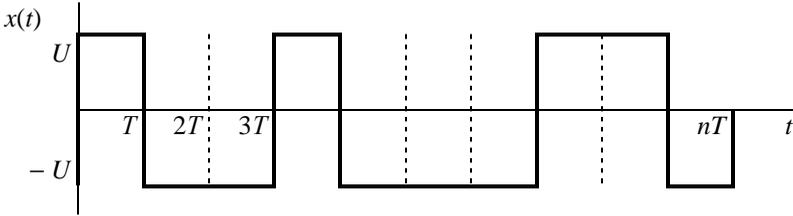


Рис. 3.3. Випадковий синхронний телеграфний сигнал

Автокореляційна функція випадкового синхронного телеграфного сигналу має трикутну форму й описується простим виразом

$$R_x(\tau) = \begin{cases} U^2 \left(1 - \frac{|\tau|}{T}\right), & |\tau| \leq T, \\ 0, & |\tau| \geq T \end{cases}$$

а його спектр має вигляд

$$G(f) = 2U T \frac{\sin^2(\pi f T)}{(\pi f T)^2}$$

Інтервал кореляції і ширину спектра випадкового синхронного телеграфного сигналу можна обчислити за методом еквівалентного прямокутника.

Гауссів білий шум. Флуктуаційна перешкода у каналах зв'язку часто передбачається нормальним (гауссовим) випадковим процесом. Обумовлено це наступним. Будучи сумою великого числа незалежних коливань, така перешкода, відповідно до граничної теореми теорії ймовірності, дійсно має розподіл, який можна вважати нормальним.

Нормальний випадковий процес $X(t)$ в будь-якому його перетині характеризується щільністю ймовірності

$$W(x) = \frac{1}{\sqrt{2\pi\sigma_x^2}} \exp\left\{-\frac{(x-m_x)^2}{2\sigma_x^2}\right\}$$

Інтегральна функція розподілу дорівнює

$$F(x) = P(X \leq x) = \frac{1}{\sqrt{2\pi\sigma_x^2}} \int_{-\infty}^x \exp\left\{-\frac{(x-m_x)^2}{2\sigma_x^2}\right\} dx =$$

$$\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\frac{x-m_x}{\sigma_x}} \exp(-y^2/2) dy = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^y \exp(-y^2/2) dy = F(y)$$

Для флукуаційної перешкоди позитивні і негативні миттєві значення зустрічаються однаково часто, тому $m_x = 0$. Дисперсія σ_x^2 в цьому випадку дорівнює середній потужності перешкоди. Таким чином, одновимірна щільністю ймовірності флукуаційної перешкоди задеться до вигляду

$$W(x) = \frac{1}{\sqrt{2\pi\sigma_x^2}} \exp\left\{-\frac{x^2}{2\sigma_x^2}\right\}$$

Електричну структуру флукуаційної перешкоди можна зобразити як послідовність нескінченно коротких імпульсів, що мають випадкову амплітуду і слідуєть один за одним через випадкові проміжки часу. Оскільки тривалість імпульсів, що становлять флукуаційну перешкоду, дуже мала, то спектральна щільність перешкоди постійна аж до дуже високих частот. При $F_e \rightarrow \infty$ випадковий процес з рівномірним енергетичним спектром характеризується відсутністю кореляції між скільки завгодно близькими його відліками. Такий випадковий процес носить назву "білого шуму" (за аналогією з білим світлом, спектр якого рівномірний в дуже широкому діапазоні частот). Білий шум, визначений як випадковий процес, що відповідає нескінченно широкому рівномірному енергетичному спектру, представляє фізично не реалізовану абстракцію. На практиці під білим шумом звичайно розуміють стаціонарний нормальний випадковий процес, спектр якого суттєво ширший за смугу пропускання того пристрою, на вході якого він діє, і рівномірний в межах цієї смуги.

Автокореляційну функцію центрованого стаціонарного випадкового процесу з рівномірним енергетичним спектром $G(f) = G_o$ в діапазоні $[0, F_e]$ визначимо як

$$R_x(\tau) = \int_0^{\infty} G(f) \cos(2\pi f \tau) df = \int_0^{F_e} G_o \cos(2\pi f \tau) df = G_o F_e \frac{\sin 2\pi F_e \tau}{2\pi F_e \tau}$$

Дисперсія (середня потужність) цього процесу

$$\sigma_x^2 = G_o F_e,$$

а нормована кореляційна функція

$$r_x(\tau) = \frac{\sin 2\pi F_a \tau}{2\pi F_a \tau}. \quad (3.3)$$

Як випливає з виразу (3.3), при $\tau = \kappa T_0 = \frac{\kappa}{2F_a}$ значення нормованої кореляційної функції $r_x(\tau)$ дорівнюють нулю. Отже, відліки, взяті через інтервали T_0 , будуть некорельовані. Оскільки цей стаціонарний процес є нормальним, то з некорельованості відліків слідує і їх незалежність. Таким чином, кореляційні властивості білого шуму повністю переносяться на дискретну вибірку, що визначає стаціонарний процес з рівномірним обмеженим спектром.

Вузькосмуговий випадковий процес. Часто для опису флуктуаційної перешкоди і деяких реальних сигналів використовують модель вузькосмугового випадкового процесу. Процес називається вузькосмуговим, якщо ширина його спектра істотно менша за середню частоту. Реалізації вузькосмугових процесів можна спостерігати на виході схем, що працюють на високих і проміжних частотах. На екрані осцилографа реалізація вузькосмугового процесу має вигляд синусоїди з повільно змінними амплітудою і частотою.

Для представлення вузькосмугового випадкового процесу або будь-якої його реалізації використовують дві рівноцінні форми:

➤ у вигляді амплітудно – частотно – модульованого коливання

$$X(t) = U(t) \cos[\omega_0 t + \varphi(t)],$$

де ω_0 – середня частота;

$U(t)$ і $\varphi(t)$ – огибаюча і фаза процесу;

➤ у вигляді суми двох амплітудно – модульованих процесів

$$X(t) = U_c(t) \cos \omega_0 t + U_s(t) \sin \omega_0 t,$$

де $U_c(t) = U(t) \cos \varphi(t)$ і $U_s(t) = U(t) \sin \varphi(t)$ – квадратурні складові.

Огибаюча і фаза вузькосмугового процесу є повільно змінними функціями в порівнянні з коливаннями на частоті ω_0 і пов'язані з квадратурними складовими співвідношеннями

$$U(t) = \sqrt{U_c^2(t) + U_s^2(t)}; \quad \varphi(t) = \arctg \frac{U_s(t)}{U_c(t)}.$$

Якщо вузькосмуговий випадковий процес нормальний, то закон розподілу його огибаючої є релеєвським

$$W(U) = \frac{U}{\sigma_x^2} \exp\left(-\frac{U^2}{2\sigma_x^2}\right),$$

а фази – рівномірним, $W(\varphi) = 1/2 \pi$

Кореляційна функція вузькосмугового процесу, спектральна щільність якого рівномірна в інтервалі частот (f_1, f_2) , визначається виразом

$$R_x(\tau) = \sigma_x^2 r_x(\tau) \cos \omega_0 \tau$$

де $r_x(\tau)$ – нормована автокореляційна функція огинаючої.

Таким чином, для визначення кореляційної функції вузькосмугового процесу необхідно знайти кореляційну функцію огинаючої і помножити її на $\cos \omega_0 \tau$.

Для передачі повідомлень по каналу зв'язку відповідні повідомленням електричні сигнали в передавачі накладаються на переносник інформації. Переносниками інформації виступають гармонічні коливання або періодичні послідовності імпульсів. У процесі передачі інформації один з параметрів переносника, який називають інформаційним, змінюється відповідно до зміни повідомлення, що передається. Такий процес називається **модуляцією**, якщо для передачі інформації використовуються неперервні сигнали, і **маніпуляцією**, при використанні для передачі інформації дискретних сигналів. Розглянемо основні види модуляції (маніпуляції).

При передачі неперервних сигналів переносником інформації виступає гармонійне коливання

$$S(t) = S_0 \cos(\omega_0 t + \varphi).$$

Інформаційним параметром може бути вибраний один з трьох параметрів електричного коливання: амплітуда, частота або початкова фаза. Відповідно розрізняють амплітудну (АМ), частотну (ЧМ) і фазову (ФМ) модуляції.

Нехай повідомлення, що передається, виражається функцією $\lambda(t)$. Тоді закон зміни амплітуди при АМ визначається виразом

$$S(t) = S_0 + K_a \lambda(t);$$

закон зміни частоти при ЧМ

$$\omega(t) = \omega_0 + K_u \lambda(t);$$

закон зміни фази при ФМ

$$\varphi(t) = \varphi_0 + K_\varphi \lambda(t),$$

де K_a, K_u, K_φ – крутизна характеристики амплітудного, частотного та фазового модуляторів.

Аналitичні вирази для сигналів мають вигляд

$$S_{AM}(t) = [S_0 + K_a \lambda(t)] \cos(\omega_0 t + \varphi_0);$$

$$S_{\omega_M}(t) = S_0 \cos[\omega_0 t + K_v \int_0^t \lambda(\tau) d\tau];$$

$$S_{\phi_M}(t) = S_0 \cos[\omega_0 t + \phi_0 + K_\phi \lambda(t)].$$

Імпульсні аналогові сигнали, що передаються, являють собою послідовності відліків $\{\lambda_k\}$, що слідує з інтервалом дискретності T_0 . Амплітуда відліків λ_k може приймати будь-які значення з інтервалу $(\lambda_{min}, \lambda_{max})$. Для передачі таких повідомлень використовуються первинний і вторинний переносники інформації. Первинним переносником є послідовність імпульсів $S(t)$

$$S(t) = \sum_{k=-\infty}^{\infty} S_0(t - kT_0).$$

Період повторення імпульсів в послідовності дорівнює інтервалу дискретності T_0 . Форма імпульсів в послідовності повинна бути близькою до прямокутної

$$S_0(t - kT_0) = S_0 \prod\left(\frac{t - kT_0}{\tau_0}\right),$$

де τ_0 – тривалість імпульсу.

Інформаційним параметром може бути один з трьох параметрів імпульсу: амплітуда, тривалість та часове положення імпульсу. Відповідно розрізняють амплітудно – імпульсну модуляцію (АІМ), імпульсну модуляцію по тривалості (ТІМ) і часову імпульсну модуляцію (ЧІМ), що називається також фазо – імпульсною модуляцією (ФІМ) (рис. 3.4).

Аналitичні вирази для довільного, наприклад k -го, імпульсу модульованої послідовності мають наступний вигляд:

$$S_k(t) = \left\{ \begin{array}{l} (S_0 + \alpha \lambda_k) \prod\left(\frac{t - kT_0}{\tau_0}\right) \quad \text{– АІМ;} \\ S_0 \prod\left(\frac{t - kT_0}{\tau_0 + \alpha \lambda_k}\right) \quad \text{– ТІМ;} \\ S_0 \prod\left(\frac{t - kT_0 - \alpha \lambda_k}{\tau_0}\right) \quad \text{– ЧІМ,} \end{array} \right.$$

де α – деякий коефіцієнт.

Коефіцієнт α вибирається таким чином, щоб виконувалися наступні умови:

- для сигналів АІМ амплітуда імпульсів $S_0 + \alpha A_k$ у всіх випадках повинна бути позитивною;
- для сигналів ТІМ тривалість імпульсів $\tau_0 + \alpha A_k$ повинна бути у всіх випадках більшою деякої мінімальної величини τ_{min} ;
- для сигналів ЧІМ часовий зсув імпульсів не повинен перевершувати деякої максимальної величини.

Послідовність імпульсів $S(t)$ є послідовністю відеоімпульсів, спектр якої лежить в низькочастотній області, включаючи нульову частоту. Тому для передачі по радіоканалу відеоімпульси перетворюються в радіосигнали за допомогою вторинної модуляції високочастотного гармонійного сигналу відеоімпульсами.

Звичайно для вторинної модуляції використовується амплітудна модуляція високочастотних коливань. Така модуляція позначається як АІМ-АМ (АІМ з вторинною АМ), ТІМ-АМ, ЧІМ-АМ.

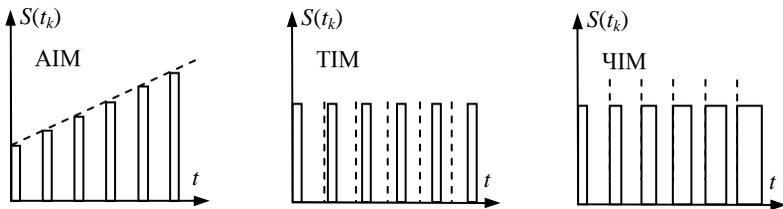


Рис. 3.4. Сигнали з АІМ, ТІМ і ЧІМ модуляцією

Шпаруватість імпульсних сигналів рівна відношенню інтервалу дискретності до тривалості імпульсів T_0 / τ_0 і може бути вибрана дуже великою. Це дозволяє в проміжках між імпульсами, що відображають один канал, передавати імпульси, що відображають інші канали. Імпульси різних каналів не перекриваються (рознесені в часі) і можуть бути розділені на приймальній стороні. Ця перевага імпульсних сигналів широко використовується в радіотелеметрії і радіозв'язку для побудови багатоканальних систем.

Об'єктом передачі в цифрових сигналах є цілі числа, що слідує одне за одним з інтервалом дискретності T_0 . Кожне з цих чисел може приймати одне з m значень $N_k \in \{0, 1, \dots, m - 1\}$.

Обмежимося розглядом найпоширенішої в теперешній час цифрової системи зв'язку – системи з кодово – імпульсною модуляцією (КІМ), в

якій цілі числа N_k записують і передають в двійковій системі числення

$$N_k = a_{k_1} a_{k_2} \dots a_{k_i} \dots a_{k_L},$$

де a_{k_i} – двійкова цифра i -го розряду при передачі k -го числа (відліку)

$$a_k \in \{0, 1\};$$

L – число двійкових розрядів, $L = \log_2 m$.

Звичайно число можливих значень елементарного повідомлення вибирають рівним цілому ступеню 2 ($2^5 = 32$, $2^6 = 64$ тощо).

Тривалість елементарних імпульсів, що відображають двійкові цифри, прийнята рівною ϵ_0 , так що передача повідомлення N_k займає інтервал $\tau_0 = L\epsilon_0$. Проміжки між відліками одного каналу заповнюються відліками інших каналів. При цьому двійкові цифри слідуєть один за одним з інтервалом τ_0 , а елементарні імпульси (або пропуски) слідуєть одна за одною неперервно.

Сигнал КІМ накладаєть на переносник – гармонійне коливання. В залежності від того, який параметр переносника прийнятий за інформаційний, розрізняють три види КІМ: КІМ з амплітудною маніпуляцією (КІМ-АМ), КІМ з частотною маніпуляцією (КІМ-ЧМ) і КІМ з фазовою маніпуляцією (КІМ-ФМ).

Тут відповідно до прийнятої термінології термін “модуляція” замінений на “маніпуляція”. Останнє підкреслює, що інформаційний параметр переносника в процесі зміни може приймати дискретні значення.

КІМ-АМ – символу “1” відповідає наявність радіоімпульсу, а символу “0” його відсутність.

КІМ-ЧМ – символу “1” відповідає імпульс з частотою ω_1 , а символу “0” – з частотою ω_2 .

КІМ-ФМ – символу “1” відповідає імпульс з початковою фазою φ_1 , а символу “0” – з початковою фазою φ_2 , звичайно $\varphi_2 = \varphi_1 \pm \pi$.

Аналітично сигнали системи передачі інформації з КІМ можна подати у вигляді неперервної послідовності елементарних імпульсів

$$S(t - t_i, a_i) = \left\{ \begin{array}{l} a_i S_0 \prod \left(\frac{t - t_i}{\tau_0} \right) \cos(\omega_0 t + \varphi) \\ S_0 \prod \left(\frac{t - t_i}{\tau_0} \right) \cos[(\omega_0 + a_i \pi)t + \varphi_0] \\ S_0 \prod \left(\frac{t - t_i}{\tau_0} \right) \cos(\omega_0 t + \varphi_0 + a_i \pi) \end{array} \right\} \begin{array}{l} \text{KIM-AM} \\ \text{KIM-ЧМ} \\ \text{KIM-ФМ,} \end{array}$$

де a_i – інформаційний параметр рівний 0 або 1;

t_i – тактове положення i -го імпульсу.

Таким чином, можна зробити висновок, що у всіх випадках електричний сигнал можна подати аналітично у вигляді функції часу і інформаційного параметра λ як $S(t, \lambda)$. У системах з КІМ $\lambda = a \in (0, 1)$, а в імпульсних аналогових системах λ – поточний відлік повідомлення.

3.2. Форми представлення сигналів

Найпоширенішим і найнеобхіднішим для практики є часове і частотне (спектральне) подання сигналів. Часова форма подання сигналу, тобто опис його зміни за часом, дозволяє легко визначити такі важливі характеристики, як тривалість, потужність, енергія. Спектральне подання визначає частотний склад сигналу. При цьому основною характеристикою є ширина спектра сигналу. Часове і спектральне подання сигналів пов'язані між собою перетворенням Фур'є.

Відомо, що будь-яка неперіодична функція часу $S(t)$ пов'язана з функцією кругової частоти $\dot{G}(\omega)$ співвідношенням

$$\dot{G}(\omega) = \int_{-\infty}^{\infty} S(t) e^{-j\omega t} dt,$$

відомим як пряме перетворення Фур'є. Функція $\dot{G}(\omega)$ називається *спектральною щільністю* або спектральною функцією. Спектральна щільність показує в кожній точці осі частот ω значення амплітуди dA гармонічної складової неперіодичного сигналу, що припадає на елементарний інтервал $d\omega$.

Зворотне перетворення Фур'є дозволяє за відомим частотним описом сигналу знайти його часовий опис

$$S(t) = \frac{1}{2\pi} \int_{-\infty}^{\infty} \dot{G}(\omega) e^{j\omega t} d\omega .$$

З пари перетворень Фур'є можна обчислити енергетичні характеристики сигналів за формулою Парсеваля

$$E_c = \frac{1}{2\pi} \int_{-\infty}^{\infty} |\dot{G}(\omega)|^2 d\omega = \frac{1}{\pi} \int_0^{\infty} |\dot{G}(\omega)|^2 d\omega ,$$

де E_c – енергія сигналу, що доводиться на смугу частот 1 Гц, яка є спектральною щільністю енергії сигналу $S(t)$.

Для частотного подання періодичних функцій використовуються тригонометрична та комплексна форми ряду Фур'є. Тригонометрична форма має такий вигляд:

$$S(t) = \frac{1}{2} a_0 + \sum_{k=1}^{\infty} (a_k \cos k\omega_0 t + b_k \sin k\omega_0 t), \quad (3.4)$$

де a_k та b_k – амплітуди нескінченного набору гармонічних коливань, що складають сигнал $S(t)$ та обчислюються за формулами (включаючи і a_0)

$$a_k = \frac{2}{T} \int_{-T/2}^{T/2} S(t) \cos k\omega_0 t dt ; \quad b_k = \frac{2}{T} \int_{-T/2}^{T/2} S(t) \sin k\omega_0 t dt . \quad (3.5)$$

Будь-яка гармоніка ряду Фур'є характеризується амплітудою A_k та початковою фазою φ_k , що пов'язані з коефіцієнтами цього ряду такими співвідношеннями:

$$A_k = \sqrt{a_k^2 + b_k^2} ; \quad \varphi_k = \arctg \frac{b_k}{a_k} . \quad (3.6)$$

Підставивши вирази (3.5), (3.6) в (3.4), отримаємо другу еквівалентну форму ряду Фур'є

$$S(t) = \frac{1}{2} A_0 + \sum_{k=1}^{\infty} A_k \cos(k\omega_0 t - \varphi_k) ,$$

де $\frac{1}{2} A_0$ – постійна складова функції $S(t)$;

$\omega_0 = \frac{2\pi}{T}$ – частота основної (першої) гармоніки;

T – період;

$A_k, k\omega_0, \varphi_k$ – амплітуда, частота і початкова фаза k -ї гармонічної складової.

Часто для обчислень використовують комплексну форму ряду Фур'є

$$S(t) = \frac{1}{2} \sum_{k=-\infty}^{\infty} \dot{A}_k e^{jk\omega_0 t},$$

де $\dot{A}_k = A_k e^{j\varphi_k}$ – комплексна амплітуда k -ї гармоніки, що визначається за формулою

$$\dot{A}_k = \frac{2}{T} \int_{-T/2}^{T/2} S(t) e^{-jk\omega_0 t} dt.$$

Ці співвідношення дозволяють знайти спектр сигналу, тобто сукупність гармонічних складових.

Приклад 3.1.

Визначити спектр періодичної послідовності прямокутних імпульсів з тривалістю τ_u , амплітудою U та періодом T .

Для визначення спектра застосуємо тригонометричну форму згідно з виразом (3.4)

$$\frac{a_0}{2} = \frac{1}{T} \int_0^{\tau_u} U \cos \theta \cdot \omega_0 t dt = \frac{1}{T} \int_0^{\tau_u} U dt = \frac{1}{T} U t \Big|_0^{\tau_u} = \frac{\tau_u}{T} U;$$

$$a_k = \frac{2}{T} \int_0^{\tau_u} U \cos k\omega_0 t dt = \frac{2}{T} \cdot \frac{U}{k\omega_0} \sin k\omega_0 t \Big|_0^{\tau_u} = \frac{2}{T} \cdot \frac{UT}{k \cdot 2\pi} \sin k\omega_0 \tau_u = \frac{U}{k\pi} \sin k\omega_0 \tau_u;$$

$$b_k = \frac{2}{T} \int_0^{\tau_u} U \sin k\omega_0 t dt = -\frac{2}{T} \cdot \frac{U}{k\omega_0} \cos k\omega_0 t \Big|_0^{\tau_u} = -\frac{2}{T} \cdot \frac{UT}{k \cdot 2\pi} (\cos k\omega_0 \tau_u - 1) =$$

$$= \frac{U}{k\pi} (1 - \cos k\omega_0 \tau_u).$$

$$A_k = \sqrt{a_k^2 + b_k^2} = \frac{U}{k\pi} \sqrt{(\sin k\omega_0 \tau_u)^2 + (1 - \cos k\omega_0 \tau_u)^2} = \frac{2U}{k\pi} \left| \sin \frac{k\omega_0 \tau_u}{2} \right|;$$

$$\varphi_k = \arctg \frac{b_k}{a_k} = \arctg \frac{1 - \cos k\omega_0 \tau_u}{\sin k\omega_0 \tau_u} = \frac{k\omega_0 \tau_u}{2}.$$

Звідси отримуємо ряд Фур'є

$$U(t) = \frac{U\tau_u}{T} \left[1 + 2 \sum_{k=1}^{\infty} \frac{\sin \frac{k\omega_0\tau_u}{2}}{\frac{k\omega_0\tau_u}{2}} \cos k\omega_0 \left(t - \frac{\tau_u}{2} \right) \right].$$

Розглянемо *властивості перетворення Фур'є*, позначивши для зручності відповідність між часовою та частотною формами сигналів подвійною стрілкою $S(t) \leftarrow \rightarrow \dot{G}(\omega)$.

Напрямок стрілок означає, що $\dot{G}(\omega) \equiv F[S(t)]$ є прямим, а $S(t) \equiv F^{-1}[\dot{G}(\omega)]$ є зворотним перетворенням Фур'є.

Властивість симетрії. Якщо $S(t) \leftarrow \rightarrow \dot{G}(\omega)$, то $\dot{G}(t) \leftarrow \rightarrow 2\pi S(-\omega)$.

Властивість суперпозиції. Якщо $S_1(t) \leftarrow \rightarrow \dot{G}_1(\omega)$ і $S_2(t) \leftarrow \rightarrow \dot{G}_2(\omega)$, то для будь-яких довільних постійних a_1 і a_2

$$a_1 S_1(t) + a_2 S_2(t) \leftarrow \rightarrow a_1 \dot{G}_1(\omega) + a_2 \dot{G}_2(\omega).$$

Властивість зміни масштабу. Для будь-якої дійсної постійної a виконується відповідність

$$S(at) \leftarrow \rightarrow \frac{1}{a} \dot{G}\left(\frac{\omega}{a}\right).$$

Теорема про зсув спектра. Якщо $S(t) \leftarrow \rightarrow \dot{G}(\omega)$, то

$$S(t)e^{j\omega_0 t} \leftarrow \rightarrow \dot{G}(\omega - \omega_0).$$

З теореми про зсув спектра витікає, що:

$$S(t) \cos \omega_0 t \leftarrow \rightarrow \frac{1}{2} [\dot{G}(\omega + \omega_0) + \dot{G}(\omega - \omega_0)];$$

$$S(t) \sin \omega_0 t \leftarrow \rightarrow \frac{1}{2} [\dot{G}(\omega + \omega_0) - \dot{G}(\omega - \omega_0)].$$

Це означає, що в основі перетворення частоти, яке широко використовується в системах зв'язку, лежить операція множення початкового сигналу $S(t)$ на гармонічну функцію $\cos \omega_0 t$ частоти ω_0 . При цьому початковий спектр переноситься на величину $\pm \omega_0$.

Властивість часового зсуву сигналу. Якщо $S(t) \leftarrow \rightarrow \dot{G}(\omega)$, то

$$S(t - t_0) \leftarrow \rightarrow \dot{G}(\omega) e^{-j\omega t_0}.$$

Ця властивість дозволяє стверджувати, що при часовому зсуві сигнала

лу $S(t)$ на величину t_0 його амплітудний спектр не змінюється. Зміни відбуваються тільки у фазовому спектрі на величину $-\omega_0 t$.

Диференціювання й інтегрування сигналів за часом. Якщо $S(t) \leftarrow \rightarrow \dot{G}(\omega)$ і перетворення Фур'є від $\frac{dS(t)}{dt}$ існує, то

$$\frac{dS(t)}{dt} \leftarrow \rightarrow (j\omega)\dot{G}(\omega); \int_{-\infty}^t S(\tau) d\tau \leftarrow \rightarrow \frac{1}{j\omega}\dot{G}(\omega),$$

за умови, що $\frac{\dot{G}(\omega)}{\omega}$ при $\omega = 0$ має кінцеве значення.

Теорема про згортку. Функція інтегрального перетворення двох сигналів має вигляд

$$f(t) \equiv f_1(t) * f_2(t) = \int_{-\infty}^{\infty} f_1(\tau) f_2(t - \tau) d\tau,$$

і називається згортокою функцій $f_1(t)$ і $f_2(t)$.

Якщо $f_1(t) \leftarrow \rightarrow \dot{G}_1(\omega)$ і $f_2(t) \leftarrow \rightarrow \dot{G}_2(\omega)$, то

$$\int_{-\infty}^{\infty} f_1(\tau) f_2(t - \tau) dt \leftarrow \rightarrow \dot{G}_1(\omega) \dot{G}_2(\omega)$$

або

$$f_1(t) * f_2(t) \leftarrow \rightarrow \dot{G}_1(\omega) \dot{G}_2(\omega).$$

Згортка за частотою. Якщо $f_1(t) \leftarrow \rightarrow \dot{G}_1(\omega)$ і $f_2(t) \leftarrow \rightarrow \dot{G}_2(\omega)$, то

$$f_1(t) f_2(t) \leftarrow \rightarrow \frac{1}{2\pi} \int_{-\infty}^{\infty} \dot{G}_1(u) \dot{G}_2(\omega - u) du$$

або

$$f_1(t) f_2(t) \leftarrow \rightarrow \frac{1}{2\pi} [\dot{G}_1(\omega) * \dot{G}_2(\omega)].$$

Алгебра згортки.

1. Комутативний закон: $f_1(t) * f_2(t) = f_2(t) * f_1(t)$.

2. Дистрибутивний закон:

$$f_1(t) * [f_2(t) + f_3(t)] = f_1(t) * f_2(t) + f_1(t) * f_3(t).$$

3. Асоціативний закон:

$$f_1(t) * [f_2(t) * f_3(t)] = [f_1(t) * f_2(t)] * f_3(t).$$

Приклад 3.2.

Трапецеїдальний сигнал, його перша і друга похідні представлені відповідно графіками на рис. 3.5, а, б, в. Необхідно знайти спектр сигналу $S(t)$.

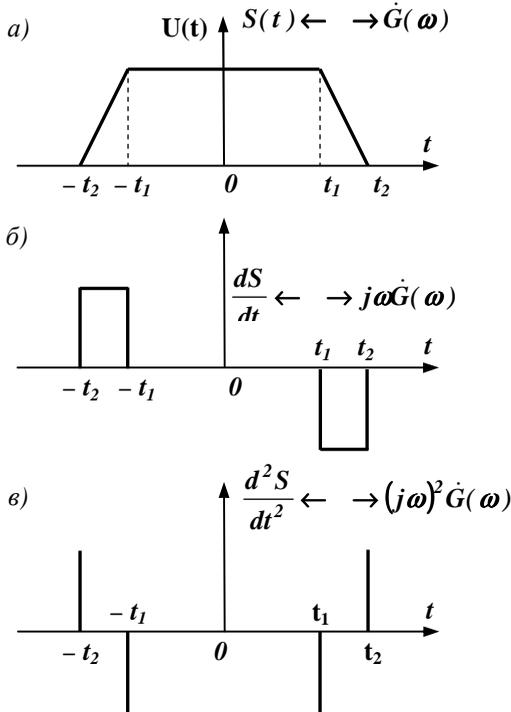


Рис. 3.5. Трапецеїдний сигнал (а), його перша (б) і друга (в) похідні

Двічі продиференціювавши сигнал $S(t)$ одержимо послідовність одиничних імпульсів однакової амплітуди $\frac{U}{t_2 - t_1}$, математичний запис якої має вигляд

$$\frac{d^2S}{dt^2} = \frac{U}{t_2 - t_1} [\delta(t + t_2) - \delta(t + t_1) - \delta(t - t_1) + \delta(t - t_2)].$$

Перетворення Фур'є одиничного імпульсу $\delta(t)$ дорівнює одиниці. Тому на підставі часового зсуву маємо $\delta(t-t_0) \leftarrow \rightarrow e^{-j\omega t_0}$. Використовуючи цей результат і властивість суперпозиції та диференціювання, частотний спектр другої похідної початкового сигналу можна записати у вигляді

$$(j\omega)^2 \dot{G}(\omega) = \frac{U}{t_2 - t_1} (e^{j\omega t_2} - e^{j\omega t_1} - e^{-j\omega t_1} + e^{-j\omega t_2}),$$

де $\dot{G}(\omega)$ – спектр початкового сигналу.

Звідси витікає, що

$$\dot{G}(\omega) = \frac{2U}{t_2 - t_1} \frac{\cos \omega t_1 - \cos \omega t_2}{\omega^2}.$$

У теорії лінійних ланцюгів згортка відома під назвою *інтеграла Дюамеля*, що записується у вигляді

$$u(t) = \int_{-\infty}^{\infty} g(\tau)h(t-\tau)d\tau = \int_{-\infty}^{\infty} h(\tau)g(t-\tau)d\tau \equiv h(t)*g(t),$$

де $g(t)$ – вхідний вплив;

$h(t)$ – імпульсна характеристика;

$u(t)$ – реакція ланцюга на вхідний вплив.

3.3. Дискретизація сигналів за часом і за рівнем. Теорема В. О. Котельникова

Оскільки дискретна форма подання сигналів дає значні переваги при зберіганні і обробці інформації, то розглянемо перетворення неперервних сигналів у дискретні.

Розрізняють квантування (дискретизацію) сигналів за часом і за рівнем. При квантуванні за часом неперервна за аргументом функція $x(t)$, що описує сигнал, перетворюється у функцію дискретного аргументу. Таке перетворення може бути виконане, якщо узяти відліки функції $x(t)$ в дискретні моменти часу t_0, t_1, \dots, t_n . В результаті функція $x(t)$ замінюється сукупністю миттєвих значень $x(t_i), i = 1, 2, \dots, n$.

Часовий інтервал між двома сусідніми фіксованими моментами часу, в яких задається дискретна функція – $T_k = t_i - t_{i-1}$, називається інтерва-

лом часового квантування або інтервалом дискретності. Величину, зворотню інтервалу часового квантування

$$f_k = \frac{1}{T_k}$$

називають частотою квантування (дискретизації).

При часовій дискретизації неперервних функцій часто користуються теоремою, що була сформульована В.О. Котельниковим і носить його ім'я.

Теорема Котельникова. Функція $x(t)$, що не має в своєму спектрі частотних складових поза інтервалом $f \in (-F, F)$, повністю визначається послідовністю своїх відліків $x(kT_0)$, $k = 0, \pm 1, \pm 2, \dots$ у моменти часу, віддалені один від одного на інтервал $T_0 = 1 / 2F$.

Значення функції $x(t)$ в довільний момент часу t обчислюється за формулою

$$x(t) = \sum_{k=-\infty}^{\infty} x(kT_0) \varphi_k(t), \quad (3.7)$$

де $\varphi_k(t)$ – k -а функція відліку

$$\varphi_k(t) = \frac{\sin 2\pi F(t - kT_0)}{2\pi F(t - kT_0)}.$$

Інакше кажучи, теорема Котельникова стверджує, що неперервна функція $x(t)$ зі спектром, обмеженим величиною F , може бути розкладена в ряд у базисі функцій відліку $\varphi_k(t)$. При цьому коефіцієнтами ряду будуть відлікові значення функції $x(kT_0)$, взяті з інтервалом дискретності

$$T_0 = \frac{1}{2F}.$$

Графічна ілюстрація розкладання неперервної функції в ряд Котельникова зображена на рис. 3.6.

Доказ теореми Котельникова. Взевши до уваги, що спектр $G(f)$ функції $x(t)$ обмежений в межах від $-F$ до F , запишемо зворотне перетворення Фур'є, що пов'яже функцію з її спектром

$$x(t) = \int_{-F}^F G(f) e^{j2\pi ft} df. \quad (3.8)$$

З другого боку, функція $G(f)$, що задана на кінцевому інтервалі $f \in (-F, F)$, може бути подана на цьому інтервалі у вигляді ряду Фур'є

(поза інтервалом $(-F, F)$ функція $G(f)$ продовжується періодично)

$$G(f) = \sum_{k=-\infty}^{\infty} C_k e^{-j2\pi \frac{k}{2F} f}, \quad (3.9)$$

де

$$C_k = \frac{1}{2F} \int_{-F}^F G(f) e^{j2\pi \frac{k}{2F} f} df.$$

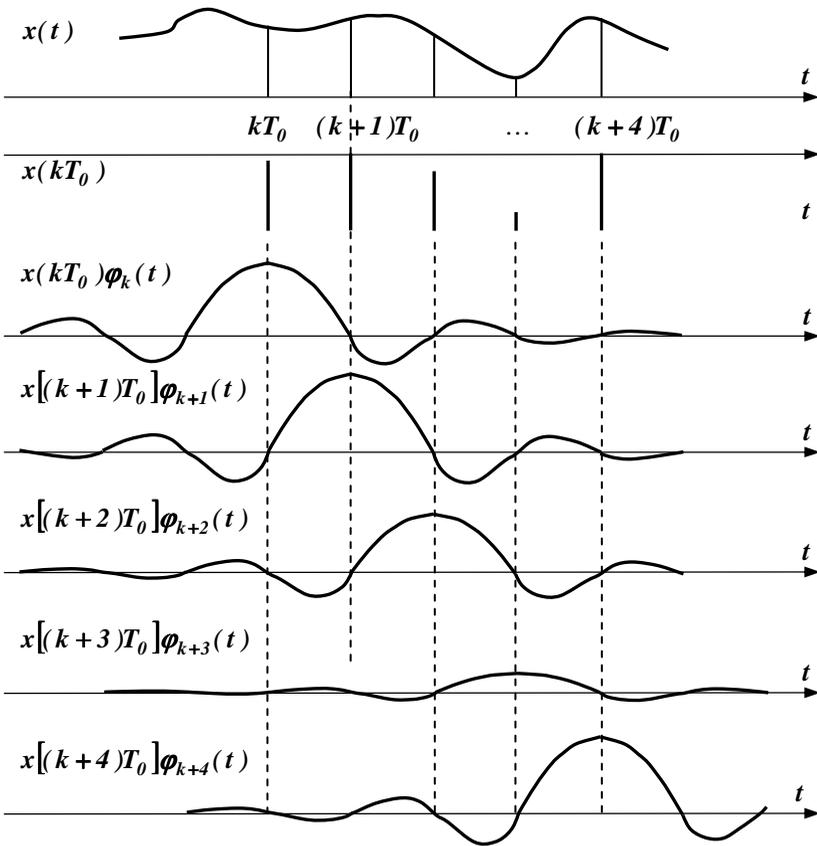


Рис. 3.6. Розкладання в ряд Котельникова неперервної функції.

Згідно з виразом (3.8)

$$C_k = \frac{1}{2F} x\left(\frac{k}{2F}\right),$$

тому замість (3.9) можна записати

$$G(f) = \frac{1}{2F} \sum_{k=-\infty}^{\infty} x(kT_0) e^{-j2\pi k T_0 f}. \quad (3.10)$$

Підставивши вираз (3.10) для спектра $G(f)$ в (3.8), після зміни порядку підсумовування й інтегрування одержимо

$$x(t) = \sum_{k=-\infty}^{\infty} x(kT_0) \left\{ \frac{1}{2F} \int_{-F}^F e^{j2\pi(t-kT_0)f} df \right\}. \quad (3.11)$$

Вираз у фігурних дужках дорівнює k -й функції відліку $\varphi_k(t)$, що підтверджується безпосередньо інтегруванням. При цьому (3.11) співпадає з твердженням теореми Котельникова.

Розглянемо *основні властивості функцій відліку* $\varphi_k(t)$.

1. Функції відліку з різними значеннями індексу k відрізняються одна від одної тільки часовим зсувом. Зокрема

$$\varphi_k(t) = \varphi_0(t - kT_0),$$

де $\varphi_0(t)$ – нульова функція відліку:

$$\varphi_0(t) = \frac{\sin 2\pi F t}{2\pi F t}. \quad (3.12)$$

Функції $\varphi_0(t)$ і $\varphi_k(t)$ зображені на рис. 3.7.

З виразу (3.12) витікає, що $\varphi_0(0) = 1$ і $\varphi_0(kT_0) = 0$ при всіх цілих значеннях k , за винятком $k = 0$. Тому в k -й відліковій точці (тобто в точці $t = kT_0$) тільки один доданок ряду, а саме, доданок з коефіцієнтом k відрізняється від нуля. Між відліковими точками функція $x(t)$ визначається сумою внесків всіх членів ряду (3.7).

2. Функції відліку з різними значеннями індексу взаємно ортогональні

$$\int_{-\infty}^{\infty} \varphi_k(t) \varphi_l(t) dt = \begin{cases} \frac{1}{2F}, & \text{при } k = l; \\ 0, & \text{при } k \neq l. \end{cases}$$

Величина $\frac{1}{2F}$ дорівнює енергії функції відліку.

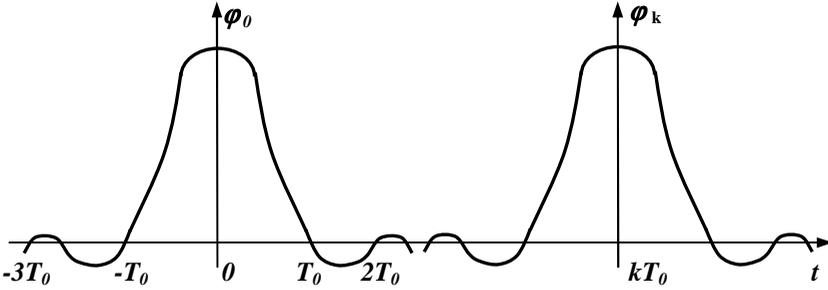


Рис. 3.7. Графіки функцій $\varphi_0(t)$ і $\varphi_k(t)$

3. Нульова функція відліку $\varphi_0(t)$ співпадає з імпульсною характеристикою ідеального фільтра. За визначенням імпульсна характеристика довільної лінійної системи – це реакція системи на вхідну дію у вигляді δ -функції $\delta(t)$.

Імпульсна $h(t)$ і частотна $k(f)$ характеристики системи пов'язані перетворенням Фур'є

$$h(t) = F^{-1}[k(f)]; \quad k(f) = F[h(t)].$$

Частотна характеристика ідеального фільтра має вигляд

$$k_\phi(f) = \begin{cases} \frac{1}{2F}, & \text{при } |f| \leq F; \\ 0, & \text{при } |f| > F. \end{cases} \quad (3.13)$$

Для імпульсної характеристики $h_\phi(t)$, одержимо

$$h_\phi(t) = F^{-1}[k_\phi(f)].$$

Із цього виразу слідує, що при подачі на вхід ідеального фільтра з характеристикою (3.13) функції $\delta(t - kT_0)$ реакція на виході матиме вигляд $\varphi_k(t)$.

Помітимо, що ідеальний фільтр фізично нездійснений і є ідеалізацією фільтра з достатньо крутим спуском частотної характеристики.

Механізм передачі неперервних функцій з обмеженим спектром по каналах зв'язку можна звести до таких основних операцій:

- функція $x(t)$ квантується за часом, тобто замінюється дискретною послідовністю відліків $x(kT_0)$;
- квантовані відліки $x(kT_0)$, що є елементарними повідомлення-

ми, передаються по каналу зв'язку з інтервалом дискретності T_0 ;

- на приймальній стороні формуються короточасні імпульси, площа (або амплітуда) яких пропорційна елементарним повідомленням $x(kT_0)$.

Приблизно формується послідовність $\{x(kT_0)\delta(t - kT_0)\}$, яка подається на ідеальний фільтр низьких частот із смугою зрізу F . У результаті кожний імпульс перетворюється в коливання $x(kT_0)\phi_k(t)$, а вся послідовність в суму, що співпадає з початковим процесом $x(t)$.

Теорема Котельникова визначає величину інтервалу дискретизації певного класу функцій і задає умови, при яких можливе безпомилкове відновлення неперервних сигналів по сукупності їх дискретних вибірок.

Проте, в реальних системах передачі інформації забезпечити суворе виконання цих умов не можливо з таких причин:

- реальні сигнали можуть бути описані лише функціями обмеженої тривалості, оскільки вони є переносниками повідомлень кінцевої довжини;
- при побудові математичного апарату Фур'є виходять з того, що функція $S(t)$ обмеженої часової тривалості в частотній області однозначно описуються лише спектральною функцією $\dot{G}(\omega)$, нескінченно тривалою по осі частот, тобто строго сигнал не може бути одночасно обмеженим за часом і за частотою;
- ідеальний фільтр нижніх частот, за допомогою якого теоретично можлива безпомилкова інтерполяція функцій, практично не реалізується, оскільки в реальних умовах він завжди є фільтром з втратами і кінцевою пам'яттю.

Іншими словами, можна зробити висновок, що формально теорема Котельникова непридатна до реальних сигналів. Проте, якщо до точності відновлення дискретизованого сигналу пред'явити певні вимоги (допустити його відновлення з заданим рівнем похибки), то теоремою Котельникова можна користуватися при дискретизації реальних сигналів, декілька змінивши інтервал дискретизації в порівнянні з величиною $T_0 = 1/2F$, що вказана в теоремі.

Один з можливих підходів до рішення задачі про наближене відновлення дискретизованого сигналу полягає в наступному.

Припустимо, що реальний сигнал $S(t)$ обмеженої тривалості має нескінченний спектр, тобто його спектральна функція $\dot{G}(\omega)$, що одержана

як перетворення Фур'є від $S(t)$, не обмежена по осі частот ω . Якщо властивості спектральної функції такі, що, починаючи з деякої частоти ω_ϵ , енергетичний спектр сигналу $\dot{G}(\omega)$ прагне до нуля, то можна стверджувати, що основна частина енергії сигналу E_c зосереджена в інтервалі частот $[-\omega_\epsilon, \omega_\epsilon]$, тобто

$$E_c = \frac{1}{\pi} \int_0^{\infty} |\dot{G}(\omega)|^2 d\omega \approx \frac{1}{\pi} \int_0^{\omega_\epsilon} |\dot{G}(\omega)|^2 d\omega.$$

За межами цього інтервалу сумарна енергія сигналу дуже мала:

$$E_\epsilon = \frac{1}{\pi} \int_{\omega_\epsilon}^{\infty} |\dot{G}(\omega)|^2 d\omega \rightarrow 0.$$

Тоді за допомогою величини відносної похибки

$$\delta_y = \frac{E_\epsilon}{E_c} = \frac{\int_{\omega_\epsilon}^{\infty} |\dot{G}(\omega)|^2 d\omega}{\int_0^{\infty} |\dot{G}(\omega)|^2 d\omega} \quad (3.14)$$

можна охарактеризувати точність подання сигналу. При цьому, реальні сигнали обмеженої часової тривалості умовно вважаються сигналами з обмеженим в смузі $[-\omega_\epsilon, \omega_\epsilon]$ частотним спектром $\dot{G}(\omega)$ і можуть бути дискретизовані з інтервалом дискретизації $T_0 = 1 / 2F$.

Такі реальні повідомлення, як мова, музика, зображення практично є процесами з обмеженим спектром. Наприклад, верхня частота спектра при передачі мови складає 3,5 ... 4 кГц, музики 8 ... 12 кГц, телевізійних зображень 6 ... 8 МГц. Таким чином, можна прийняти, що реальні сигнали $S(t)$ мають кінцеву тривалість і одночасно обмежені по частоті величиною F . Якщо при цьому фільтр нижніх частот вважати ідеальним, то ряд Котельникова можна обмежити кінцевим числом членів, які потрапляють в інтервал $t \in (0, T)$, тобто для яких $0 \leq kT_0 \leq T$. Число таких ненульових відліків n приблизно дорівнює відношенню тривалості повідомлення до інтервалу дискретності

$$n = \frac{T}{T_0} = 2F_\epsilon T, \quad F_\epsilon = \frac{\omega_\epsilon}{2\pi}.$$

При цьому оцінку $S_{ou}(t)$ реального сигналу $S(t)$ знайдемо як

$$S_{\text{оц}}(t) = \sum_{k=0}^{2F_c T} S(kT_0) \frac{\sin 2\pi F_c (t - kT_0)}{2\pi F_c (t - kT_0)}. \quad (3.15)$$

Вона відрізнятиметься від $S(t)$ не більше, ніж на величину відносної похибки δ_y , визначену в (3.14).

Енергія сигналу тоді буде дорівнювати

$$E_c = \int_{t_0}^{t_k} S^2(t) dt = \frac{1}{2F} \sum_{k=0}^{2F_c T} S^2(kT_0). \quad (3.16)$$

Відповідно до вищевведених положень вирази (3.15), (3.16) є наближеними. У них замість знака рівності необхідно писати знак приближеної рівності. Але цього не роблять через наявність перешкод, оскільки функція $S(t)$ не може бути абсолютно точно передана по каналу зв'язку.

Розглянемо приклад. Знайти відносну похибку δ_y при поданні рядом Котельникова експоненціального сигналу $S(t) = U_0 e^{-\alpha t}$, $t \geq 0$.

Знайдемо енергетичний спектр $\dot{G}(\omega)$ сигналу $S(t)$:

$$\dot{G}(\omega) = U_0 \int_0^{\infty} e^{-(\alpha + j\omega)t} dt = \frac{U_0}{\alpha + j\omega}.$$

Амплітудний спектр $|\dot{G}(\omega)|$ знайдемо як модуль спектральної функції

$$|\dot{G}(\omega)| = \frac{U_0}{\sqrt{\alpha^2 + \omega^2}}.$$

Знайдемо E_c та E_ε

$$E_c = \frac{1}{\pi} \int_0^{\infty} \frac{U_0^2}{\sqrt{\alpha^2 + \omega^2}} d\omega = \frac{U_0^2}{\pi\alpha} \cdot \frac{\pi}{2} = \frac{U_0^2}{2\alpha};$$

$$E_\varepsilon = \frac{1}{\pi} \int_{\omega_\varepsilon}^{\infty} \frac{U_0^2}{\alpha^2 + \omega^2} d\omega = \frac{U_0^2}{\pi\alpha} \left(\frac{\pi}{2} - \arctg \frac{\omega_\varepsilon}{\alpha} \right).$$

Знайдемо відносну похибку δ_y як відношення E_ε до E_c

$$\delta_y = \frac{E_\varepsilon}{E_c} = 1 - \frac{2}{\pi} \arctg \frac{\omega_\varepsilon}{\alpha}.$$

Для одночасного врахування похибки, що вносяться за рахунок необ-

меженості спектра реальних сигналів і відмінності амплітудно – частотної і фазочастотної характеристик реальних фільтрів нижніх частот від відповідних характеристик ідеального фільтра, на практиці рекомендується вибирати інтервал дискретності в 1,5 ... 5 разів менший, ніж це витікає з теорема Котельникова:

$$T_0 = \frac{1}{(3 \dots 10)F_s}.$$

З цієї формули виходить, що на практиці частота дискретизації вибирається до деякої міри довільно і визначається необхідним ступенем наближення $S_{out}(t)$ до $S(t)$. Якщо енергія відкинutoї частини спектра E_ϵ складає малу частку повної енергії сигналу E_c , то похибка відновлення сигналу по дискретних вибірках виявляється незначною. Встановлено, що величина похибки при цьому лежить в межах

$$\frac{E_\epsilon}{E_c} \leq \delta_y \leq \frac{3E_\epsilon}{E_c}.$$

Отже, теорема Котельникова встановлює принципову можливість подання неперервної функції неперервного часу послідовністю її миттєвих значень, узятих в дискретних точках часової осі. Таку операцію часто називають імпульсним перетворенням неперервної функції часу.

Вище було показано, що передачу будь-якого повідомлення $\lambda(t)$ можна звести до передачі чисел $\lambda_k = \lambda(kT_0)$ з інтервалом дискретності $T_0 = 1/2F$. Ці числа мають неперервну шкалу рівнів і сигнал, сформований на їх основі, буде імпульсним аналоговим сигналом. Проте, процес дискретизації повідомлень можна продовжити, а саме: замінити неперервну шкалу рівнів дискретною. Процес заміни неперервної шкали рівнів дискретною називається **квантуванням за рівнем** або просто квантуванням сигналів.

Механізм квантування зводиться до того, що встановлюється дискретна шкала рівнів $\lambda^{(1)}, \lambda^{(2)}, \dots, \lambda^{(m)}$ і замість відлікового значення $\lambda_k = \lambda(kT_0)$ за неперервною шкалою рівнів передається найближче значення за встановленою дискретною шкалою рівнів. Інтервал між сусідніми дискретними рівнями звичайно приймається постійним $\lambda^{(i+1)} - \lambda^{(i)} = \delta$ і називається **кроком квантування**. Отже, в дискретному сигналі, елементарні повідомлення є не значеннями відліків, а значеннями найближчих дозволених дискретних рівнів.

Очевидно, що квантування призводить до викривлення повідомлень.

Якщо повідомлення, одержане в результаті квантування відліку $\lambda_k = \lambda(kT_0)$, тобто квантоване повідомлення, позначити λ_k^* , то

$$\lambda_k^* = \lambda_k - \xi_k,$$

де ξ_k – різниця між початковим значенням елементарного повідомлення λ_k і найближчим дозволеним рівнем, що називається шумом квантування.

На рис. 3.8 зображені: сітка, що визначає моменти відліків і рівнів квантування, неперервне повідомлення (пунктирна крива на рис. 3.8, а), квантовані відліки λ_k (жирні суцільні лінії на рис. 3.8, а) і шуми квантування ξ_k (рис. 3.8, б).

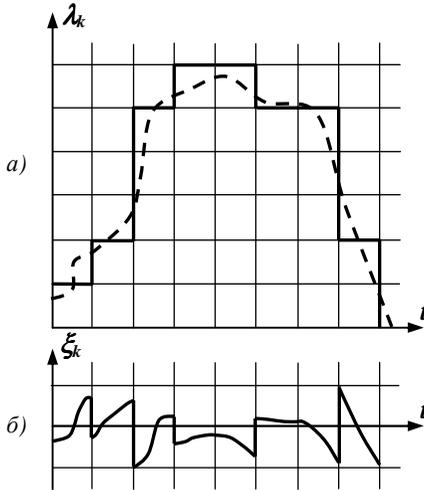


Рис. 3.8. Квантування неперервного сигналу за рівнем (а) та шуми квантування (б)

Шуми квантування або спотворення, обумовлені квантуванням, не мають суттєвого значення, якщо ці спотворення менше спотворень, допустимих заданими технічними умовами.

Помилка квантування є функцією величини кроку квантування δ . При вибраному кроці квантування δ і відомому розмаху квантованого сигналу $[\lambda_{max} - \lambda_{min}]$ кількість рівнів квантування m дорівнює

$$m = \frac{\lambda_{max} - \lambda_{min}}{\delta} + 1.$$

При малому кроці квантування δ шум квантування $\xi_k(t)$ може бути розглянутий як послідовність відрізків прямих ліній зі змінною крутизною (рис. 3.8), обмежених межами $\pm\delta/2$.

Відносна помилка квантування при вибраному кроці квантування визначається кількістю рівнів квантування m . Для її зменшення кількість рівнів квантування повинна бути збільшена.

Вибір величини кроку квантування визначається двома чинниками.

1. Точністю квантованого подання початкової функції, яка задається у вигляді величини відносної помилки

$$\Delta_{max} = \frac{\lambda_{max} - \lambda_{min}}{\delta_{max} - \delta_{min}}.$$

Оскільки Δ_{max} обернено пропорційна кількості рівнів квантування m , то

$$m = \frac{1}{\Delta_{max}}; \tag{3.17}$$

2. Рівнем адитивних перешкод в каналі зв'язку, призначеному для передачі квантованих значень сигналу. На квантоване значення сигналу накладається адитивна перешкода $n(t)$. Якщо величини перешкод (їх розмах) не перевищують величини кроку квантування δ , то перешкоди при передачі ніколи не зможуть вивести квантований сигнал, що передається, із зони, що належить переданому рівню.

Шуми квантування завжди мають місце і їх величина визначає точність роботи системи. При виборі кроку квантування необхідно задовольняти суперечливі вимоги підвищення точності роботи системи з квантуванням (зменшення δ , тобто збільшення m) і підвищення перешкодостійкості квантованих сигналів (збільшення δ). Цю суперечність вирішують таким чином: виходячи з необхідної точності Δ_{max} , вибирають кількість рівнів квантування сигналу за формулою (3.17), а необхідну перешкодостійкість можна додати шляхом посилення квантованого сигналу, збільшуючи тим самим величину кроку квантування δ .

Точне значення ймовірності спотворення квантованого сигналу адитивною перешкодою $n(t)$ може бути обчислено як

$$P_{споте} = P\left[|n(t)| \geq \frac{\delta}{2}\right] = \int_{-\delta/2}^{\delta/2} \varphi(n) dn,$$

де $\varphi(n)$ – щільність розподілу миттєвих значень стаціонарної перешкоди $n(t)$.

У квантованому на m рівнів сигналі можна пронумерувати всі рівні цифрами $0, 1, \dots, m-1$ і замість величини рівня квантування передавати відповідну цифру $N_k \in (0, 1, \dots, m-1)$. Систему зв'язку, в якій об'єктами передачі є цифри, називають **цифровою системою зв'язку**.

Таким чином, будь-які повідомлення, що передаються по каналах зв'язку, можна подати у вигляді послідовності цифр, наступних одна за одною з інтервалом дискретності $T_0 = 1/2F$.

3.4. Основні види випадкових процесів, що протікають у СОІУ

У системах передачі інформації дуже часто зустрічаються випадкові процеси, що протікають за часом приблизно однорідно. Ці процеси мають вигляд неперервних випадкових коливань навколо деякого середнього значення. При цьому ні середнє значення, ні характер цих коливань не зазнають істотних змін за часом. Такі випадкові процеси називаються **стаціонарними**.

Як приклади стаціонарних випадкових процесів можна привести шуми на виході електронних пристроїв, випадкові коливання в ланцюгах живлення тощо.

У будь-якій динамічній системі випадковий процес починається з так званого “перехідного” процесу і потім переходить в сталий режим, який з деяким наближенням можна вважати стаціонарним. Строго кажучи, стаціонарні процеси нескінченні за часом, тобто не мають ні початку, ні кінця. Реально такі процеси не існують. Проте багато випадкових процесів на певних відрізках часу з певним наближенням можна вважати стаціонарними.

Відомо два поняття стаціонарності процесів: стаціонарність у вузькому значенні і стаціонарність в широкому значенні.

Під стаціонарними процесами у вузькому значенні розуміються випадкові процеси, для яких функція розподілу щільності ймовірності $w_n(x_1, t_1; x_2, t_2; \dots; x_n, t_n)$ довільного порядку n не змінюються при будь-якому зсуві всієї групи точок t_1, t_2, \dots, t_n уздовж осі часу, тобто для будь-яких n і τ виконується така умова:

$$w_n(x_1, t_1; x_2, t_2; \dots; x_n, t_n) = w_n(x_1, t_{1+\tau}; x_2, t_{2+\tau}; \dots; x_n, t_{n+\tau}).$$

З приведеного виразу виходить, що для стаціонарних процесів одновимірна функція розподілу щільності імовірності не залежить від часу, тобто

$$w_1(x, t_1) = w_1(x, t_{1+\tau}) = w_1(x), \quad (3.18)$$

а двовимірна функція розподілу щільності імовірності залежить тільки від різниці часу $\tau = t_2 - t_1$, тобто

$$w_2(x_1, t_1; x_2, t_2) = w_2(x_1, x_2, t_2 - t_1) = w_2(x_1, x_2, \tau).$$

Оскільки математичне очікування і дисперсія виражаються через одновимірну функцію розподілу щільності ймовірності, то на підставі виразу (3.18) можна стверджувати, що для стаціонарного процесу математичне очікування і дисперсія не залежать від часу. Із-за залежності двовимірної функції розподілу тільки від різниці часу $\tau = t_2 - t_1$ кореляційна функція стаціонарного процесу також залежить тільки від різниці часу τ .

Таким чином, для стаціонарних процесів можна записати

$$\begin{aligned} M[x(t)] &= M(x); \\ D[x(t)] &= D(x); \\ R_x(t_1, t_2) &= R_x(\tau). \end{aligned} \quad (3.19)$$

На практиці найчастіше зустрічаються випадкові процеси, для яких при виконанні умов виразу (3.19) моменти вищих порядків залежать від часу. Тому поняття стаціонарності доцільно розширити, прийнявши за основу визначення стаціонарності умови (3.19).

У зв'язку з вищевикладеним введено поняття стаціонарності в широкому значенні згідно з яким *стаціонарними процесами* є такі випадкові процеси, у яких математичне очікування і дисперсія не залежать від часу, а кореляційна функція залежить тільки від різниці часу $\tau = t_2 - t_1$.

Випадкові процеси, стаціонарні у вузькому значенні, будуть завжди стаціонарними в широкому значенні, але не навпаки.

Стаціонарні випадкові процеси за своєю природою простіші, ніж не-стаціонарні, і описуються простішими характеристиками. З огляду на те, що стаціонарні процеси зустрічаються на практиці дуже часто, одержала широке застосування спеціальна теорія стаціонарних випадкових процесів.

Розглянемо властивості кореляційної функції стаціонарного випадкового процесу. Визначимо, як поводить себе кореляційна функція при необмеженому збільшенні часового інтервалу $\tau = t_2 - t_1$.

Зі збільшенням часового інтервалу τ залежність між величинами $x(t)$ і $x(t + \tau)$ слабшає. При $\tau \rightarrow \infty$ ці величини стають незалежними.

Тоді з урахуванням того, що математичне очікування добутку випадкових незалежних величин дорівнює добутку математичних сподівань співмножників і того, що для стаціонарного процесу математичне очікування не залежить від часу, одержимо

$$\lim_{\tau \rightarrow \infty} R_x(\tau) = \lim_{\tau \rightarrow \infty} M_I[x(t)x(t+\tau)] = \lim_{\tau \rightarrow \infty} [M_I[x(t)]M_I[x(t+\tau)]] = M^2(x).$$

Таким чином, при необмеженому збільшенні аргументу τ кореляційна функція прагне до квадрата математичного очікування випадкового процесу.

Отже, при $\tau \rightarrow \infty$ кореляційна функція дорівнює потужності постійної складової реалізації випадкового стаціонарного процесу.

Зі зменшенням часового інтервалу τ залежність між величинами $x(t)$ і $x(t+\tau)$ посилюється, і при $\tau \rightarrow 0$ одержимо

$$\lim_{\tau \rightarrow 0} R_x(\tau) = \lim_{\tau \rightarrow 0} M_I[x(t)x(t+\tau)] = M_I[x^2(t)] = M_2[x(t)].$$

Таким чином, при $\tau = 0$ кореляційна функція дорівнює початковому моменту другого порядку функції $x(t)$.

Отже, дисперсія стаціонарного випадкового процесу визначається так:

$$D(x) = R_x(0) - R_x(\infty).$$

Через незалежність функції розподілу щільності ймовірності стаціонарного випадкового процесу від початку відліку часу кореляційна функція є парною функцією τ , тобто

$$R_x(\tau) = R_x(-\tau).$$

Можна показати, що кореляційна функція за абсолютним значенням максимальна при $\tau = 0$. Дійсно, якщо розглянути математичне очікування квадрата суми або різниці величин $x(t)$ і $x(t+\tau)$, то можна одержати

$$\begin{aligned} M_I\{[x(t) \pm x(t+\tau)]^2\} &= M_I[x^2(t)] \pm 2M_I[x(t)x(t+\tau)] + M_I[x^2(t+\tau)] = \\ &= 2R_x(0) \pm 2R_x(\tau). \end{aligned}$$

Оскільки середнє значення додатної величини (квадрата суми або різниці двох величин) не може бути від'ємним, то $2R_x(0) \pm 2R_x(\tau) \geq 0$, звідки

$$|R_x(\tau)| \leq |R_x(0)|.$$

На рис. 3.9 зображені типові криві кореляційних функцій $R_x(\tau)$. Як видно з рисунка, асимптотичне наближення функції $R_x(\tau)$ до сталого

значення $M^2(x)$ може бути як монотонним (рис. 3.9, а), так і немонотонним (рис. 3.9, б).

На практиці часто замість випадкового процесу $x(t)$ розглядають його відхилення від математичного очікування $x_0(t) = x(t) - M(x)$, що називається *пульсаціями* або *флуктуаціями* процесу (центрованим випадковим процесом).

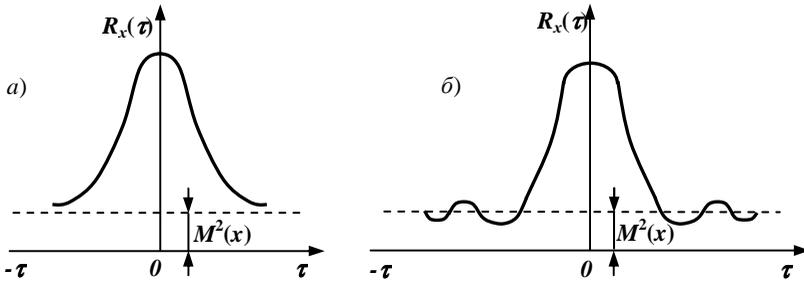


Рис. 3.9. Типові криві монотонної (а) і немонотонної (б) кореляційних функцій

Автокореляційна функція такого процесу обчислюється як

$$R_{x_0}(\tau) = R_x(\tau) - m_x^2$$

і називається автокореляційною функцією флуктуацій або *коваріаційною функцією*. Максимальне значення $R_{x_0}(0)$ дорівнює дисперсії, а $R_{x_0}(\infty) \rightarrow 0$.

Можна записати, що

$$r_{x_0}(\tau) = \frac{R_{x_0}(\tau)}{R_{x_0}(0)} = \frac{R_x(\tau) - m_x^2}{D(x)}.$$

Максимальне значення цього виразу

$$r_{x_0}(\tau) = 1.$$

Існує клас випадкових процесів, що мають важливу для практичних застосувань властивість ергодичності.

Випадковий процес називається *ергодичним*, якщо усереднення по множині з ймовірністю, скільки завгодно близькою до одиниці, дорівнює усередненню за часом.

Отже, для ергодичних процесів, справедлива рівність

$$m_x = M_1[x(t)] = \bar{x};$$

$$D[x(t)] = M_1\{[x(t) - M_1\{x(t)\}]^2\} = \overline{[x(t) - \bar{x}]^2};$$

$$\sigma^2(x) = M_1[x^2(t)] = \overline{x^2};$$

$$R_{xx}(\tau) = M_1[x(t)x(t+\tau)] = \overline{x(t)x(t+\tau)}.$$

Розкривши вирази, одержимо:

$$m_x = \int_{-\infty}^{\infty} x w_1(x) dx = \lim_{T \rightarrow \infty} \frac{1}{2T} \int_{-T}^T x_i(t) dt;$$

$$D(x) = \int_{-\infty}^{\infty} [x - M_1(x)]^2 w_1(x) dx = \lim_{T \rightarrow \infty} \frac{1}{2T} \int_{-T}^T [x_i(t) - \bar{x}]^2 dt;$$

$$\sigma^2(x) = \int_{-\infty}^{\infty} x^2 w_1(x) dx = \lim_{T \rightarrow \infty} \frac{1}{2T} \int_{-T}^T x_i^2(t) dt;$$

$$R_x(\tau) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} x_1 x_2 w_2(x_1, x_2, \tau) dx_1 dx_2 = \lim_{T \rightarrow \infty} \frac{1}{2T} \int_{-T}^T x_i(t) x_i(t+\tau) dt.$$

Ергодична властивість випадкового процесу має велике практичне значення. При дослідженні таких процесів немає необхідності вивчати велику сукупність реалізацій, а достатньо лише однієї реалізації, що спостерігається протягом тривалого проміжку часу. Наприклад, статистичні властивості флуктуаційних шумів на виході електронних підсилювачів можна вивчати протягом достатньо тривалого часу на одному підсилювачі, а потім результати цього дослідження розповсюдити на всі ідентичні пристрої.

3.5. Енергетичний спектр сигналу

Розглянемо конкретну реалізацію $x^{(k)}(t)$ стаціонарного випадкового процесу $x(t)$, задану на нескінченному інтервалі $t \in (-\infty, \infty)$. При спектральному поданні функція $x^{(k)}(t)$ не задовольняє умові інтегрування, що гарантує можливість подання реальних процесів за допомогою інтеграла Фур'є. Потрібна абсолютна інтегрованість

$$\int_{-\infty}^{\infty} |x^{(k)}(t)| dt < \infty \quad (3.20)$$

або хоча б інтегрованість в квадрати

$$\int_{-\infty}^{\infty} [x^{(k)}(t)]^2 dt < \infty, \quad (3.21)$$

що забезпечує збіжність інтеграла Фур'є до функції $x^{(k)}(t)$.

Однак, випадкові сигнали, що визначені на всій осі часу, мають нескінченну енергію. Крім того, для випадкового процесу $x(t)$ частотний спектр (у класичному уявленні) також є випадковою функцією.

Для того, що б обійти ці труднощі, введемо в розгляд зрізану реалізацію $x_T^{(k)}(t)$ процесу $x(t)$, яка тотожно дорівнює нулю поза інтервалом $|t| \leq T$

$$x_T^{(k)}(t) = \begin{cases} x^{(k)}(t), & \text{коли } |t| \leq T \\ 0, & \text{коли } |t| > T \end{cases}. \quad (3.22)$$

Зрізана реалізація $x_T^{(k)}(t)$ задовольняє умовам інтегрованості (3.20) та (3.21). Для неї може бути визначений спектр, який позначимо як $g_T^{(k)}(f)$.

Виразимо середню потужність реалізації процесу $P^{(k)}$ (яка для реальних процесів завжди є кінцевою) через зрізану реалізацію:

$$P^{(k)} = \lim_{T \rightarrow \infty} \frac{1}{2T} \int_{-T}^T [x^{(k)}(t)]^2 dt = \lim_{T \rightarrow \infty} \frac{1}{2T} \int_{-\infty}^{\infty} [x_T^{(k)}(t)]^2 dt,$$

і, скориставшись рівністю Парсеваля, отримаємо:

$$\left[\int_{-\infty}^{\infty} x^2(t) dt = \int_{-\infty}^{\infty} |g(f)|^2 df \right] \quad (3.23)$$

Перетворимо вираз (3.23) до вигляду:

$$P^{(k)} = \lim_{T \rightarrow \infty} \frac{1}{2T} \int_{-\infty}^{\infty} |g_T^{(k)}(f)|^2 df.$$

Далі внесемо операцію обчислення межі під знак інтеграла, скориставшись при цьому позначенням

$$G_x^{(k)}(f) = \lim_{T \rightarrow \infty} \frac{1}{2T} \left| g_T^{(k)}(f) \right|^2.$$

У результаті можна записати

$$P^{(k)} = \int_{-\infty}^{\infty} G_x^{(k)}(f) df.$$

Функція $G_x^{(k)}(f)$ має ясний фізичний сенс – це спектральна щільність потужності $P^{(k)}$ k -ї реалізації процесу $x^{(k)}(t)$. Вона характеризує розподіл повної потужності $P^{(k)}$ за частотами і є середньою потужністю, що доводиться на 1 Гц при даній частоті f .

Частина потужності, що зосереджена в довільній смузі частот $f \in (f_1, f_2)$, визначається шляхом обчислення інтеграла

$$\int_{f_1}^{f_2} G_x^{(k)}(f) df.$$

Введену таким чином спектральну щільність потужності $G_x^{(k)}(f)$ називають також енергетичним спектром функції $x^{(k)}(t)$, так як розмірність функції G дорівнює відношенню потужності до частоти

$$\left[G_x^{(k)}(f) \right] = \left[\frac{\text{потужність}}{\text{частота}} \right] = [\text{потужність} \times \text{час}] = [\text{енергія}].$$

У загальному випадку функція $G_x^{(k)}(f)$ є характеристикою реалізації $x^{(k)}(t)$ і для різних реалізацій виходить різною.

Для отримання енергетичного спектра $G_x(f)$ процесу $x(t)$ потрібно ще зробити усереднення по ансамблю реалізацій

$$G_x(f) = \langle G_x^{(k)}(f) \rangle. \tag{3.23}$$

Теорема Вінера – Хінчина. А. Хінчин і Н. Вінер незалежно один від одного встановили, що енергетичний спектр $G_x(f)$ стаціонарного процесу $x(t)$ і його основна характеристика – кореляційна функція $R_x(\tau)$ зв'язані між собою перетворенням Фур'є (теорема Вінера – Хінчина). Для доведення цієї теореми розглянемо часову кореляційну функцію

$$R_x^{(k)}(\tau) = \lim_{T \rightarrow \infty} \frac{1}{2T} \int_{-T}^T x^{(k)}(t) x^{(k)}(t + \tau) dt,$$

яку виразимо через зрізану реалізацію (3.22):

$$R_x^{(k)}(\tau) = \lim_{T \rightarrow \infty} \frac{1}{2T} \int_{-\infty}^{\infty} x_T^{(k)}(t) x_T^{(k)}(t + \tau) dt.$$

Знаючи спектр зрізаного процесу $x_T^{(k)}(t)$ запишемо спектр зсунутого за часом процесу $x_T^{(k)}(t + \tau)$

$$g_T^{(k)}(f) \exp(-j2\pi f \tau).$$

Виразивши $x_T^{(k)}(t)$ і $x_T^{(k)}(t + \tau)$ через їх спектри, одержимо

$$\begin{aligned} R_x^{(k)}(\tau) &= \lim_{T \rightarrow \infty} \frac{1}{2T} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} g_T(f_1) e^{j2\pi f_1 t} df_1 \int_{-\infty}^{\infty} g_T(f_2) e^{j2\pi f_2 (t + \tau)} df_2 dt = \\ &= \lim_{T \rightarrow \infty} \frac{1}{2T} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} g_T^{(k)}(f_1) g_T^{(k)}(f_2) e^{j2\pi(f_1 + f_2)t} e^{j2\pi f \tau} df_1 df_2 dt. \end{aligned}$$

З урахуванням того, що

$$\int_{-\infty}^{\infty} e^{j2\pi(f_1 + f_2)t} dt = \delta(f_1 + f_2) \text{ і } g(-f) = g^*(f),$$

маємо

$$R_x^{(k)}(\tau) = \lim_{T \rightarrow \infty} \frac{1}{2T} \int_{-\infty}^{\infty} |g_T^{(k)}(f)|^2 e^{j2\pi f \tau} df.$$

Далі, знову переходячи до границі під знаком інтеграла і скориставшись позначенням для енергетичного спектра, одержимо

$$R_x^{(k)}(\tau) = \int_{-\infty}^{\infty} G_x^{(k)}(f) e^{j2\pi f \tau} df. \quad (3.25)$$

Цей вираз є зворотним перетворенням Фур'є, що пов'язує функцію

частоти $G_x^{(k)}(f)$ з функцією часу $R_x^{(k)}(\tau)$.

Пряме перетворення Фур'є матиме вигляд

$$G_x^{(k)}(f) = \int_{-\infty}^{\infty} R_x^{(k)}(\tau) e^{-j2\pi f\tau} d\tau. \quad (3.26)$$

Одержана закономірність, що виражена парою перетворень Фур'є (3.25), (3.26) носить загальний характер і полягає в наступному. Якщо детермінований процес, зокрема реалізація випадкового процесу $x^{(k)}(t)$, має обмежену середню потужність, то часова кореляційна функція і енергетичний спектр цього процесу є парою перетворень Фур'є.

Для того, щоб від характеристик реалізацій перейти до характеристик процесів в цілому, усереднимо одержану пару перетворень Фур'є (3.25) і (2.26) по ансамблю реалізацій. Усереднення характеристик, що входять в праві і ліві частини рівностей (3.25) і (3.26) з урахуванням стаціонарності процесу $x(t)$, дає

$$\langle R_x^{(k)}(\tau) \rangle = \lim_{T \rightarrow \infty} \frac{1}{2T} \int_{-T}^T \langle x_T^{(k)}(t) x_T^{(k)}(t+\tau) \rangle dt = R_x(\tau)$$

і за визначенням (3.24):

$$\langle G_x^{(k)}(f) \rangle = G_x(f).$$

У результаті одержимо твердження теореми Вінера – Хінчина про те, що кореляційна функція $R_x(\tau)$ і енергетичний спектр $G_x(f)$ стаціонарного випадкового процесу $x(t)$ являють собою пару перетворень Фур'є

$$G_x(f) = \int_{-\infty}^{\infty} R_x(\tau) e^{-j2\pi f\tau} d\tau; \quad R_x(\tau) = \int_{-\infty}^{\infty} G_x(f) e^{j2\pi f\tau} df.$$

Останнє співвідношення вказує на те, що в рамках кореляційної теорії, основною характеристикою стаціонарного процесу $x(t)$ замість кореляційної функції $R_x(\tau)$ може використовуватися енергетичний спектр $G_x(f)$.

Під ефективною шириною спектра прийнято розуміти ширину смуги частот, в межах якої зосереджена переважна частина (звичайно 95 %) потужності процесу. Проте, для випадкових процесів, що характеризуються нерівномірним спектром, ефективну ширину смуги спектра оцінюють за енергетичним критерієм методом еквівалентного прямокутника. Відповідно до цього методу ефективна смуга енергетичного спектра визначається

співвідношенням

$$F_{ef} = \frac{\int_0^{\infty} G_x(f) df}{G_{xmax}(f)} = \frac{R_x(0)}{G_{xmax}(f)},$$

де $G_{xmax}(f)$ – максимальне значення $G_x(f)$ в смузі частот енергетичного процесу.

Для стаціонарного випадкового процесу, що не містить детермінованих складових, завжди існує таке значення $\tau = \tau_{кор}$, що при $\tau \geq \tau_{кор}$ величини $x(t)$ і $x(t + \tau)$ можна практично вважати некорельованими. Величина $\tau_{кор}$ називається часом (інтервалом) кореляції. Миттєві значення процесу, розділені проміжком $\tau_{кор}$, вважають не пов'язаними між собою ні за знаком, ні за величиною. Іноді $\tau_{кор}$ визначається як часовий інтервал, протягом якого значення $r_x(\tau)$ спадає до деякої величини β , як показано на рис. 3.10, а. Час кореляції визначають як основу прямокутника, площа якого дорівнює площі між кривою модуля $r_x(\tau)$ і додатною піввіссю часу, а висота – одиниці (див. рис. 3.10, б)

$$\tau_{кор} = \frac{\int_0^{\infty} |R_x(\tau)| d\tau}{R_x(0)}.$$

Для знакозмінних кореляційних функцій іноді час кореляції визначається як інтервал між початком координат і точкою, в якій $r_x(\tau)$ або $R_x(\tau)$ перший раз перетворюються в нуль (рис. 3.10, в).

Загальна закономірність для випадкових процесів полягає у тому, що добуток ефективної ширини спектра на час кореляції є величиною близькою до одиниці, тобто величина інтервалу кореляції $\tau_{кор}$ пов'язана з шириною спектра F_{ef} обернено пропорційною залежністю: чим менший інтервал кореляції, тим ширший спектр випадкового процесу.

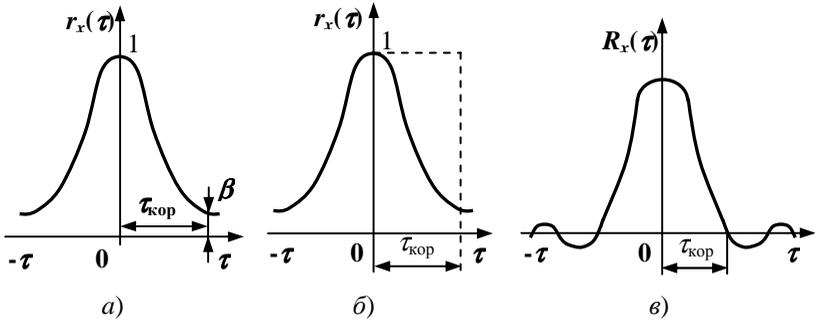


Рис. 3.10. Приклади визначення часу кореляції

Розглянемо приклад. Визначити кореляційну функцію стаціонарного процесу з рівномірним енергетичним спектром, обмеженим частотою F :

$$G_x(f) = \begin{cases} \frac{N_0}{2}, & \text{коли } |f| \leq F \\ 0, & \text{коли } |f| > F \end{cases}.$$

Знайти ефективну смугу енергетичного спектра F_{ef} та час кореляції $\tau_{кор}$.

Параметр N_0 – потужність процесу, що припадає на 1 Гц смуги частот, є основною характеристикою процесу з рівномірним спектром. Наявність коефіцієнта $1/2$ обумовлена тим, що реальний спектр, укладений у смугі $f \in (0, F)$, виходячи з умов зручності аналітичного представлення, розподілений між двома смугами $f \in (0, F)$ і $f \in (-F, 0)$. Повна потужність P_x (або дисперсія σ_x^2) процесу дорівнює добутку ширини спектра F (в області позитивних частот) на потужність, що припадає на 1 Гц смуги частот (N_0)

$$P_x = \sigma_x^2 = \int_{-\infty}^{\infty} G_x(f) df = FN_0.$$

Кореляційна функція процесу

$$R_x(\tau) = \int_{-\infty}^{\infty} G_x(f) e^{j2\pi f \tau} df = \frac{N_0}{2} \int_{-F}^F e^{j2\pi f \tau} df = N_0 F \frac{\sin 2\pi F \tau}{2\pi F \tau}$$

співпадає (з точністю до коефіцієнта $N_0 F$) з функцією відліку $\phi_0(\tau)$.

Кореляційна функція $R_x(\tau)$ перетворюється в нуль в точках, $k = \pm 1, \pm 2, \dots$. Це значить, що перетини процесу $x(t)$, які відстають один від одного на інтервал кратний величині $1/2F$, некорельовані.

Знайдемо F_{ef} та $\tau_{кор}$.

$$F_{ef} = \frac{R(0)}{G_{x \max}} = \frac{N_0 F}{N_0 / 2} = 2F \quad \text{або} \quad F_{ef} = \frac{2 \int_0^F \frac{N_0}{2} df}{N_0 / 2} = \frac{4 \frac{N_0}{2} f \Big|_0^F}{N_0} = 2F ;$$

$$\begin{aligned} \tau_{кор} &= \frac{\int_0^{\infty} N_0 F \frac{\sin 2\pi F \tau}{2\pi F \tau} d\tau}{N_0 F} = \left| \frac{2\pi F \tau = x}{d\tau = \frac{dx}{2\pi F}} \right| = \int_0^{\infty} \frac{1}{2\pi F} \frac{\sin x}{x} dx = \frac{1}{2\pi F} \int_0^{\infty} \frac{\sin x}{x} dx = \\ &= \frac{1}{2\pi F} Si x \Big|_0^{\infty} = \frac{1}{2\pi F} \pi = \frac{1}{2F} \left\{ Si = \int_0^y \frac{\sin x}{x} dx, \text{ при } y = \infty \quad Si = \pi \right\}. \end{aligned}$$

Дійсно, так як $\tau_{кор} = \frac{1}{2F}$, то перетини процесу $x(t)$, які відстають один від одного на інтервал кратний величині $1/2F$, некорельовані.

3.6. Спектральне подання дискретизованих сигналів

На практиці часто потрібно подати сигнал $S(t)$ у вигляді частотних вибірок спектральної щільності $S(j\omega)$ сигналу, а не його часових вибірок $S(n\Delta t_0)$.

Тоді для функції спектра $S(j\omega)$ можна скласти ряд, користуючись властивістю взаємної заміни частоти на час і навпаки для парних функцій. З цією метою базисна функція $\varphi_n(t) = \text{sinc}[\omega_m(t - n\Delta t_0)]$ повинна бути замінена базисною функцією вигляду

$$\varphi_n(\omega) = \frac{\text{sinc}\left[\frac{T_c}{2}(\omega - n\Delta\omega)\right]}{\frac{T_c}{2}(\omega - n\Delta\omega)} = \text{sinc}\left[\frac{T_c}{2}\left(\omega - n\frac{2\pi}{T_c}\right)\right], \quad (3.27)$$

яка отримана з функції $\varphi_n(t)$ заміною t на ω , ω_m на $T_c/2$ і $\Delta t_0 = 1/2 f_m$ на $\Delta\omega = 2\pi/T_c$.

Тоді вираз для ряду Котельникова в частотній області запишеться як

$$S(j\omega) = \sum_{n=-f_m T_c}^{f_m T_c} S(n\Delta\omega) \frac{\sin\left[\frac{T_c}{2}(\omega - n\Delta\omega)\right]}{\frac{T_c}{2}(\omega - n\Delta\omega)} = \sum_{n=-f_m T_c}^{f_m T_c} S\left(n\frac{2\pi}{T_c}\right) \operatorname{sinc}\frac{T_c}{2}\left(\omega - n\frac{2\pi}{T_c}\right). \quad (3.28)$$

Відповідно до виразу (3.28) на рис. 3.11 наведено приклад дискретизації спектра довільного сигналу за теоремою Котельникова, де $\Delta\omega$ - ширина частотної вибірки спектра дискретизованого сигналу.

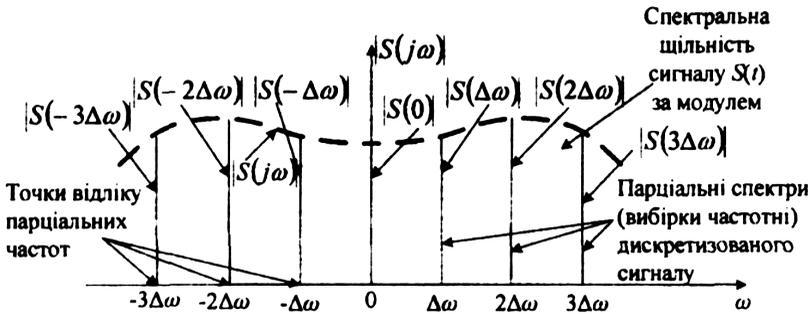


Рис. 3.11. Приклад дискретизованого спектра довільного сигналу за теоремою Котельникова

Аналіз виразу (3.28) і рис. 3.11 показує, що якщо здійснюються часові вибірки відповідно до ряду Котельникова, то часовий інтервал між ними (інтервал дискретизації за часом) не повинен перевищувати значення $\Delta t_0 \leq 1/2 f_m$, а при реалізації частотних вибірок частотний інтервал (інтервал дискретизації за частотою) не повинен перевищувати значення $\Delta\omega \leq 2\pi/T_c$.

При ширині спектра сигналу, що дорівнює $\Delta\omega_c = 2\omega_m$, число частотних вибірок складе $N = 2\omega_m/\Delta\omega = 2f_m T_c$, тобто відповідає представленню сигналу $S(t)$ рядом Котельникова (2.51).

У загальному випадку вибірки $S(n2\pi/T_c)$ у виразі (3.28) є комплексними числами і в кожній точці відліку на осі частот повинні бути задані два параметри: дійсна і уявна частини цієї вибірки (модуль і аргумент).

Таким чином, при частотному представленні сигналу $S(t)$ загальне число параметрів виявляється удвічі більшим, ніж при часовому представленні, коли вибірки $S(n/2f_m)$ є дійсними числами. Така надмірність у частотному представленні сигналу усувається за умови, що $S(n2\pi/T_c)$ і $S(-n2\pi/T_c)$ є комплексно-зв'язаними функціями, тому завдання однієї з них однозначно визначає іншу. Отже, спектр дискретизованого сигналу повністю характеризується сукупністю комплексних вибірок (відліків), узятих тільки в області позитивних частот, і числом незалежних параметрів (мір свободи) сигналу $N = 2f_m T_c$, як і при представленні сигналу в часовій області.

3.7. Особливості процесу дискретизації сигналів

Процес дискретизації сигналів, здійснюваний на боці, що передає, по суті є одним з видів імпульсної модуляції сигналів. Він лежить в основі всіх імпульсних і цифрових видів зв'язку. Тому технічні пристрої, що забезпечують дискретизацію сигналів, можна назвати модуляторами або дискретизаторами, в якості яких часто використовуються різні електронні ключі. Процес дискретизації можна також розглядати як результат множення сигналу $S(t)$ на допоміжну періодичну послідовність $y_T(t)$ коротких тактових імпульсів прямокутної форми з періодом $T = \Delta t_\theta = 1/2f_m$, тривалістю $\tau_i \ll T$ і амплітудою $U_i \gg S_{max}(t)$. Отже, дискретизований сигнал з кроком (тактом) Δt_θ можна записати за допомогою виразу

$$S_T(n\Delta t_\theta) = S(t)y_T(n\Delta t_\theta). \quad (3.29)$$

Структурна схема дискретизатора зображена на рис. 3.12.



Рис. 3.12. Структурна схема дискретизатора

Під час появи чергового імпульсу з генератора тактових імпульсів (ГТІ) на електронний ключ останній відкривається і на виході дискретизатора з'являється відлік (вибірка) сигналу $\delta(i)$ дискретизатора, що діє на вході, в даний момент часу. За відсутності імпульсу на вході 2 від ГТІ електронний ключ закритий і на виході дискретизатора напруга дорівнює нулю. Процес часової дискретизації сигналу $S(t)$ зображений на рис. 3.13. Для визначення вимог до величини $\tau_i/T = \tau_i/\Delta t_o = 2\tau_i f_m$ розглянемо структуру спектра дискретизованого сигналу.

Вважаємо, що спектральна щільність $S(j\omega)$ початкового континуального сигналу $S(t)$ відома відповідно до прямого перетворення Фур'є

$$S(j\omega) = \int_{-\infty}^{\infty} S(t)e^{-j\omega t} dt.$$

Запишемо вираз для спектра періодичної послідовності прямокутних імпульсів зі шпаруватістю $q = T/\tau_i = \Delta t_o/\tau_i$ відповідно до ряду Фур'є в такому вигляді:

$$y_T(n\Delta t_o) = U_i \left[\frac{\tau_i}{T} + 2 \sum_{n=1}^{\infty} \frac{1}{n} \sin\left(\frac{n\omega\tau_i}{2}\right) \cos n\omega\tau_i \right] = U_i \frac{\tau_i}{T} \left[1 + 2 \sum_{n=1}^{\infty} \text{sinc}\left(\frac{n\pi\tau_i}{T}\right) \cos n\omega\tau_i \right]. \quad (3.30)$$

де ω_1 - частота дискретизації сигналу $S(n\Delta t_o)$, $\omega_1 = \frac{2\pi}{T} = \omega_o$.

Підставши вираз (3.30)

$$S_T(n\Delta t_o) = U_i \frac{\tau_i}{T} \left[S(t) + 2S \sum_{n=1}^{\infty} \text{sinc}\left(\frac{n\pi\tau_i}{T}\right) \cos n\omega_1 t \right]. \quad (3.31)$$

Аналіз виразу (3.31) показує, що першому його доданку відповідає спектральна щільність $S(j\omega)$ початкового сигналу, а кожному з добутоків $S(t)\cos n\omega_1 t$ з урахуванням теореми про зсув спектра сигналу (властивість модуляції) відповідає спектральна щільність з двох парціальних (окремих) складових $0,5\{S[j(\omega - n\omega_1)] + S[j(\omega + n\omega_1)]\}$. Таким чином, спектральна щільність дискретизованого сигналу $S(t)$ запишеться як

$$S_T(nj\Delta\omega) = U_i \frac{\tau_i}{T} \left\{ S(j\omega) + \sum_{n=1}^{\infty} \text{sinc}\left(\frac{n\pi\tau_i}{T}\right) S[j(\omega - n\omega_1)] + \sum_{n=1}^{\infty} \text{sinc}\left(\frac{n\pi\tau_i}{T}\right) S[j(\omega + n\omega_1)] \right\}.$$

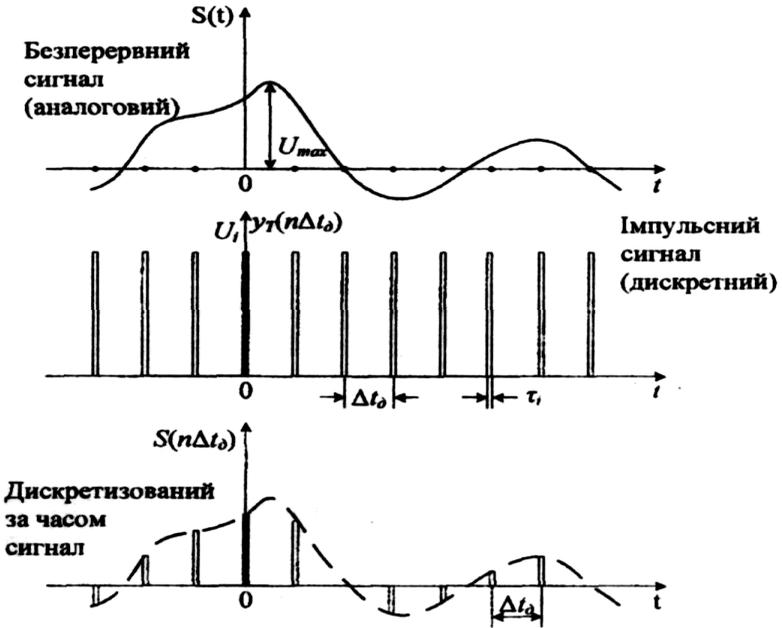


Рис. 3.13. Графіки, що пояснюють процес дискретизації безперервного сигналу $S(t)$

З урахуванням того, що $\lim_{n \rightarrow 0} \sin(\theta) = 1$ можна записати:

$$S_T(nj\Delta\omega) = U_i \frac{\tau_i}{T} \sum_{n=-\infty}^{\infty} \text{sinc}\left(\frac{n\pi\tau_i}{T}\right) S[j(\omega - n\omega_1)] \quad (3.32)$$

На рис. 3.14, а, б, в зображені відповідно спектральна щільність початкового сигналу $S(t)$, спектр періодичної послідовності прямокутної форми зі шпаруватістю $\Delta t_o/\tau_i = 4$ і спектральна щільність дискретизованого сигналу.

На підставі вищевикладеного можна зробити такі висновки:

1. Спектр дискретизованого сигналу $S(n\Delta t_o)$ складається з нескінченної послідовності парціальних спектральних щільностей (спектрів) $S(j\omega_n)$ початкового сигналу $S(t)$ зрушених на частотні інтервали

$\omega_1 = \omega_2 = \frac{2\pi}{T} = \frac{2\pi}{\Delta t_\delta}$, модуль максимальної щільності яких убиває згідно із

законом $\text{sinc}\left(\frac{n\pi\tau_u}{T}\right)$

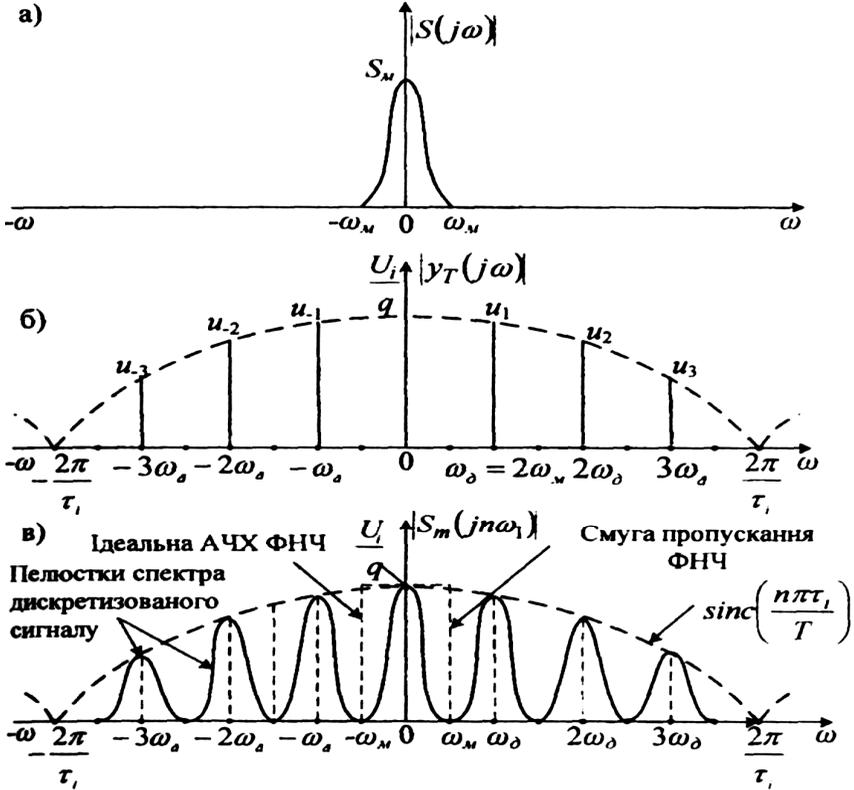


Рис. 3.14. Графіки спектрів: а) початкового сигналу; б) періодичної послідовності прямокутних імпульсів зі шпаруватістю $q = 4$; в) дискретизованого сигналу

2. Якщо крок (інтервал) дискретизації відповідно до теореми відліків Котельникова вибрати з умови $T = \Delta t_\delta \leq 1/2 f_m = \pi/\omega_m$, то окремі (парціальні) спектри не перекриваються і можуть бути виділені фільтром нижніх частот (ФНЧ). На практиці інтервал дискретизації Δt_δ зазвичай вибирають у

декілька разів менше порівняно з $\Delta t_\delta = 1/2 f_m$. Це необхідно для підвищення точності відтворення сигналу і полегшення реалізації ФНЧ на приймальному боці.

З. Із зменшенням відношення $\tau_i/\Delta t_\delta$ пелюстки спектру дискретизованого сигналу убувають швидше при $\tau_i/\Delta t_\delta \rightarrow 0$, тобто під час переходу сигналу $y_T(n\Delta t_\delta)$ до δ -функції спектр дискретизованого сигналу набуває строго періодичної структури а ширина його пелюсток прагне до нуля. Таким чином, послідовність часових відліків набуває вигляд послідовності δ -функції з ваговими коефіцієнтами, що дорівнюють значеннями сигналу $S(t)$ в точках відліку $n\Delta t_\delta$, що ілюструється рис. 3.15.

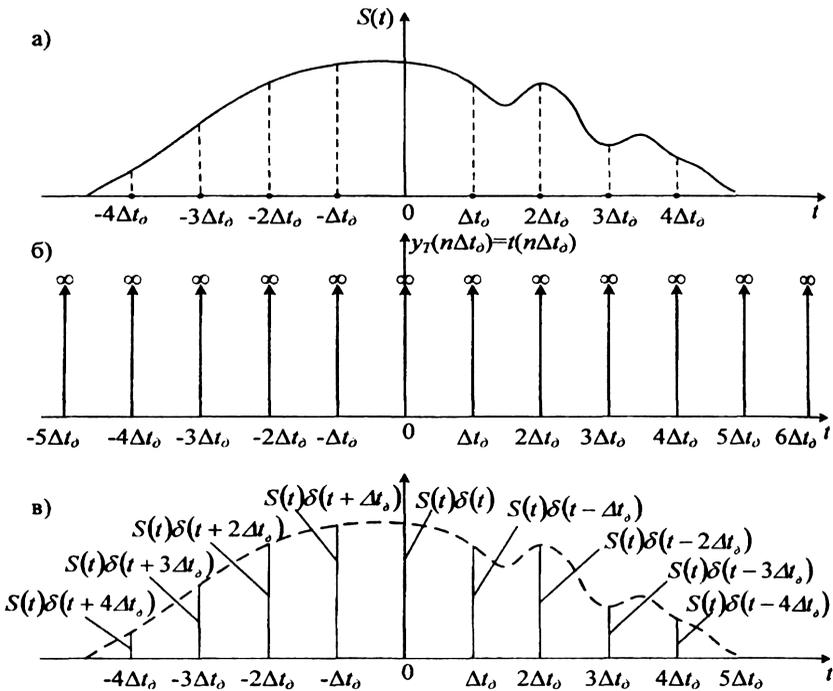


Рис. 3.15. Графіки часових функцій: а) початкового сигналу;
 б) послідовності δ -функцій;
 в) відліків дискретизованого сигналу при $\tau_i/\Delta t_\delta \rightarrow 0$

Тоді вираз (3.30) запишеться у вигляді δ -функції

$$y_T(n\Delta t_\delta) = \sum_{n=-\infty}^{\infty} \delta(t - nT) \quad (3.33)$$

Підставивши вираз (3.33) у вираз (3.29), отримаємо

$$S_T(n\Delta t_\delta) = \sum_{n=-\infty}^{\infty} S(n\Delta t_\delta) \delta(T - n\Delta t_\delta) \quad (3.34)$$

Тоді спектральну щільність дискретизованого сигналу з урахуванням виразу (3.33) можна записати як

$$S_T(nj\Delta\omega) = \frac{1}{\Delta t_\delta} \sum_{n=-\infty}^{\infty} S[j(\omega - n\omega_1)] \quad (3.35)$$

При цьому слід зазначити, що енергія дискретизованого сигналу, виражена через δ -функції, нескінченно велика. Отже, і енергія його спектра нескінченно велика. На практиці використовують тактові імпульси, що виробляються ГТІ, з кінцевою енергією. У цьому випадку спектр $S_T(nj\Delta\omega)$ при $\omega \rightarrow 0$ убуває відповідно до виразу (3.32). Таким чином, представлення сигналу $S_T(n\Delta t_\delta)$ з урахуванням виразу (3.34) істотно спрощує спектральний аналіз дискретизованих сигналів. Наприклад, спектральну щільність $S_T(nj\Delta\omega)$ можна визначити безпосередньо за сукупністю відліків $S(n\Delta t_\delta)$ без звернення до спектра $S(j\omega)$ початкового сигналу $S(t)$. Якщо застосувати пряме перетворення Фур'є до виразу (3.35) при $n = 0, 1, 2, \dots$, то отримаємо

$$\begin{aligned} S_T(j\omega) &= \int_{-\infty}^{\infty} S_T(t) e^{-j\omega t} dt = \int_{-\infty}^{\infty} e^{-j\omega t} \sum_{n=0}^{\infty} S_T(n\Delta t_\delta) \delta(t - n\Delta t_\delta) dt \\ &= \sum_{n=0}^{\infty} S_T(n\Delta t_\delta) \int_{-\infty}^{\infty} e^{-j\omega t} \delta(t - n\Delta t_\delta) dt = \sum_{n=0}^{\infty} S_T(n\Delta t_\delta) e^{-jn\omega\Delta t_\delta}. \end{aligned} \quad (3.36)$$

За своєю розмірністю функції $S(j\omega)$ і $S_T(nj\Delta\omega)$ відрізняються одна від одної. Перша з них (спектральна щільність) має розмірність $\frac{B}{\Gamma\omega} = B \cdot c$, а друга має розмірність B , оскільки спектр дискретизованого сигналу дискретний (лінійчатий).

3.8. Контрольні питання

1. Назвіть основні характеристики сигналів.
2. Дайте визначення часовій та частотній формі подання сигналів.
3. Поясніть основні співвідношення теорії перетворення Фур'є.
4. Поясніть теорему Котельникова.
5. Поясніть властивості функцій відліку.
6. Поясніть порядок застосування теореми Котельникова для дискретизації реальних процесів
7. Поясніть порядок розрахунку похибки подання реальних процесів рядом Котельникова.
8. Поясніть порядок квантування повідомлень по рівню.
9. Перелічіть прості моментні функції випадкових процесів.
10. Дайте визначення кореляційної функції та поясніть її властивості.
11. Дайте визначення стаціонарного випадкового процесу.
12. Дайте визначення ергодичного випадкового процесу.
13. Дайте визначення енергетичного спектра стаціонарного випадкового процесу.
14. Поясніть теорему Вінера – Хінчина.
15. Поясніть порядок розрахунку ефективної ширини спектра та інтервалу кореляції.
16. Поясніть сутність спектрального подання дискретизованих сигналів.
17. Поясніть особливості дискретизації сигналів

Розділ 4

Види та моделі каналів зв'язку у системах обробки інформації та управління

Розглянуто класифікацію каналів зв'язку, моделі дискретного та неперервного каналів зв'язку, канали передачі інформації зі змінними параметрами, оцінка кількості інформації та пропускну здатність дискретного та неперервного каналів зв'язку, узгодження джерел інформації з каналами зв'язку, ефективне кодування Шеннона – Фано та Хаффмана. Також наведено контрольні питання.

4.1. Моделі каналів зв'язку

4.1.1. Класифікація каналів зв'язку

При теоретичному аналізі процесів передачі інформації під **каналом зв'язку** розуміють сукупність технічних засобів і середовища розповсюдження (лінії зв'язку), що забезпечують передачу повідомлень і відповідних їм сигналів між деякими точками (перетинами) системи зв'язку, вибраними відповідно до тих задач, що стоять.

Можна виділити два основні напрями класифікації каналів і відповідних їм моделей, що виходять із самої природи та характеру переданих системою передачі інформації повідомлень (первинних сигналів), які ми раніше розділили на два типи: дискретні та неперервні.

Відповідно розрізняють дискретні і неперервні канали зв'язку (моделі каналів зв'язку). У дискретних каналах зв'язку повідомлення на вході і виході (у перетинах) каналу зв'язку є дискретними, в неперервних каналах – неперервними.

Якщо перетини беруться в проміжних точках каналу зв'язку, то, прив'язуючись вже до вигляду сигналу в цих перетинах, які можуть бути неперервними незалежно від характеру повідомлень, переданих в системі передачі інформації, розглядаються також дискретно – неперервні і неперервно – дискретні канали. У першому випадку на вхід каналу поступають дискретні сигнали, а з виходу знімаються неперервні, в другому – навпаки. У результаті в одній і тій же системі передачі інформації можна виділити

як дискретні, так і неперервні канали (і відповідно канали змішаного типу). Все залежить від того, які вибрані точки входу і виходу (перетини) каналу.

Вибір таких точок найчастіше диктується тим, що визначені раніше функції, що здійснюються над сигналами в передавачі і приймачі, у багатьох випадках виконуються окремими відносно самостійними функціонально закінченими пристроями. Наприклад, в сучасних системах передачі дискретних повідомлень прийнято розрізняти такі дві групи пристроїв: кодеки і модеми. **Модемами** називають пристрої, що перетворюють код в сигнал і сигнал в код (модулятори–демодулятори). Оптимізація модему дозволяє знайти для заданих умов передачі інформації найкращий вигляд сигналу і відповідно оптимальний спосіб його приймання. **Кодеками** називають пристрої, що перетворюють повідомлення в код і код в повідомлення (кодери – декодери). Оптимізація кодека при заданих статистичних характеристиках решти частини системи передачі інформації дозволяє визначити оптимальні методи кодування і декодування.

При класифікації враховують і інші особливості каналних пристроїв: тип лінії зв'язку (фізична лінія, радіолінія, оптична лінія); смугу частот, що відводиться для сигналу (вузькосмуговий, широкосмуговий); технічну швидкість передачі дискретних сигналів (низькошвидкісні, середньошвидкісні, високошвидкісні).

Канали зв'язку є основною ланкою будь-якої системи передачі інформації. Класифікацію каналів зв'язку можна здійснити по різних ознаках (табл. 4.1).

Оптичні дротові - світловоди (оптоволоконний канал) - використовують у стаціонарних системах з великим обсягом інформації, що передається й підвищеними вимогами до швидкості передачі, захищеності від можливого підслуховування та електромагнітних перешкод. Знайшли застосування при організації як глобальних, так і локальних обчислювальних мереж. Головним елементом оптоволоконного кабелю є волоконний світловод - високоякісне скляне (пластикове) волокно завдовжки близько мікрона, що оточене твердим заповнювачем і зверху захищене спеціальною оболонкою. Швидкість передачі інформації може досягати 1000 Мбит/с. Це дуже дорогий спосіб передачі інформації й застосовується для прокладки досить відповідальних каналів зв'язку. Наприклад, за допомогою такого кабелю з'єднуються всі столиці більшості країн світу, великі міста (Москва - Санкт-Петербург).

Оптичні бездротові - вони використовують промінь лазер для передачі сигналу між приймально - передаючими пристроями. Однак, на відміну від волоконної оптики, сигнал передається через відкрите повітряне середо-

вище, а не по оптичному волокну. Для прийому й передачі цифрового сигналу між бездротовими оптичними пристроями між ними не повинне бути ніяких перешкод (таких, наприклад, як дерева). Бездротові оптичні системи використовуються для створення високошвидкісних і безпечних каналів зв'язку, які можна розгорнути протягом дуже малого проміжку часу.

Таблиця 4.1

Класифікація каналів зв'язку

№	Ознака класифікації	Характеристики каналів зв'язку
1	Фізична природа сигналу, що передається	Оптичні та електричні: - дротові (електричні дроти, кабелі, світловоди); - бездротові (радіоканали, інфрачервоні канали й т.д.).
2	Форма подання інформації, що передається	Аналогові - представляють інформацію в безперервній формі у вигляді безперервного сигналу якої-небудь фізичної природи. Цифрові - представляють інформацію в цифровій (перервно - дискретній, імпульсній) формі сигналів якої-небудь фізичної природи.
3	Час існування	Канали, що комутуються - тимчасові, створюються тільки на час передачі інформації (по закінченні передачі інформації й роз'єднанні - знищуються). Канали, що некомутуються - створюються на тривалий час із певними постійними характеристиками. Їх ще називають виділеними.
4	Швидкість передачі інформації	Низькошвидкісні (від 2400-9600 біт/с). Середньошвидкісні (від 9600-56000 біт/с). Високошвидкісні (понад 56 кбіт/с).
5	Смуга частот, що відводиться для сигналу	Вузькосмугові. Широкосмугові.

Такі системи застосовуються для організації тимчасових каналів зв'язку під час виставок, конференцій, спортивних заходів або для швидкого відновлення зв'язку при аварії волоконно-оптичної лінії.

Електричні дротові - електричні дроти (телефонні), кабелі (кручена пара (групи скручених проводів)).

Кабелі крученої пари - застосовують у локальних обчислювальних мережах.

Радіочастотні кабелі застосовують телевізійних мережах, кабельному телебаченні, у міжблочних з'єднаннях радіотехнічних систем.

Електричні бездротові - радіоканали (КХ, УКХ, ВЧ, НВЧ).

4.1.2. Модель дискретного каналу зв'язку

Об'єктом передачі в дискретному каналі є кодові символи. Розглянемо канал дискретну систему передачі даних, що зображена на рис. 4.1 перетинами B і B^* , по якому передається кодовий символ b_i , що може приймати одне з M значень b_1, b_2, \dots, b_M .

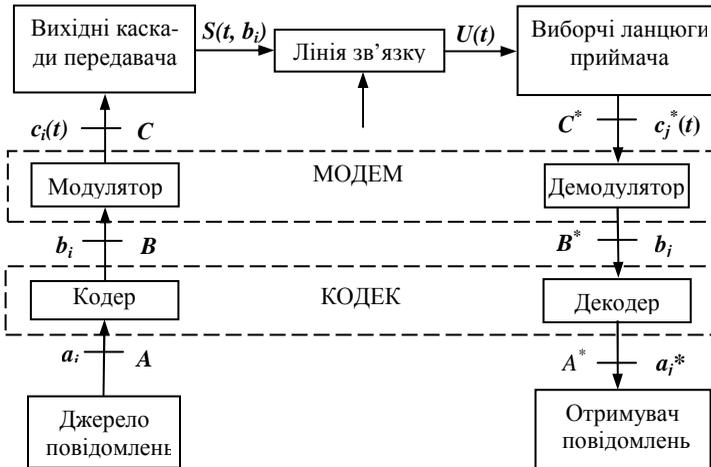


Рис. 4.1. Структурна схема системи передачі дискретної інформації

Дискретний канал вважається математично описаним, якщо заданий алфавіт кодових символів на вході b_i ($i = 1, \dots, M$) разом з їх ймовірністю $P(b_i)$ (якщо джерело має пам'ять, то повинні бути задані апіорна й умовна ймовірності передачі символів), алфавіт кодових символів на виході b_j^* ($j = 1, \dots, M$) і значення ймовірності переходів $P(b_j^* / b_i)$, тобто ймовірність того, що на виході каналу з'явиться символ b_j^* за умови, що на

вхід поданий символ b_i .

В моделі каналу можливі переходи вхідних символів у вихідні описуються у вигляді матриці $\|P(b_j^* / b_i)\|$ розмірності $M \times M$, що називається матрицею перехідних ймовірностей або *канальною матрицею*.

При розгляді складного експерименту XY знання цих характеристик є вичерпним для статистичного аналізу процесу передачі – приймання окремого кодового символу. Зокрема, з їх допомогою визначаються:

➤ сумісна ймовірність подачі символу b_i на вхід і появи символу b_j^* на виході

$$P(b_i, b_j^*) = P(b_i)P(b_j^* / b_i) = P(b_j^*)P(b_i^* / b_i);$$

➤ безумовна ймовірність появи символу b_j^* на виході каналу

$$P(b_j^*) = \sum_{i=1}^m P(b_i, b_j^*);$$

➤ умовна ймовірність того, що на вхід поданий символ b_i за умови, що на виході з'явився символ b_j^* (апостеріорна ймовірність)

$$P(b_i / b_j^*) = \frac{P(b_i)P(b_j^* / b_i)}{\sum_{i=1}^m P(b_i)P(b_j^* / b_i)}.$$

Дискретний канал називається однорідним (стаціонарним) і без пам'яті, якщо ймовірність переходів $P(b_j^* / b_i)$ для кожної пари (i, j) не змінюється за часом і не залежить від символів, що були передані раніше.

Якщо ймовірність $P(b_j^* / b_i)$ залежить від часу, то канал називається *неоднорідним* (нестационарним); якщо ж вона залежить від символів переданих раніше, то канал називається каналом з *пам'яттю*.

Якщо в однорідному дискретному каналі алфавіти на вході і виході однакові ($M = M^*$) і для будь-якої пари $i \neq j$ ймовірності $P(b_j^* / b_i) = p_0 / (M - 1)$, а для пари $i = j$ ймовірності $P(b_j^* / b_i) = q = 1 - p_0$, то такий канал називають *симетричним каналом без стирання*. При $M = 2$ приходимо до моделі двійкового симетричного каналу. Якщо ж об'єм алфавіту символів на виході каналу M^* перевищує

об'єм алфавіту вхідних символів M , то канал називають *каналом із стиранням*.

Найчастіше на практиці зустрічаються дискретні канали із стиранням, в яких $M^* = M + I$. У цих каналах алфавіт вихідних символів містить один додатковий символ, який використовується для відмови від ухвалення рішення про символ, що приймається, в тих випадках, коли він не може бути визначений з необхідною надійністю. При появі такого символу можна послати запит на передавальну сторону системи передачі інформації на повторення пердачи символу.

В дискретних каналах зв'язку повідомлення передаються за допомогою послідовностей символів дискретного джерела найчастіше однаковою для всіх повідомлень довжини. Такий спосіб передачі повідомлень називається *блоковим*, а повідомлення ідентифікуються по блоку кодових символів або дискретних сигналів, що відображають ці символи. Кодер у цьому випадку виконує задачу перетворення блоку інформаційних символів в кодовий блок, що має властивість (за рахунок кодування) протистояти помилкам, що виникають в каналі зв'язку.

В цьому випадку, користуючись додаванням в дискретному векторному просторі (порозрядним, за модулем основи коду M), для будь-якої моделі дискретного каналу можна записати

$$b_j^* = b_i + l_i,$$

де b_i і b_j^* – випадкові послідовності (кодові комбінації або блоки) з n символів на вході і виході каналу;

l_i – випадковий вектор помилок, який в загальному випадку залежить від b_i .

Часто недостатньо знати ймовірності поодиноких помилок (при посимвольному прийманні). Необхідно визначити статистичні особливості груп помилок, особливості їх групування в межах одного блоку переданого повідомлення.

Відомі моделі помилок в дискретних каналах зв'язку відрізняються розподілом імовірності вектора l . Звернемо увагу на моделі помилок при двійковому кодуванні ($M = 2$) і симетричному каналі. У цьому випадку компоненти (розряди) вектора помилок приймають значення 0 і 1 . Всяка 1 у векторі помилки означає, що у відповідному місці переданої послідовності символ прийнятий помилково, а 0 означає безпомилкове прийняття.

Двома найпоширенішими типами моделей джерел помилок є модель потоку незалежних помилок і модель статистично залежних потоків помилок.

Доцільність використання тієї чи іншої моделі джерела помилок визначається дослідженням статистичних властивостей дискретних каналів на основі тестових випробувань. У цьому випадку, на вхід каналу зв'язку подають наперед підготовлену послідовність кодових блоків і, шляхом поелементного порівняння переданої послідовності з прийнятою, відтворюється послідовність помилок, яка називається потоком помилок.

Якщо в результаті статистичних випробувань каналу встановлено, що в потоці помилок безумовні частоти помилок p_0 дорівнюють умовним їх частотам, то такі канали вважаються каналами з незалежними помилками або *каналами без пам'яті* і їх моделюють однорідними двійковими послідовностями. Символи в таких послідовностях характеризуються постійною за часом ймовірністю $P(l_i = 1) = p_0$ і $P(l_i = 0) = 1 - p_0 = q_0$, а їх умовна ймовірність дорівнює безумовній

$$P(l_i = 1 / l_{i-1} = 0) = P(l_i = 1 / l_{i-1} = 1) = P(l_i = 1) = p_0;$$

$$P(l_i = 0 / l_{i-1} = 0) = P(l_i = 0 / l_{i-1} = 1) = P(l_i = 0) = p_0.$$

Закон розподілу кратностей (ваг) помилок для послідовностей символів довжиною n описується відомою в теорії ймовірності формулою Бернуллі, яка відома під назвою біноміального закону розподілу ймовірності

$$P_n(w_l) = C_n^{w_l} p_0^{w_l} (1 - p_0)^{n - w_l},$$

де $p_0^{w_l} (1 - p_0)^{n - w_l}$ – ймовірність поєднання у векторі помилок w_l одиничних і $n - w_l$ нульових символів;

$$C_n^{w_l} \text{ – число різних поєднань помилок кратності } w_l.$$

Модель каналу з незалежними помилками є зручною для обчислення всіх характеристик каналу, проте в реальних умовах помилки є залежними і мають тенденцію до групування.

4.1.3. Модель неперервного каналу зв'язку

Визначимо неперервний канал зв'язку як канал, що здійснює передачу з входу на вихід сигналів, що математично описуються неперервними функціями часу $S(t)$.

Перетворення вхідного сигналу $S_{вх}(t)$ у вихідний $S_{вих}(t) = J_k[S_{вх}(t)]$ у неперервному каналі здійснюється за допомогою перетворювачів, кінцева мета яких – забезпечити взаємооднозначну відповідність між $S_{вх}(t)$ і $S_{вих}(t)$.

В залежності від властивостей чотириполюсників, якими моделюють процеси перетворення сигналу в каналі зв'язку, виділяють такі їх види: лінійні і нелінійні, безінерційні (що не мають пам'яті) й інерційні (з пам'яттю). Розрізняють також канали з постійними і змінними параметрами. Лінійні перетворення J_k вхідного сигналу $S_{ex}(t)$ у вихідний $S_{eux}(t)$ описуються лінійним оператором L_k , який описує може бути заданий в частотній або часовій області. Лінійний оператор у частотній області задається у вигляді комплексної передаточної функції

$$J_k = L_k(f, t) = \dot{K}(f, t) = \left| \dot{K}(f, t) \right| e^{j\varphi_k(f, t)},$$

де $\left| \dot{K}(f, t) \right|$ – амплітудно – частотна характеристика каналу;

$\varphi_k(f, t)$ – фазочастотна характеристика каналу.

У часовій області лінійний оператор задається у вигляді імпульсної перехідної характеристики $h(t, \tau)$, яка пов'язана з $\dot{K}(f, t)$ парою перетворення Фур'є:

$$h(t, \tau) = \int_{-\infty}^{\infty} \dot{K}(f, t) e^{j2\pi f \tau} df;$$

$$\dot{K}(f, t) = \int_{-\infty}^{\infty} h(t, \tau) e^{-j2\pi f \tau} d\tau.$$

Імпульсна характеристика $h(t, \tau)$ (як і передаточна функція) у загальному випадку є функцією двох змінних, що визначають реакцію системи у момент часу τ на δ -імпульс, поданий на її вхід. Наявність аргументу t враховує, що параметри каналу можуть бути змінними за часом.

Вихідний сигнал $S_{eux}(t)$ при відомому вхідному сигналі $S_{ex}(t)$ і лінійному операторі L_k обчислюється як

$$S_{eux} = \int_{-\infty}^{\infty} h(t, \tau) S_{ex}(t - \tau) d\tau = \int_{-\infty}^{\infty} \dot{K}(f, t) G_{ex}(f) e^{j2\pi f t} df.$$

Вихідний сигнал $S_{eux}(t)$ не відрізнятиметься формою від вхідного $S_{ex}(t)$ (з точністю до масштабного коефіцієнта і постійної часової затримки τ_0) лише за умов, коли:

➤ параметри каналу зв'язку, що описується лінійним чотириполюсником, можуть вважатися незмінними за часом $\dot{K}(f, t) = \dot{K}(f)$;

➤ амплітудно – частотна характеристика каналу буде рівномірною

$$|\dot{K}(f)| = K_0;$$

➤ фазочастотна характеристика буде лінійною
 $\Phi_k(f) = 2\pi(f - f_0)\tau$.

Неідеальність амплітудно – частотної і фазочастотної характеристик каналу і їх залежність від часу призводять до спотворень сигналів (зміни форми вихідного сигналу відносно вхідного). Ці спотворення називають *лінійними*.

Лінійні спотворення виникають в лінійному інерційному чотириполюснику і обумовлюються наявністю в них реактивних елементів. Вони виявляються в появі перехідних процесів і виникненні шумів інтерференції. У зв'язку з цим чотириполюсники з неідеальними (відмінними від $|\dot{K}(f)| = K_0$, $\Phi_k(f) = 2\pi(f - f_0)\tau$) характеристиками моделюють канали з пам'яттю.

Нелінійні спотворення пояснюються нелінійністю наскрізної амплітудної характеристики каналу зв'язку $S_{вих}(t) = f[S_{вх}(t)]$. Нелінійні системи з інерційністю поки що не мають загальних методів аналізу, тому на них детально зупинятися не будемо.

Особливістю спотворень сигналів, пов'язаних з неідеальністю характеристик каналів є принципова можливість їх усунення (якщо вони мають детермінований характер).

У реальних каналах, проте, мають місце і випадкові зміни за часом імпульсної перехідної характеристики або передаточної функції. Ці випадкові зміни характеристик каналу приводять до, так званих, мультиплікативних перешкод. У каналі зв'язку, звичайно, присутні і адитивні перешкоди. Тому для математичного опису каналів зв'язку необхідно домовитися про математичні моделі діючих в каналі перешкод. Тому розглянемо моделі неперервних каналів, що найбільш часто використовуються, пов'язані з відповідними моделями перешкод різних типів, які в основному і визначають структуру моделі неперервного каналу зв'язку.

Ідеальним каналом прийнято вважати неперервний канал, в якому відсутні перешкоди (адитивного) і мультиплікативного характеру, а вхідний $S_{вх}(t)$ і вихідний $S_{вих}(t)$ сигнали пов'язані регулярними співвідношеннями.

Відмітимо, що повним описом такого каналу є завдання оператора J_k і вказівка обмежень, що накладаються на вхідні сигнали: ΔF_c , P_{cp} , P_{max} , T_c . Наявність цих обмежень характерна для всіх типів неперервних каналів, тому надалі вони завжди передбачаються заданими, хоча це спеці-

ально обумовлюватися не буде.

До ідеальних каналів іноді можна віднести ряд високоякісних некомутованих дротяних каналів, проте, ця модель мало відповідає реальним умовам.

Розрахунки параметрів ідеальних каналів і сигналів на їх виході здійснюються при моделюванні їх чотирьохполосниками з постійними або змінними за відомим законом параметрами.

Моделлю Гауссова каналу зв'язку описується канал, в якому реалізація коливання $u(t)$, що приймається, є сумою неспотвореного переданого сигналу $S(t)$ і реалізації нормальної флуктуаційної стаціонарної перешкоди $n(t)$ з нульовим середнім значенням

$$u(t) = \mu_0(t)S(t - \tau_0(t)) + n(t).$$

Час затримки $\tau_0(t)$ сигналу $S(t)$ в каналі і множник передачі (коефіцієнт загасання) $\mu_0(t)$ вважаються невинпадковими функціями, відомими в точці приймання.

Завдання гауссового каналу зводиться до опису властивостей нормальної перешкоди $n(t)$ з зазначенням її кореляційної функції $R_n(t, \tau)$ або енергетичного спектру $G_n(f)$. При цьому перешкоду $n(t)$, залежно від вказаних вище характеристик, називають "білим шумом" або "гауссовою перешкодою".

Під "білим шумом" розуміється стаціонарне флуктуаційне коливання, що має рівномірний спектр у всьому діапазоні частот від 0 до ∞ . Така перешкода, як вже було встановлено, має функцію кореляції у вигляді δ -функції і називається некорельованою.

Якщо спектр перешкоди рівномірний в обмеженій смузі частот і рівний нулю поза цією смугою, то таке флуктуаційне коливання називають перешкодою з рівномірним обмеженим спектром.

На відміну від "білого шуму" небілим називають шум, що має нерівномірний спектр і корельовані між собою значення.

Гауссовою або нормальною називають перешкоду, миттєві значення якої розподілені по нормальному (гауссовому) закону. Відзначимо, що в цьому випадку математичний опис перешкоди дозволяє, як і у разі розглянутого раніше дискретного каналу, ввести в розгляд щільність імовірності вхідних сигналів $S(t)$ і умовну щільність імовірності переходу $p(u(t)/s(t))$, яка дає вичерпний опис неперервного каналу.

Неперервний канал називається однорідним (стаціонарним), якщо щільність імовірності $p(u(t)/s(t))$ не залежить від часу. *Канал не має*

пам'яті, якщо значення вихідного сигналу $u(t)$ у момент часу t залежать тільки від вхідного сигналу $S(t)$ в деякий момент часу. Якщо ж значення сигналу $S(t)$ у момент часу t залежить від вхідних сигналів в попередні моменти часу, то **канал має пам'ять**.

4.1.4. Канали передачі інформації зі змінними параметрами

До каналів зв'язку зі змінними параметрами відносять гауссів канал з флюктуючою фазою сигналу в точці приймання; однопроменевий канал зв'язку з завмираннями, обумовленими змінами умов розповсюдження радіосигналу; багатопроменевий радіоканал, що викликає в точці приймання інтерференцію сигналів, які пройшли різний шлях. Сигнал на виході таких каналів в загальному вигляді описується виразом

$$u(t) = \sum_{j=1}^l \{ \mu_j(t) S[t - \tau_j(t)] + n_j(t) \}$$

де l – кількість промінів розповсюдження сигналу в просторі;
 $\mu_j(t)$ – параметр загасання сигналу в кожному промені;
 $\tau_j(t)$ – фазова затримка (запізнювання) сигналу в кожному промені;
 $n_j(t)$ – адитивна компоненту перешкоди в j -му промені.

Такими моделями описується більшість реальних радіоканалів середніх, коротких і УК хвиль з тропосферним та іоносферним розповсюдженням. Саме в цих каналах виявляється найбільшою мірою багатопроменевість і випадкові зміни коефіцієнтів передачі окремого променя. Внаслідок цього амплітудні і фазові співвідношення в точці приймання випадковим чином змінюються, викликаючи, так звані, завмирання сигналу.

Залежно від кореляції флюктуації амплітуд і фаз окремих частотних складових сигналу в точці приймання розрізняють завмирання загальні і селективні.

Завмирання називаються **загальними**, коли кореляція флюктуації частотних складових сигналу настільки значна, що можна вважати підсумкову передаточну функцію каналу $|K(f)|$ і фазовий зсув $\varphi_j(f)$ однаковими для всіх частот сигналу.

Селективні завмирання характеризуються тим, що окремі ділянки частотного спектра сигналу флюктуірують за своїми законами і незалежно

одна від одної.

Загальні і селективні завмирання – це дві зручні моделі, до яких наближаються реальні канали з завмираннями.

Якщо відмінності в загасаннях окремих частотних складових незначні, то можна вважати, що сигнал, який приймається, відрізняється від переданого випадковим коефіцієнтом передачі μ і випадковим, але приблизно однаковим для всіх частотних складових, зсувом фази φ . Саме такі завмирання називають загальними або рівними, оскільки співвідношення між амплітудами і фазами складових вихідного сигналу не змінюються. Для опису таких моделей вже необхідно знати статистичні властивості процесів, що визначають закони зміни амплітуд і фаз в кожному промені.

При великій кількості променів суму сигналів на виході каналу можна вважати нормально розподіленою випадковою величиною з нульовим середнім значенням і обмеженою дисперсією. У таких каналах випадкові зміни інтенсивності (коефіцієнта передачі каналу) в точці приймання апроксимуються розподілом Релея

$$p(\mu) = \frac{\mu}{\sigma^2} e^{-\frac{\mu^2}{2\sigma^2}}, \quad \mu \geq 0$$
$$p(\mu) = 0, \quad \mu < 0.$$

Тут $\sigma = \sqrt{\mu^2 / 2}$ – середньоквадратичне значення коефіцієнта передачі каналу зв'язку з завмиранням.

Для випадкової фази сигналу при цьому використовують рівномірний розподіл

$$p(\varphi) = \begin{cases} \frac{1}{2\pi}, & \varphi \in (0, 2\pi) \\ 0, & \varphi \notin (0, 2\pi) \end{cases}$$

Релеєвські завмирання переважають в ультракороткохвильовому діапазоні при дальньому іоносферному і тропосферному розповсюдженні, а також зустрічаються в діапазонах середніх і коротких хвиль.

Оскільки в каналах зі змінними параметрами рівень сигналу може бути порівняний з рівнем шуму, то достовірність інформації, що приймається, різко зменшується.

За час тривалості елементарного сигналу значення його амплітуди і початкової фази залишаються незмінними. Оскільки значення амплітуди вхідного сигналу величина випадкова, то відношення енергії посилки до

спектральної щільності потужності шуму h_0^2 і ймовірність помилкового прийняття окремої посилки $P_{ном}$ також будуть випадковими величинами.

Для знаходження середньої ймовірності помилки необхідно усереднити $P_{ном}$ за всіма можливими значеннями h_0^2 . У припущенні, що завмирання розподілені за релеєвським законом, ймовірність помилки визначається таким виразом:

$$P_{ном} = \frac{1}{2 + \gamma_c^2 / h_0^2},$$

де γ_c – постійний коефіцієнт, залежний від класу використовуваних двійкових сигналів.

При одній і тій же середній потужності передавача перешкодостійкість у каналі з завмираннями істотно гірше, ніж у каналі з постійними параметрами. Для отримання малої ймовірності помилки у каналі з завмираннями необхідно створювати значне перевищення сигналу над шумом. Наприклад, щоб добитися ймовірності помилки 10^{-5} в каналі з релеєвськими завмираннями, необхідно збільшити потужність передавача в порівнянні з каналом без завмирання приблизно в 4500 разів.

Одним з основних способів підвищення перешкодостійкості при завмираннях сигналу є рознесення приймання. У цьому випадку рішення про передане повідомлення ухвалюється не поодинці, а по декількох несучих одне і теж повідомлення, сигналах. Один і той же сигнал може одночасно передаватися на різних частотах (частотне рознесення) або повторятися кілька разів через певні інтервали часу (часове рознесення). Сигнал від одного передавача може прийматися відразу на декілька антен, розташованих на деякій відстані одна від одної (просторове рознесення). Можливе також рознесення за кутом приходу променя, за поляризацією, за часом запізнювання. На практиці використовують дві – три гілки рознесення. Збільшення кількості гілок рознесення трохи збільшують вірність передачі але не виправдовує ускладнення обладнання.

4.2. Пропускна здатність каналів зв'язку

4.2.1. Оцінка кількості інформації та пропускна здатність дискретного каналу зв'язку

За відсутності в каналі зв'язку перешкод, символи, що передаються і

приймаються, пов'язані однозначно і кількість прийнятої інформації на виході каналу завжди дорівнює кількості інформації, переданої від джерела. Дія перешкод на сигнали, що передаються, призводить до руйнування і необоротної втрати частини інформації. Задача визначення інформаційних характеристик каналів в цих умовах є дуже важливою, оскільки практично не існує систем передачі без перешкод.

Повідомлення дискретного джерела перетворюються в дискретні сигнали, що поступають в канал. Сигнальні символи на вході каналу позначимо $b_1, b_2, \dots, b_i, \dots, b_M$, а на виході – $b_1^*, b_2^*, \dots, b_j^*, \dots, b_N^*$. У загальному випадку розмірності алфавітів на вході і виході каналу можуть не співпадати ($M \neq N$). Наприклад, на практиці зустрічаються канали, в яких $N = M + 1$, оскільки вихідний алфавіт містить додатковий символ стирання, який з'являється тоді, коли немає можливості надійно визначити переданий символ.

Якщо в каналі є перешкоди, то символи, що передаються і приймаються, будуть пов'язані неоднозначно і в процесі передачі символ b_i з різним ступенем імовірності може перейти в будь-який з символів b_j^* і, навпаки, прийнятий символ b_j^* може з'явитися в результаті відправлення будь-якого з символів b_i .

Розглянемо способи інформаційного опису каналів за наявності в них перешкод. Спочатку розглянемо канал зв'язку з боку приймача. При цьому відомі прийнятий символ b_j^* і відповідна ймовірність $P(b_j^*)$. З отриманням символу b_j^* можна припустити, що був посланий якийсь з символів $b_1, b_2, \dots, b_i, \dots, b_M$. Отже, ймовірність посилки символу b_i в канал характеризуватиметься вже не апіорною ймовірністю $P(b_i)$, а деякою умовною апостеріорною ймовірністю $P(b_i / b_j^*)$ – ймовірністю передачі символу b_i , якщо прийнятий символ b_j^* . Розглянута ситуація схематично зображена на рис 4.2.

Оскільки в каналі з перешкодами, прийнятому символу b_j^* може відповідати передача одного з декількох символів b_i , то після приймання b_j^* залишається деяка невизначеність відносно переданого символу.

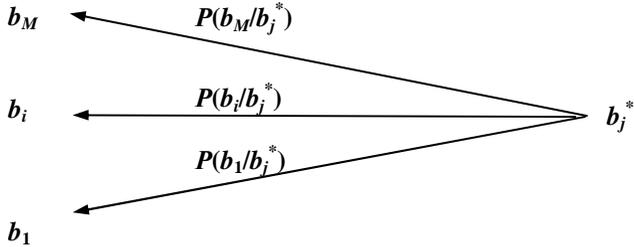


Рис. 4.2. Опис каналу зв'язку з боку приймача

Наприклад, прийнятий символ b_1 . Якби не було перешкод, то з упевненістю можна сказати, що був посланий символ b_1 . Але наявність перешкод позбавляє нас повної упевненості в цьому. Ми все ще припускаємо, що був посланий символ b_1 , але й припускаємо можливість, що міг бути посланий і інший символ. Тому одержана інформація менша за ту, яку ми одержали б за відсутності перешкод на величину цієї невизначеності. Знаючи апостеріорну ймовірність $P(b_i / b_j^*)$ і ймовірність $P(b_j^*)$, можна знайти умовну ентропію $H(B / B^*)$

$$H(B / B^*) = - \sum_{j=1}^N p(b_j^*) \sum_{i=1}^M p(b_i / b_j^*) \log p(b_i / b_j^*).$$

Ця ентропія характеризує середню кількість інформації, що міститься у вхідному символі за умови, що вже стали відомі символи, що приймаються. Середня ж кількість інформації, що посилається з кожним символом в канал, визначається апіорною ймовірністю і дорівнює

$$H(B) = - \sum_{i=1}^M P(b_i) \log P(b_i),$$

де ймовірність $P(b_i)$ може бути обчислена за формулою

$$P(b_i) = \sum_{j=1}^N P(b_i, b_j^*) = \sum_{j=1}^N P(b_j^*) P(b_i / b_j^*).$$

У загальному випадку знання послідовності вихідних символів знижує в середньому первинну невизначеність послідовності символів, що поступають у канал зв'язку. Отже, середня кількість інформації, яку ще може принести одержувачеві один символ в каналі з перешкодами, дорівнює різниці між $H(B)$ і $H(B / B^*)$

$$I(\mathbf{B}, \mathbf{B}^*) = H(\mathbf{B}) - H(\mathbf{B} / \mathbf{B}^*). \quad (4.1)$$

Величина $I(\mathbf{B}, \mathbf{B}^*)$ називається *взаємною інформацією* між множи-нами \mathbf{B} і \mathbf{B}^* . Вона характеризує середню кількість інформації, що міститься в символі множини \mathbf{B}^* відносно символу множини \mathbf{B} і є однією з основних інформаційних характеристик каналу з перешкодами.

Формула (4.1) показує, що середня взаємна інформація $I(\mathbf{B}, \mathbf{B}^*)$ дорівнює різниці між середньою кількістю інформації, що міститься в символі до і після приймання. При цьому величина $H(\mathbf{B})$ характеризує середню на символ кількість посланої в канал інформації, а $I(\mathbf{B}, \mathbf{B}^*)$ – середню на символ кількість прийнятої інформації. Умовну ентропію $H(\mathbf{B} / \mathbf{B}^*)$, рівну різниці між $H(\mathbf{B})$ і $I(\mathbf{B}, \mathbf{B}^*)$, можна вважати середньою кількістю втраченої кожним символом інформації. Її також називають *ненадійністю каналу*.

Таким чином, формула (4.1) має таке просте фізичне значення: середня на символ кількість переданої по каналу зв'язку з перешкодами інформації дорівнює різниці між кількістю інформації на вході каналу і кількістю інформації, втраченої в каналі через перешкоди.

Розглянемо межі, в яких змінюється величина $I(\mathbf{B}, \mathbf{B}^*)$. Оскільки для умовної ентропії справедливе співвідношення $0 \leq H(\mathbf{B} / \mathbf{B}^*) \leq H(\mathbf{B})$, то $I(\mathbf{B}, \mathbf{B}^*)$ може приймати значення в діапазоні від $H(\mathbf{B})$ до нуля. При цьому рівність $H(\mathbf{B} / \mathbf{B}^*) = 0$, що відповідає $I(\mathbf{B}, \mathbf{B}^*) = H(\mathbf{B})$, має місце в тому випадку, коли при кожному b_j^* умовна ймовірність $P(b_i / b_j^*)$ передачі символу b_i дорівнює одиниці, а всі інші $P(b_i / b_j^*) = 0$. Це означає, що, знаючи послідовність вихідних символів $b^*(t)$, можна точно встановлювати послідовність переданих символів $b(t)$. Іншими словами, $b^*(t)$ містить повну інформацію про $b(t)$. Ця ситуація характерна для каналу, в якому перешкоди відсутні. Інший крайній випадок, коли $H(\mathbf{B} / \mathbf{B}^*) = H(\mathbf{B})$, має місце, якщо послідовності вхідних і вихідних символів незалежні. В цьому випадку знання $b^*(t)$ не зменшує невизначеності $b(t)$, тобто $b^*(t)$ не містить ніякої інформації про $b(t)$. Ця ситуація характерна для каналу з дуже сильними перешкодами або при обриві зв'язку.

Приклад 4.1.

Двійковий канал зв'язку з перешкодами описаний з боку приймача. Імовірності реєстрації символів b_1^* , b_2^* такі: $P(b_1^*) = 0,65$, $P(b_2^*) = 0,35$. Апостеріорна ймовірність посилки символів $P(b_1 / b_1^*) = 0,98$, $P(b_2 / b_1^*) = 0,02$, $P(b_1 / b_2^*) = 0,06$, $P(b_2 / b_2^*) = 0,94$.

Обчислити середню на символ кількість інформації, що передається по цьому каналу зв'язку.

Знаходимо умовну ентропію $H(B / B^*)$

$$H(B / B^*) = -\sum_i P(b_i^*) \sum_j P(b_j / b_i^*) \log P(b_j / b_i^*) = -0,65 \cdot (0,98 \cdot \log 0,98 + 0,02 \cdot \log 0,02) - 0,35 \cdot (0,94 \cdot \log 0,94 + 0,06 \cdot \log 0,06) = 0,210 \text{ біт/симв}$$

Обчислимо ймовірності $P(b_i)$ і ентропію $H(B)$

$$P(b_1) = \sum_j P(b_j^*) P(b_1 / b_j^*) = P(b_1^*) P(b_1 / b_1^*) + P(b_2^*) P(b_1 / b_2^*) = 0,65 \cdot 0,98 + 0,35 \cdot 0,06 = 0,66;$$

$$P(b_2) = 1 - P(b_1) = 1 - 0,66 = 0,34$$

$$H(B) = -\sum_{i=1}^2 P(b_i) \log P(b_i) = -0,66 \cdot \log 0,66 - 0,34 \cdot \log 0,34 = 0,925 \text{ біт/симв.}$$

Обчислимо $I(B, B^*)$:

$$I(B, B^*) = H(B) - H(B / B^*) = 0,925 - 0,210 = 0,715 \text{ біт.}$$

Розглянемо тепер опис каналу зв'язку з боку передавача. В цьому випадку відомі переданий символ b_i , безумовна ймовірність $P(b_i)$ і умовна ймовірність $P(b_j^* / b_i)$, що характеризують ймовірність того, що при передачі символу b_i по каналу з перешкодами буде одержаний символ b_j^* . Ці ймовірності називаються перехідними. Така ситуація схематично зображена на рис. 4.3.

Обчисливши безумовну ймовірність $P(b_j^*)$ за формулою

$$P(b_j^*) = \sum_{i=1}^M P(b_i, b_j^*) = \sum_{i=1}^M P(b_i) P(b_j^* / b_i),$$

можна знайти ентропію вихідних символів каналу

$$H(\mathbf{B}^*) = - \sum_{j=1}^N P(b_j^*) \log P(b_j^*).$$

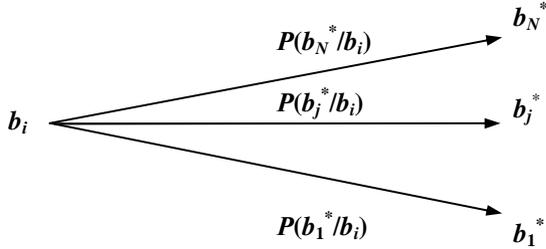


Рис. 4.3. Опис каналу зв'язку з боку передавача

Частина цієї інформації є корисною (інформація про вхідні символи b_i), а частина – помилковою (створеною перешкодами в каналі).

Знаючи ймовірність $P(b_i)$ і перехідну ймовірність $P(b_j^*/b_i)$ можна розрахувати умовну ентропію $H(\mathbf{B}^*/B)$

$$H(\mathbf{B}^*/B) = - \sum_{i=1}^M P(b_i) \sum_{j=1}^N P(b_j^*/b_i) \log P(b_j^*/b_i).$$

Величина $H(\mathbf{B}^*/B)$ визначає інформацію, що міститься в послідовності вихідних символів $b^*(t)$ при відомій послідовності вхідних символів $b(t)$ з розрахунку на один символ. Оскільки вихідна послідовність відрізняється від вхідної виключно через перешкоди в каналі, то $H(\mathbf{B}^*/B)$ характеризує інформацію саме про перешкоди в каналі і називається *ентропією шуму*. Отже, в середньому кожен символ доставляє одержувачеві кількість інформації, що визначається різницею між $H(\mathbf{B}^*)$ і $H(\mathbf{B}^*/B)$

$$I(B, \mathbf{B}^*) = H(\mathbf{B}^*) - H(\mathbf{B}^*/B). \quad (4.2)$$

Приклад 4.2.

Двійковий канал зв'язку з перешкодами описаний з боку передавача. Ймовірність символів $P(b_1) = 0,6$, $P(b_2) = 0,4$. Умовна ймовірність пе-

реходів $P(b_1^* / b_1) = 0,95$, $P(b_2^* / b_1) = 0,05$, $P(b_1^* / b_2) = 0,1$,
 $P(b_2^* / b_2) = 0,9$.

Обчислити середню на символ кількість інформації, що передається по цьому каналу.

Знаходимо умовну ентропію $H(B^* / B)$.

$$\begin{aligned} H(B^* / B) &= -\sum_{i=1}^2 P(b_i) \sum_{j=1}^2 P(b_j^* / b_i) \log P(b_j^* / b_i) = \\ &= -0,6 \cdot (0,95 \cdot \log 0,95 - 0,05 \cdot \log 0,05) - \\ &= -0,4 \cdot (0,90 \cdot \log 0,90 - 0,10 \cdot \log 0,10) = 0,360 \text{ біт}. \end{aligned}$$

Обчислюємо ймовірності $P(b_i^*)$ і ентропію $H(B^*)$.

$$\begin{aligned} P(b_1^*) &= \sum_{i=1}^2 P(b_i) P(b_1^* / b_i) = P(b_1) P(b_1^* / b_1) + P(b_2) P(b_1^* / b_2) = \\ &= 0,6 \cdot 0,95 + 0,4 \cdot 0,1 = 0,61; \end{aligned}$$

$$P(b_2^*) = 1 - P(b_1^*) = 1 - 0,61 = 0,39 .$$

$$H(B^*) = -\sum_{i=1}^2 P(b_i^*) \log P(b_i^*) = -0,61 \cdot \log 0,61 - 0,39 \cdot \log 0,39 = 0,965 \text{ біт}.$$

Отримаємо

$$I(B, B^*) = H(B^*) - H(B^* / B) = 0,965 - 0,360 = 0,605 \text{ біт} .$$

Формули (4.1) і (4.2) наочно зображені на рис. 4.4.

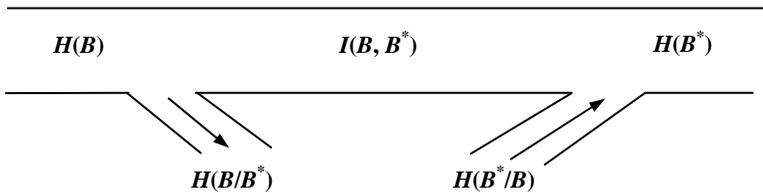


Рис. 4.4. Передача інформації по каналу зв'язку з перешкодами

Тут $H(B)$ – середня кількість інформації, що поступає з кожним символом в канал, а $H(B^*)$ – середня кількість інформації, що доставляється кожним прийнятим символом.

Величина $H(B/B^*)$ є середньою на символ кількістю інформації, що втрачається з каналу; $H(B^*/B)$ – середня кількість інформації, що поступає в канал.

Кожний з наборів $P(b_i)$, $P(b_j^*/b_i)$ і $P(b_j^*)$, $P(b_i/b_j^*)$ є інформаційно повним, оскільки за допомогою будь-якого з них шляхом перетворень можна одержати всі інші інформаційні характеристики каналу.

Хай всі символи b_i , як і відповідні їм символи b_j^* , мають середню тривалість τ_k . Тоді в середньому за одиницю часу по каналу з перешкодами передається кількість інформації $I'(B, B^*)$, що дорівнює:

$$\begin{aligned} I'(B, B^*) &= \frac{I(B, B^*)}{\tau_k} = \\ &= v_k [H(B) - H(B/B^*)] = v_k [H(B^*) - H(B^*/B)], \end{aligned} \quad (4.3)$$

де $v_k = 1/\tau_k$ – швидкість послілки символів в канал.

Величина $I'(B, B^*)$ називається *швидкістю передачі інформації по каналу*.

У співвідношенні (4.3) з чотирьох ентропій одна – $H(B)$ визначається джерелом дискретних повідомлень, а інші три залежать як від властивостей джерела, так і від властивостей каналу. Отже, швидкість передачі інформації не може повною мірою охарактеризувати інформаційні можливості каналу. Необхідно знайти оцінку здатності самого каналу передавати інформацію.

Уявимо, що на вхід каналу можна подавати від джерела символи, розподіл ймовірностей яких можна змінювати. При цьому, очевидно, що швидкість передачі інформації при одній і тій же швидкості послілки символів в каналі і одній і тій же перешкоди буде різною. Максимально можлива швидкість передачі інформації при заданих властивостях каналу зв'язку називається пропускною здібністю каналу зв'язку.

Пропускна здатність каналу C визначається шляхом максимізації виразу (4.3)

$$C = \max_{P(b_i)} I'(B, B^*) = v_k \max_{P(b_i)} I(B, B^*). \quad (4.4)$$

Максимізація здійснюється шляхом вибору оптимального розподілу ймовірностей $P(b_i)$ при заданих v_k і N .

Таким чином, на відміну від швидкості передачі інформації, яка залежить і від статистики джерела, і від властивостей каналу зв'язку, пропуск-

на здатність каналу є характеристикою його самого. Вона не залежить від статистики джерела повідомлень і характеризує граничні можливості каналу відносно передачі середньої кількості інформації за одиницю часу.

Приклад 4.3.

Обчислити пропускну здатність дискретного каналу зв'язку, якщо тривалість символів $\tau_k = 10^{-3} \text{ с}$, а умовна ймовірність переходів $P(b_1^* / b_1) = 0,999$, $P(b_2^* / b_1) = 0,01$, $P(b_1^* / b_2) = 0,01$, $P(b_2^* / b_2) = 0,7$.

Пропускна здатність цього каналу обчислюється шляхом максимізації величини $I(B, B^*)$ по всіх можливих статистиках $P(b_i)$. Отже, необхідно розрахувати швидкість передачі інформації при різних розподілах ймовірності символів $P(b_1)$ і $P(b_2)$ та знайти максимальну. Методика розрахунку швидкості передачі така ж, як і в попередньому прикладі. Результати рішення надані в табл. 4.2.

Аналіз результатів показує, що пропускна здатність каналу зв'язку, що досліджується, буде при $P(b_1) \approx 0,6$, $P(b_2) \approx 0,4$.

Якщо в каналі зв'язку перешкоди роблять однаковий вплив на всі символи, що передаються, то канал називається симетричним. У такому каналі ймовірність всіх помилкових переходів однакова, так само як однакова і ймовірність правильного прийняття всіх символів.

Визначимо пропускну здатність двійкового симетричного каналу зв'язку з перешкодами, в який символи поступають із швидкістю ν_k . Символи, що передаються, b_1 і b_2 незалежні. Ймовірність перетворення в результаті дії перешкод кожного з них $P(b_j^* / b_i) = P_{ном}$. На рис. 4.5 зображені можливі варіанти передачі і прийняття символів по двійковому каналу зв'язку.

Таблиця 4.2

Результати вирішення задачі максимізації величини $I(B, B^*)$

$P(b_1)$	$P(b_2)$	$P(b_1^*)$	$P(b_2^*)$	$H(B^*)$ біт	$H(B^*/B)$ біт	$I(B, B^*)$ біт	$\Gamma(B, B^*)$ біт/с
0,4	0,6	0,58	0,42	0,9814	0,5294	0,452	452
0,5	0,5	0,65	0,35	0,9341	0,4411	0,493	493
0,6	0,4	0,72	0,28	0,8554	0,3531	0,502	502
0,7	0,3	0,79	0,21	0,7415	0,2651	0,476	476

Згідно виразу (4.4) маємо

$$C = v_k \max_{P(b_i)} [H(B^*) - H(B^* / B)].$$

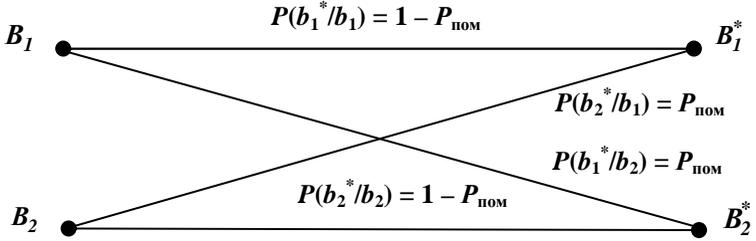


Рис. 4.5. Двійковий симетричний канал зв'язку

Визначимо ентропію шуму

$$\begin{aligned} H(B^* / B) &= -\sum_{i=1}^2 P(b_i) \sum_{j=1}^2 P(b_j^* / b_i) \log P(b_j^* / b_i) = \\ &= -P(b_1) [(1 - P_{ном}) \log(1 - P_{ном}) + P_{ном} \log P_{ном}] - \\ &= -P(b_2) [P_{ном} \log P_{ном} + (1 - P_{ном}) \log(1 - P_{ном})] = \\ &= -[P(b_1) + P(b_2)] [P_{ном} \log P_{ном} + (1 - P_{ном}) \log(1 - P_{ном})] = \\ &= -P_{ном} \log P_{ном} - (1 - P_{ном}) \log(1 - P_{ном}). \end{aligned}$$

Виявляється, що з причини симетрії каналу зв'язку умовна ентропія $H(B^* / B)$ не залежить від статистики вхідних символів, а визначається тільки перехідною ймовірністю. Тому максимальна швидкість передачі інформації досягається тоді, коли прийняті символи b_1^* і b_2^* незалежні і рівноймовірні, що в свою чергу має місце при рівноймовірних символах, що передаються.

Отже, $H(B^*)_{max} = 1$. Тоді пропускна здатність дорівнює:

$$C = v_k [1 + P_{ном} \log P_{ном} + (1 - P_{ном}) \log(1 - P_{ном})].$$

На рис. 4.6 зображена залежність C від імовірності помилки для двійкового каналу.

При $P_{ном} = 0$ пропускна здатність максимальна і дорівнює v_k . Збільшення $P_{ном}$ приводить до зниження пропускної здатності, яка стає рів-

ною нулю при $P_{ном} = 0,5$. В цьому випадку повністю зникає яка-небудь залежність між символами, що передаються і приймаються. Значення $P_{ном} = 0,5$ є граничним для двійкового каналу. Випадок $P_{ном} = 0,5$ називається обривом каналу. Те, що пропускна здатність при $P_{ном} = 1$ така ж, як при $P_{ном} = 0$ (канал без перешкод), пояснюється тим, що при $P_{ном} = 1$ для правильного відновлення символів, що передаються, достатньо інвертувати всі вихідні символи.

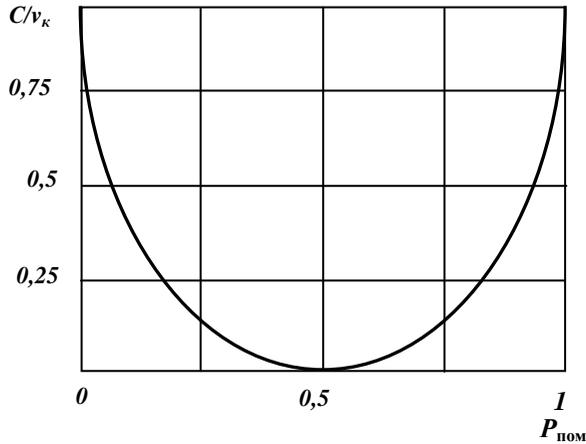


Рис. 4.6. Залежність пропускної здатності двійкового симетричного каналу від імовірності помилкового прийняття символу

З поняттям пропускної здатності каналу пов'язана одна з найважливіших теорем теорії інформації – **теорема Шеннона** про оптимальне кодування. Стосовно дискретного джерела теорема свідчить: якщо продуктивність джерела повідомлень менша пропускної здатності каналу $H'(A) < C$, то існує спосіб оптимального кодування і декодування (перетворення повідомлень в сигнал на передачі і зворотнього його перетворення в повідомлення на прийманні), при якому ймовірність помилки може бути зроблена як завгодно малою. Якщо $H'(A) > C$, то такого способу не існує.

Середня ймовірність помилки при оптимальному кодуванні обчислюється співвідношенням

$$P_{ном} = 2^{-T[C-H'(A)]},$$

де T – тривалість сигналу, відповідної послідовності символів джерела досить великої довжини n ; $C - H'(A)$ визначає запас пропускнуої здатності каналу.

Для дискретного каналу без шумів теорема оптимального кодування формулюється таким чином: якщо продуктивність джерела менша пропускнуої здатності каналу, то існують способи кодування і декодування, що забезпечують скільки завгодно високу надійність відповідності прийнятих комбінацій переданим.

4.2.2. Оцінка кількості інформації та пропускнуа здатність неперервного каналу зв'язку

Розглянемо спрощену схему СПІ, що зображена на рис. 4.7. Схема СПІ складається з джерела, яке створює повідомлення $x(t)$, каналу зв'язку, джерела адитивних перешкод $n(t)$ і адресата, до якого поступає коливання $y(t) = x(t) + n(t)$.

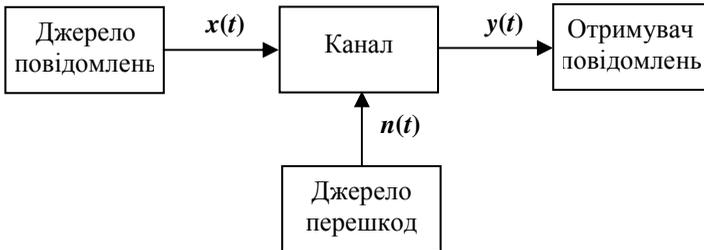


Рис. 4.7. Спрощена схема СПІ

Перешкода є нормальним стаціонарним процесом з нульовим середнім значенням і рівномірним обмеженим спектром. За класифікацією це гауссів канал.

Вважатимемо, що канал пропускає без спотворення всі частоти $|f| < F$, а вищі частоти видаляє. Тоді всі процеси $x(t)$, $n(t)$ і $y(t)$ можна вважати процесами, обмеженими по спектру частотою F , і їх можна відповідно до теореми Котельникова подати послідовністю відліків $y_1 = x_1 + n_1, \dots, y_m = x_m + n_m$, що настають один за одним з інтервалом дискретності $T_0 = 1 / 2F$.

Для інформаційного опису неперервного каналу використовують по-

няття ентропії і кількості інформації для неперервної випадкової величини.

Тоді можна описати кількість інформації, що міститься в одному вихідному відліку щодо одного вхідного відліку, співвідношеннями, аналогічними співвідношенням (4.1) і (4.2):

$$I(x, y) = h(x) - h(x/y) = h(y) - h(y/x), \quad (4.5)$$

де диференціальна ентропія визначається такими виразами:

$$h(x) = - \int_{-\infty}^{\infty} w(x) \log w(x) dx; \quad h(x/y) = - \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} w(x) w(y/x) \log w(y/x) dx dy;$$

$$h(y) = - \int_{-\infty}^{\infty} w(y) \log w(y) dy; \quad h(y/x) = - \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} w(y) w(x/y) \log w(x/y) dx dy.$$

Визначимо пропускну здатність цього каналу, тобто найбільшу кількість інформації, яку можна передати по цьому каналу за 1 секунду (або максимальну швидкість передачі інформації). Шлях розв'язання задачі такий.

1. Визначаємо кількість інформації, що передається по каналу за T секунд $I(T)$.

2. Визначаємо максимальну кількість інформації, що передається по каналу за T секунд $I_{max}(T)$, шляхом максимізації $I(T)$ за всіма можливими джерелами повідомлень, тобто по всіх можливих $x(t)$.

3. Знаходимо пропускну здатність каналу

$$C = I'_{max} = \frac{I_{max}(T)}{T}.$$

Кількість інформації $I(T)$, що передається по каналу за T секунд можна розрахувати по-різному. Можна, наприклад, розрахувати кількість інформації, що припадає на один відлік (з урахуванням взаємозалежності відліків) і помножити його на число відліків $m = 2FT$. У цьому випадку зручно зробити інакше.

Запишемо вираз для кількості інформації, що міститься в сукупності m відліків, тобто

$$I(T) = h(y_1, y_2, \dots, y_m) - h(y_1, y_2, \dots, y_m / x_1, x_2, \dots, x_m),$$

де $h(y_1, y_2, \dots, y_m)$ – ентропія сукупності відліків y_1, y_2, \dots, y_m ;

$h(y_1, y_2, \dots, y_m / x_1, x_2, \dots, x_m)$ – середня умовна ентропія сукупності відліків y_1, y_2, \dots, y_m за умови, що задана сукупність відліків x_1, x_2, \dots, x_m , що передаються.

Оскільки сукупність x_1, x_2, \dots, x_m відома, то невизначеність сукуп-

ності $y_1 = x_1 + n_1, \dots, y_m = x_m + n_m$ дорівнює невизначеності (ентропії) $h(n_1, n_2, \dots, n_m)$ сукупності відліків перешкоди n_1, n_2, \dots, n_m :

$$h(y_1, y_2, \dots, y_m / x_1, x_2, \dots, x_m) = h(n_1, n_2, \dots, n_m) \quad \text{і відповідно}$$

$$I(T) = h(y_1, y_2, \dots, y_m) - h(n_1, n_2, \dots, n_m). \quad (4.6)$$

Ентропію перешкоди $h(n_1, n_2, \dots, n_m)$ можна обчислити, оскільки вид перешкоди $n(t)$ заданий. Це нормальний стаціонарний процес з рівномірним спектром, обмеженим по частоті величиною F . Тому всі відліки n_1, n_2, \dots, n_m перешкоди $n(t)$ статистично незалежні випадкові величини, розподілені за нормальним законом

$$w(n_j) = \frac{1}{\sqrt{2\pi P_n}} \exp\left(-\frac{n_j^2}{2P_n}\right), \quad j = 1, 2, \dots, m$$

де P_n – потужність перешкоди, що дорівнює дисперсії відліку

$$P_n = \sigma_{n_i}^2 = FN_0,$$

де N_0 – спектральна щільність потужності перешкоди.

Ентропія $h(n_j)$ нормального розподілу обчислювалась нами і дорівнює

$$h(n_j) = \log \sqrt{2\pi \sigma_n^2} = \log \sqrt{2\pi P_n}$$

Відповідно, взявши до уваги статистичну незалежність відліків n_1, n_2, \dots, n_m , знаходимо

$$h(n_1, n_2, \dots, n_m) = mh(n_i) = 2FT \log \sqrt{2\pi P_n}. \quad (4.7)$$

Звернемо увагу на один проміжний результат. Згідно (4.6) вплив перешкод, що заважають, виявляється в зменшенні кількості інформації, яка передається по каналу. При цьому цей вплив тим більший, чим більша ентропія перешкоди $n(t)$. Ентропія перешкоди, тобто ентропія сукупності випадкових величин n_1, n_2, \dots, n_m , при даній дисперсії цих величин (потужності перешкоди P_n) буде максимально можливою, якщо всі величини n_1, n_2, \dots, n_m незалежні і розподілені за нормальним законом. Останнє має місце, коли випадковий процес $n(t)$ є нормальним стаціонарним процесом з рівномірним спектром, обмеженим по частоті величиною F .

Оскільки статистичні властивості перешкоди і, зокрема, величини $h(n_1, n_2, \dots, n_m)$ задані, залишається максимізувати ентропію

$h(y_1, y_2, \dots, y_m)$. Ентропія $h(y_1, y_2, \dots, y_m)$ сукупності відліків $y_1 = x_1 + n_1, \dots, y_m = x_m + n_m$ за умови, що дисперсія відліку $\sigma_{y_i}^2$ задана (дорівнює $P_c + P_n$ – сумі середньої потужності сигналу P_c і перешкоди P_n) одержувачеві коливань, якщо повідомлення таке, що всі відліки y_1, y_2, \dots, y_m незалежні і розподілені за нормальним законом. За аналогією з (4.7) одержуємо

$$h_{\max}(y_1, \dots, y_m) = mh(y_i) = 2FT \log \sqrt{2\pi(P_c + P_n)}$$

Для того, щоб всі елементи $y_1 = x_1 + n_1, \dots, y_m = x_m + n_m$ так само, як і елементи сукупності n_1, n_2, \dots, n_m , були незалежними нормальними величинами, необхідно, щоб незалежними нормальними величинами були відліки повідомлення x_1, x_2, \dots, x_m . При цьому процес $x(t)$ буде нормальним процесом з рівномірним спектром, обмеженим по частоті величиною F .

Таким чином, по каналу зі смугою пропускання $|f| < F$, в якому діє гауссова перешкода передається максимально можлива кількість інформації, коли повідомлення $x(t)$ є нормальним процесом з рівномірним спектром, обмеженим по частоті величиною F , тобто коли повідомлення по своїй статистичній структурі подібне перешкоді (є шумоподібним).

Найбільша кількість інформації, що передається по каналу за T секунд,

$$I_{\max}(T) = h_{\max}(y_1, y_2, \dots, y_m) - h(n_1, n_2, \dots, n_m)$$

або

$$I_{\max}(T) = FT \log(1 + P_c / P_n) \quad (4.8)$$

і пропускна здатність каналу

$$C = \frac{I_{\max}(T)}{T} = F \log \left(1 + \frac{P_c}{P_n} \right). \quad (4.9)$$

Приклад 4.4.

По каналу зв'язку без пам'яті передається сигнал $x(t)$, (нормальний випадковий процес з нульовим середнім значенням) з дисперсією $\sigma_s^2 = 8 \text{ мВт}$ і рівномірним енергетичним спектром G_0 у смузі частот каналу $F_k = 3100 \text{ Гц}$. У каналі діє незалежна від сигналу перешкода $n(t)$ типу "білий шум" зі спектром $G_{ш} = 3,22 \cdot 10^{-7} \text{ Вт/Гц}$, нормальним розподілом і нульовим середнім значенням. Обчислити кількість інформації, що

передана по каналу.

Кількість інформації обчислюється згідно з виразом (4.5)

$$I(x, y) = h(y) - h(y/x),$$

де $h(y/x) = h(n) = \log \sqrt{2\pi\sigma_n^2}$;

$$h(y) = \log \sqrt{2\pi(\sigma_s^2 + \sigma_n^2)} .$$

$$\begin{aligned} \text{Тоді } I(x, y) &= \log \sqrt{2\pi(\sigma_s^2 + \sigma_n^2)} - \log \sqrt{2\pi\sigma_n^2} = \log \frac{\sqrt{2\pi(\sigma_s^2 + \sigma_n^2)}}{\sqrt{2\pi\sigma_n^2}} = \\ &= \log \sqrt{1 + \frac{\sigma_s^2}{\sigma_n^2}} = \frac{1}{2} \log \left(1 + \frac{\sigma_s^2}{\sigma_n^2} \right) = 1,58 \text{ біт/відлік} . \end{aligned}$$

Наведені формули для максимальної кількості інформації, яка передається по каналу (4.8), і для пропускної здатності каналу (4.9) виведені Шеноном в більш загальному вигляді носять назву формул або теореми Шенона для неперервного каналу.

Зокрема, при смузі пропускання каналу $|f| \in (f_0 - 0,5\Delta f, f_0 + 0,5\Delta f)$ формули Шеннона приймають такий вигляд:

$$I_{max}(T) = \Delta f T \log(1 + P_c / P_n) \text{ дв. од.}$$

$$C = \Delta f \log(1 + P_c / P_n) \text{ дв. од./сек} .$$

Теорема Шеннона для неперервного каналу цікава з двох точок зору. По-перше, формули встановлюють теоретичну межу швидкості передачі інформації по каналах зв'язку, яка принципово не може бути перевершена. Ця межа реалізується, якщо вхідний сигнал $x(t)$ – нормальний процес з рівномірною спектральною щільністю в смузі частот F . Інакше швидкість передачі інформації буде менша C . Зіставлення швидкості передачі інформації в реальній системі I' з теоретичною межею C характеризує якість системи і ступінь її досконалості.

По-друге, теорема затверджує наступне: якщо джерело створює повідомлення, ентродія – ентропія h_ϵ (ентропія за 1 секунду) яких не перевищує величини C , що встановлена формулою (4.9), то можна передати інформацію з правильністю відновлення, найближчою до заданої. Теорія знову затверджує існування досить досконалих систем, але не вказує шляху побудови цих систем.

Нарешті, із співвідношення (4.8) виходить, що кількість інформації,

що передається по каналу в добре спроектованій системі, повинна приблизно дорівнювати добутку тривалості повідомлення T , ширини смуги пропускання каналу F і так званого динамічного діапазону $D = \log(1 + P_c / P_n)$, який є монотонною функцією відношення потужностей сигналу та перешкоди. Одну і ту ж кількість інформації можна одержати при різних значеннях цих трьох співмножників. Тому при передачі заданої кількості інформації I можна здійснити обмін часу передачі T на ширину смуги F , ширину смуги Δf або тривалість передачі T – на динамічний діапазон D .

Найбільш просто здійснити обмін часу T на ширину смуги F . Для цього повідомлення, що передається, з верхньою частотою F записують на магнітофонну стрічку. При передачі повідомлення відтворюється зі швидкістю збільшеною (зменшеною) у k разів. Відповідно збільшується (зменшується) у k разів верхня частота спектра повідомлення.

З формули виходить можливість обміну смуги пропускання на потужність сигналу і навпаки. Проте, оскільки C залежить від F лінійно, а від відношення P_c / P_n – за логарифмічним законом, компенсувати можливе скорочення смуги пропускання збільшенням потужності сигналу, як правило недоцільно. Ефективнішим є зворотний обмін потужності сигналу на смугу пропускання.

Розглянемо, як залежить пропускна здатність неперервного каналу від величини смуги пропускання. Виразивши середню потужність перешкоди P_n через ширину смуги F і спектральну щільність потужності перешкоди N_0 , формулу (4.9) можна записати так:

$$C = F \log \left(1 + \frac{P_c}{FN_0} \right).$$

При збільшенні F пропускна здатність C спочатку швидко зростає, як зображено на рис. 4.8, а потім асимптотично прагне до межі:

$$C_\infty = \lim_{F \rightarrow \infty} C = \frac{P_c}{N_0} \log e.$$

Останній результат може бути знайдений, якщо врахувати, що $\ln(1 + \alpha) \approx \alpha$ при $\alpha \rightarrow \infty$.

Таким чином, пропускна здатність каналу з нескінченно широкою смугою пропускання не перевищує рівня

$$C_\infty = 1,443 \frac{P_c}{N_0}. \tag{4.10}$$

З цієї формули добре видно взаємозв'язок основних характеристик

каналу зв'язку. Одну і ту ж кількість інформації можна передати по каналах з абсолютно різними значеннями співмножників F , T і D , лише були б однаковими їх добутки.

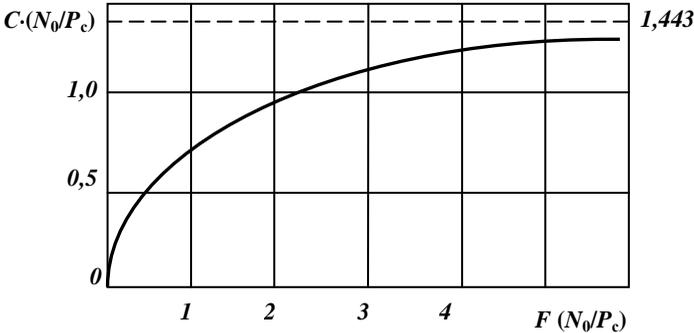


Рис. 4.8. Залежність пропускної здатності гауссовського каналу від його смуги пропускання

Отже, яким би великим не був шум в каналі зв'язку, по ньому можна передавати будь-яку кількість інформації, якщо час передачі необмежений. Якщо ж час обмежений, то для передачі заданої кількості інформації відношення енергії сигналу до спектральної щільності потужності шуму $h_0^2 = P_c T / N_0$ повинне перевищувати деяку порогову величину. Дійсно, при будь-якій смузі F пропускна здатність C не може перевищити граничне значення (4.10).

При цьому $TC < TC_\infty = 1,443(P_c T / N_0)$ і, отже, для передачі одного біта інформації необхідно мати $h_0^2 > 0,693$.

Цікавішими виходять результати обміну (за рахунок відповідного вибору модуляції і кодування) смуги частот на динамічний діапазон D із збереженням незмінної тривалості повідомлення ($T = const$), тобто, як прийнято говорити, при передачі в масштабі часу 1:1. Розширення смуги частот F повідомлення в k разів дозволяє у стільки ж разів зменшити динамічний діапазон D . Необхідне відношення сигнал/перешкода P_c / P_n при цьому зменшується значно сильніше через логарифмічну залежність між D і P_c / P_n . Останнє при заданій інтенсивності перешкод у каналі зв'язку дозволяє зменшити потужність сигналу P_c на вході приймача, тобто зменшити потужність пристрою, що передає, або при тій же потужності передаючого пристрою збільшити дальність радіозв'язку.

Використовується також обмін часу T на динамічний діапазон D (на відношення P_c / P_n). За рахунок збільшення тривалості передачі T повідомлення зменшують необхідне значення D , що призводить до істотного зменшення необхідної потужності пристрою, що передає, або відповідного збільшення дальності зв'язку.

4.3. Методи ефективного кодування інформації у каналах зв'язку

4.3.1. Узгодження джерел інформації з каналами зв'язку

Швидкість передачі інформації залежить від властивостей джерела інформації, каналу зв'язку та перешкод. Для передачі інформації без утрат зі швидкістю рівною пропускній здатності необхідно узгодити джерело повідомлень з каналом зв'язку.

Фізичним об'ємом сигналу V_c називають добуток трьох його фізичних характеристик: тривалості сигналу T_c , ширини спектра F_c і динамічного діапазону рівнів сигналу (по потужності) D_c

$$V_c = T_c F_c D_c ,$$

де $D_c = 10 \lg \frac{P_{max}}{P_{min}}$;

P_{max} – максимальне (пікове) значення потужності сигналу;

P_{min} – мінімальне значення потужності сигналу.

При наявності шумів у каналі допустимий мінімальний рівень потужності P_{min} визначається середньою потужністю цих шумів. Тому можна записати

$$D_c = 10 \lg \frac{P_{max}}{P_{ш}} . \tag{4.11}$$

Відношення середніх потужностей сигналу та шуму $P_c / P_{ш}$ називають відношенням сигнал/шум.

Аналогічно фізичному об'єму сигналу вводять характеристику, яка називається фізичним об'ємом каналу

$$V_k = T_k F_k D_k ,$$

де T_k – час використання каналу;

F_K – смуга частот, що пропускаються каналом;

D_K – динамічний діапазон рівнів, що пропускаються каналом з допустимими помилками.

Для передачі сигналу, що має об'єм V_c , з досить високою якістю необхідно, щоб виконувалась нерівність

$$V_c \leq V_K. \quad (4.12)$$

При цьому необхідно, щоб

$$T_c \leq T_K, F_c \leq F_K, D_c \leq D_K. \quad (4.13)$$

Виконання цих умов означає, що джерело можна вважати повністю узгодженим за фізичними характеристикам з каналом зв'язку.

При невиконанні хоча б однієї з нерівностей (4.13), якщо виконується (4.12), для узгодження повідомлення з каналом необхідне його перетворення за формою.

Таким чином, величина

$$\alpha = \frac{V_K}{V_c}, (0 < \alpha \leq 1)$$

може бути мірою ефективності використання фізичних параметрів каналу.

Приклад 4.5.

Нехай канал зв'язку зі смугою $F_K = 10 \text{ кГц}$ передбачається використовувати на протязі $T_K = 10 \text{ секунд}$. У каналі діє шум з рівномірною спектральною щільністю потужності $G_{ш} = 10^{-4} \text{ мВт/Гц}$. Яка гранична потужність сигналу, що може бути переданий по цьому каналу, якщо фізичний обсяг каналу $V_K = 1\,000\,000$?

Для узгодження джерела повідомлень з каналом зв'язку необхідно, щоб $V_c \leq V_K$ і $D_c \leq D_K$. Так як $V_K = T_K F_K D_K$, то $D_c = \frac{V_K}{T_K F_K}$.

Використавши вираз (4.11), отримуємо

$$D_c = 10 \lg \frac{P_{max}}{P_{ш}} \Rightarrow P_{max} = P_{ш} \cdot 10^{\frac{D_c}{10}}.$$

Підставивши значення, знаходимо:

$$D_c = \frac{V_K}{T_K F_K} = 10 \Rightarrow P_{max} = 10 P_{ш};$$

$$P_{ш} = G_{ш} F_K = 1 \text{ мВт} \Rightarrow P_{max} = 10 \text{ мВт}.$$

4.3.2. Ефективне кодування Шеннона - Фано

Статистичне кодування незалежних символів джерела вперше було запропоноване Шенноном і Фано. Методика побудови коду наступна: символи алфавіту джерела виписуються в порядку спадання ймовірності. Потім вони розділяються на дві групи так, щоб суми ймовірностей в кожній з груп були б, якщо можна, однаковими. Першій групі присвоюємо кодовий символ 0 (або 1), а другий – 1 (або 0). Кожна з одержаних груп, в свою чергу, розбивається на дві підгрупи з однаковою сумарною ймовірністю і знов першій підгрупі присвоюємо символ 0 (або 1), а другий – 1 (або 0) і т.д.

Застосуємо цю методику для розглянутого раніше джерела з нерівноймовірними символами.

Після першого розбиття першій групі, до якої увійшло повідомлення x_1 , як перший кодовий символ присвоюємо 0 , а другий, куди увійшли x_2 , x_3 і x_4 присвоюємо 1 . Далі другу групу розбиваємо на дві рівноймовірні підгрупи і першій присвоюємо символ 0 , а другий 1 . А підгрупу, що залишилася, яка складається з двох повідомлень x_3 і x_4 , знову розбиваємо на дві частини і першій з них присвоюємо 0 , а другий 1 . Підсумкові кодові комбінації мають вигляд: $x_1 = 0$, $x_2 = 10$, $x_3 = 110$, $x_4 = 111$. Приклад кодування Шеннона – Фано зображений на рис. 4.9. При такій процедурі, дійсно, найбільш імовірні повідомлення одержують найкоротші кодові позначення, а найменш імовірні – довгі.

Середня кількість кодових символів \bar{n} , що приходяться на букву повідомлення при такому кодуванні

$$\bar{n} = \sum_{i=1}^M n_i P(x_i) = \sum_{i=1}^4 n_i P(x_i) = 1 \cdot 0,5 + 2 \cdot 0,25 + 3 \cdot 0,125 + 3 \cdot 0,125 = 1,75$$

дорівнює ентропії джерела.

Таким чином, побудований код реалізує граничні результати, вказані теоремою, і в цьому значенні може бути названий оптимальним статистичним кодом.

Якщо ймовірність появи символів джерела не є степенем двійки, то неможливо розбити їх на групи з рівною сумарною ймовірністю. Тоді проводять наближене розбиття, але при цьому одержані результати будуть гіршими. Для поліпшення ефективності коду в цьому випадку необхідно переходити від кодування поодиноких символів до кодування повідомлень, складених з великої кількості символів (блокове або укрупнене кодування).

x_i	$P(x_i)$	Кодування			Код
x_1	0,5	} 1	–	–	1
x_2	0,25	} 0	} 1	–	01
x_3	0,125		} 0	} 1	001
x_4	0,125	} 0	} 0	} 0	000

Рис. 4.9. Метод кодування Шеннона – Фано

Приклад 4.6.

Розглянемо цей принцип на прикладі кодування повідомлень джерела, алфавіт якого складається всього з двох букв x_1 і x_2 з ймовірністю появи $P(x_1) = 0,89$, $P(x_2) = 0,11$. При по буквенному кодуванні на передачу кожної букви потрібен один кодовий символ – або 0 , або 1 , тоді як ентропія джерела дорівнює приблизно $0,5$ біт. При поблочному кодуванні відбувається як би збільшення первинного алфавіту. При кодуванні по дві букви в блоці алфавіт укрупненого джерела матиме вигляд: x_1x_1 , x_1x_2 , x_2x_1 , x_2x_2 . Оскільки букви статистично не зв'язані, ймовірність блоків визначається добутком імовірності складових букв: $P(x_1x_1) = 0,792$, $P(x_1x_2) = P(x_2x_1) = 0,098$, $P(x_2x_2) = 0,012$. Кодові комбінації, одержані за методикою Шеннона – Фано, мають вигляд: $x_1x_1 = 0$, $x_1x_2 = 10$, $x_2x_1 = 110$, $x_2x_2 = 111$. Середня кількість кодових символів на блок $\bar{n} = 1 \cdot 0,792 + 2 \cdot 0,098 + 3 \cdot 0,098 + 3 \cdot 0,012 = 1,318$, а на одну букву дорівнює $0,659$.

Кодування блоків, що містять по три букви, дає ще більший ефект. Кількість кодових символів на блок дорівнює $1,658$, а на одну букву $0,552$, що всього на 11% більше ентропії джерела. Збільшуючи і далі число символів в блоці, можна скільки завгодно наблизитися до теоретичного мінімуму – ентропії джерела.

Збільшення ефективності при статистичному кодуванні шляхом укрупнення блоків не пов'язане з урахуванням все більш далеких міжсимвольних залежностей, оскільки розглянуте джерело має алфавіт з некорельованими символами. Підвищення ефективності визначається лише тим, що розширений набір імовірності, який виходить при укрупненні, дозволяє ділити блоки на підгрупи, сумарна ймовірність яких все менше і менше відрізняється одна від одної. Це і дає можливість скільки завгодно близько підійти до межі. Проте, укрупнення – це універсальний спосіб зменшення

надмірності не тільки при нерівномірності символів, але і при їх взаємній залежності. Дійсно, якщо символи джерела об'єднати в довгі повідомлення (блоки), то від символів попереднього блоку залежать тільки декілька символів подальшого блоку і ця залежність зменшуватиметься з віддаленням символу від початку блоку. Чим більше символів в блоці, тим більше буде символів, які не залежать від попередніх блоків. Відбувається декореляція символів, тобто усувається їх взаємозалежність, і при дуже великій довжині блоку укрупнений алфавіт складатиметься з незалежних один від одного повідомлень.

Наочно значення укрупнення може бути пояснено на прикладі буквенного тексту. Якщо ймовірнісні зв'язки між буквами в будь-якій мові відносно сильні, то між словами вони менші, ще менші між фразами, абзацами. Тому, застосовуючи кодування слів, фраз, абзаців, можна достатньо повно усунути надмірність, обумовлену ймовірнісними зв'язками.

Блокове кодування дозволяє побудувати оптимальний код для будь-якого джерела. Це забезпечує збільшення швидкості передачі, але його використання призводить до запізнення отримання інформації. На передавальній стороні необхідно спочатку накопичити весь блок, а потім здійснити його кодування, аналогічно на приймальній стороні декодування також може бути здійснене тільки після накопичення всього блока.

4.3.3. Ефективне кодування Хаффмана

Іншим найпоширенішим алгоритмом, на основі якого будуються нерівномірні коди, є алгоритм Хаффмана, що дозволяє будувати нерівномірний код, який може давати найкоротшу середню довжину коду для алфавіту, що використовують.

Процес кодування починається з переліку вхідних символів разом з їх ймовірністю (або частотами появи) в порядку спадання. Кожній гілці дерева присвоюється її ваговий коефіцієнт, рівний ймовірності цієї гілки. Два входи з найнижчою ймовірністю об'єднуються, щоб утворити нову гілку з їх загальною ймовірністю. Після кожного об'єднання гілки переупорядковуються, при цьому нова гілка ставиться зверху гілок з рівною ймовірністю. Приклад кодування Хаффмана зображений на рис. 4.10.

Після формування дерева, щоб розрізнити дві гілки кожній гілці присвоюється символ *1* або *0*. Для кожного символу вхідного алфавіту записується відповідний йому код за напрямом гілки від її кінця. Для цього прикладу середня довжина коду дорівнює 2,4 біт на символ. Для порівняння рівномірний код повинен був мати 3 символи.

Ефективність кодування Хаффмана зростає зі збільшенням кількості

символів вхідного алфавіту. Розглянемо приклад, зображений на рис. 4.11.

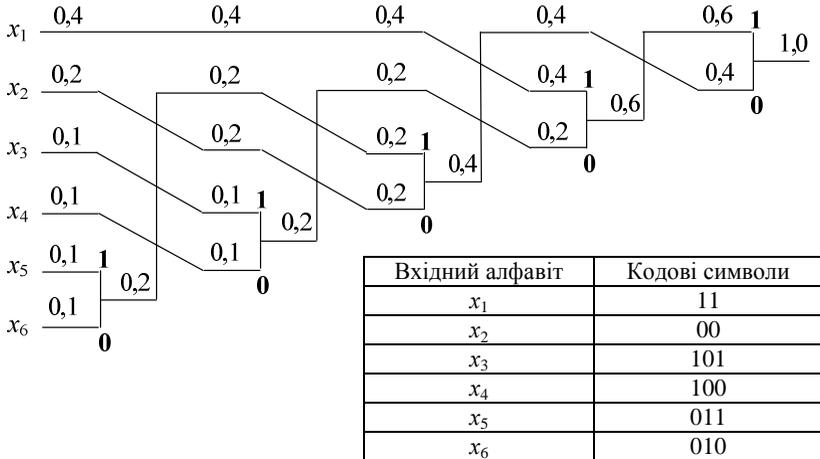


Рис. 4.10. Дерево кодування Хаффмана

Для цього прикладу середня довжина коду становить 1 біт на символ і дорівнює довжині рівномірного коду. Щоб поліпшити ефективність кодування слід укрупнити алфавіт джерела шляхом вибору двох символів, ймовірність яких буде дорівнювати добутку імовірностей символів, що зображено на рис. 4.12.

Для цього прикладу середня довжина коду дорівнює 1,56 біт на символ. Для порівняння рівномірний код повинен був мати 2 символи.

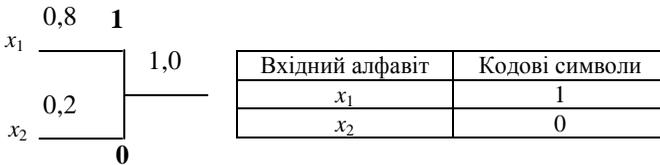


Рис. 4.11. Кодування Хаффмана без укрупнення символів

Існують такі методи кодування, що забезпечують усунення або значне зменшення надмірності, пов'язаної з взаємозалежністю близько розташованих елементарних повідомлень.

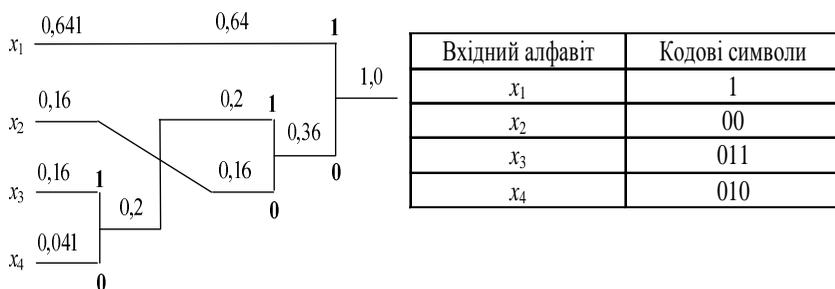


Рис. 4.12. Кодування Хаффмана з укрупненням символів

Методи ефективного кодування, що дозволяють записувати повідомлення таким числом двійкових символів, яке трохи відрізняється від ентропії джерел повідомлень, є одним з основних розділів сучасної теорії кодування. Останнє обумовлене великим прикладним значенням ефективного кодування, особливо в космічних лініях зв'язку. Ефективне кодування дозволяє записати і передати повідомлення за допомогою меншого числа двійкових символів. Разом з тим не завжди потрібно прагнути до повного усунення надмірності. Деяка надмірність, особливо якщо вона відповідним чином введена в повідомлення, корисна для підвищення перешкодостійкості зв'язку.

4.4. Контрольні питання

1. Дайте визначення та поясніть класифікацію каналів зв'язку.
2. Поясніть модель дискретного каналу зв'язку.
3. Поясніть модель неперервного каналу зв'язку.
4. Поясніть модель каналів зв'язку зі змінними параметрами.
5. Визначте кількість інформації, що передається по неперервному каналу зв'язку.
6. Визначте пропускну здатність неперервного каналу зв'язку.
7. Визначте кількість інформації, що передається по дискретному каналу зв'язку.
8. Визначте пропускну здатність дискретного каналу зв'язку.
9. Визначте пропускну здатність двійкового симетричного каналу.
10. Поясніть суть узгодження джерел повідомлень з каналом зв'язку.
11. Поясніть призначення методів ефективного кодування інформації.
12. Поясніть суть ефективного кодування Шеннона – Фано.
13. Поясніть суть ефективного кодування Хаффмана.

Розділ 5

Перешкодостійке кодування даних у системах обробки інформації та управління

Розглянуто основні поняття та визначення перешкодостійкого кодування, класифікацію перешкодостійких кодів, основні принципи та характеристики перешкодостійкого кодування, лінійні групові перешкодостійкі коди, лінійні циклічні перешкодостійкі коди, згортувальні перешкодостійкі коди, підвищення достовірності передачі та обробки інформації в COIU з безнадмірним кодуванням. Також наведено контрольні питання.

5.1. Основні поняття та визначення перешкодостійкого кодування. Класифікація перешкодостійких кодів

Одним з основних показників якості передачі інформації по каналах зв'язку (зараз ми говоримо про передачу дискретної інформації) є, як ми вже відзначали раніше, **достовірність**. Вона може бути охарактеризована ймовірністю помилкового декодування (приймання) кодової комбінації відповідної окремому повідомленню первинного коду.

Вимоги до достовірності передачі дуже різноманітні і залежать від призначення системи передачі інформації. Вважається, що ймовірність помилки на кодову комбінацію не повинна перевищувати 10^{-6} ... 10^{-9} . В особливо відповідальних системах існують ще жорсткіші вимоги.

Ймовірність помилкового прийняття символу в каналах, використовуваних для передачі дискретної інформації, лежить в межах 10^{-3} ... 10^{-5} .

Всі існуючі способи підвищення достовірності передачі можна розділити на три групи:

- заходи експлуатаційного і профілактичного характеру (зменшення числа джерел перешкод, поліпшення стабільності роботи основних вузлів, резервування тощо);
- зменшення ймовірності помилкового прийняття за рахунок підвищення відношення сигнал/перешкода (вибір методів модуляції, приймання, тривалості, спектрів, потужності);

- використання перешкодостійких кодів.

Перешкодостійке кодування є одним з найбільш ефективних засобів збільшення достовірності зв'язку.

До теперішнього часу розроблена велика кількість перешкодостійких кодів. Принципи їх побудови надзвичайно різноманітні, проте, за своєю структурою всі перешкодостійкі коди діляться на дві великі групи: блокові і неперервні. При **блоковому кодуванні** кожна буква повідомлення (або послідовність букв) перетворюється в певну послідовність (блок) кодових символів, що називається **кодовою комбінацією**. При **неперервному кодуванні** кодові символи визначаються всією послідовністю (або значною частиною послідовності) елементів повідомлення (інформаційних символів) і не можуть бути розділені на окремі відособлені кодові комбінації.

На практиці найчастіше використовуються блокові коди, що в свою чергу діляться на рівномірні і нерівномірні. У **рівномірних кодах** всі кодові комбінації містять однакову кількість символів і передаються по каналу елементами сигналу незмінної тривалості. Це значно спрощує техніку передачі і приймання повідомлень. У **нерівномірних кодах** кількість символів в комбінаціях, відповідних різним повідомленням, різне. Вони не знайшли широкого практичного застосування з причини складності техніки їх формування і обробки.

Рівномірні коди діляться також на роздільні і нероздільні. У **роздільних кодах** функції окремих символів кодової комбінації чітко розмежовуються на інформаційні і контрольні (перевірочні). Повідомлення, що передаються, визначаються k інформаційними символами. Надмірні (контрольні, перевірочні) r символи доповнюють кодову комбінацію до $n = k + r$ символів, через що такі блокові коди позначають як (n, k) коди.

Найбільш численний клас роздільних кодів становлять **лінійні коди**. Основна їхня особливість полягає в тому, що контрольні символи утворюються як лінійні комбінації інформаційних символів. У свою чергу, лінійні коди можуть бути розбиті на два підкласи: систематичні й несистематичні. **Систематичні коди**, у яких значення перевірочних символів визначаються в результаті проведення лінійних операцій над інформаційними символами. Виявлення і виправлення помилок здійснюється для таких кодів формалізовано, за чіткими правилами, що дозволяє автоматизувати процес передачі повідомлень та зменшити складність апаратури. Всі двійкові систематичні коди є груповими. Останні характеризуються приналежністю кодових комбінацій до групи, що володіє такою властивістю, що сума по модулі дві будь-який пари комбінацій знову дає комбінацію, що належить до цієї групи.

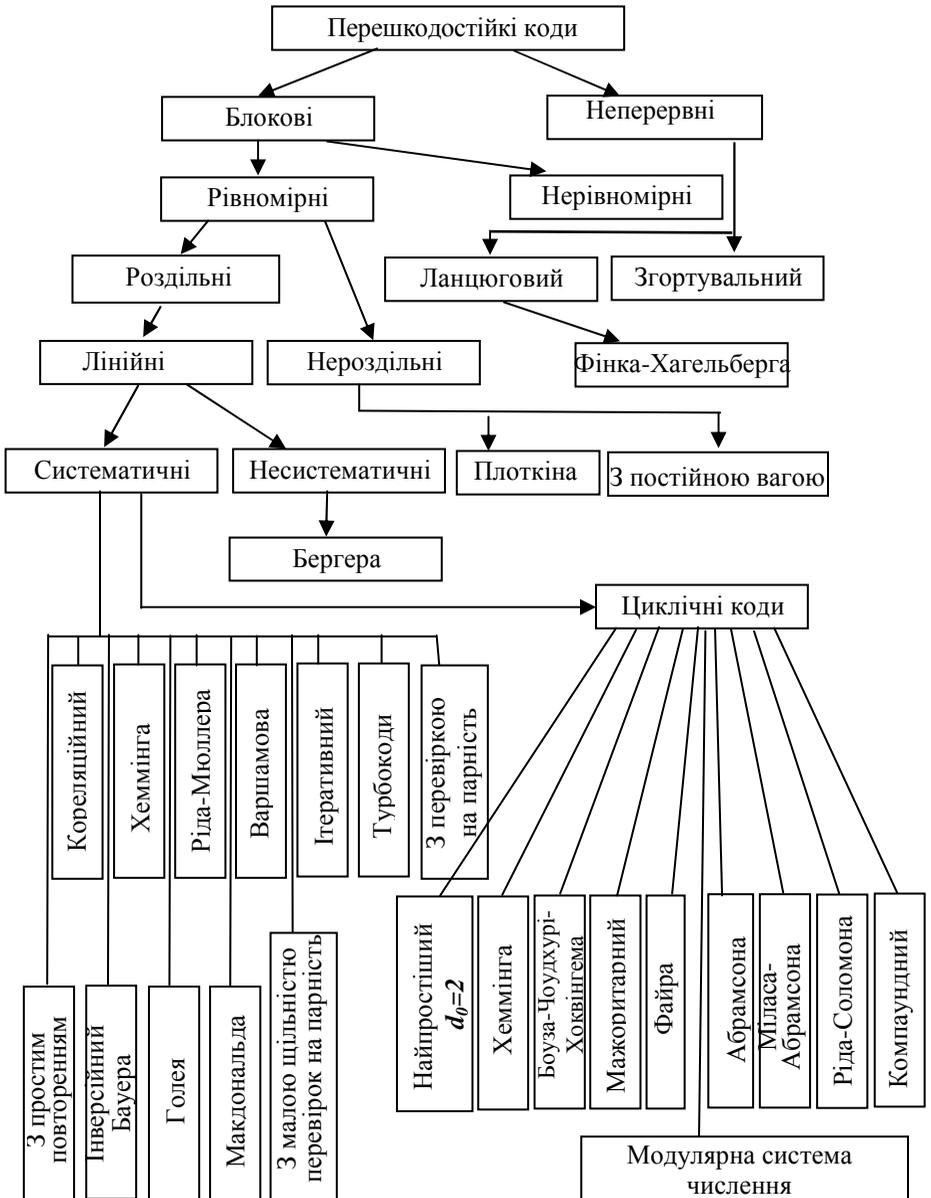


Рис. 5.1. Загальна класифікація перешкодостійких кодів

Лінійні коди, які не можуть бути віднесені до підкласу систематичних, називаються несистематичними.

Найбільше розповсюдження серед блокових кодів знайшли коди з перевіркою на парність, з повторенням символів, рівноважні коди, коди Хеммінга та циклічні коди. До останнього класу належать коди Боуза – Чоудхурі – Хоквінгема (БЧХ) і коди Ріда – Соломона (РС), що набули найбільшого поширення в техніці зв'язку.

Загальна класифікація перешкодостійких кодів представлена на рис. 5.1.

5.2. Основні принципи та характеристики перешкодостійкого кодування

Розглянемо загальну постановку задачі перешкодостійкого кодування повідомлень. Від джерела інформації поступає послідовність елементарних повідомлень b_i . Кодування полягає у тому, що послідовність символів джерела замінюється послідовністю m -ічних кодових символів (надалі розглядатимемо тільки двійкові коди, для яких $m = 2$). Вказане перетворення є взаємооднозначним, що і дозволяє здійснити в приймачі декодування, тобто відновити повідомлення за прийнятою кодовою комбінацією.

В результаті дії перешкоди деякі кодові символи в приймачі виділяються спотвореними – одиничні елементи комбінації сприймаються як нульові і навпаки. Може бути передбачений і режим стирання символів, коли рішення про приймання деяких з них не може бути виконано з необхідною надійністю (впевненістю).

Мета перешкодостійкого кодування повідомлень – перетворення повідомлень b_i , $i = 1, 2, \dots, m$ в послідовність кодових символів b_j , $j = 1, 2, \dots, n$, яка має властивість виявлення присутності в ній помилок або виявлення і виправлення цих помилок.

Відразу відзначимо, що не існує кодів кінцевої довжини, які дозволяють знайти і, тим більше, виправити всі можливі помилки. Можна побудувати лише коди, що знаходять або виправляють деяку кількість помилок певного вигляду (звично найімовірніших або найбільш небезпечних).

Ця мета може бути досягнута тільки введенням надмірності, тобто збільшенням числа кодових символів в послідовності, що передається, відносно символів, що забезпечують однозначне подання повідомлень, що передаються (інформаційних символів). Наявність додаткових (надмірних) символів дозволяє накласти на послідовності символів, що передаються

(кодові комбінації), додаткові зв'язки (умови) між ними, перевірка яких на приймальній стороні дає можливість знайти і виправити помилки. Вся сукупність можливих кодових комбінацій в цьому випадку називається перешкодостійким (коректуючим або надмірним) кодом.

Ця мета може бути досягнута тільки введенням надмірності, тобто збільшенням числа кодових символів в послідовності, що передається, відносно символів, що забезпечують однозначне подання повідомлень, що передаються (інформаційних символів). Наявність додаткових (надмірних) символів дозволяє накласти на послідовності символів, що передаються (кодові комбінації), додаткові зв'язки (умови) між ними, перевірка яких на приймальній стороні дає можливість знайти і виправити помилки. Вся сукупність можливих кодових комбінацій в цьому випадку називається перешкодостійким (коректуючим або надмірним) кодом.

Отже, здатність коду знаходити і виправляти помилки обумовлена наявністю надмірних символів. Розглянемо, яким же чином їх введення в кодові комбінації рівномірного блокового коду дозволяє підвищити достовірність передачі повідомлень.

Розглянемо множину n -розрядних комбінацій блокового рівномірного коду. Для двійкових кодів всього можна побудувати 2^n різних комбінацій. У звичайному, некоректуючому, коді розрядність кодової комбінації n вибирається так, щоб кількість комбінацій була мінімально необхідна для подання всіх переданих повідомлень

$$N = 2^n \geq K \quad (5.1)$$

(практично в цьому випадку кодові комбінації – це двійкове подання номерів переданих повідомлень). При цьому всі комбінації коду використовуються при передачі (при записі рівняння (5.1)).

Перешкодостійкі коди будуються так, що кількість можливих кодових комбінацій N істотно перевищує кількість кодованих повідомлень. При цьому частина кодових комбінацій, які називаються дозволеними, використовується для кодування. Їх кількість дорівнює $N_{\text{д}} = K = 2^k$. Інша частина комбінацій для кодування не використовується, і вони називаються забороненими. Кількість заборонених комбінацій дорівнює 2^r або 2^{n-k} .

На приймальній стороні відомо, які з комбінацій є дозволеними, а які забороненими. Тому, якщо передана комбінація в результаті помилки перетвориться в деяку заборонену комбінацію, то така помилка буде знайдена або виправлена. Ясно, що помилки, які призводять до утворення іншої дозволеної комбінації не можуть бути виявленими або виправленими. Проте, при розумному підході до побудови коду, може досягатися дуже

мала імовірність не знайденої помилки. При цьому очевидно, що ймовірність трансформації однієї дозволеної комбінації в іншу дозволена тим менша, чим більше комбінації відрізняються одна від одної. Відмінність між комбінаціями b_i і b_j рівномірного коду прийнято характеризувати відстанню Хеммінга d_{ij} , яка дорівнює кількості позицій з неспівпадаючими символами (вазі вектора $b = b_i \oplus b_j - w_{ij}$). Кількість відмінних від 0 символів в кодовому слові b_i називається його *вагою* w_i . Наприклад, кодові комбінації **1100101** і **1011100** відрізняються символами в чотирьох розрядах, тому $b = 0111001$ і відстань Хеммінга дорівнює чотирьом.

Для будь-якого коду $1 \leq d_{ij} \leq n$. Мінімальна відстань між дозволеними комбінаціями в цьому коді називається *мінімальною кодовою відстанню* і позначається d_{min} .

Таким чином, якщо код має кодову відстань d_{min} , то це означає, що дозволені комбінації цього коду відрізняються одна від одної не менше ніж в d_{min} символах і тільки поява d_{min} і більше помилок в прийнятій комбінації можуть перевести її в іншу дозволена комбінація.

З другого боку, якщо кількість помилок в комбінації буде менша ніж d_{min} , то стає зрозумілим, що така комбінація помилок призведе до забороненої комбінації.

У цілому в процесі передачі інформації можна розрізнати три ситуації: спотворення (помилки) відсутні, спотворення виявляються (прийнята заборонена комбінація) і спотворення не виявляються – одна дозволена комбінація переходить в іншу дозволена. Говорять, що в каналі відбулася помилка кратності t , якщо в кодовій комбінації прийнято помилково t символів. В результаті можна дійти висновку, що максимальна кількість помилок, яка достовірно виявляється в комбінації перешкодостійкого коду, пов'язана з кодовою відстанню наступним співвідношенням:

$$t_{zn} = d_{min} - 1.$$

При $d_{min} \leq t_{zn} + 1$ або при $t \geq t_{zn}$ прийнята кодова комбінація може виявитися дозволеною і помилка не буде знайдена. Але і при $t \geq t_{zn}$ можливі ситуації, коли комбінація виявляється забороненою, тобто частково виявлятимуться і помилки кратності більшої, ніж t_{zn} .

Як приклад, розглянемо властивості трирозрядного коду, що до знаходження помилок. При $d_{min} = 1$ дозволені комбінації – це все комбінації коду **000**, **001**, **010**, **011**, **100**, **101**, **110**, **111**. Будь-яка поодинокі помилка

трансформує кожну з цих комбінацій в іншу дозволена. Таким чином достовірне виявлення помилок неможливе.

При $d_{min} = 2$ підмножина дозволених комбінацій може бути створена за принципом парності в них числа одиниць, тобто *000, 011, 101, 110*. До заборонених комбінацій віднесемо решту комбінацій: *001, 010, 100, 111*. Жодна із заборонених кодових комбінацій при поодинокій помилці не переходить в іншу дозволена комбінацію, тобто при $d_{min} = 2$ код достовірно знаходить всі поодинокі помилки. Що стосується помилок вищої кратності, то частина з них виявляється, а частина ні. Так виявляються всі триразові помилки, проте двократні помилки переводять одну дозволена кодову комбінацію в іншу і не можуть бути знайдені. Збільшення кодової відстані до $d_{min} = 3$ дозволяє використати для передачі тільки дві кодові комбінації *000* і *111* або *001* і *110* і тощо. Але в цьому випадку і двократна помилка не може перевести одну дозволена кодову комбінацію в іншу.

Модель трирозрядного коду можна використати і для пояснення принципів використання надмірності для виправлення помилок. Основою цього є припущення про те, що чим більша кратність помилки, тим вона менше ймовірна. Це припущення добре узгоджується з біноміальною моделлю помилок в дискретному каналі зв'язку. В цьому випадку при помилках найбільшу ймовірність матимуть помилкові комбінації, віддалені від переданої дозволена на відстань $d = 1$, менш ймовірними будуть переходи в комбінації, віддалені від переданої на відстань $d = 2$.

Як результат, в процесі приймання – передачі кодових комбінацій по каналу зв'язку з помилками, кожна з дозволених (переданих) комбінацій трансформується в деяку множину прийнятих кодових комбінацій, локалізованих навколо переданої дозволена кодової комбінації (якщо її відображати точкою відповідного n -мірного простору, як зображено на рис. 5.1).

Збільшуючи відстань між центрами цих областей в n -мірному просторі (крапками, що відповідні дозволеним кодовим комбінаціям), можна реалізувати процедуру виправлення помилок заданої кратності, якщо ухвалювати рішення про декодування тієї дозволена комбінації, відстань якої від прийнятої (забороненої) кодової комбінації виявляється мінімальною (декодування за найменшою відстанню). Цей метод декодування є оптимальним для симетричного каналу (для інших може бути і не оптимальним).

Тепер легко зрозуміти, що максимальна кількість помилок, які достовірно виправляються пов'язана з кодовою відстанню такими нерівностями:

$$\text{➤ якщо } d_{min} \text{ – непарне, то } t_{вип} \leq \frac{d_{min} - 1}{2};$$

➤ якщо d_{min} – парне, то $t_{випр} \leq \frac{d_{min}}{2} - 1$.

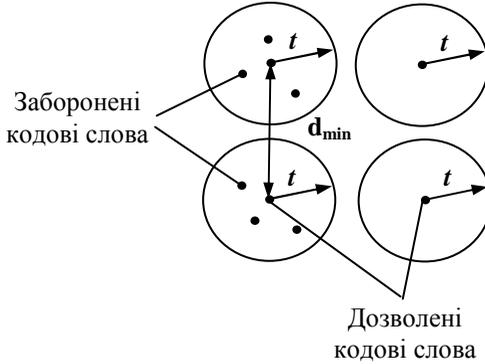


Рис. 5.1 Сфери декодування

Дійсно, для виправлення помилок кратності t необхідно включити в кожному з вказаних вище підмножин всі заборонені кодові комбінації, віддалені від дозволеної на відстань $d = t$. Для того, щоб сусідні підмножини не перетиналися, відстань між найближчими дозволеними комбінаціями повинна бути не менше $2t + 1$.

Таким чином, код має властивість знаходити і виправляти t -кратні помилки, якщо виконується умова:

$$d_{min} \geq 2t + 1.$$

Звернемося знов до трирозрядного коду. За дозволені комбінації приймемо 000 і 111 . Тоді дозволеним комбінації 000 відповідає підмножина заборонених комбінацій $001, 010, 100$, що утворюються за рахунок виникнення одноразової помилки. Подібним же чином дозволеним комбінації 111 відповідає підмножина заборонених комбінацій $110, 101, 011$.

При одноразовому спотворенні будь-якої з двох дозволених комбінацій, комбінація, що приймається, не вийде за межі “своєї” підмножини і помилка буде виправлена. Що стосується подвійних помилок, то вони виявляються, але при їх виправленні ухвалюються невірні рішення. Потрійні помилки не виявляються взагалі.

Перешкодостійке кодування можна застосовувати також в дискретних каналах із стиранням. Якщо в прийнятій комбінації спотворених символів немає, а є тільки t_{cm} стертих (непізнаних) символів, то при виконанні умови $t_{cm} \leq d_{min} - 1$ ці символи можуть бути відновлені при

декодуванні за мінімумом відстані. Один і той же код може декодуватися з виправленням помилок і стирань. У загальному випадку код з відстанню d_{min} виправляє будь-які $t \leq t_{cm}$ стирань і будь-які $t \leq t_{sun}$ помилок, якщо $d_{min} \geq 2t_{sun} + t_{cm} + 1$.

Крім поєднань помилок і стирань, що повністю виправляються і знаходяться, кратність яких визначається кодовою відстанню, коди з корекцією часто виправляють або знаходять і багато інших поєднань помилок великої кратності.

Кодова відстань коду d_{min} є основним показником його здатності, щодо знаходження і виправлення помилок. Збільшуючи довжину коду n і зберігаючи кількість дозволених кодових комбінацій, можна набути скільки завгодно велике значення d_{min} . Але зі збільшенням n зменшується швидкість передачі повідомлень. Якщо довжина коду n задана, то будь-яке значення $d_{min} \leq n$ можна одержати, зменшуючи кількість дозволених комбінацій, але при цьому зменшується і кількість повідомлень, які можна закодувати. Отже, задачу пошуку найкращого коду необхідно формулювати так: при заданих n і N_0 знайти код, який має більше значення d_{min} .

Характеристикою перешкодостійкого коду, яка вказує ступінь подовження кодової комбінації, є надмірність. Відносна надмірність може бути записана співвідношенням

$$\eta_k = \frac{n - k}{n} = 1 - \frac{\log K}{n \log m}.$$

Другою характеристикою є відносна швидкість коду

$$R_n = \frac{\log K}{n \log m} = \frac{k}{n} = 1 - \eta_k.$$

Коди, що забезпечують задану коректуючу здатність при мінімальній надмірності, називаються оптимальними. Але загального методу пошуку оптимальних кодів в наш час не існує.

Кодова відстань d_{min} повністю характеризує стійкість коду щодо заданого рівня перешкод. Проте, в реальних умовах кількість спотворених символів в кодовій комбінації може з певною ймовірністю перевищити t . В цьому випадку перешкодостійкість коду зручно описувати статистичними показниками. До їх числа належать ймовірність правильного прийняття P_{np} , ймовірність помилки $P_{ном}$. Цю ймовірність можна визначити, знаючи структуру коду і статистику перешкод. Знайдемо P_{np} та $P_{ном}$ для каналу з

незалежними помилками.

Ймовірність помилкового декодування кодових комбінацій. При передачі інформації безнадмірним кодом в системах без зворотного зв'язку використовуються всі кодові комбінації. При цьому помилкове прийняття хоча б одного кодового символу призводить до переходу однієї дозволеної кодової комбінації в іншу. Отже, умовою правильного прийняття кодової комбінації є правильне прийняття кожного символу. Знаючи ймовірність помилкового прийняття символу p_0 , можна знайти ймовірність його правильного прийняття $p_{np} = 1 - p_0$. Якщо спотворення окремих символів незалежні, то ймовірність правильного прийняття всієї кодової комбінації дорівнює

$$P_{np} = (1 - p_0)^n \approx np_0.$$

Таким чином, у системах з безнадмірним кодуванням ймовірність помилкового прийняття кодової комбінації приблизно в n разів більша ймовірності помилкового прийняття символу.

Оцінимо ймовірність спотворення кодової комбінації перешкодостійкого коду з $n = k + r$ символів. Оскільки такий код дозволяє виявляти або виправляти частину помилок, то, мабуть, не всі помилки при прийманні окремих символів призводять до неправильної реєстрації кодової комбінації. Нехай кратність помилки, що виявляється або виправляється перешкодостійким кодом, дорівнює t . Тоді ймовірність правильної реєстрації комбінацій перешкодостійкого коду дорівнює ймовірності того, що комбінація з n елементів містить не більше t помилок. Позначимо ймовірність помилкового приймання символу перешкодостійкого коду як p_0 . Ймовірність того, що в кодовій комбінації на i позиціях відбулася помилка, а на $n - i$ позиціях помилок немає, дорівнює $p_0^i (1 - p_0)^{n-i}$. У кодовій комбінації помилка на i позиціях може відбутися у всіляких сполученнях цих позицій. Кількість таких сполучень дорівнює

$$C_n^i = \frac{n!}{i!(n-i)!}.$$

Отже, ймовірність того, що в кодовій комбінації з n символів з'явиться помилка кратністю i (у будь-якому сполученні позицій), визначається як

$$P_i = C_n^i p_0^i (1 - p_0)^{n-i}.$$

Ймовірність того, що комбінація з n елементів містить не більше t помилок, дорівнює

$$P_t(i \leq t) = \sum_{i=0}^t C_n^i p_0 (1 - p_0)^{n-i}.$$

Цей вираз можна розглядати як ймовірність виявлення або виправлення помилок, тому що за умовою було прийнято, що всі помилки кратності t та менше можуть бути виявлені або виправлені.

Якщо при передачі виникнуть помилки кратності $t+1$ і вище, то такі помилки вже не будуть виявлені або виправлені. Отже, повну ймовірність не виявлення або не виправлення помилок, що і визначає ймовірність спотворення кодової комбінації перешкодостійкого коду, можна знайти за формулою

$$P_{\text{ном}} = 1 - \sum_{i=0}^t C_n^i p_0^i (1 - p_0)^{n-i} = \sum_{j=t+1}^n C_n^j p_0^j (1 - p_0)^{n-j}.$$

Конкретизуємо останній вираз з урахуванням способу декодування. Ввівши в нього параметр d_{\min} і взявши до уваги зв'язок між кодовою відстанню та кількістю помилок, що виявляються або виправляються, отримаємо наступні оцінки ймовірності помилкового декодування при виправленні помилок $P_{\text{ном}}^{\text{випр}}$ і ймовірності невиявленої помилки при виявленні помилок $P_{\text{ном}}^{\text{виявл}}$

$$P_{\text{ном}}^{\text{випр}} \leq 1 - \sum_{i=0}^{(d_{\min}-1)/2} C_n^i p_0^i (1 - p_0)^{n-i};$$

$$P_{\text{ном}}^{\text{виявл}} \leq 1 - \sum_{i=0}^{d_{\min}-1} C_n^i p_0^i (1 - p_0)^{n-i}.$$

Необхідно відзначити, що отримані формули справедливі для того випадку, коли розглянутий код виправляє (або виявляє) всі помилки – однократні, двократні і так далі до t -кратних включно. Всі інші помилки, починаючи з кратності $t+1$ і вище, цей код не виправляє (не виявляє). Більшість реальних кодів виправляють (або виявляють) і частину помилок більш високої кратності, ніж t . При розрахунку коригуючих характеристик конкретних кодів цю обставину необхідно враховувати.

Порівнюючи ймовірності помилкового приймання кодових комбінацій перешкодостійкого коду з ймовірністю помилкового приймання безнадмірної кодової комбінації, можна встановити, при яких умовах застосування перешкодостійкого коду можна підвищити перешкодостійкість. Ясно, що таке порівняння повинне відбуватися при деяких однакових умовах. Найчастіше порівняння за перешкодостійкості систем зв'язку, що ви-

користують різні коди, здійснюється при однаковій швидкості передачі інформації. При цьому час, що відводиться на передачу комбінацій первинного й перешкодостійкого кодів, повинен бути однаковим.

Отже, тривалість елементарних сигналів при перешкодостійкому кодуванні буде меншою тривалості елементарних сигналів при безнадмірному кодуванні. Скорочення тривалості сигналів при заданій середній потужності зменшує їхню енергію, що призводить до збільшення ймовірності помилкового приймання символу перешкодостійкого коду. В цих умовах застосування перешкодостійкого коду доцільно лише в тому випадку, якщо підвищення перешкодостійкості за рахунок виявлення або виправлення помилок перекиє її зниження за рахунок збільшення p_0 .

Аналіз отриманих виразів показує, що ефективність перешкодостійких кодів зростає зі збільшенням достовірності прийняття окремих символів. При низькій же достовірності прийняття символів використання перешкодостійких кодів може призвести навіть до негативних наслідків, тому що переважним може виявитися збільшення ймовірності помилкового прийняття елементарних сигналів із-за зменшення їхньої енергії при збільшенні надмірності.

Остання обставина – зменшення енергії елементарного сигналу при збільшенні коригуючих можливостей кодів, безумовно знижує ефективність перешкодостійкого кодування. Однак, перешкодостійкі коди вигідно відрізняються від безнадмірних здатністю усувати будь-які помилки, якщо їхня кількість в інтервалі тривалості кодової комбінації не перевищує виправляючої здатності перешкодостійкого коду.

Розглянуті вище загальні принципи перешкодостійкого кодування показують, що процес виявлення і виправлення помилок може бути просто реалізований шляхом порівняння прийнятої комбінації зі всіма дозволеними. Незбіг прийнятої комбінації ні з однією з дозволених свідчить про наявність помилок. Виправлення помилок зводиться до пошуку комбінації, найближчої до прийнятої дозвільної комбінації.

Проте така процедура навіть при помірних значеннях n вимагає пам'яті з об'ємом, який не завжди може бути реалізований (складність пропорційна 2^n).

Основний напрям розробки теорії перешкодостійкого кодування полягає у пошуку таких кодів, для яких відбір різних кодових комбінацій, виявлення і виправлення помилок здійснювалися б не шляхом перебору, а за допомогою достатньо простих регулярних правил, які можуть бути реалізовані технічно з невеликими (мінімальними) апаратними витратами.

5.3. Лінійні групові перешкодостійкі коди

Систематичні лінійні коди будують таким чином. Спочатку розглядається безнадмірний код довжиною k , що є множиною всіх k -ічних послідовностей двійкових символів, які називаються інформаційними. Потім до кожної з цих послідовностей, за визначенням для коду правилом приписуються $r = n - k$ перевірочних символів. Для лінійних кодів ці перевірочні символи отримують в результаті лінійних операцій над інформаційними символами.

Умовимося, що інформаційні символи розташовуються на перших k , а перевірочні на останніх $r = n - k$ позиціях кодової комбінації. Інформаційні символи будемо позначати як b_i , а перевірочні як β_j , де $i = 1, 2, \dots, k$, $j = 1, 2, \dots, r$. Тоді l -та комбінація перешкодостійкого коду може бути записана у вигляді

$$B_l = b_{l1} b_{l2} \dots b_{lk} \beta_{l1} \beta_{l2} \dots \beta_{lr}.$$

Для лінійних групових кодів може виконуватися умова, що лінійна операція над будь-якими двома і більше дозволеними кодовими комбінаціями приводить до нової комбінації, що також належить до числа дозволених. Як лінійна групова операція використовується складання за модулем 2. У цьому випадку говорять, що дозвалені кодові комбінації систематичного лінійного коду утворюють групу. Звідси йде і назва цих кодів.

Очевидно, що в будь-який груповий код входить і нульова комбінація, а тому кодова відстань групового коду дорівнює мінімальній вазі ненульових комбінацій.

Побудова конкретного перешкодостійкого коду здійснюється, виходячи з необхідного об'єму коду і статистичних даних про кратність найімовірніших помилок у каналі зв'язку, що використовується. Об'єм коду визначається кількістю переданих повідомлень (кількістю інформаційних розрядів k звичайного безнадмірного коду), а кількість належних виправленню помилок визначає кількість надмірних (контрольних) розрядів (символів).

Методику визначення кількості контрольних символів розглянемо на прикладі побудови кодів, що виправляють поодинокі помилки.

Якщо перешкодостійкий код має довжину $n = k + r$, то кількість поодиноких всіляких помилок дорівнює n . Для кодів, що виправляють помилки, знання тільки факту виникнення помилки є недостатнім. Для того, щоб виправити помилку необхідно знати ще і місце, де вона відбулася. Для цього контрольні символи повинні дозволяти виконати перевірки, за до-

помогою яких можна було б визначити місце помилки. Ці контрольні числа називаються пізнавачами помилок або *синдромами*. Тому кількість контрольних символів повинна бути такою, щоб кількість сформованих за їх допомогою синдромів була не меншою кількості можливих помилок. Отже, для виправлення поодиноких помилок необхідна кількість перевірочних символів повинна задовольняти умові

$$2^r - 1 \geq C_n^1 = n$$

і дорівнювати

$$r = \lfloor \log_2(n + 1) \rfloor. \tag{5.2}$$

Знак $\lfloor \]$ тут означає, що береться округлене значення до найближчого більшого цілого числа. Розрахунки, виконані за цими співвідношеннями для кодів з $d_{min} = 3$, зведені в табл. 5.1.

Таблиця 5.1

Результати розрахунків для лінійних групових кодів

<i>n</i>	<i>k</i>	<i>r</i>
3	1	2
4	1	3
5	2	3
6	3	3
7	4	3
8	4	4
9	5	4
10	6	4
11	7	4
12	8	4
13	9	4
14	10	4
15	11	4

Формулу (5.2) зручно використовувати, якщо відома повна довжина

коду n . Якщо ж відома кількість інформаційних символів k , то розрахунки ведуться за емпіричною формулою

$$r = \lfloor \log_2((k+1) + \lfloor \log_2(k+1) \rfloor) \rfloor.$$

Найбільш економічними з погляду мінімізації надмірних символів при максимумі інформаційних символів є коди, для яких $\log_2(n+1)$ виражається цілим числом, наприклад коди (3,1); (7,4); (15,11); (31,26); (63,57) і т.д. Надмірність цих кодів повністю витрачається на виправлення всіх однократних помилок. Ніяка помилка вищої кратності не може бути виправлена.

Коди з іншим розподілом інформаційних і контрольних символів, наприклад коди (8,4), (9,4) можуть виправляти всі поодинокі помилки і частину подвійних.

Код, що виправляє всі помилки кратності $t \leq t_{\text{вун}}$ і не виправляє жодного поєднання помилок вищої кратності $t = t_{\text{вун}} + 1$, називається **досконалим**. Код, що виправляє всі поєднання помилок $t \leq t_{\text{вун}} + 1$, але не виправляє жодного поєднання помилок вищої кратності $t \geq t_{\text{вун}} + 1$, називається **квазідосконалим**.

Якщо необхідно виправляти не тільки поодинокі помилки, а і всі подвійні незалежні помилки, то кількість перевірочних символів визначається за співвідношенням

$$2^r - 1 \geq C_n^1 + C_n^2.$$

У загальному випадку для виправлення всіх незалежних помилок, до кратності t включно, кількість перевірочних символів визначається як

$$2^r - 1 \geq C_n^1 + C_n^2 + \dots + C_n^t.$$

В наведених співвідношеннях указується теоретична межа мінімально можливої кількості перевірочних символів, яку не завжди вдається досягнути на практиці. Щоб уникнути неоднозначності при декодуванні помилок різної кратності, кількість перевірочних символів часто доводиться брати більшою, ніж це впливає з відповідних співвідношень.

Правило побудови лінійного коду повністю визначається заданням функціональної залежності набору перевірочних символів від інформаційних. Для лінійних кодів ця залежність буде лінійною

$$\beta_j = \sum_{i=1}^k c_{ij} b_{li}, \quad j = 1, 2, \dots, r. \quad (5.3)$$

де c_{ij} – коефіцієнти, що можуть приймати значення 0 або 1, додавання яких виконується за модулем 2.

Записавши (5.3) в розгорнутому вигляді, одержимо r співвідношень, при допомозі яких за інформаційними символами кодової комбінації знаходяться перевірочні

$$\begin{aligned} \beta_{11} &= c_{11}b_{11} + c_{21}b_{12} + \dots + c_{k1}b_{1k}; \\ \beta_{12} &= c_{12}b_{11} + c_{22}b_{12} + \dots + c_{k2}b_{1k}; \\ &\dots\dots\dots \\ \beta_{1r} &= c_{1r}b_{11} + c_{2r}b_{12} + \dots + c_{kr}b_{1k}. \end{aligned} \tag{5.4}$$

Задання r співвідношень вигляду (5.4) повністю визначає правило побудови лінійного коду. Ці співвідношення в свою чергу визначаються заданням kr двійкових коефіцієнтів c_{ij} . Задавши kr двійкових коефіцієнтів c_{ij} і підставляючи у співвідношення (5.4) по черзі всі інформаційні комбінації, можна одержати значення перевірочних символів для кожної з них і, таким чином, сформувати всі комбінації перешкодостійкого коду.

Лінійні групові коди можуть бути описані (задані) компактніше за допомогою матриць. Раніше наголошувалося, що всі 2^k дозволених комбінацій лінійного групового коду утворюють групу. З цієї групи можна виділити k незалежних комбінацій і об'єднати їх у матрицю розмірністю $k \times n$ (k рядків та n стовпців):

$$G_{n \times k} = \begin{vmatrix} b_{11} & b_{12} & \dots & b_{1k} & \beta_{11} & \beta_{12} & \dots & \beta_{1r} \\ b_{21} & b_{22} & \dots & b_{2k} & \beta_{21} & \beta_{22} & \dots & \beta_{2r} \\ & & & \dots & & & & \\ b_{k1} & b_{k2} & \dots & b_{kk} & \beta_{k1} & \beta_{k2} & \dots & \beta_{kr} \end{vmatrix}.$$

Лінійна незалежність комбінацій (рядків) $G_{n \times k}$ означає, що жодна з них не може бути створена додаванням інших рядків.

Матриця $G_{n \times k}$ називається *породжувальною*, оскільки дозволяє одержати всі дозвалені комбінації коду шляхом додавання за модулем 2 усіх можливих поєднань рядків (по два, по три і т.д.).

Породжувальну матрицю можна представити двома матрицями – інформаційною, яка містить тільки інформаційні символи, і додатковою (перевірочною), що містить перевірочні розряди. Інформаційна матриця квадратна, розмірністю $k \times k$, розмірність додаткової матриці $k \times r$.

Як інформаційну матрицю дуже зручно взяти одиничну матрицю

$$\begin{pmatrix} 10 \dots 0 \\ 01 \dots 0 \\ \dots \\ 00 \dots 1 \end{pmatrix}.$$

В цьому випадку породжувальна матриця лінійного коду називається **канонічною**. Будь-яку породжувальну матрицю можна звести до канонічного вигляду

$$G_{n \times k} = \begin{pmatrix} 100 \dots 0 \beta_{11} \beta_{12} \dots \beta_{1r} \\ 010 \dots 0 \beta_{21} \beta_{22} \dots \beta_{2r} \\ \dots \\ 000 \dots 1 \beta_{k1} \beta_{k2} \dots \beta_{kr} \end{pmatrix}.$$

Встановимо зв'язок між коефіцієнтами c_{ij} співвідношення (5.4) з символами β_{ij} додаткової матриці. Для цього у співвідношення (5.4) по черзі підставимо рядки інформаційної (одиничної) матриці

$$\begin{aligned} \beta_{11} &= c_{11} \cdot 1 + c_{21} \cdot 0 + \dots + c_{k1} \cdot 0 = c_{11}; \\ \beta_{12} &= c_{12} \cdot 1 + c_{22} \cdot 0 + \dots + c_{k2} \cdot 0 = c_{12}; \\ \beta_{13} &= c_{13} \cdot 1 + c_{23} \cdot 0 + \dots + c_{k3} \cdot 0 = c_{13}; \\ &\dots \\ \beta_{1r} &= c_{1r} \cdot 1 + c_{2r} \cdot 0 + \dots + c_{kr} \cdot 0 = c_{1r}. \end{aligned}$$

Виконавши аналогічні операції для інших рядків одиничної матриці, встановимо тотожність коефіцієнтів c_{ij} і перевірочних символів β_{ij} , де $i = 1$.

Отже, перевірочні символи всіх дозволених комбінацій виражаються через перевірочні символи породжувальної матриці і інформаційні символи кодової комбінації, що дозволяє співвідношення (5.4) переписати в еквівалентному вигляді

$$\begin{aligned} \beta_{1_1} &= \beta_{11}b_{1_1} + \beta_{21}b_{1_2} + \dots + \beta_{k1}b_{1_k}; \\ \beta_{1_2} &= \beta_{12}b_{1_1} + \beta_{22}b_{1_2} + \dots + \beta_{k2}b_{1_k}; \\ &\dots \\ \beta_{1_r} &= \beta_{1r}b_{1_1} + \beta_{2r}b_{1_2} + \dots + \beta_{kr}b_{1_k}. \end{aligned} \tag{5.5}$$

Таким чином, лінійний (n, k) код визначається kr двійковими числами, які у принципі можуть виражатися довільно. Тому при заданих n і k можуть бути побудовані 2^k різних лінійних (n, k) кодів. Задача полягає в тому, щоб вибрати оптимальний варіант коду. Зробити це простим перебо-

ром трудно з причини великої кількості варіантів. Так, наприклад, при $n = 30$, $k = 20$ кількість різних лінійних кодів дуже велика ($2^{20} > 10^6$). Для того, щоб одержати код із заданим d_{min} , не вдаючись до повного перебору, на коефіцієнти β_{ij} накладаються деякі обмеження, які враховуються при виборі додаткової матриці.

Резонно вважати, що елементи додаткової матриці необхідно вибирати так, щоб забезпечити максимально можливу відстань між дозволеними комбінаціями. Для цього ваги рядків додаткової матриці повинні бути великими. З другого боку, не можна всі рядки додаткової матриці зробити одиничними, оскільки в цьому випадку відстань між дозволеними комбінаціями визначатиметься тільки відстанню між рядками інформаційної матриці, яка дорівнює двом. Тому бажано, щоб рядки додаткової матриці маючи велику вагу, в той же час відрізнялися як можливо більшою кількістю розрядів. Ці очевидні міркування дозволили сформулювати вимоги до додаткової матриці.

Для того, щоб матриця розміром $k \times r$ була додатковою для (n, k) коду із заданою мінімальною відстанню d_{min} , необхідно і достатньо, щоб комбінація, що виходить в результаті додавання за модулем 2 l її рядків ($1 \leq l \leq k$), містила не менше, ніж $d_{min} - 1$ відмінних від нуля символів. Дійсно, серед k інформаційних символів кожного рядка породжувальної матриці є тільки один, відмінний від нуля, при цьому для різних комбінацій він розташовується на різних позиціях. Тому серед перших k символів комбінації B_l , одержаних в результаті додавання за модулем 2 l її рядків, завжди знайдеться точно l відмінних від нуля символів. А кожна комбінація B_l групового коду повинна мати вагу не меншу, ніж d_{min} і, отже, серед її останніх r символів повинно бути не менше, ніж $d_{min} - 1$ відмінних від нуля.

Через вказані обставини вага кожного рядка додаткової матриці повинна бути не меншою $d_{min} - 1$, а рядки повинні відрізнятися між собою не менше, ніж в $d_{min} - 2$ позиціях. Вказані положення справедливі для кодів з будь-якою кодовою відстанню.

Приклад 5.1.

Розглянемо приклад побудови породжувальної матриці лінійного групового коду, що виправляє всі поодинокі помилки при передачі **16** повідомлень.

Для передачі **16** повідомлень необхідно мати чотири інформаційні ро-

зряди ($16 = 2^4$). Для кодів, що виправляють одну помилку ($d_{min} = 3$), кількість перевірочних символів наведена в табл. 5.1. При $k = 4$ $r = 3$. Тоді $n = k + r = 4 + 3 = 7$. Враховуючи, що вага кожного рядка додаткової матриці повинна бути не менше $d_{min} - 1 = 3 - 1 = 2$, вибираємо, як рядки додаткової матриці, тризначні комбінації з числом одиниць, більшим або рівним 2: *111, 110, 101, 011*. Побудована матриця має вигляд

$$G_{7 \times 4} = \begin{Bmatrix} 1000111 \\ 0100110 \\ 0010101 \\ 0001011 \end{Bmatrix}, \text{ або } G_{7 \times 4} = \begin{Bmatrix} 1000011 \\ 0100101 \\ 0010110 \\ 0001111 \end{Bmatrix}.$$

Виявлення і виправлення помилок лінійним кодом засноване на перевірці виконання співвідношень (5.5) для символів прийнятої комбінації $V^* = b_1^* b_2^* \dots b_k^* \beta_1^* \beta_2^* \dots \beta_r^*$ та на аналізі результатів цієї перевірки.

Для цього з прийнятих інформаційних символів відповідно до співвідношення (5.5), тобто за такими ж, що й на передавальній стороні, правилами формуються перевірочні розряди β_{ij}^* , які порівнюють з прийнятими контрольними $\beta_j^* + \beta_j^{**} = S_j$. Кількість перевірок дорівнює кількості перевірочних символів.

У результаті перевірок утворюється контрольне число $S_1 S_2 \dots S_r$, яке називається синдромом або пізнавачем, де S_j – двійковий символ, що дорівнює нулю, якщо в системі перевірок (5.5) j -а рівність виконана, і одиниці, якщо вона не виконана. Нульовий синдром указує на те, що символи прийняті правильно або відбулася помилка, що не знаходиться. Якщо хоча б один розряд контрольного числа містить одиницю, то в прийнятій комбінації є помилка. Оскільки спотворення одного з елементів b_i (або β_j) одержує цілком певну рівність, то кожному з $2^r - 1$ ненульових синдромів відповідає своя помилка, яка і виправляється.

Приклад 5.2.

Розглянемо на прикладі, яким чином кожному синдрому ставиться у відповідність своя помилка. Нехай груповий код побудований за такою матрицею:

$$G_{7 \times 4} = \begin{vmatrix} 1000111 \\ 0100110 \\ 0010101 \\ 0001011 \end{vmatrix} = \begin{vmatrix} 1000 \\ 0100 \\ 0010 \\ 0001 \end{vmatrix} \cdot \begin{vmatrix} 111 \\ 110 \\ 101 \\ 011 \end{vmatrix}.$$

Система перевірок для цього коду має вигляд

$$\beta_1^* + \beta_{11}b_1^* + \beta_{21}b_2^* + \beta_{31}b_3^* + \beta_{41}b_4^* = b_1^* + b_2^* + b_3^* = S_1;$$

$$\beta_2^* + \beta_{12}b_1^* + \beta_{22}b_2^* + \beta_{32}b_3^* + \beta_{42}b_4^* = b_1^* + b_2^* + b_4^* = S_2;$$

$$\beta_3^* + \beta_{13}b_1^* + \beta_{23}b_2^* + \beta_{33}b_3^* + \beta_{43}b_4^* = b_1^* + b_3^* + b_4^* = S_3.$$

Взявши до уваги, що код призначений тільки для виправлення однієї помилки, проаналізуємо одержану систему перевірок.

Символ β_1^* входить тільки в перше рівняння. Отже, якщо він спотворений, то синдром дорівнює 100 . Якщо спотворені символи β_2^* і β_3^* , кожний з яких також входить тільки в одне рівняння, синдроми мають вигляд 010 і 001 . Якщо спотворений символ b_1^* , що входить у всі три рівняння, то виникає синдром 111 . Спотвореним символам b_2^* , b_3^* і b_4^* , кожний з яких входить тільки до двох певних рівнянь, відповідають синдроми 110 , 101 і 011 . Визначивши за допомогою синдрому, який символ спотворений, змінюють його значення і, тим самим, відновлюють правильну інформацію.

Хай передавалися кодові комбінації 0110011 , 1110100 , 1101010 , що належать цьому коду. Через перешкоди відбулися спотворення в першому розряді першої комбінації, в першому розряді другої комбінації і шостому розряді третьої комбінації, тобто вони прийняті у вигляді 1110011 , 0110100 , 1101000 .

Знаходимо контрольні числа відповідно до системи перевірок. Для першої комбінації

$$\beta_1^* \oplus b_1^* \oplus b_2^* \oplus b_3^* = 0 \oplus 1 \oplus 1 \oplus 1 = 1;$$

$$\beta_2^* \oplus b_1^* \oplus b_2^* \oplus b_4^* = 1 \oplus 1 \oplus 1 \oplus 0 = 1;$$

$$\beta_3^* \oplus b_1^* \oplus b_3^* \oplus b_4^* = 1 \oplus 1 \oplus 1 \oplus 0 = 1.$$

Синдром 111 показує, що помилка відбулася в першому розряді і символ 1 необхідно замінити 0 .

Для другої комбінації

$$1 \oplus 0 \oplus 1 \oplus 1 = 1;$$

$$0 \oplus 0 \oplus 1 \oplus 0 = 1;$$

$$0 \oplus 0 \oplus 1 \oplus 0 = 1.$$

Синдром **111** показує, що помилка в першому розряді.

Для третьої комбі-

$$0 \oplus 1 \oplus 1 \oplus 0 = 0; \quad \text{нації}$$

$$0 \oplus 1 \oplus 1 \oplus 1 = 1;$$

$$0 \oplus 1 \oplus 0 \oplus 1 = 0.$$

Синдром **010** показує, що помилка в шостому розряді.

Синдром можна побудувати так, щоб одержаний при перевірках результат $S_1 S_2 \dots S_r$ прямо указував номер спотвореного розряду.

Таким чином, перевагою лінійних групових кодів є те, що в декодері не потрібно зберігати всі 2^k дозволених кодових комбінацій. Достатньо зберігати тільки k рядків додаткової матриці і таблицю синдромів. Проте, при $n \geq 100$ і декількох помилках, що виправляються, реалізація декодуючих пристроїв стає проблематичною.

Найбільш широке поширення одержали кодуючі і декодуючі пристрої, виконані на основі регістрів зсуву. Реалізація цього методу проста і дозволяє створити високонадійні схеми на базі інтегральної технології і забезпечує можливість зміни параметрів кодових комбінацій.

Кодуючий пристрій, що формує лінійний (n, k) код, складається з n -розрядного регістра зсуву і r суматорів за модулем 2, що зображено на рис. 5.2. У регістрі k чарунок призначені для інформаційних розрядів, а інші r чарунок – для перевірочних розрядів. Кожний з r суматорів за модулем 2 служить для формування перевірочного символу, що знаходиться на визначеній позиції. Інформаційні чарунки регістра підключаються до відповідних суматорів за правилами побудови конкретного перешкодостійкого коду.

Пристрій працює таким чином. Кодова комбінація первинного (безнадмірного) коду записується паралельно в k інформаційних чарунках регістра. Далі у всіх r двійкових суматорах формуються перевірочні символи, що записуються в r перевірочних чарунках регістра. На цьому формування кодової комбінації перешкодостійкого коду закінчується і починається її вивід з регістра шляхом подачі на нього імпульсів зсуву (тактових імпульсів) від генератора тактових імпульсів (на рис. 5.2 і далі на всіх схемах кодуючих і декодуючих пристроїв, в основі яких лежать регістри зсуву, з метою спрощення рисунків генератори тактових імпульсів не показу-

ні). Після n тактових імпульсів кодова комбінація виводиться з регістра, а сам регістр готовий до запису і формування наступної кодової комбінації.

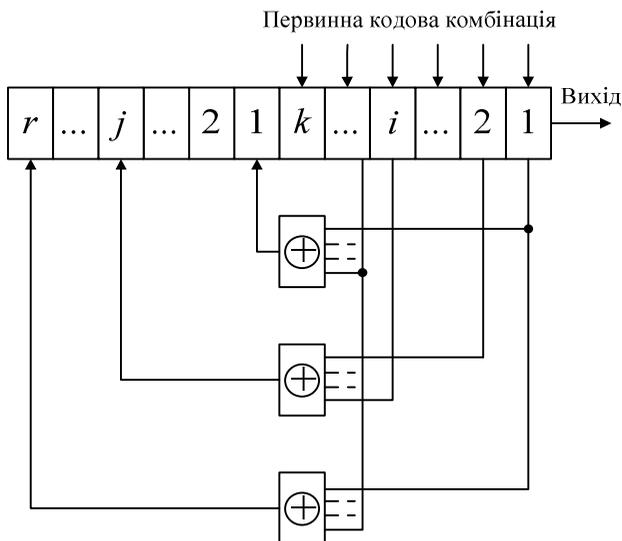


Рис. 5.2. Структурна схема кодуючого пристрою лінійного (n, k) коду

Розглянемо принцип роботи декодуючого пристрою, структурна схема якого зображена на рис. 5.3. Пристрій складається з n -розрядного приймального регістра, r суматорів за модулем 2 і аналізатора помилок. Прийнята кодова комбінація, частина символів якої може бути спотворена перешкодою, записується в n чарунок регістра. Суматори за модулем 2 підключаються до чарунок регістра зсуву відповідно до перевірочних рівностей для даного коду. Якщо в прийнятій кодовій комбінації помилок немає, то на виходах усіх суматорів формуються нулі. При наявності в прийнятій кодовій комбінації спотворень, на виходах деяких суматорів з'являться одиниці. У цьому випадку аналізатор помилок сформує сигнал "помилка".

Для виправлення помилок схема декодуючого пристрою повинна бути ускладнена в порівнянні з розглянутою, тому що в неї необхідно ввести ряд додаткових вузлів: пристрій для запам'ятовування кодової комбінації, що виправляється, логічні пристрої для визначення спотворених розрядів і їхнього виправлення тощо. При великому числі надмірних символів і довших кодах декодуючий пристрій виходить дуже складним.

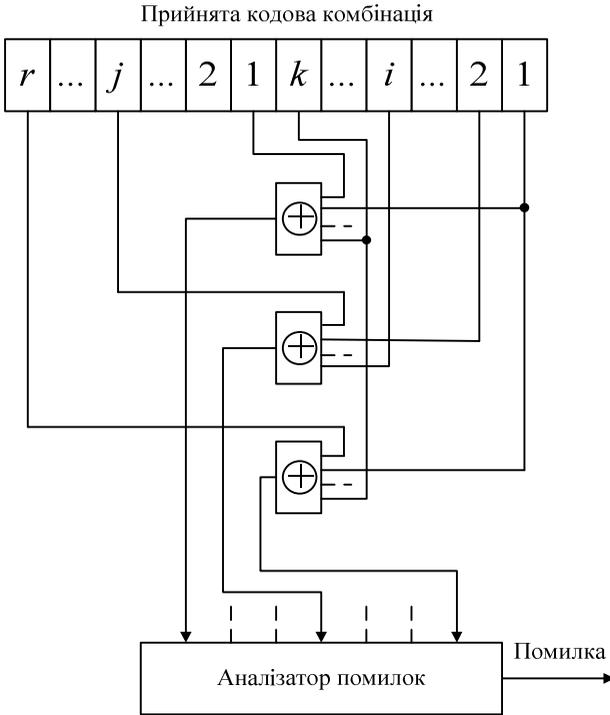


Рис. 5.3. Структурна схема декодуючого пристрою лінійного (n, k) коду

5.4. Коди Хеммінга

Розглянемо завдання коду Хеммінга для виправлення однократних помилок на прикладі коду $(7,4)$. Складемо три рівняння формування перевірочних символів коду (за числом перевірочних символів у кодовій комбінації):

$$\left. \begin{aligned} b_1 \oplus b_2 \oplus b_3 &= \beta_1 \\ b_1 \oplus b_2 \oplus b_4 &= \beta_2 \\ b_1 \oplus b_3 \oplus b_4 &= \beta_3 \end{aligned} \right\}, \quad (5.6)$$

Тут виконувється складання за модулем 2. З рівнянь формування легко впливають рівняння перевірок за модулем 2:

$$\left. \begin{aligned} b_1 \oplus b_2 \oplus b_3 \oplus \beta_1 &= 0 \\ b_1 \oplus b_2 \oplus b_4 \oplus \beta_2 &= 0 \\ b_1 \oplus b_3 \oplus b_4 \oplus \beta_3 &= 0 \end{aligned} \right\} \quad (5.7)$$

Перевірочна і породжувальна матриці коду відповідно мають такий вигляд:

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}, \quad G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

Перевірочна матриця H є символічним записом рівняння перевірок де одиницями позначаються символи, що беруть участь у перевірках, а нулями решта всіх символів комбінації (n, k) коду. Перевірочна матриця H складається з $(n - k)$ рядків і n стовпців.

У даному випадку мінімальна кодова відстань $d_{min} = 3$.

Кодери для лінійних (n, k) кодів можуть бути побудовані підставі співвідношення (5.6), що визначає спосіб формування кодової комбінації за заданими інформаційними символами.

Структурна схема кодера, що формує перевіірочні символи відповідно до рівнянь (5.7) для систематичного коду Хеммінга (7,4), наведена на рис. 5.4.

Кодер містить семирозрядний регістр зсуву (РЗ) і три суматори за модулем 2. Чотири інформаційні символи $b_1 - b_4$ поступають від джерела інформації ДІ в РЗ.

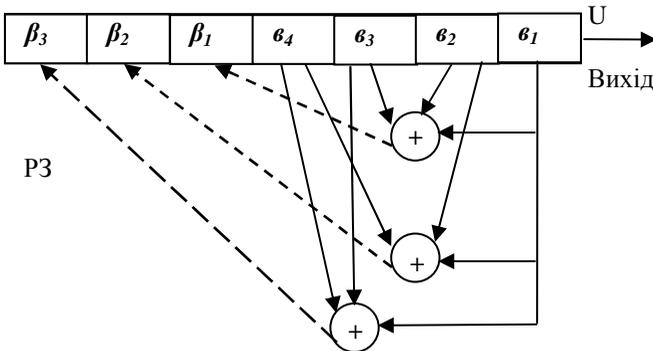


Рис. 5.4. Структурна схема кодера Хеммінга

Складанням за модулем 2 певних інформаційних символів (5.6) за один такт формуються перевірочні символи $\beta_1 - \beta_3$, які записуються в РЗ. Після чого сформована таким чином кодова комбінація U поступає з РЗ в канал зв'язку.

Декодування лінійних (n, k) кодів полягає у виявленні і(або) виправленні помилки в прийнятій комбінації U' . Для цього визначається синдром (ознака) прийнятої комбінації вигляду

$$U' = (c_1, c_2, c_3, \dots, c_{n-k}) = U'H^T.$$

Синдромом є вектор-рядок з $(n - k)$ символів можна подати як

$$C_j = \sum_{i=1}^k a'_i p_{ij} \oplus a_{k+j}, \quad j = 1, n-k.$$

Оскільки прийнята комбінація U' може відрізнитися від переданої кодової комбінації U на величину помилки $U' = U + E$, то синдром C визначається тільки вектором помилки E

$$C = U'H^T = (U \oplus E)H^T = UH^T \oplus EH^T = EH^T,$$

оскільки $UH^T = 0$.

Якщо $C = 0$ то помилки в комбінації U' не було ($E = 0$) або під впливом помилки ($E \neq 0$) одна дозволена кодова комбінація перейшла в іншу дозволена кодову комбінацію.

Якщо $C \neq 0$, у прийнятій комбінації є помилка, і для її виявлення необхідно обчислити синдром.

Виправлення помилок у прийнятій комбінації можливе, якщо встановлена взаємно однозначна відповідність між синдромом і конфігурацією помилки (однократна, двократна і т. д.). Таку відповідність можна встановити підстановкою вектора помилки $E = (e_1, e_2, \dots, e_n)$, тоді

$$C = \sum_{i=1}^n e_i H_i^T,$$

де H_i^T - стовпець перевірочної матриці.

Таким чином при однократній помилці e_i вектор помилки E може мати вигляд $100\dots 0, 010\dots 0, \dots 00\dots 1$, тобто синдром співпадає з i -тим стовпцем матриці H або i -тим спотвореним символом прийнятої комбінації. Взаємна однозначна відповідність між синдромом C , а також помилкою e_i забезпечується, якщо стовпці перевірочної матриці різні і не нульові. У разі помилки другої кратності e_i, e_j (вектор помилки E має вигляд $101\dots 0$,

011...0, ...10...1) синдром формується складанням i -го і j -го стовпців матриці H , при цьому їх сума не повинна співпадати з жодним із стовпців матриці. Така умова може бути забезпечена певним вибором матриці H .

За обчисленням синдромом $C = (c_1, c_2, \dots, c_n)$ здійснюється оцінка символів e_i вектора помилки E і оцінка символу переданої комбінації

$$\hat{a}_i = a'_i \oplus \hat{e}_i = a_i \oplus e_i \oplus \hat{e}_i$$

При цьому \hat{a}_i правильна, якщо правильно оцінено символ завади $\hat{e}_i = a_i$.

Розглянемо процедуру декодування коду Хеммінга (7.4). Схема декодера (рис. 5.5) містить регістр зсуву (РЗ), в який з каналу поступає комбінація U' . Три суматори за модулем 2 здійснюють три перевірки відповідно до співвідношень (5.7). Виходи суматорів підводяться на вхід схеми «АБО» для фіксації однократних і двократних помилок і на входи чотирьох дешифраторів помилок (схема I) за числом інформаційних символів комбінації.

Під час надходження всієї комбінації в РЗ її символи відповідно до співвідношень (5.7) подаються на три суматори для вироблення складових синдрому $C = (c_1, c_2, c_3)$. Якщо складові синдрому рівні, то згідно з рівняннями перевірок (5.7) помилки в прийнятій комбінації не було або даною перевіркою вона не виявлена. Якщо лише один з $c_i \neq 0$, то є помилка. Таким чином, синдром помилки є сукупність результатів рівнянь перевірок, яка відповідає i -му спотвореному символу прийнятої комбінації. Оскільки стовпці матриці H різні (згідно з виразом (5.7)), то однократні помилки будуть виправлені. Для цього у схемі декодера встановлені дешифратори помилок (схеми I), налаштовані на комбінації, що відповідають першим чотирьом стовпцям матриці H .

Припустимо, що при перевірці комбінації на наявність помилок на виходах суматорів отримана комбінація вигляду III . тоді на виході схеми «АБО» з'являються одиниці, що означає наявність помилки, і на виході першого дешифратора також з'явиться 1, а значення b_i в РЗ змінено на зворотне. Це означає, що для коду Хеммінга оцінка символу здійснюється за правилом $\hat{b}_i = b_i \oplus 1$.

Недоліком такої схеми декодера є швидке збільшення кількості дешифраторів помилок при зростанні числа інформаційних символів (n, k) коду, що обмежує їх застосування і вимагає використання лінійних кодів, які дозволяють зменшити об'єм обладнання декодера.

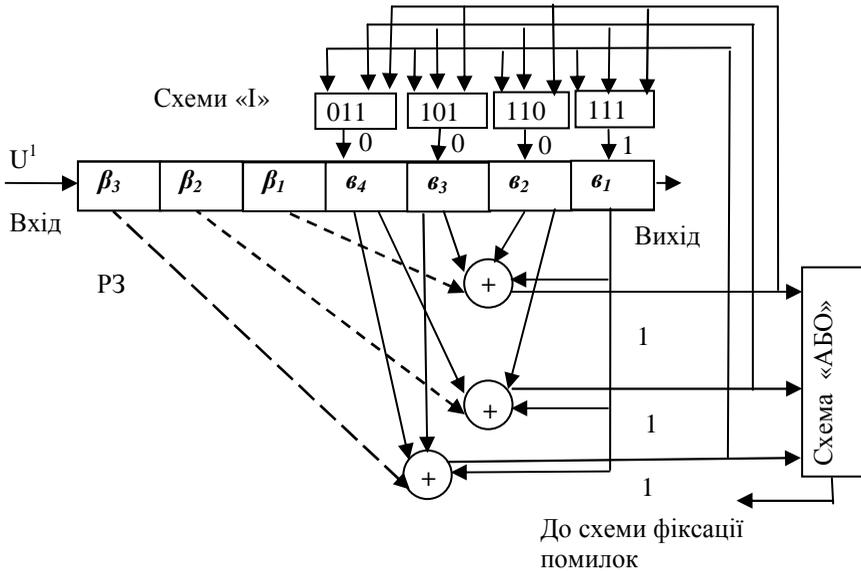


Рис. 5.5. Структурна схема декодера Хеммінга

5.5. Лінійні циклічні перешкодостійкі коди

Перевагою використання лінійних групових кодів є те, що в кодері і декодері не потрібно зберігати всі 2^k різних комбінацій, а при декодуванні не потрібно обчислювати 2^k кодових відстань. Достатньо зберігати k рядків додаткової матриці, а в процесі кодування перевіряти r рівностей. В порівнянні з табличним способом це спрощує кодування і декодування з виявленням помилок. Проте, для виправлення помилок необхідно в декодері перебрати таблицю синдромів, об'єм якої швидко зростає зі збільшенням довжини коду і кількості помилок, що виправляються. Це призводить до того, що при значеннях n рівних декільком десяткам реалізація декодуючого пристрою може стати утрудненою.

Спростити техніку кодування і особливо декодування вдалося, коли серед лінійних групових кодів було знайдено один з класів кодів, який отримав назву циклічного. Особливістю **циклічного коду**, через яку він отримав свою назву, є те, що k лінійно незалежних рядків його матриці додатково пов'язані умовою циклічності. Це означає, що всі лінійно

незалежні комбінації коду можуть бути отримані послідовним зсувом на один розряд єдиної “базової” комбінації. Кількість можливих циклічних (n, k) кодів значно менше кількості різних групових (n, k) кодів. Проте, властивість циклічності дозволяє значно зменшити об’єм пам’яті кодера і декодера при виявленні помилок і реалізувати виправлення поодиноких помилок так же просто, як і виявлення. Виправлення багатократних помилок при використанні циклічних кодів може бути реалізоване простіше, ніж при довільних лінійних кодах. Все це і визначило широке застосування циклічних кодів в сучасних системах передачі інформації.

Формування циклічних кодів засновано на відображенні кодових комбінацій елементами алгебри поліномів. Основою такого опису є подання кодової комбінації довжини n як полінома степеня $n-1$, що містить фіктивну змінну x . Показники степеня змінної x відповідають номерам розрядів (позиціям), а коефіцієнтами при x є символи 1 або 0 (для двійкових комбінацій). При цьому найменшому розряду числа відповідає фіктивна змінна $x^0 = 1$.

Запишемо, наприклад, у вигляді полінома п’ятирозрядну двійкову кодову комбінацію **10101**

$$B(x) = 1 \cdot x^4 + 0 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x + 1 \cdot x^0$$

Виконуючи операцію множення перемінних x на відповідні коефіцієнти, отримаємо

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

Подання кодових комбінацій як поліномів дозволяє крім операцій додавання і множення на символи β_{ij} , які використовувалися при формуванні довільних лінійних кодів, ввести ще й операції множення і ділення поліномів і отримати за рахунок цього додаткові ознаки для виявлення дозволених комбінацій.

Суть циклічного кодування зводиться до наступного. Дозволені кодові комбінації (дозволені поліноми) циклічного коду створюються шляхом множення деякого полінома (утворюючого) $P(x)$ на поліноми $B_i(x)$, які являють собою комбінації безнадмірного коду. На приймальній стороні ухвалена комбінація піддається зворотньому перетворенню її полінома на поліном $P(x)$. Якщо при діленні не утворюється лишок (лишок від ділення дорівнює нулю), комбінація вважається дозволеною і повідомлення, яке міститься в ній декодується.

Такий випадок можливий за відсутності перешкоди або при такій перешкоді, яка трансформує одну дозволена комбінація в іншу. Якщо при діленні утворюється не нульовий лишок, комбінація вважається забороне-

ною. Наявність лишка дозволяє виявити помилку, а вигляд лишка – визначити номер (або номери) помилкового розряду, тобто виправити помилку.

Нагадаємо основні правила, за якими виконуються операції алгебри над поліномами з двійковими коефіцієнтами.

Додавання поліномів зводиться до складання за модулем 2 коефіцієнтів при членах з однаковими степенями.

Як приклад, розглянемо суму поліномів

$$B_1(x) = x^6 + x^5 + x^3 + x^2 + 1 \text{ і } B_2(x) = x^5 + x^4 + x^2$$

$$B_1(x) \rightarrow 1101101$$

$$B_2(x) \rightarrow 0110100$$

$$B_1(x) + B_2(x) \rightarrow 1011001 \rightarrow x^6 + x^4 + x^3 + 1$$

У полі двійкових чисел операції додавання і віднімання (за модулем 2) еквівалентні. Це дозволяє при всіх операціях над поліномами (включаючи і ділення) користуватися тільки додаванням за модулем 2, а при перенесенні членів рівності з однієї частини в іншу не змінювати знаки.

Ділення поліномів виконується звичайним алгебраїчним способом, тільки замість віднімання проміжних результатів їх додають за модулем 2.

Розглянемо приклад. Розділимо поліном $x^6 + x^4 + x^3 + 1 \rightarrow 1011001$ на поліном $x^4 + 1 \rightarrow 10001$.

$$\begin{array}{r} x^6 + x^4 + x^3 \quad | \quad x^4 + 1 \\ \underline{x^6 + x^2} \quad | \quad x^2 + 1 \\ x^4 + x^3 + x^2 \\ \underline{ x^4 + 1} \\ x^3 + x^2 + 1 \leftarrow \text{Є} \hat{\text{e}} \phi \hat{\text{i}} \hat{\text{e}} \end{array}$$

Ділення поліномів виконується до тих пір, поки степінь останньої лишка не стане меншою степеня дільника.

Визначимо тепер операцію множення. Незавжди встановити, що операція множення поліномів (з перенесенням), може дати поліноми більш високого степеня, ніж $n - 1$. Відповідні їм кодові комбінації будуть мати кількість розрядів більшу, ніж n , і вони не будуть належати до цієї множини. Тому для циклічного коду вводиться операція, яка отримала назву **символічного множення**. При виконанні цієї операції поліноми перемножуються за звичайними правилами, але з приведенням подібних за модулем 2. Якщо старший степінь добутку не перевищує $n - 1$, то це перетворення і є результатом символічного множення. Якщо старший степінь перетво-

рення більший або рівний n , то поліном перетворення ділиться на поліном $x^n + 1$ і результатом символічного множення вважається лишок від ділення (тобто символічне множення є множенням за модулем $x^n + 1$). При такому множенні перетворення будь-яких двох поліномів з групи поліномів ступеня $n-1$ має степінь, яка не перевищує $n-1$, тобто степінь помилки завжди менша за степінь дільника. Крім того, множення за модулем $x^n + 1$ дозволяє математично записати й операцію циклічного зсуву кодового полінома $B(x)$. Цей зсув еквівалентний простому множенню (за модулем $x^n + 1$) $B(x)$ на x і не призводить до появи поліномів ступеня більшого, ніж $n-1$.

Розглянемо приклад. Нехай кодовий поліном має вигляд $B(x) = x + 1 \rightarrow 00 \dots 011$. Множення його на x призводить до появи нового полінома і нової комбінації, яка є циклічним зсувом попередньої:

$$B_1(x) = xB(x) = x(x + 1) = x^2 + x \rightarrow 00 \dots 0110$$

Наступний зсув переміщує одиниці кодової комбінації ще на один розряд вліво

$$B_2(x) = x^2B(x) = xB_1(x) = x(x^2 + x) = x^3 + x^2 \rightarrow 00 \dots 01100$$

Степінь отриманих поліномів менший n і відповідний поліном не виходить за межі групи. Але після перемноження $x(x^{n-1} + x^{n-2})$ одержуємо поліном $x^n + x^{n-1}$, що виходить за межі групи. Виконуючи символічне множення, розділимо цей поліном на $x^n + 1$.

Лишок від ділення $x^{n-1} + 1 \rightarrow 10 \dots 01$, по-перше, не виходить за межі групи; а по-друге, являє собою результат чергового циклічного зсуву.

Існують декілька різних способів кодування циклічних кодів. Принципово просто комбінації циклічного коду можна отримати, помноживши поліноми $B_i(x)$, відповідні комбінаціям безнадмірного коду (інформаційним символам), на утворюючий поліном $P(x)$. Такий спосіб легко реалізується, але він має недолік, який полягає в тому, що комбінації коду, які виходять, в результаті множення, не містять інформаційних символів в явному вигляді, тобто такий код є нероздільним. Внаслідок цього після виправлення помилок ухвалені комбінації необхідно додатково ділити на утворюючий поліном.

Звичайно прагнуть отримати код роздільного типу, тобто у такому вигляді, коли під інформаційні символи відводиться k членів із старшими степенями полінома відповідного коду, а під r контрольних символів –

члени, що залишилися, з низькими степенями. Щоб отримати такий роздільний (систематичний) код, застосовується наступна процедура кодування.

Поліном $B_i(x)$, відповідний k -розрядній комбінації безнадмірного коду, помножується на x^m , де $m = n - k$, що еквівалентно дописуванню справа до комбінації безнадмірного коду m нулів. Потім перетворення $x^m B_i(x)$ ділиться на породжувальний поліном. В загальному випадку результат ділення складається з цілого числа $Q(x)$ і лишка $R(x)$

$$x^m B_i(x) = Q(x)P(x) + R(x).$$

Обчислена лишок $R(x)$ використовується для утворення циклічного коду у вигляді суми

$$B(x) = x^m B_i(x) + R(x)$$

Оскільки додавання і віднімання за модулем 2 дають один і той же результат, то неважко помітити, що $B(x) = Q(x)P(x)$, тобто отримана комбінація задовольняє вимогам подільності на породжувальний поліном.

Оскільки степінь полінома $P(x)$ вибирається рівним m , степінь лишка $R(x)$ не перевищує $m - 1$ і, отже, вказана операція додавання рівносильна приписуванню лишка $R(x)$, виконуючої роль перевірочних символів, до $B_i(x)$ збоку молодших розрядів.

Розглянемо приклад. Закодувати циклічним кодом з $d_{min} = 3$ чотирирозрядну інформаційну комбінацію $1001 \rightarrow B_i(x) = x^3 + 1$.

Визначивши необхідну кількість контрольних символів $r = 3$, з таблиці примітивних поліномів вибираємо породжувальний поліном третього степеня $P(x) = x^3 + x^2 + 1 \rightarrow 1101$. Помножуючи x^m на $B_i(x)$, одержуємо $x^3(x^3 + 1) = x^6 + x^3$ (для двійкової комбінації це означає просте приписування справа трьох нулів: 1001000). Розділивши $x^m B_i(x)$ на породжувальний поліном, знаходимо лишківу, яка дорівнює $x + 1$.

Оскільки лишка є контрольними розрядами, то їхні довжини повинні дорівнювати r . У разі браку розряду до лишка приписується зліва необхідна кількість нулів. Тому лишок $x + 1 \rightarrow 11$ повинна бути записана як 011 .

Тоді $B(x) = x^m B_i(x) + R(x) = x^6 + x^3 + x + 1$ є кодовою

комбінацією циклічного коду і має вигляд **1001011** (для двійкової комбінації приписані три нулі необхідно замінити лишківєю). В отриманій комбінації **1001** – інформаційні символи, **011** – контрольні.

Якби комбінація циклічного коду формувалася множенням інформаційної комбінації (полінома) на породжувальний поліном, то вона мала б вигляд **1100101**. Інформаційні і контрольні символи тут нероздільні.

Розглянутим способом можна закодувати всі повідомлення, які треба передати. Проте для повного опису (визначення) всіх кодових комбінацій циклічного коду достатньо, як і для будь-якого групового коду, записати тільки лінійно незалежні комбінації і об'єднати їх в породжувальну матрицю. Породжувальна матриця містить k рядків, які доцільно використовувати як рядки одиничної матриці зі своїми лишокми. Побудова матриці циклічного коду, зводиться, таким чином, до складання одиничної матриці, множення кожного її рядка на x^r (для двійкової комбінації – до добавки справа r нулів) і отримання додаткової матриці лишків шляхом ділення $x^r B_i(x)$ на породжувальний поліном $P(x)$.

Розглянемо приклад. Скласти породжувальну матрицю циклічного коду (7, 4). Помноживши рядки одиничної матриці

$$\begin{pmatrix} 1000 \\ 0100 \\ 0010 \\ 0001 \end{pmatrix}$$

на $x^r = x^3$, отримаємо матрицю проміжних комбінацій з $n = k + r = 7$ стовпців і $k = 4$ рядків

$$\begin{pmatrix} 1000000 \\ 0100000 \\ 0010000 \\ 0001000 \end{pmatrix}.$$

Після ділення кожного рядка цієї матриці на породжувальний поліном $P(x) = x^3 + x^2 + 1$ одержуємо лишки **110**, **011**, **111**, **101**, що використовуються як додаткова матриця. Породжувальна матриця має вигляд

$$\begin{pmatrix} 1000110 \\ 0100011 \\ 0010111 \\ 0001101 \end{pmatrix}.$$

Рядки цієї матриці являють собою перші комбінації шуканого коду. Інші комбінації виходять в результаті підсумовування за модулем 2 всіляких поєднань її рядків.

Відзначимо, що породжувальна матриця може бути побудована і в результаті безпосереднього множення одиничної матриці на породжувальний поліном:

$$1000 \times 1101 = 1101000;$$

$$0100 \times 1101 = 0110100;$$

$$0010 \times 1101 = 0010100;$$

$$0001 \times 1101 = 0001101.$$

Повний набір кодових комбінацій буде мати такий же вигляд, як і в раніше розглянутому випадку.

Весь набір дозволених кодових комбінацій, отриманий за допомогою породжувальної матриці дозволяє закодувати 2^k повідомлень, де для розглянутих кодів k приймає такі дискретні значення: 4 – для коду $(7, 4)$, 11 – для коду $(15, 11)$ тощо. При необхідності можна зменшити кількість комбінацій коду, побудувавши укорочений циклічний код. Для цього в породжувальній матриці необхідно викреслити j перших рядків і стільки ж стовпців зліва. Отриманий укорочений циклічний $(n - k, k - j)$ код має такі ж характеристики, що і початковий.

Дія перешкод на кодові комбінації може бути описана за допомогою поліномів помилок $N_j(x)$. Члени полінома $N_j(x)$ розташовані на позиціях, відповідних спотвореним розрядам. Тому перешкода, що спотворює один $v + 1$ розряд кодової комбінації, може бути описана одночленом $N_v(x) = x^v$. Перешкода, що спотворює $v + 1$ та $\mu + 1$ ($v > \mu$) розряди має вигляд $N_{v, \mu}(x) = x^v + x^\mu$. Взаємодія кодової комбінації з перешкодою призводить до того, що на приймальній стороні спотворена комбінація описується поліномом $B^*(x) = B(x) + N(x)$. Помилки в циклічних кодах виявляються і виправляються за допомогою лишка від ділення отриманої комбінації на породжувальний поліном. Якщо при

передачі по каналу зв'язку помилок не було, то $B^*(x) = B(x)$ і ухвалений поліном ділиться на $P(x)$ без лишка. Якщо ухвалена комбінація, не ділиться на $P(x)$ без лишка, то це свідчить про те, що виникла помилка.

Лишок, що виникає при діленні полінома $B^*(x)$ на породжувальний поліном $P(x)$, дорівнює лишка від ділення $N_j(x)$ на $P(x)$. Дійсно

$$\frac{B^*(x)}{P(x)} = \frac{B_i(x)}{P(x)} = \frac{N_j(x)}{P(x)}. \quad (5.8)$$

Отже, помилка може бути виявлена в тому і лише в тому випадку, якщо поліном помилок не ділиться без лишка на $P(x)$.

Для виправлення виявлених помилок код будується так, щоб поліноми помилок, які підлягають виправленню, давали при діленні на $P(x)$ різні лишка.

Розглянемо процес виправлення помилок на прикладі коду (7, 4).

Як впливає з виразу (5.8) лишка $R(x)$, які з'являються після ділення тих поліномів, у яких спотворені однакові розряди, є однаковими.

Прийнято вважати, що розрядність двійкових еквівалентів лишків завжди на одиницю менша розрядності дільника. Визначимо види лишків. Лишок від ділення на $P(x) = x^3 + x^2 + 1 \rightarrow 1101$ будь-якого дозволеного полінома степеня r при спотвореному першому розряді

$$R_0(x) = \frac{N_0(x)}{P(x)} = \frac{1}{x^3 + x^2 + 1} = 1 \rightarrow 001$$

(поліном $N_0(x)$ на $P(x)$ не ділиться, тому значущі символи лишка $R_0(x)$ і $N_0(x)$ співпадають, але степінь $R_0(x)$ зменшується до $r - 1$).

Лишок при спотворенні другого розряду

$$R_1(x) = \frac{N_1(x)}{P(x)} = \frac{x}{x^3 + x^2 + 1} = x \rightarrow 010.$$

$$R_2(x) = \frac{N_2(x)}{P(x)} = \frac{x^2}{x^3 + x^2 + 1} = x^2 \rightarrow 100;$$

$$R_3(x) = \frac{N_3(x)}{P(x)} = \frac{x^3}{x^3 + x^2 + 1} = x^2 + 1 \rightarrow 101;$$

$$R_4(x) = \frac{N_4(x)}{P(x)} = \frac{x^4}{x^3 + x^2 + 1} = x^2 + x + 1 \rightarrow 111;$$

$$R_5(x) = \frac{N_5(x)}{P(x)} = \frac{x^5}{x^3 + x^2 + 1} = x + 1 \rightarrow 011;$$

$$R_6(x) = \frac{N_6(x)}{P(x)} = \frac{x^6}{x^3 + x^2 + 1} = x^2 + x \rightarrow 110.$$

Таким чином, кожному спотвореному розряду відповідає своя лишок. Тому на приймальній стороні порівнюють отриману лишківку з наявною таблицею, щоб визначити номер спотвореного розряду.

Розглянута процедура декодування циклічних кодів показує, що виправлення поодиноких помилок реалізується дуже просто. Виправлення многократних помилок при циклічному кодуванні хоча й здійснюється дещо простіше, ніж при довільному лінійному коді, але в загальному випадку залишається достатньо громіздким. Виправлення помилок великої кратності ефективнішими і простішими методами вдається реалізувати при використанні найважливішого класу циклічних кодів – кодів Боуза – Чоудхурі – Хоквінгема (БЧХ).

На дозволену множину кодових комбінацій при циклічному кодуванні накладаються додаткове обмеження в порівнянні з рештою лінійних кодів: подільність на породжувальний поліном $P(x)$. Іншими словами, породжувальний поліном виділяє з усієї групи поліномів $n-1$ -го степеня особливу підгрупу, елементи якої діляться без лишка на $P(x)$. Саме ця ознака спрощує апаратну реалізацію кодуючих і декодуючих пристроїв. Оскільки склад групи визначається видом породжувального полінома $P(x)$, то його задання – один з головних етапів при циклічному кодуванні. Розглянемо основні вимоги до породжувального полінома та методику його вибору, орієнтуючись для простоти викладу на коди, що виправляють поодинокі помилки ($d_{min} = 3$).

Для того, щоб усі поліноми, відповідні кодовим комбінаціям циклічного коду, ділилися без лишка на $P(x)$, достатньо, щоб на нього ділилися без лишка всі поліноми, що відображають кодові комбінації породжувальної матриці. Останні можуть бути одержані циклічним зсувом. Вони будуть лишківкою від ділення поліномів $B(x)P(x)$ (символічне множення) на біном $x^n + 1$.

Тому можна записати

$$B(x)P(x) = Q(x)(x^n + 1) + R(x),$$

де $Q(x)$ – частка від ділення. Використовуючи правило перенесення доданків, маємо

$$R(x) = Q(x)(x^n + 1) + B(x)P(x)$$

Звідси ясно, що всі поліноми матриці, а тому і всі поліноми коду будуть ділитися без лишка тільки в тому випадку, якщо на $P(x)$ без лишка ділитиметься поліном $x^n + 1$.

Так, щоб $P(x)$ міг сформувати циклічний код, він повинен бути дільником полінома $x^n + 1$. Це перша і основна вимога до $P(x)$.

Вся решта вимог до породжувального полінома розроблена з метою поліпшення кодуєчих властивостей циклічного коду. Без виконання першої вимоги циклічний код побудувати взагалі неможливо.

Визначниками помилок на приймальній стороні є лишки від ділення прийнятих комбінацій на породжувальний поліном. Кожному варіанту спотворення повинна відповідати свій лишок. Чим більше різних лишків може виникнути від дільника комбінацій, що спотворені перешкодами, тим більшу кількість різних варіантів спотворень здатний знайти і розпізнати код, тим вищі його коректуючі властивості.

Найбільша можлива кількість лишків, що дорівнює $2^m - 1$ (виключаючи нульову), може забезпечити незвідний (простий) поліном степеня m . Це такий поліном, який ділиться тільки сам на себе і на одиницю і не ділиться ні на який інший поліном. Але тут виникає запитання, чи задовольняють незвідні поліноми першої вимози, тобто чи є вони дільниками бінома $x^n + 1$.

Доведено, що біном $x^n + 1$ ділиться без лишка на простий поліном степеня m , якщо $n = 2^m - 1$. Більш того біном ділиться в цьому випадку і на інші прості поліноми, степені яких кратні m .

Розглянемо приклад. Розглянемо біном $x^{15} + 1$. Його степінь $n = 15$ може бути записаний як $2^m - 1$ ($m = 4$). Отже, біном $x^{15} + 1$ ділитиметься без лишка на прості поліноми ступенів 4, 2, 1. Існують таблиці розкладання двочленів $x^n + 1$ на незвідні поліноми. Цей поліном (двочлен) $x^{15} + 1$ може бути записаний у вигляді множення п'яти незвідних поліномів

$$x^{15} + 1 = (x + 1)(x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1).$$

При використанні, як породжувального, будь-якого з поліномів, що входять в розкладання, буде одержано циклічний код довжиною $n = 15$.

Але коректуючі здібності цього коду, які визначаються кількістю різних лишків, що виникають при діленні спотворених комбінацій на $P(x)$, будуть неоднакові.

З табл. 5.2 видно, що як породжувальний поліном для циклічного коду з $n = 15$ потрібно брати поліноми $x^4 + x^3 + 1$ і $x^4 + x + 1$, кількість різних лишків яких дорівнює 15. Коди, одержані за допомогою цих поліномів, здатні виправити будь-яку поодинокую помилку.

Таблиця 5.2

Кількість різних лишків для різних поліномів			
Поліном	Степінь полінома	Максимально можлива кількість різних лишків $2^m - 1$	Реальна кіль- кість різних лишків
$x + 1$	1	1	1
$x^2 + x + 1$	2	3	3
$x^4 + x^3 + 1$	4	15	15
$x^4 + x + 1$	4	15	15
$x^4 + x^3 + x^2 + x + 1$	4	15	5

Проте використовувати для цієї же мети поліном $x^4 + x^3 + x^2 + x + 1$ не можна, оскільки він створює тільки 5 різних лишків. Це пояснюється тим, що цей поліном входить в розкладання не тільки двочлена $x^{15} + 1$, але і двочлена $x^5 + 1$. Породжувальним поліномом, доцільно вибрати незвідний поліном $P(x)$, який є дільником двочлена $x^n + 1$ і не входить в розкладання жодного двочлена $x^\lambda + 1$, де $\lambda < n$. Такі незвідні поліноми називаються примітивними. Таким чином, друга вимога до породжувального полінома полягає в тому, щоб він був незвідним і примітивним.

При заданому значенні n рівність $n = 2^m - 1$ однозначно визначає значення степенів незвідних (простих) примітивних поліномів, які можуть бути взяті як породжувальні.

Відмітимо, що можна побудувати циклічні коди і для довжин, відмінних від $2^m - 1$. Проте, ці коди будуть малоефективними. Тому, коли говорять про циклічні коди, то завжди мають на увазі, що їх довжина

задовольняє рівності $n = 2^m - 1$.

Формування циклічних кодів, як і будь-яких лінійних, починається з складання безнадмірних інформаційних комбінацій – поліномів $B_i(x)$, степінь яких $(k - 1)$ визначається кількістю повідомлень, що належать передачі (кількістю дозволених кодових комбінацій $K = 2^k$). Далі поліном $B_i(x)$ множиться на породжувальний поліном $P(x)$ степеня m . При цьому кількість дозволених поліномів не змінюється, але їх степінь зростає до величини $k - 1 + m = n - 1$, оскільки при перемножуванні степені поліномів складаються.

Множення безнадмірної кодової комбінації – інформаційного полінома $B_i(x)$ на $P(x)$ вводить в код таку ж надмірність, як і звичне додавання до інформаційних розрядів $r = m$ контрольних. Таким чином, степінь m породжувального полінома повинний бути не менше кількості контрольних символів r , а кількість його ненульових членів повинна бути не меншою мінімальної кодової відстані d_{min} . Це третя вимога до $P(x)$.

Для кодів, що виправляють поодинокі помилки, кількість різних не нульових залишків повинна дорівнювати кількості розрядів кодової комбінації n , оскільки в кожному з них можливі спотворення, які потрібно відрізнити одне від одного. Оскільки степінь породжувального полінома дорівнює кількості контрольних символів, то вибір степеня цього полінома зводиться до вибору кількості контрольних символів, а це робиться так само як і для будь-якого групового коду, що виправляє поодинокі помилку:

$$r = \log_2(n + 1)$$

або

$$r = \lfloor \log_2((k + 1) + \lfloor \log_2(k + 1) \rfloor) \rfloor.$$

У табл. 5.3 наведені всі примітивні незвідні поліноми і їх двійкові еквіваленти до сьомого степеня включно.

Таким чином, розглянуті загальні принципи перешкодостійкого кодування а також найбільш поширені класи циклічних блокових кодів показують, що процес виявлення і виправлення помилок може бути просто реалізований шляхом порівняння ухваленої комбінації зі всіма дозволеними. Незбіг ухваленої комбінації ані з однією з дозволених свідчить про наявність помилок. Виправлення помилок зводиться до знаходження найближчої до ухваленої дозволеної комбінації.

Проте, така процедура навіть при помірних значеннях n вимагає пам'яті з об'ємом, який не завжди може бути реалізований (складність пропорційна 2^n).

Основний напрям опрацювання теорії перешкодостійкого кодування

полягає у пошуку таких кодів, для яких відбір різних кодових комбінацій, виявлення і виправлення помилок здійснювалися б не шляхом перебору, а за допомогою достатньо простих регулярних правил, які можуть бути реалізовані технічно з невеликими (мінімальними) апаратними витратами.

Таблиця 5.3

Примітивні незвідні поліноми і їх двійкові еквіваленти

Примітивні незвідні поліноми	Двійкові еквіваленти	Примітивні незвідні поліноми	Двійкові еквіваленти
$x + 1$	11	$x^6 + x^5 + x^2 + x + 1$	1100111
$x^2 + x + 1$	111	$x^6 + x^5 + x^4 + x + 1$	1110011
$x^3 + x + 1$	1011	$x^6 + x^5 + x^3 + x^2 + 1$	1101101
$x^3 + x^2 + 1$	1101	$x^6 + x^4 + x^3 + x + 1$	1011011
$x^4 + x + 1$	10011	$x^7 + x^3 + 1$	10001001
$x^4 + x^3 + 1$	11001	$x^7 + x + 1$	10000011
$x^5 + x^2 + 1$	100101	$x^7 + x^3 + x^2 + x + 1$	10001111
$x^5 + x^3 + 1$	101001	$x^7 + x^6 + x^4 + x^2 + 1$	11010101
$x^5 + x^4 + x^2 + x + 1$	110111	$x^7 + x^4 + x^3 + x^2 + 1$	10011101
$x^5 + x^4 + x^3 + x + 1$	111011	$x^7 + x^6 + x^3 + x + 1$	11001011
$x^5 + x^4 + x^3 + x^2 + 1$	111101	$x^7 + x^6 + x^5 + x^2 + 1$	11100101
$x^5 + x^3 + x^2 + x + 1$	101111	$x^7 + x^6 + x^5 + x + 1$	11100011
$x^6 + x + 1$	1000011	$x^7 + x^5 + x^4 + x^3 + x^2 + x + 1$	10111111
$x^6 + x^5 + 1$	1100001	$x^7 + x^6 + x^3 + x + 1$	11001011

Циклічність перестановок при формуванні дозволених кодових комбінацій циклічного коду лежить в основі техніки побудови кодуєчих і декодуєчих пристроїв циклічних кодів. Ця техніка застосовує регістри зсуву у вигляді тригерних ланцюжків з тими або іншими зворотними зв'язками. Такі регістри зсуву називають також багатотактними лінійними перемикальними схемами або фільтрами Хаффмана.

Для побудови лінійних послідовних схем використовуються такі види елементарних пристроїв.

1. Суматор, що має, як правило, два входи й один вихід, при цьому для двійкових кодів підсумовування здійснюється за модулем 2 (рис. 5.2, а).
2. Запам'ятовуючий пристрій, що має один вхід і один вихід і являє собою одну тригерну чарунку (один розряд) регістра зсуву (рис. 5.2, б).
3. Пристрій множення на постійну величину, що має один вхід і один вихід (рис. 5.2, в).

Лінійними перемикальними схемами з кінцевою кількістю станів на-

зиваються будь-які схеми, що містять кінцеву кількість суматорів, пристроїв пам'яті та пристроїв множення на константу, з'єднаних будь-яким припустимим засобом.

Пристрої затримки, що включені послідовно, складають регістр зсуву, в чарунках якого вихідний символ збігається з вхідним символом у попередній момент часу. На регістр зсуву також надходять тактові імпульси, за допомогою яких здійснюється просування по розрядах записаної кодової інформації. Як правило, ланцюги подачі тактових імпульсів на схемах не показують.

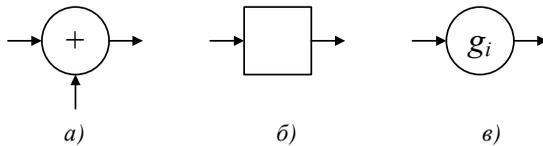


Рис. 5.6. Елементарні пристрої, що використовуються для побудови лінійних перемикальних схем

При формуванні й обробці двійкових циклічних кодів введення в схему помножувача на константу, що дорівнює 1, еквівалентно введенню додаткового з'єднання, а помножувач на константу, що дорівнює 0, відповідає відсутності такого з'єднання.

Передбачається, що на вхід регістра зсуву, що входить до складу лінійної послідовної схеми, кодова комбінація подається послідовно з періодичністю, що дорівнює періоду проходження тактових імпульсів. Аналогічно, послідовно за часом, з'являються кодові символи на виході регістра зсуву. Коли входом або виходом є поліном, що представляє при двійковій обробці набір 1 і 0 , то на вхідному або вихідному кінці регістра зсуву з'являються тільки коефіцієнти 1 або 0 , починаючи з коефіцієнтів вищих порядків. Це обумовлюється тим, що при діленні у дільника спочатку повинні бути оброблені коефіцієнти вищих порядків.

Розглянемо схеми множення та ділення будь-яких поліномів на деякий фіксований поліном.

Перший варіант лінійної послідовної схеми для множення поліномів зображений на рис. 5.7. Схема використовується для множення будь-якого полінома на вході $A(x) = a_0 + a_1x + a_2x^2 + \dots + a_kx^k$ на фіксований поліном $G(x) = g_0 + g_1x + g_2x^2 + \dots + g_rx^r$.

Передбачається, що спочатку всі розряди регістра зсуву містять нулі,

а на вхід надходять коефіцієнти полінома $A(x)$, починаючи з коефіцієнтів вищих порядків (зі старших розрядів), після чого надходить r нулів.

Добуток поліномів можна записати у такому вигляді:

$$A(x)G(x) = a_0g_0 + (a_0g_1 + a_1g_0)x + \dots + a_kg_r x^{k+r}. \quad (5.9)$$

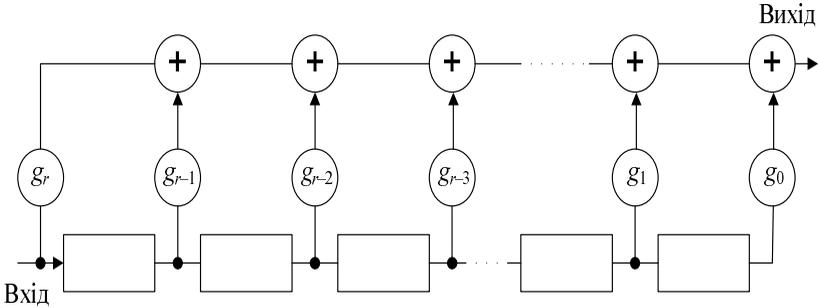


Рис. 5.5. Схема множення поліномів (перший варіант)

Коли на вході схеми з'являється перший (старший) коефіцієнт полінома $A(x)$, то він помножить в першому пристрої множення на g_r і з'явиться на виході вже як результат множення $a_k g_r$, пройшовши через всі схеми додавання за модулем 2. Крім того, a_k запишеться в перший розряд регістра зсуву, а всі інші розряди будуть містити нулі.

Через одиницю часу, з появою наступного тактового імпульсу, на вході з'явиться a_{k-1} , що перемножить з g_r і додається в першій схемі додавання за модулем 2 з $a_k g_{r-1}$, сформувавши на виході суму $a_{k-1}g_r + a_k g_{r-1}$, тобто другий коефіцієнт добутку $A(x)G(x)$. Подальші операції здійснюються аналогічно. Після $r+k$ зсувів регістр зсуву повністю обнуляється і на виході з'являється значення $a_0 g_0$, яке дорівнює першому коефіцієнту добутку (5.9).

Розглянемо тепер другий варіант лінійної послідовної схеми для множення поліномів (рис. 5.8).

У цьому варіанті коефіцієнти добутку формуються безпосередньо в регістрі зсуву. Після того, як перший символ буде поданий на вхід, на виході з'явиться останній коефіцієнт (5.9) $a_k g_r$, а розряди регістра зсуву будуть містити тільки нулі. Після одного зсуву чарунки регістра містять елементи $a_k g_0, a_k g_1, \dots, a_k g_{r-1}$, а вхід дорівнює a_{k-1} . При цьому вихід

регістра дорівнює $a_k g_{r-1} + a_{k-1} g_r$, тобто дорівнює другому коефіцієнту (5.9). Після появи чергового тактового імпульсу на виході схеми з'являється третій коефіцієнт (5.9). Подальші операції здійснюються аналогічно.

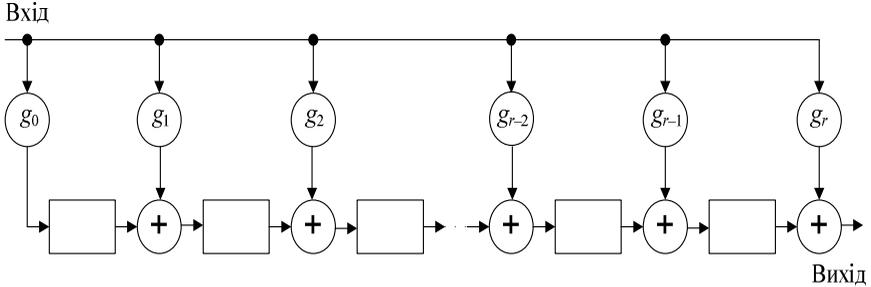


Рис. 5.8. Схема множення поліномів (другий варіант)

Схеми множення можуть мати більше, ніж один вхід, якщо додати до схеми, зображеної на рис. 5.8, другий ланцюжок пристроїв множення, пов'язаних з відповідними схемами додавання за модулем 2. Тоді схема буде реалізовувати процедуру додавання добутків двох пар поліномів:

$$C(x) = A_1(x)G_1(x) + A_2(x)G_2(x),$$

при цьому запам'ятовувальний пристрій у вигляді регістра зсуву буде тільки один (рис. 5.9.).

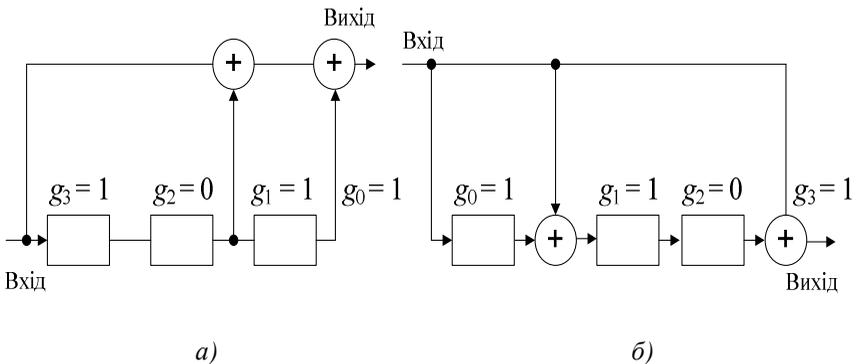


Рис. 5.9. Схеми множення поліномів для кодуючих пристроїв циклічного (7, 4) коду: перший варіант (а), другий варіант (б)

Приклад 5.3.

Побудувати схеми множення поліномів (за двома розглянутими варіантами) для кодуючих пристроїв циклічного (7, 4) коду. Як породжувальний поліном будемо використовувати поліном $G(x) = x^3 + x + 1$.

Застосування в кодерах методу множення призводить до формування нероздільних циклічних кодів. Тому для побудови кодеру використовують ділення поліномів на базі лінійних послідовних схем.

Перший варіант схеми ділення полінома

$$A(x) = a_0 + a_1x + a_2x^2 + \dots + a_kx^k$$

на поліном

$$G(x) = g_0 + g_1x + g_2x^2 + \dots + g_kx^k$$

зображений на рис. 5.10.

У вихідному стані всі чарунки регістра зсуву містять нулі. Для ділення поліномів регістр охоплений зворотним зв'язком, тобто вихід регістра з'єднується з входом.

Для перших r зсувів, тобто доти, поки перший вхідний символ не досягне кінця регістра зсуву, вихід приймає значення θ . Після цього на виході з'являється перший ненульовий вихідний сигнал, що дорівнює $a_k g_r$ – першому коефіцієнту частки. Для кожного коефіцієнта частки g_j необхідно відняти від діленого поліном $G(x)$. Це віднімання здійснюється за допомогою зворотного зв'язку. Після k зсувів на виході регістра з'явиться частка від ділення, а лишок від ділення буде знаходитися у чарунках регістра зсуву.

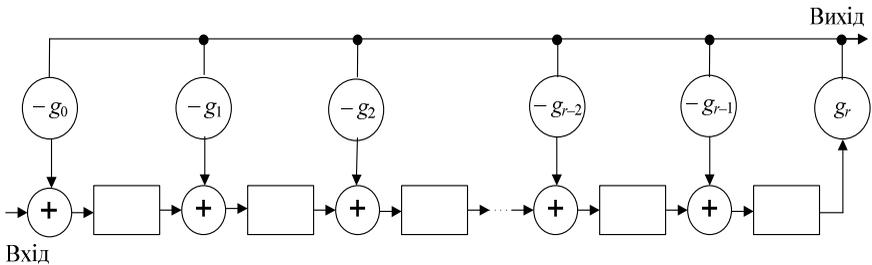


Рис. 5.10. Схема ділення поліномів (перший варіант)

При побудові кодуючих пристроїв циклічних кодів, а також генераторів різних кодових послідовностей, зокрема, послідовностей максимальної

довжини (M -послідовностей), застосовується в ряді випадків так званий генераторний поліном $H(x)$. Цей поліном називають також перевірочним, якщо він утворюється при діленні бінома $1 + x^n$ на породжувальний поліном $G(x)$

$$H(x) = \frac{1 + x^n}{G(x)}. \quad (5.10)$$

Другий варіант схеми ділення зображений на рис. 5.11.

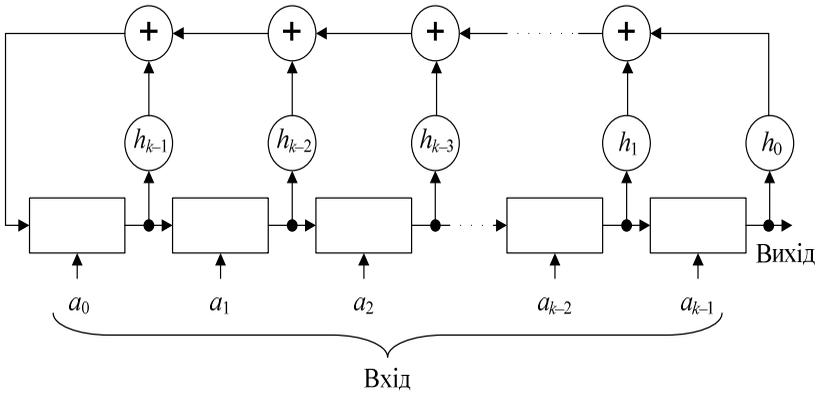


Рис. 5.11. Схема ділення поліномів (другий варіант)

При використанні цієї схеми, як кодуючого пристрою циклічного коду вихідну кодову комбінацію $A(x)$ записують паралельно в k розрядів регістра зсуву.

З першим тактом на вихід буде виданий коефіцієнт $b_{n-1} = a_{k-1}$, відбудеться зсув вправо в регістрі і в чарунку пам'яті, що звільниться, буде записане обчислене значення перевірного біта

$$r_{n-k-1} = h_0 a_{k-1} + h_1 a_{k-2} + \dots + h_{k-1} a_0.$$

З другим тактом на виході буде зчитаний коефіцієнт $b_{n-2} = a_{k-2}$, відбудеться зсув і в першу чарунку регістра, що звільнилася, запишеться другий перевірочний біт $r_{n-k-2} = h_0 a_{k-2} + h_1 a_{k-3} + \dots + h_{k-1} r_{n-k-1}$. Через $n-k$ тактів будуть обчислені всі $n-k$ перевірочних символів $r_0, r_1, \dots, r_{n-k-1}$ і записані в регістр зсуву. Після k тактів, тобто після виводу на вихід всіх інформаційних символів, стануть виводитися перевірочні

символи в тій же порядку, у якому вони обчислювалися. На виході утворюється блоковий код. Після k тактів процес кодування однієї комбінації $A(x)$ закінчується і регістр зсуву приймає вихідний стан. Для кодування наступної комбінації необхідно стерти $A(x)$, ввести в регістр нову кодову комбінацію $A_j(x)$ і повторити цикл із n тактів.

Розглянемо конкретніше роботу цієї схеми на прикладі використання її як кодуючого пристрою циклічного коду. Для цього:

1) побудуємо схему кодуючого пристрою циклічного $(7, 4)$ коду з породжувальним поліномом $G(x) = 1 + x + x^3$, шляхом обчислення блока перевірочних символів, використовуючи перевірочний поліном $H(x)$;

2) простежимо потактно процес кодування і стан елементів схеми при кодуванні вхідної комбінації $1001 - A(x) = 1 + x^3$.

Побудова схеми кодуючого пристрою визначається перевірочним поліномом (5.10)

$$H(x) = \frac{1 + x^7}{1 + x + x^3} = 1 + x + x^2 + x^4.$$

Так як $k = 4$, то кількість розрядів регістра зсуву дорівнює чотирьом. З вигляду перевірочного полінома визначаємо, що $h_0 = h_1 = h_2 = h_4 = 1$, $h_3 = 0$. Схема кодуючого пристрою для умов прикладу, що розглядається, зображена на рис. 5.12. Стан чарунок регістра зсуву й виходу схеми потактно показано у табл. 5.4.

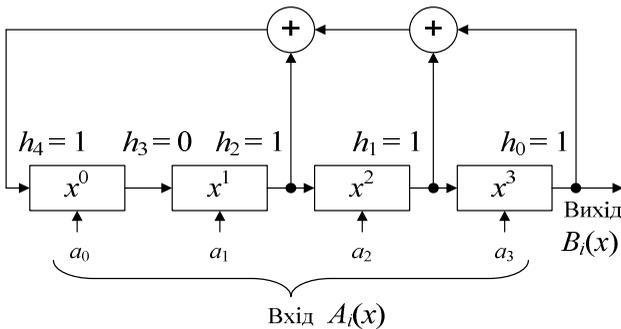


Рис. 5.12. Схема кодеру циклічного $(7, 4)$ коду

У вихідному стані в чарунки регістра зсуву записуються інформаційні символи $A(x) = 1 + x^3 \rightarrow 1001$. З огляду на наявність зворотного зв'язку в 208

регістрі, додавання за модулем 2 виходів чарунок x^1 , x^2 і x^3 дасть символ запису в чарунку x^0 .

Після першого зсуву в чарунку x^0 буде записаний символ перевірконої групи r_1 , що при наступних зсувах надійде на вихід регістра. З табл. 5.1 видно, що після $n = 7$ тактів, на виході утвориться комбінація **0111001** (старший розряд попереду).

При цьому чарунки регістра зсуву приймають вихідне значення **1001** і при необхідності можливе повторення процедури кодування цієї ж кодової комбінації $A(x)$ шляхом подачі чергових $n = 7$ тактів. Таким чином, цей спосіб кодування так само, як і перший варіант схеми для ділення поліномів, забезпечує одержання кодових комбінацій роздільного циклічного коду. Крім того, подібна лінійна послідовна схема може бути використана для генерації певної кодової комбінації, зокрема, M -послідовностей.

Таблиця 5.4

Стани чарунок регістра зсуву й виходу для схеми кодеру циклічного (7, 4) коду

Номер такту	Стан чарунок				Вихід
	x^0	x^1	x^2	x^3	
$A(x)$	1	0	0	1	–
1	1	1	0	0	1
2	1	1	1	0	0
3	0	1	1	1	0
4	1	0	1	1	1
5	0	1	0	1	1
6	0	0	1	0	1
7	1	0	0	1	0

Розгляд варіантів побудови схем, що виконують операції множення та ділення поліномів, з метою використання в кодах циклічних кодів, дозволяє зробити такі висновки.

1. У кодуючих пристроях циклічних кодів процедура множення поліномів призводить до одержання нероздільних кодів, що ускладнює їх наступне декодування. Тому операція множення рідко використовується в пристроях формування й обробки циклічних кодів.

2. При діленні на породжувальний поліном $G(x)$, код на виході кодуємого пристрою виходить роздільним і регістр зсуву містить r розрядів. Якщо в більшості випадків використовуються коди, у яких кількість пере-

Приклад 5.4.

Побудувати схему кодуючого пристрою, що забезпечує кодування циклічного(7, 4) коду з породжувальним поліномом $G(x) = 1 + x + x^3$, шляхом визначення перевірконої групи методом ділення поліномів і визначення лишка $R(x)$. Простежити за тактами процес кодування та стани елементів схеми при кодуванні вихідного полінома $A(x) = 1 + x^3 \rightarrow 1001$. Схема кодера для умов прикладу зображена на рис. 5.13, а стани чарунок регістра зсуву та виходу для схеми кодера потактно наведені у табл. 5.5.

Таблиця 5.5

Стани чарунок регістра зсуву та виходу для схеми кодера циклічного (7, 4) коду

Номер такту	Вхід	Стан					
		чарунок			ключів		
		x^0	x^1	x^2	Вихід	&1	&2
0	–	0	0	0	–		
1	1	1	1	0	1		
2	0	0	1	1	0	Замкнутий	Розімкнутий
3	0	1	1	1	0		
4	1	0	1	1	1		
5	–	0	0	1	1		
6	–	0	0	0	1	Розімкнутий	Замкнутий
7	–	0	0	0	0		

Поряд з відзначеними особливостями побудови кодуючої схеми пристрій доповнений двома ключовими схемами, роль яких виконують схеми логічного множення (схеми **&1** – **&1** і **&2**, відповідно). Протягом перших $k = 4$ тактів на другий вхід схеми **&1** надходять тактові імпульси (ТІ), забезпечуючи проходження символів від вихідного суматора в ланцюг зворотного зв'язку регістра. З 5-го по 7-й такти тактові імпульси на другий вхід схеми **&1** не надходять. При цьому зворотний зв'язок розривається. У цей час тактові імпульси надходять на другий вхід схеми **&2**, завдяки чому вихід регістра зсуву підключається до виходу всього кодуючого пристрою, забезпечуючи видачу лишка від ділення кодової комбінації $A(x)$ на породжувальний поліном $G(x)$ на вихід для підставлення перевірочних символів до $A(x)$.

З табл. 5.5 видно, що після 4-го такту в регістрі зсуву утвориться залишок 011 , тобто $R(x) = x + x^2$, а протягом n тактів на вихід надходить кодова комбінація $0111001 \rightarrow x + x^2 + x^3 + x^6$ (старшим розрядом уперед).

При апаратній реалізації декодерів циклічного коду для визначення синдрому використовують схему, що здійснює процедуру ділення полінома на поліном. Схема декодера циклічного $(7, 4)$ коду зображена на рис. 5.14. При побудові декодуючих пристроїв треба додатково включити запам'ятовуючий пристрій (буферний регістр) на k елементів і схему опитування залишку при діленні.

Ця схема складається зі схеми логічного додавання (АБО) на r входів і схеми логічного множення на два входи. Регістр зсуву та зворотні зв'язки повинні відповідати структурі породжувального полінома $G(x)$, тобто кількість чарунок регістра повинна дорівнювати r , а замкнутий зворотний зв'язок повинен відповідати не нульовим коефіцієнтам полінома $G(x)$.

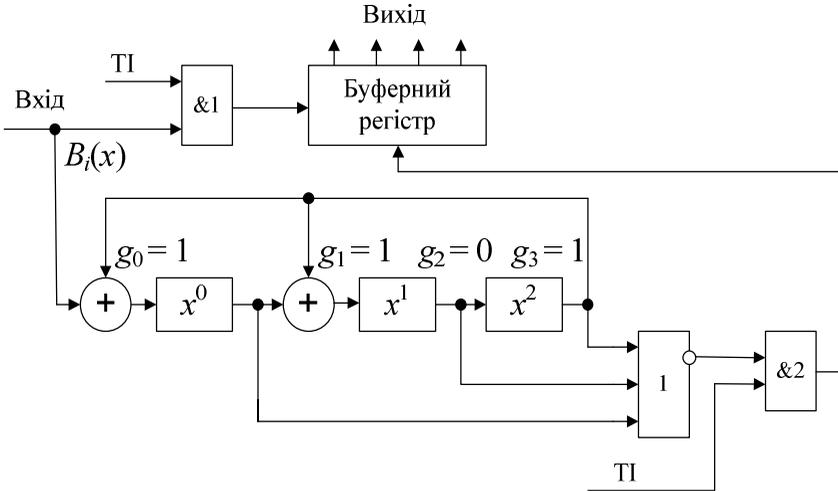


Рис. 5.14. Схема декодера циклічного $(7, 4)$ коду

Розглянемо приклад. Побудувати схему декодуючого пристрою циклічного $(7, 4)$ коду з породжувальним поліномом $G(x) = 1 + x + x^3$ і за тактами імпульсів, що зсувають, проаналізувати його роботу. Схема декодуючого пристрою повинна вирішувати завдання виявлення помилок.

У табл. 5.6 надані стани чарунок регістра при декодуванні вхідної кодової комбінації $B_i(x) = x + x^2 + x^3 + x^6 \rightarrow 0111001$, прийнятої без помилок.

Декодуєчий пристрій працює так. Кодова комбінація $B_i(x)$ старшим розрядом уперед надходить на регістр зсуву для визначення лишка від ділення її у запам'ятовувальний пристрій на k елементів через відкриту схему &1, що через k тактів закривається, тому що припиняється подача тактових імпульсів на один із входів схеми &1. При цьому в запам'ятовуючому пристрої запам'ятовуються k інформаційних символів прийнятої кодової комбінації $B_i(x)$.

У регістр зсуву надходять усі n елементів $B_i(x)$, і після n тактів відбувається опитування стану чарунок регістра шляхом подачі циклового імпульсу на схему &2. Якщо $R(x) \neq 0$, то на виході схеми &2 імпульс не з'явиться і зчитування з запам'ятовуючого пристрою прийнятих інформаційних символів не відбудеться. Якщо $R(x) = 0$, то імпульс, що з'явиться на виході &2, дозволяє передати $A(x)$ на вихід і видати чотири інформаційні біти одержувачеві повідомлень.

Таблиця 5.6

Стани чарунок регістра зсуву при декодуванні вхідної кодової комбінації 0111001

Вхід $B(x)$	Номер такту	Стан чарунок			Вихід регістра
		x^0	x^1	x^2	
–	Початковий стан	0	0	0	–
1	1	1	0	0	0
0	2	0	1	0	0
0	3	0	0	1	0
1	4	0	1	0	1
1	5	1	0	1	0
1	6	0	0	0	1
0	7	0	0	0	0

Для виправлення помилок схема декодуєчого пристрою ускладнюється. Інформацію про розряди, у яких відбулася помилка містить синдром, що одержаний у результаті ділення поліномів. Схема декодера з виправленням помилок зображена на рис. 5.15.

Символи кодової комбінації, що містять помилку, послідовно, починаючи зі старшого розряду, вводяться в n -розрядний буферний регістр

зсуву й одночасно в схему обчислювача синдрому, де за n тактів ділення обчислюється лишок, що у випадку синхронної неперервної передачі кодівих комбінацій відразу ж переписується в аналогічний регістр схеми аналізатора синдрому.

До складу схеми аналізатора синдрому може входити постійний запам'ятовуючий пристрій, у якому записані всі можливі конфігурації синдромів з відповідними їм векторами помилок. Кодові комбінації векторів помилок містять "одиничні" символи на тих позиціях, які в процесі передачі повідомлення по каналу зв'язку виявилися спотвореними перешкодами.

Локаатор помилок (визначник місця помилок) являє собою комбінаторно – логічну схему, що видає на вихід одиничні символи в ті моменти часу, коли кожний з помилкових символів прийнятої кодової комбінації займає в буферному регістрі крайню праву чарунку. При наступному тактовому зсуві локаатор помилки формує символ 1 , що надходить на суматор за модулем 2 , де виправляється спотворений символ.

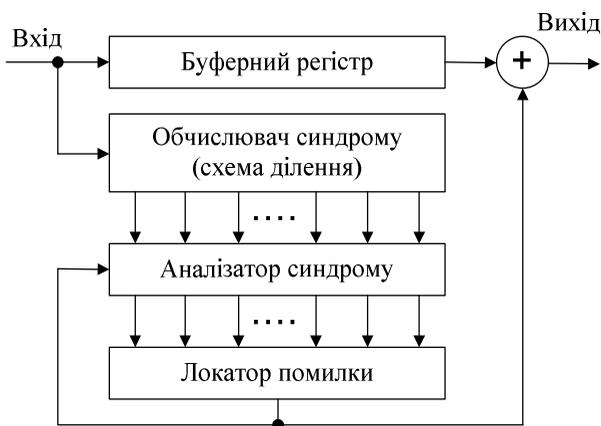


Рис. 5.15. Схема декодера з виправленням помилок

Одночасно по ланцюгу зворотного зв'язку з виходу локаатора помилки подається одиничний символ на аналізатор синдрому, що в ряді конкретних схемних рішень спрощує його побудову. Складність аналізатора синдрому й локаатора помилки залежить від числа помилок, що виправляються. Ясно, що найпростіші схемні рішення утворюються при обробці кодів, розрахованих на виправлення одиночних помилок.

Як видно з розгляду логіки роботи схеми декодера, найбільш склад-

ною його частиною є необхідність запам'ятовування заздалегідь обчислених синдромних поліномів і відповідних їм векторів помилок. Достойнством циклічних кодів є те, що аналізатор синдрому можна значно спростити, скориставшись алгебраїчною структурою коду для відшукування зв'язків між синдромами при великій кількості помилок, що виправляються.

5.6. Згортувальні перешкодостійкі коди

При використанні для захисту від помилок блокових кодів інформаційна послідовність розбивається на окремі блоки, що кодуються незалежно один від одного. Таким чином, закодована послідовність стає послідовністю незалежних слів однакової довжини.

При використанні згортувальних кодів потік даних розбивається на набагато менші блоки довжиною k символів (в окремому випадку $k_0 = 1$), які називаються *кадрами інформаційних символів*.

Кадри інформаційних символів кодуються кадрами кодових символів довжиною n_0 символів. При цьому кодування кадру інформаційних символів у кадр кодового слова здійснюється з урахуванням попередніх m кадрів інформаційних символів. Процедура кодування, таким чином, зв'язує між собою послідовні кадри кодових слів. Передана послідовність стає одним напівнескінченим кодовим словом.

Основними характеристиками згортувальних кодів є такі величини:

- – k_0 – розмір кадру інформаційних символів;
- – n_0 – розмір кадру кодових символів;
- – m – довжина пам'яті коду;
- – $k = (m + 1)k_0$ – інформаційна довжина слова;
- – $n = (m + 1)n_0$ – кодова довжина блока.

Кодова довжина блока – це довжина кодової послідовності, на якій зберігається вплив одного кадру інформаційних символів.

Нарешті, згортувальний код має ще один важливий параметр – *швидкість* $R = k / n$, що характеризує ступінь надмірності коду, яка вводиться для забезпечення виправляючих властивостей коду.

Як і блокові, згортувальні коди можуть бути систематичними і несистематичними й визначаються як лінійні згортувальні (n, k) коди.

Систематичним згортувальним кодом є такий код, для якого у вхідній послідовності кодових символів утримується без зміни послідовність інформаційних символів. У протилежному випадку згортувальний код є несистематичним.

Згортувальні коди мають дуже просту схему кодування. Інформаційні символи послідовно надходять у реєстр зсуву, при цьому кодові символи являють собою суму за модулем 2 вмісту чарунок пам'яті реєстра зсуву й вхідних символів. Приклади схем кодерів для систематичного (8, 4) й не-систематичного (6, 3) згортувальних кодів зображені на рис. 5.16.

Можливі різні способи опису згортувальних кодів, наприклад, за допомогою породжувальної матриці. Правда, із-за нескінченності послідовності, що кодується, й породжувальна матриця буде мати нескінченні розміри.

Більш зручним способом опису згортувального коду є його завдання за допомогою імпульсної перехідної характеристики еквівалентного фільтра Хаффмана (лінійної послідовної схеми або реєстра зсуву зі зворотними зв'язками) або відповідного йому породжувального полінома.

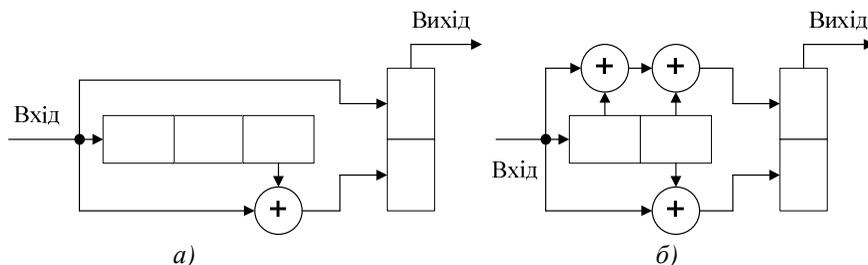


Рис. 5.16. Приклади схем кодерів для (8, 4) систематичного (а) і (6, 3) несистематичного (б) згортувальних кодів

Імпульсна перехідна характеристика фільтра (а кодер згортувального коду, по суті є фільтром) – це реакція на одиничний вплив вигляду $\bar{\delta} = 100000 \dots$. Для кодерів, що зображені на рис. 5.16, імпульсні характеристики будуть мати вигляд

$$h_1 = 11\ 00\ 00\ 01\ 00\ 00 ;$$

$$h_2 = 11\ 10\ 11\ 00\ 00\ 00 .$$

Ще одна форма завдання згортувальних кодів – це використання породжувальних поліномів, однозначно пов'язаних з імпульсною перехідною характеристикою еквівалентного фільтра,

$$h_1(x) = 1 + x + x^7 ;$$

$$h_2(x) = 1 + x + x^2 + x^4 + x^5 .$$

При цьому кодова послідовність U на виході згортувального кодера утворюється у результаті згортки вхідної інформаційної послідовності m з імпульсною перехідною характеристикою h .

Розглянемо приклади кодування послідовностей з використанням імпульсної характеристики еквівалентного фільтра.

Приклад 5.5.

Нехай $m = 110 \dots$, тоді для кодера з імпульсною перехідною характеристикою $h = 110000010000 \dots$:

$$\begin{array}{r} U = 110000010000 \dots \\ \underline{ 1100000100 \dots} \\ U = 11110001010000 \dots, \end{array}$$

або $m = 1011000 \dots$:

$$\begin{array}{r} U = 11000001000000 \dots \\ 1100000100 \dots \\ \underline{ 11000001 \dots} \\ U = 1100111000010100 \dots, \end{array}$$

Іноді зручніше розглядати повний породжувальний поліном $G(x)$ згортувального коду як сукупність декількох поліномів менших ступенів, що відповідають чарункам вихідного регістра кодера. Так, для кодера на рис. 5.17 відповідні часткові породжувальні поліноми будуть такими:

$$\begin{aligned} G_1(x) &= 1 + x + x^2; \\ G_2(x) &= 1 + x^2. \end{aligned}$$

Приклад 5.6.

Нехай, наприклад, кодується послідовність $m = 1010 \dots$. Відповідний інформаційний поліном запишеться як $m(x) = 1 + x^2$.

Тоді на вході першої чарунки вихідного регістра при кодуванні буде послідовність $U_1 = 11011000 \dots$, якій відповідає поліном $U_1(x) = 1 + x + x^3 + x^4$, а на вході другої чарунки буде послідовність $U_2 = 10001000 \dots$ і, відповідно, поліном $U_2(x) = 1 + x^4$.

Легко помітити, що при цьому справедливі рівності

$$\begin{aligned} U_1(x) &= m(x)G_1(x); \\ U_2(x) &= m(x)G_2(x). \end{aligned}$$

Така форма запису зручна, оскільки видно структуру пристрою, що кодує (за набором поліномів можна відразу синтезувати пристрій). На

практиці поліноми задаються набором своїх коефіцієнтів. У табл. 5.7 наведені приклади кодерів згортувальних кодів, заданих своїми коефіцієнтами при ступенях породжувальних поліномів.

Таблиця 5.7.

Коефіцієнти породжувальних поліномів деяких згортувальних кодів

G_1	G_2
111	101
1111	1101
11101	10011
111011	1010011
110001	11111001

Як приклад кодера з $k_0 \neq 1$ можна привести кодер згортувального (12, 9) коду Вайнера – Еша з параметрами: $k_0 = 3$, $n_0 = 4$, $k = 9$, $n = 12$, $R = 3/4$, що зображений на рис. 5.17.

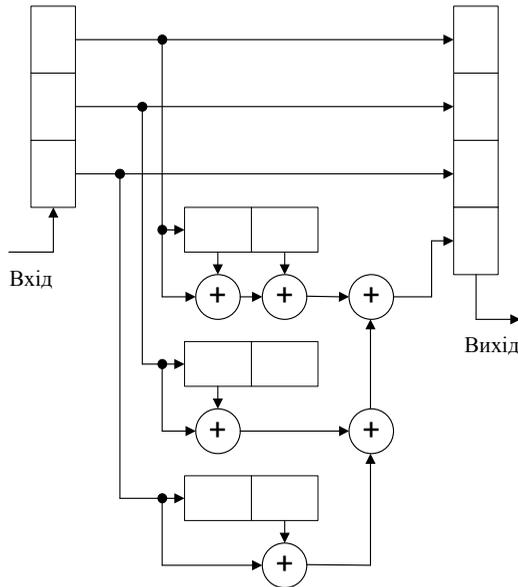


Рис. 5.17. Схема кодера згортувального (12, 9) коду Вайнера – Еша

Приклад 5.7.

Нехай, наприклад, $m = 100\ 000\ 000 \dots$. Тоді кодове слово $U = 1001\ 0001\ 0001\ 0000$. Видно, що це – систематичний код, у якому до трьох інформаційних символів додається один перевірочний, залежний від значень інформаційних символів не тільки поточного кадру, але й двох попередніх кадрів. При цьому вплив одного кадру інформаційних символів поширюється на 12 символів кодової послідовності, тобто кодова довжина блоку для цього коду $n = 12$.

Ще одним способом опису й ілюстрації роботи згортувальних кодів є використання так званого кодового дерева.

Розглянемо згортувальний (6, 3) код зі схемою, зображеною на рис. 5.16, б. Відповідне цьому кодеру кодове дерево – послідовність вихідних станів кодера при подачі на його вхід ланцюжка вхідних символів 0 і 1 – зображене на рис. 5.18.

На діаграмі рис. 5.18 зображені вхідні та вихідні послідовності кодера: вхідні — напрямком руху по дереву (нагору – 0 , униз – 1), вихідні — символами уздовж ребер дерева. При цьому кодування складається в прямованні вправо по кодовому дереву.

Наприклад, вхідна послідовність $m = 01000 \dots$ кодується як $U = 0011101100000 \dots$, послідовність $m = 1010100000 \dots$ – як $U = 1110001000 \dots$.

Якщо уважно подивитися на будову зображеного на рис. 5.18 кодового дерева, можна помітити, що починаючи з четвертого ребра його структура повторюється, тобто яким би не був перший крок, починаючи з четвертого ребра значення вихідних символів кодера повторюються. Однакові ж вузли можуть бути об'єднані, і тоді починаючи з деякого перетину розмір кодового дерева перестане збільшуватися.

Інакше кажучи, вихідна кодова послідовність у певний момент перестає залежати від значень вхідних символів, введених у кодер раніше.

Дійсно, з рис. 5.18 видно, що, коли третій вхідний символ вводиться у кодер, перший вхідний символ залишає регістр зсуву і не зможе надалі впливати на вихідні символи кодера.

З урахуванням цього необмежене кодове дерево, зображене на рис. 5.18, переходить в обмежену ґратчасту діаграму (кодове дерево з вузлами, що зливаються), зображену на рис. 5.19.

Кодування згортувальним кодами з використанням ґратчастої діаграми, як і у випадку з кодовим деревом, являє собою надзвичайно просту процедуру: чергові символи вхідної послідовності визначають напрямки руху з вузлів ґрат: якщо 0 , то йдемо по верхньому ребру, якщо 1 – по ниж-

ньому ребру. Однак, на відміну від кодового дерева гратчаста діаграма не розростається по ширині з кожним кроком, а має, починаючи з третього перетину, постійну ширину.

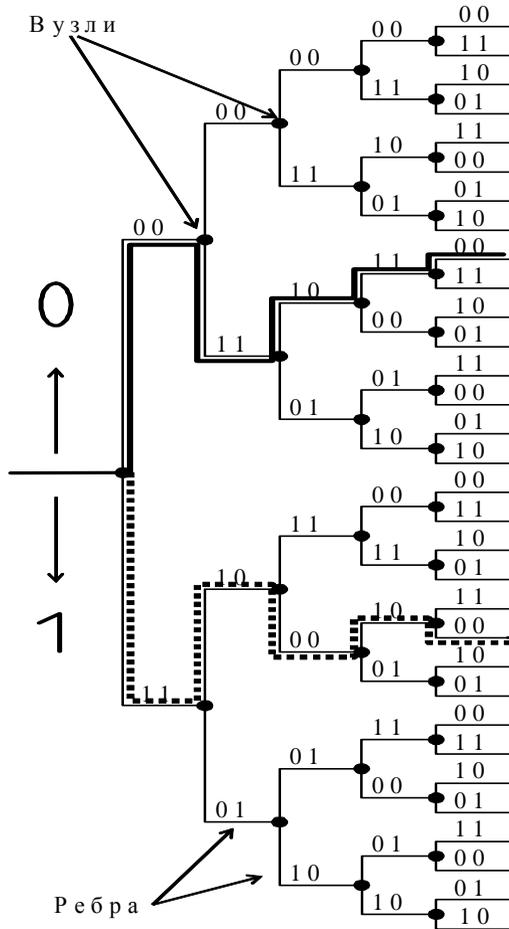


Рис. 5.18. Кодове дерево згортувального (6, 3) коду

Як приклад, закодуємо за допомогою гратчастої діаграми кілька інформаційних послідовностей.

Нехай $m = 0110000 \dots$. Відповідна їй кодова послідовність буде мати

вигляд $U = 001101011100 \dots$,

або $m = 110100 \dots$, тоді $U = 1101010010110000 \dots$

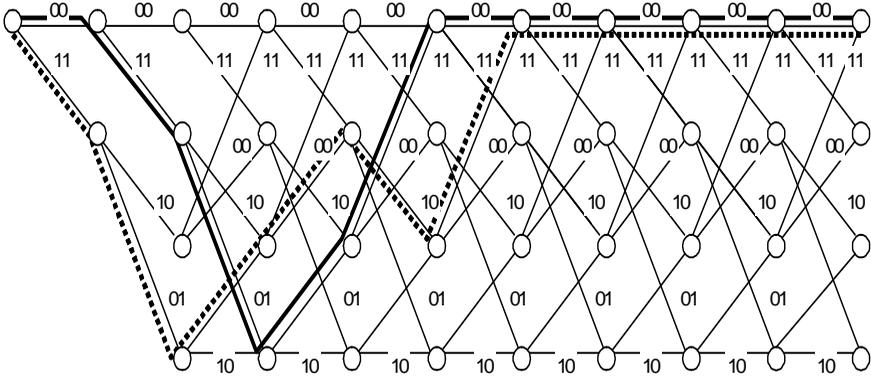


Рис. 5.19. Гратчаста діаграма згортувального $(6, 3)$ коду

Найкращою схемою декодування коригувальних кодів, як ми вже відзначали, є декодування методом максимальної правдоподібності.

Для двійкового симетричного каналу без пам'яті (каналу, у якому ймовірності передачі 0 і 1 , а також ймовірності помилок виду $0 \rightarrow 1$ і $1 \rightarrow 0$ однакові, помилки в j -му і i -му символах коду незалежні) декодер максимальної правдоподібності зводиться до декодера мінімальної відстані Хеммінга. Останній обчислює відстань Хеммінга між прийнятою послідовністю r і всіма можливими кодовими векторами U_i та виносить рішення на користь того вектора, що виявляється ближче до прийнятого.

Очевидно, що в загальному випадку такий декодер виявляється дуже складним і при великих розмірах кодів n і k практично нереалізованим. Характерна структура згортувальних кодів (повторюваність структури за межами вікна довжиною n) дозволяє створити цілком прийнятний за складністю декодер максимальної правдоподібності. Уперше ідея такого декодера була запропонована Вітербі. Працює він так.

Припустимо, на вхід декодера надійшов сегмент послідовності r довжиною b , що перевищує кодову довжину блока n . Назвемо b вікном декодування. Порівнюємо всі кодові слова цього коду (у межах сегмента довжиною b) з прийнятим словом і виберемо кодове слово, найближче до прийнятого. Перший інформаційний кадр обраного кодового слова приймемо як оцінку інформаційного кадру декодованого слова.

Після цього у декодер вводиться n_0 нових символів, а введені раніше самі старі n_0 символів скидаються, і процес повторюється для визначення наступного інформаційного кадру.

Таким чином, декодер Витербі послідовно обробляє кадр за кадром, рухаючись по ґратах, аналогічних тим, що використовуються кодером. У кожний момент часу декодер не знає, у якому вузлі перебуває кодер, і не намагається його декодувати. Замість цього декодер за прийнятою послідовністю визначає найбільш правдоподібний шлях до кожного вузла та відстань між кожним таким шляхом і прийнятою послідовністю. Ця відстань називається *мірою розходження шляху*. За оцінку прийнятої послідовності вибирається сегмент, що має найменшу міру розходження. Шлях з найменшою мірою розходження називається *шляхом, що вижив*.

Приклад 5.8.

Розглянемо роботу декодера Витербі на простому прикладі. Уважасмо, що кодування здійснюється з використанням згортувального (6, 3) коду (схема кодера зображена на рис. 5.16, б, ґратчаста діаграма, що відповідає цьому кодеру, – на рис. 5.19).

Користуючись ґратчастою діаграмою кодера, спробуємо, прийнявши деякий сегмент r , простежити найбільш імовірний шлях кодера. При цьому для кожного перетину ґратчастої діаграми будемо відзначати міру розходження шляху до кожного її вузла.

Припустимо, що передано кодову послідовність $U = 0000000 \dots$, а прийнята послідовність має вигляд $r = 10001000 00 \dots$, тобто в першому й у третьому кадрах кодового слова виникли помилки. Як ми вже переконалися, процедура та результат декодування не залежать від переданого кодового слова і визначаються тільки помилкою, що міститься у прийнятій послідовності. Тому найпростіше вважати, що передано нульову послідовність, тобто $U = 0000000 \dots$.

Прийнявши першу пару символів (10), визначимо міру розходження для першого перетину ґрат (рис. 5.19), прийнявши наступну пару символів (00), – для другого перетину й т.д. При цьому із вхідних у кожний вузол шляхів залишаємо шлях з меншим розходженням, оскільки шлях з більшим на цей момент розходженням вже не зможе стати надалі коротшим.

Помітимо, що для розглянутого прикладу, починаючи з четвертого рівня метрика (або міра розходження) нульового шляху менша будь-якої іншої метрики. Оскільки помилок у каналі більше не було, видно, що, зрештою як відповідь, буде обраний саме цей шлях. Із цього прикладу також видно, що шляхи, що вижили, можуть досить довго відрізнитися один від одного.

Однак, на шостому – сьомому рівні перші сім ребер всіх шляхів, що вижили, збігаються один з одним. У цей момент відповідно до алгоритму Витербі й приймається рішення про передані символи, тому що всі шляхи, що вижили, виходять із однієї вершини, тобто відповідають одному інформаційному символу. Процедура декодування послідовності, що має дві помилки, ілюструється послідовністю, зображеною на рис. 5.20.

Глибина, на якій відбувається злиття шляхів, що вижили, не може бути обчислена заздалегідь. Вона є випадковою величиною, що залежить від кратності й імовірності виникаючих у каналі помилок. Тому на практиці звичайно не чекають злиття шляхів, а встановлюють фіксовану глибину декодування.

З рис. 5.20, є видно, що ступінь розходження метрик правильного і неправильного шляхів досить велика ($d_{np} = 2$, $d_{ном} = 4$), тобто в цьому випадку можна було б обмежити глибину декодування величиною $b \leq 6$. На практиці глибину декодування звичайно вибирають у діапазоні $n \leq b \leq n + l$, де l – кількість помилок, що виправляється цим кодом.

З рис. 5.20 також видно, що, незважаючи на наявність у прийнятому фрагменті двох помилок, його декодування відбулося без помилки і як відповідь буде прийнята передана нульова послідовність.

Характеристики згортувальних кодів, як і будь-яких інших кодів, поліпшуються зі збільшенням їхнього розміру, у цьому випадку – кодової довжини блока n . При цьому, однак, декодер Витербі стає нереалізовано складним. Так, при $n = 10$ він повинен пам'ятати вже не менш $2^{10} = 1024$ шляхів, що виживуть.

Для зменшення складності декодера максимальної правдоподібності при великих n була розроблена стратегія, що ігнорує малоімовірні шляхи пошуку по ґратах. Однак рішення про те, щоб остаточно відкинути цей шлях, не приймається. Час від часу декодер повертається назад і продовжує залишений шлях.

Подібні стратегії пошуку найбільш імовірного шляху по ґратах відомі під загальною назвою послідовного декодування. На відміну від оптимальної процедури Витербі послідовний декодер, переглянувши перший кадр, переходить у черговий вузол решітки з найменшим на цей момент розходженням. Із цього вузла він аналізує наступний кадр, вибираючи ребро, найближче до цього кадра, і переходить у наступний вузол, і так далі.

При відсутності помилок ця процедура працює дуже добре, однак при виникненні помилок на якому-небудь кроці декодер може випадково вибрати неправильну гілку.

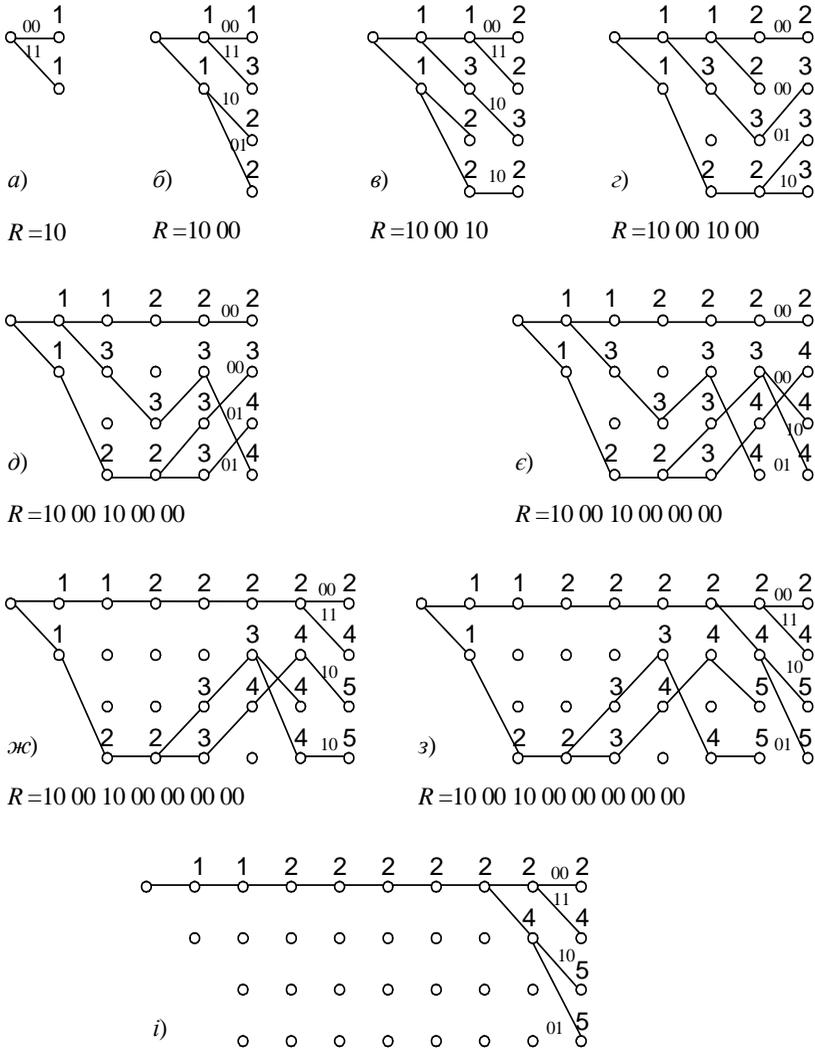


Рис. 5.20. Декодування декодером Витербі послідовності з двома помилками

Якщо він продовжить просуватися по неправильному шляху, то незабаром виявить, що відбувається занадто багато помилок, і розходження шляху почне швидко наростати. Але це будуть помилки декодера, а не

каналу. Тому декодер повертається на кілька кадрів назад і починає аналізувати інші шляхи, поки не знайде найбільш правдоподібний. Потім він буде просуватися уздовж цього нового шляху.

Загальним недоліком методу послідовного декодування є велика кількість повернень до попередніх вузлів, що збільшує час пошуку найбільш правдоподібного шляху. Вхідна послідовність при цьому для уникнення втрати даних повинна зберігатися в буферному регістрі. Через обмежений об'єм пам'яті регістра можливо його переповнення й відмова від декодування.

5.7. Підвищення достовірності передачі та обробки інформації в СОІУ з безнадмірним кодуванням

Підвищення достовірності в системах з безнадмірним кодуванням можна забезпечити шляхом багаторазової передачі однієї й тієї ж кодової комбінації. На приймальній стороні здійснюється порівняння або за символами кодових комбінацій, або за самими кодовими комбінаціями (посимвольна перевірка та групова перевірка) і рішення застосовується на користь таких символів або кодових комбінацій, які мають найбільшу кількість збігів (критерій більшості або мажоритарний принцип). Для того, щоб виключити невизначеність при прийманні, повідомлення в таких системах повинне передаватися не менше трьох разів. Дійсно, нехай по каналу передається кодова комбінація, що відповідає букві *A*. Якщо при першому прийманні ця буква прийнята правильно, а при другому прийомі замість букви *A* прийнята, наприклад, буква *M*, то виникає невизначеність і вибрати букву на підставі критерію більшості не вважається можливим. Якщо ж буква *A* буде передана третій раз і прийнята правильно, то на підставі критерію більшості вона й вибирається.

Безумовно, при сильних перешкодах не виключена можливість появи невизначеності і при трьох передачах, якщо щоразу кодові комбінації будуть декодуватися як різні букви (наприклад *A*, *M* або *B*). У цьому випадку невизначеність при триразовій передачі можна виключити шляхом п'ятиразової передачі.

Розглянемо методику визначення ймовірності помилкового декодування кодової комбінації при її багаторазовому повторенні.

Припустимо, що *n*-символьна комбінація передається три рази. На приймальній стороні здійснюється порівняння за комбінаціями (групова перевірка). Правильне рішення при триразовому повторенні виходить тоді, коли кодова комбінація всі три рази прийнята без помилок або коли вона прийнята без помилок два рази. Ймовірність першої події дорівнює

$(1 - P_{ном})^{3n}$. Імовірність другої події дорівнює

$$3(1 - P_{ном})^{2n} [1 - (P_{ном})^n],$$

де 3 – кількість варіантів, коли із трьох кодових комбінацій одна прийнята з помилкою;

$(1 - P_{ном})^{2n}$ – імовірність правильного прийняття двох кодових комбінацій;

$[1 - (P_{ном})^n]$ – імовірність помилкового прийняття однієї кодової комбінації.

Таким чином, імовірність того, що кодова комбінація при триразовому повторенні й груповій перевірці буде прийнята з помилкою, може бути знайдена за формулою:

$$P_{ном}(3) = 1 - (1 - P_{ном})^{3n} - 3(1 - P_{ном})^{2n} [1 - (P_{ном})^n].$$

У системах з посимвольною перевіркою здійснюється порівняння прийнятих комбінацій по символах. Значення символу (1 або 0) визначається по більшості. Так само, як і при груповому підсумовуванні, кількість передач повинна бути непарною.

При триразовій передачі кодовий символ буде зафіксований правильно, якщо він прийнятий без помилки всі три рази або двічі прийнятий без помилки, а один раз з помилкою. З урахуванням цього ймовірність правильного прийняття символу дорівнює

$$(1 - P_{ном})^3 + 3P_{ном}(1 - P_{ном})^2.$$

Отже, імовірність правильного прийому кодової комбінації, утвореної з n трьохсимвольних груп буде дорівнювати

$$P_{нр}(3) = \left[(1 - P_{ном})^3 + 3P_{ном}(1 - P_{ном})^2 \right]^n,$$

а ймовірність помилкового декодування дорівнює

$$P_{ном}(3) = 1 - \left[(1 - P_{ном})^3 + 3P_{ном}(1 - P_{ном})^2 \right]^n.$$

Аналіз отриманих формул показує, що система з посимвольною перевіркою більш ефективна, ніж система із груповою перевіркою.

Поряд з багаторазовою передачею комбінацій первинного коду, для підвищення вірності застосовується й багаторазова передача комбінацій перешкодостійкого коду. Один з можливих варіантів такої системи функціонує таким способом. Кодова комбінація повторюється кілька разів. При кожному прийнятті здійснюється декодування з метою виявлення помилок. Якщо при першому прийнятті помилки не виявлено, що відповідає правильній передачі або наявності помилок, що не виявляються, то комбінація вважається дозволеною і не замінюється комбінаціями з наступних

передач. Якщо ж при першому прийманні виявлена помилка, то здійснюється заміна на кодову комбінацію, прийняту при другому прийманні. Якщо помилка виявлена і при повторній передачі, то відбувається заміна кодової комбінації з третьої передачі. Кожне повторення зменшує ймовірність помилкового декодування кодової комбінації. Залежно від якості каналу, ефективності виявлення помилок перешкодостійким кодом, а також від вимог до достовірності інформації в системі встановлюється певна кількість повторів.

Повідомлення в системах з повтореннями можуть передаватися послідовно по одному каналу або одночасно по декількох каналах. Обидва способи, в принципі, ідентичні за своїми можливостями відносно підвищення достовірності і вибір того або іншого способу залежить від конкретних умов і вимог до швидкості передачі.

Підвищення достовірності за рахунок багаторазових повторів призводить при незмінній тривалості елементарного символу до зменшення швидкості передачі. Подібна ситуація розглянута при переході від безнадмірного коду до перешкодостійкого. Цю обставину необхідно враховувати при оцінці ефективності застосування таких систем.

Надмірність перешкодостійких кодів у цілому завжди більша, ніж необхідно для корекції помилок. Дійсно, надмірність мають всі кодові комбінації, а помилки містять тільки деякі з них. Було б доцільним вводити надмірність, що залежить від стану каналу, тобто з ростом кількості помилок надмірність збільшувати, а при їх зменшенні – надмірність зменшувати. Надмірність, необхідна для виявлення помилок, завжди менша, ніж надмірність, необхідна для їх виправлення. Технічна реалізація виявлення помилок також істотно простіша. Тому частіше всього перешкодостійкі коди застосовуються з метою виявлення помилок, а підвищення достовірності передачі дискретних повідомлень досягається за рахунок введення додаткового зворотного каналу. По цьому каналу тим або іншим способом передається інформація, що характеризує умови приймання по прямому каналу, що дозволяє оцінити вплив перешкоди на кожний окремий відрізок повідомлення в ході його передачі і регулювати на підставі цієї інформації надмірність, що вводиться.

У загальному випадку система зв'язку повинна забезпечувати передачу повідомлень в обох напрямках, тому що на обох кінцевих пунктах є і джерела інформації і її одержувачі. За таких умов з'являється можливість використати частину пропускну здатності кожного з каналів для передачі додаткових даних, призначених для підвищення достовірності.

Щоб наочно викласти суть принципів функціонування систем зі зворотним зв'язком, розглянемо окремий випадок, коли передача повідомлень

відбувається лише в одному напрямку, а канал другого напрямку використовується тільки для зворотного зв'язку. Структурна схема такої системи зв'язку зображена на рис. 5.21. У схему входять передавач прямого каналу (ППК), приймач прямого каналу (ПрПК), передавач зворотного каналу (ПЗК) і приймач зворотного каналу (ПрЗК).

Залежно від того, на якій стороні здійснюється перевірка правильності переданого повідомлення, системи зі зворотним зв'язком можна підрозділити на системи з інформаційним зворотним зв'язком (ІЗЗ) і системи з керуючим зворотним зв'язком (КЗЗ).

У системах з керуючим зворотним зв'язком або з перезапитом, перевірка правильності переданого повідомлення здійснюється на приймальній стороні за встановленим правилом. Потім приймається рішення або про направлення декодованого повідомлення одержувачеві (у цьому випадку по зворотному каналу може посилатися підтвердження), або про направлення по зворотному каналу запиту на повторення, на зміну способу передачі, і т.д.

У системах з інформаційним зворотним зв'язком або з порівнянням, рішення про те, які зміни вносити в процесі передачі повідомлень, приймається на передавальній стороні на підставі тієї інформації, що надходить по зворотному каналу. Найчастіше приймається рішення про повторення помилково прийнятих повідомлень, але можливі рішення і про зміну коду, і про припинення передачі при поганому стані каналу.

У системах з комбінованим зворотним зв'язком рішення про помилкове прийняття кодової комбінації приймається на приймальній стороні, а рішення про необхідність повторної передачі приймається на передавальній стороні.

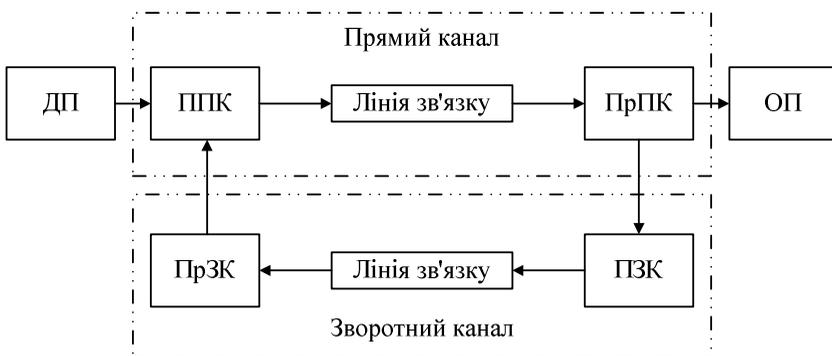


Рис. 5.21. Структурна схема системи зв'язку зі зворотним каналом

Системи зі зворотним зв'язком підрозділяються також на системи з обмеженою і необмеженою кількістю повторень. У системах з необмеженою кількістю повторень кожна кодова комбінація повторюється доти, поки приймач або передавач не ухвалить рішення щодо видачі цієї комбінації споживачеві. У системах з обмеженою кількістю повторень кожна кодова комбінація може повторюватися не більше декількох разів, після чого канал бракується.

Більшість існуючих систем з керуючим зворотним зв'язком належить до систем з перезапитом. Найпоширенішою серед них є система з виявленням помилок на приймальній стороні за допомогою кодів, що виявляють помилки. Прийняті кодові комбінації розбиваються на дозволені і заборонені групи. Якщо комбінація віднесена до дозволеної, то вважається, що така ж комбінація була й передана, і вона направляється одержувачеві. При цьому по зворотному каналу передається сигнал підтвердження. Після одержання сигналу підтвердження керуючий пристрій видає команду на передачу наступної кодової комбінації з одночасним записом її в буферний запам'ятовувальний пристрій передавача. При цьому раніше передана кодова комбінація, що зберігалася тут, стирається.

Очевидно, що в цій системі можливий випадок, коли під дією перешкод одна дозволена кодова комбінація може бути переведена в іншу. Однак імовірність такої помилки можна зробити досить малою, вибираючи відповідний код.

Якщо прийнята комбінація віднесена до групи заборонених, то на приймальній стороні формується сигнал перезапиту, по якому повторюється передача відповідної кодової комбінації.

Ефективність використання пропускної здібності каналу зв'язку в подібних системах порівняно невелика, тому що прямий канал простоє в проміжки часу між передачами кодових комбінацій, чекаючи одержання сигналів підтвердження або перезапиту. Прагнення до більш повного використання каналів призвело до розробки систем, у яких передавач посилає в лінію неперервну послідовність комбінацій, не очікуючи одержання сигналів підтвердження. Приймач стирає лише ті комбінації, в яких виявлені помилки, і по них дає сигнал перезапиту. Інші комбінації видаються одержувачеві повідомлень за їх надходженням. При реалізації такої системи виникають труднощі, викликані кінцевим часом передачі і розповсюдження сигналів. Дійсно, нехай у деякий момент часу закінчилося прийняття кодової комбінації, у якій виявлена помилка, і починається передача сигналу перезапиту по зворотному каналу. До цього моменту по прямому каналу вже ведеться передача наступної кодової комбінації, а якщо тривалість розповсюдження сигналу в каналі перевищує тривалість кодової

комбінації, то передавач відправить у лінію одну або кілька комбінацій. Ще якась кількість кодових комбінацій буде передана до того моменту, поки буде прийнятий і декодований сигнал перезапиту. Таким чином, при неперервній передачі за час між моментом виявлення помилки і приходом повторної кодової комбінації буде прийнято ще M комбінацій.

Так як передавач повторює лише комбінації, по яких прийнятий сигнал перезапиту, то в результаті повторення з запізнюванням на M комбінацій порядок проходження комбінацій в інформації, що видається одержувачеві повідомлень, буде відрізнятись від порядку надходження кодових комбінацій у систему. Але одержувачеві кодові комбінації повинні бути видані у тому ж порядку, в якому вони передавалися. Тому M комбінацій, прийнятих після виявлення помилки, повинні зберігатися в деякому буферному пристрої пам'яті до моменту, поки не буде прийнята повторена комбінація. Оскільки й у повторених комбінаціях може бути виявлена помилка, ємність буферної пам'яті потрібно збільшити ще в кілька разів, забезпечивши її до того ж складною системою введення і виведення інформації.

Щоб уникнути ускладнення і подорожчання приймачів використовують трохи видозмінену систему з перезапитом, у якій після виявлення помилки приймач блокується, тобто не приймає M наступних комбінацій. У передавальній частині пристрій пам'яті завжди зберігає $M+1$ останніх переданих комбінацій. Після одержання сигналу перезапиту повторюється не тільки помилково прийнята комбінація, але й весь інший зміст. При цьому зберігається порядок надходження кодових комбінацій одержувачеві, можливість переповнення пристрою пам'яті виключається, керування введенням і виведенням інформації досить прості.

Визначимо основні характеристики системи з керуючим зворотним зв'язком при перешкодостійкому кодуванні.

При передачі кодової комбінації в системі можливі такі ситуації:

- перешкода не спотворила комбінацію і з імовірністю P_{np} вона прийнята правильно;
- через дію перешкод комбінація перейшла в іншу дозволена комбінацію, тобто з імовірністю $P_{нев}$ виникла помилка, що не може бути виявлена;
- через дію перешкод комбінація перейшла в заборонену, тобто з імовірністю $P_{ви}$ виникла помилка, що виявляється.

У першому і у другому випадках декодовані повідомлення направляються одержувачеві, в останньому випадку комбінація бракується й по зворотньому каналу направляється запит, після якого все повторюється

спочатку.

Помилка, що не виявляється, може виникнути в першому циклі, в другому циклі, в третьому і т.д. При цьому одержувачеві буде передана помилкова інформація. Отже, система може бути охарактеризована залишковою ймовірністю помилкового прийняття кодової комбінації $P_{ном\ зал}$. Ця ймовірність складається з ймовірності невиявленої помилки при першій передачі, при другій передачі і т.д. Якщо комбінація приймалася m разів із виявленням помилки, а потім була прийнята з невиявленням помилки, то ймовірність цієї події дорівнює $P_{ен}^m P_{нев}$. Тоді для $P_{ном\ ост}$ можна записати

$$P_{ном\ зал} = P_{нев} + P_{ен}P_{нев} + P_{ен}^2P_{нев} + \dots = P_{нев} \sum_{m=0}^{\infty} P_{ен}^m = \frac{P_{нев}}{1 - P_{ен}}. \quad (5.11)$$

Ймовірності $P_{пр}$, $P_{нвп}$ і $P_{вп}$ можна визначити знаючи структуру коду та параметри каналу. Ймовірність невиявлення помилки може бути оцінена за формулою

$$P_{нев} \leq 1 - \sum_{i=0}^{d_{min}-1} C_n^i p_0^i (1 - p_0)^{n-i}.$$

Ймовірність правильного прийняття може бути знайдена за очевидною формулою $P_{пр} = (1 - p_0)^n \approx np_0$. Ймовірність виявлення помилки можна одержати виходячи з того, що $P_{пр} + P_{нев} + P_{ен} = 1$. З огляду на те, що в системі з перезапитом код повинен бути обраний так, щоб $P_{нев} \ll P_{ен}$, для $P_{виявл}$ маємо $P_{ен} \approx 1 - (1 - p_0)^n$.

Швидкість передачі в системах з КЗЗ визначається не тільки відношенням k/n , але і втратою часу на повторення. У зв'язку з цим системи зі зворотним зв'язком можна охарактеризувати також відносною швидкістю передачі R' , під якою розуміється відношення математичного очікування числа інформаційних символів, що надійшли до одержувача, до загального числа кодових символів, що надійшли в канал. Кодова комбінація надходить до одержувача тільки тоді, коли в ній не виявлені помилки. Отже, при одержанні кожної кодової комбінації одержувачеві з ймовірністю $1 - P_{ен}$ видається k інформаційних символів. Тому

$$R' = \frac{k}{n} (1 - P_{ен}).$$

Оскільки $P_{ен}$ залежить від стану каналу, то і надмірність у системі з КЗЗ змінюється також відповідно до стану каналу.

В системах із блокуванням відносна швидкість передачі ще менша, тому що при запиті повторюється не одна, а кілька кодових комбінацій.

При розгляді характеристик систем з керуючим зворотним зв'язком не враховувалася ймовірність виникнення помилок у сигналах підтвердження і перезапиту, що найчастіше допустимо, тому що такими сигналами вибираються перешкодозахищені кодові послідовності. Проте, в реальних каналах ймовірність помилкового прийняття цих сигналів все-таки не дорівнює нулю й необхідно враховувати можливість того, що сигнал підтвердження буде прийнятий як перезапит або навпаки. При цьому виникають специфічні помилки у прийнятій інформації. Якщо при правильному прийнятті по прямому каналу у зворотному каналі відбувається трансформація сигналу підтвердження в сигнал запиту, то система повторює передачу кодової комбінації, в результаті чого відбувається вставка. У тих же випадках, коли при передачі по прямому каналу приймач виявляє помилки, а у зворотному каналі відбувається трансформація сигналу запиту в сигнал підтвердження, передавач видає нове повідомлення. При цьому попередні повідомлення стираються і відбувається випадання.

Для боротьби з випаданнями та вставками, крім захисту сигналів підтвердження і перезапиту за допомогою кодів, приймаються спеціальні заходи. Так, для зменшення кількості випадань у зворотному каналі встановлюється несиметричне правило декодування, при якому ймовірність помилкового прийняття сигналу перезапиту мізерно мала за рахунок збільшення ймовірності помилкового прийняття сигналу підтвердження. Для того щоб часті помилки при передачі сигналу підтвердження не призводили до появи зайвих вставок, до кожної кодової комбінації додають розпізнавальні символи, що вказують на те, чи передається ця комбінація вперше, чи повторюється. Якщо на декодер надійде повторна комбінація, а перед цим перезапиту не було, то вона стирається і не надходить до одержувача.

Всі ці заходи, як легко бачити, вимагають деякого збільшення надмірності й ускладнення апаратури.

Застосування систем з керуючим зворотним зв'язком ефективно в каналах, де змінюється ймовірність помилки. Коли $P_{\text{пом кор}}$ стає близькою до $1/2$, настає обривання зв'язку, тому що пропускна здатність каналу падає майже до нуля. При цьому система перебуває в режимі постійного перезапиту. Але якщо вона побудована раціонально, то одержувачеві помилкова інформація не видається. При поліпшенні перешкодової обстановки швидкість передачі збільшується, а вірність продовжує залишатися на заданому рівні. Таким чином, система з КЗЗ як би пристосовується до стану каналу. Це є важливим достоїнством системи з КЗЗ.

У найпоширеніших системах з інформаційним зворотним зв'язком

прийняті приймачем кодові комбінації або символи повністю передаються по зворотному каналу на передавач, де відбувається їх порівняння з переданими повідомленнями. У випадку збігу комбінацій прямого та зворотного каналів здійснюється передача наступної комбінації, а у випадку відмінності – повтор раніше переданої. Такий інформаційний зворотний зв'язок називають повним або ретрансляційним.

При ідеальному зворотному каналі повний інформаційний зворотний зв'язок дозволяє без застосування перешкодостійких кодів забезпечити абсолютно достовірну передачу інформації в прямому напрямку. Передавач у цьому випадку виявляє всі помилки приймача і при відсутності обмежень на затримку завжди має можливість виправити їх.

У реальних системах при повному інформаційному зворотному зв'язку не виявляються лише так звані дзеркальні помилки, тобто помилки, що відбуваються в тому самому символі двічі: при передачі по прямому й зворотному каналах.

Недоліком описаної системи є мала продуктивність, оскільки на передачу кожної інформаційної комбінації витрачається принаймні (при відсутності повторних передач) час

$$\Delta t = 2 t_k + 2 t_p ,$$

де t_k – час передачі кодової комбінації;

t_p – час розповсюдження сигналів між станціями.

Більш високу пропускну здібність забезпечують системи з ІЗЗ, у яких здійснюється неперервна передача інформаційних комбінацій.

У таких системах тільки у випадку незбігу комбінацій прямого і зворотного каналів передавач припиняє передачу чергових комбінацій і робить повторення помилкової комбінації. У буферних запам'ятовуючих пристроях передавача і приймача при цьому зберігається не одна, а M інформаційних комбінацій. З прийняттям сигналу незбігу стираються всі M комбінацій, а по прямому каналу слідом за сигналом стирання повторюються всі M комбінацій.

Визначимо для розглянутої системи ймовірність відсутності перекручувань і ймовірності виявлення та не виявлення помилок в одному циклі. У системі з ІЗЗ перекручування не виявляється тільки в тому випадку, якщо кодова комбінація B_i перетворилася в прямому каналі в B_j , а у зворотньому каналі відбувається інверсна трансформація B_j в B_i . Тому, що використовується безнадмірне кодування, то ймовірність правильного приймання по прямому каналу

$$P_{пр}^{(прям)} = (1 - P_{пом}^{(прям)})^n ,$$

а по зворотному каналу

$$P_{np}^{(звор)} = (1 - P_{пом}^{(звор)})^n .$$

Імовірність відсутності перекручувань після повного циклу передачі

$$P_{np} = P_{np}^{(прям)} P_{np}^{(звор)} = (1 - P_{пом}^{(прям)})^n (1 - P_{пом}^{(звор)})^n . \quad (5.12)$$

Імовірність перетворення в прямому каналі кодової комбінації B_i у B_j обчислюється за формулою

$$P_{пом}^{(прям)} = 1 - P_{np}^{(прям)} = 1 - (1 - P_{пом}^{(прям)})^n .$$

Імовірність зворотної трансформації B_j у B_i за умови, що передача $N = 2^n$ комбінацій рівномірна, обчислюється за формулою

$$P_{пом}^{(звор)} = \frac{1 - P_{np}^{(звор)}}{N} = \frac{1 - (1 - P_{пом}^{(звор)})^n}{N} .$$

Загальна ймовірність не виявлення помилки при одноразовій передачі

$$P_{не} = P_{пом}^{(прям)} P_{пом}^{(звор)} = \frac{1}{N^n} [1 - (1 - P_{пом}^{(прям)})^n] [(1 - P_{пом}^{(звор)})^n] . \quad (5.13)$$

Формули (5.12) і (5.13) описують два можливих результати одного циклу обміну інформацією. Третій результат, що доповнює правильну передачу й помилку, що не виявляється, до повної групи подій – помилка, що виявляється. Імовірність такої події

$$P_{ен} = 1 - P_{неп} - P_{np} .$$

В системі з інформаційним зворотним зв'язком ситуації, що призводять до не виявлення перекручування кодової комбінації, точно такі ж, як і в системі з КЗЗ, внаслідок чого залишкова ймовірність помилкового прийняття кодової комбінації може бути обчислена за формулою (5.11).

Основною проблемою при побудові системи з інформаційним зворотним зв'язком є захист від трансформації службових сигналів у комбінацію основного повідомлення або навпаки. Тому завжди необхідно вводити певну надмірність, щоб захистити службові сигнали від таких трансформацій. Для цього застосовують перешкодостійке кодування.

Звичайно по прямому каналу передають тільки інформаційні символи, а перевіірочні запам'ятовуються на передавальній стороні. Прийняті інформаційні символи також піддаються кодуванню на приймальній стороні й по зворотному каналу посилають тільки перевіірочні символи. На передавальній стороні прийняті по зворотному каналу перевіірочні символи порівнюються з перевіірочними символами, що зберігаються, на передавальній стороні. Якщо вони не збігаються, то по прямому каналу посилається сигнал заперечення і здійснюється повторення.

Системи з різними зворотними зв'язками мають певні переваги і не-

доліки, які треба врахувати при їх використанні. Перевага систем з ІЗЗ полягає в можливості використання безнадмірних кодів. Це обумовлює простоту їх технічної реалізації. Для них характерна простота роботи і висока достовірність передачі. Недоліки цих систем полягають у тому, що видача споживачеві навіть правильно отриманої інформації затримується доти, доки після аналізу інформації з передавальної сторони не буде отриманий сигнал підтвердження. В системах з ІЗЗ однаково завантажений як прямий, так і зворотний канали зв'язку.

Головна перевага систем з КЗЗ полягає в тому, що правильна інформація видається споживачеві практично без затримки. Ці системи мають високу достовірність і низьку завантаженість зворотного каналу. До недоліків цих систем слід віднести необхідність використання надмірного перешкодостійкого коду. Це обумовлює необхідність використання кодуєчих і декодуєчих пристроїв, що ускладнює побудову і роботу апаратури. В них значно завантажений прямий канал.

Система з комбінованим зворотним зв'язком мають певні комбінації властивостей, притаманних системам з інформаційним і керуючим зворотним зв'язком. Досліди підказують, що коли перешкоди в прямому і зворотному каналах однакові, то як інформаційний, так і керуючий зворотний зв'язок забезпечують приблизно однакову достовірність. Канали зв'язку в цілому також завантажені однаково. Системи з ІЗЗ доцільно розробляти і використовувати в тих випадках, коли потрібна максимальна простота побудови системи і допускається затримка використання отриманої інформації. Якщо така затримка недопустима, то слід використати систему з КЗЗ.

Практична реалізація розглянутих видів зворотного зв'язку дає можливість забезпечити потрібну достовірність передачі повідомлень системами при незначному їх ускладненні і припустимих економічних витратах.

Теорія систем зі зворотним зв'язком досить складна та ще далеко до завершення; багато досліджень виконані з істотними допущеннями й ідеалізацією. Проте, використання каналу зворотного зв'язку у всіх випадках, де це можливо, є однією з основних тенденцій розвитку систем зв'язку.

5.8. Контрольні запитання

1. Дайте класифікацію перешкодостійких кодів.
2. Поясніть загальні принципи перешкодостійкого кодування.
3. Що таке мінімальна кодова відстань?
4. Що таке вага кодового слова. Чому дорівнює мінімальна кодова відстань для лінійних кодів?

5. Поясніть порядок розрахунку характеристик перешкодостійких кодів.
6. Поясніть порядок вибору породжувальної матриці лінійного коду.
7. Поясніть порядок побудови лінійного коду за допомогою породжувальної матриці .
8. Що таке синдром кодового слова. Від чого він залежить?
9. Поясніть порядок побудови перевірконої матриці лінійного коду.
10. Поясніть порядок декодування лінійного коду за допомогою перевірконої матриці.
11. Поясніть принципи побудови кодуючих і декодуючих пристроїв лінійних групових кодів.
12. Дайте визначення лінійних циклічних кодів.
13. Назвіть вимоги до породжувального полінома циклічних кодів.
14. Поясніть принципи побудови пристроїв кодування циклічних кодів на схемах множення.
15. Поясніть принципи побудови пристроїв кодування циклічних кодів на схемах розподілу поліномів.
16. Поясніть принципи побудови пристроїв декодування циклічних кодів.
17. Поясніть принцип побудови згортувальних кодів.
18. Поясніть принцип декодування згортувальних кодів за алгоритмом Витербі.
19. Поясніть принципи багаторазової передачі кодових комбінацій.
20. Поясніть сутність систем передачі інформації зі зворотним зв'язком.
21. У чому суть систем передачі інформації з керуючим зворотним зв'язком?
22. У чому суть систем передачі інформації з інформаційним зворотним зв'язком?

Розділ 6

Кодування даних у модулярній системі числення

Розглянуті загальні відомості, поняття та визначення модулярної системи числення, методи кодування та обробки інформації у МСЧ, Також наведено контрольні питання.

6.1. Загальні відомості про модулярну систему числення

Теоретичні основи побудови числової системи у рамках модулярної системи числення (МСЧ) є розвитком широко відомого у теорії чисел розділу порівнянь. В 1955 - 1957 р.р. вчені А. Свобода, М. Валах і інші указали на можливість надлишкового кодування цілих чисел у СОІУ за допомогою набору лишків $\{a_i\}$ від ділення цих чисел на взаємно попарно прості натуральні числа $\{m_i\}$, $i = \overline{1, n}$, що мають назву основ або модулів МСЧ.

Зворотне завдання відновлення числа A_k по сукупності його лишків $\{a_i\}$ відомо давно, як "китайська теорема про лишки". Вперше в літературі історія розвитку системи числення в залишкових класах описана в трактаті китайського математика Сунь-Цзи, що жив у першому сторіччі нашої ери. Його вважають творцем знаменитої "китайської теореми про лишки" (КТЛ). Використання результатів цієї теореми дозволяє однозначно визначити вихідне число по сукупності лишків, які утворюються при розподілі даного числа на сукупність дільників. Результати досліджень вчених математиків і істориків показали, що рахунок часу в календарі народу Майя й вираховування часу в Юліанському календарі виконувалися також за допомогою кодів МСЧ.

Повне теоретичне дослідження й місце "китайської теореми про лишки" у теорії чисел провів німецький математик Карл Гаус у своїх працях по теорії чисел - "Арифметичні дослідження".

Інтерес до КТЛ викликаний науково-практичними дослідженнями, що присвячені пошукам шляхів підвищення ефективності використання СОІУ. У першу чергу це відносилось до швидкодії (продуктивності) виконання арифметичних операцій. Перші проекти реально діючих штатних стаціонарних управляючих обчислювальних комплексів (УОК) К-340А,

"Алмаз", 5E53 показали високу ефективність застосування кодів МСЧ для підвищення продуктивності й надійності функціонування СОІУ.

Крім цього розроблялися системи передачі даних, де використовувалося завадостійке кодування у МСЧ і надшвидкодуючі бортові системи обробки інформації підвищеної надійності, які використовувалися в системі управління літальними апаратами військового призначення для наведення цілей і стиску інформації. Зокрема, було показано, що застосування кодів МСЧ у супутникових системах космічного зв'язку дозволяє істотно підвищити надійність і ефективність зв'язку.

Наприкінці двадцятого сторіччя значно зросла практична зацікавленість до використання непозиційного кодування у МСЧ. У процесі досліджень специфіки й можливостей непозиційних кодових структур вченими Акушським І. Я., Юдицьким Д. І., Лукіним Ф. В. і іншими було знайдено шлях практичної реалізації коригувальних кодів, що придатні для виявлення й виправлення помилок при обробці інформації у динаміці обчислювального процесу. Торгашев В. А. і ін. показали, що застосування кодів у МСЧ дозволяє змінювати у процесі рішення завдання кількісне співвідношення між числом інформаційних і контрольних основ.

Дослідження проведені в області застосування непозиційних кодових структур МСЧ у гіперкомплексній області показали, що використання першої фундаментальної теореми Гауса дозволяє замінити виконання раціональних операцій над найменшими комплексними лишками виконання тих же операцій над відповідними їм дійсними лишками по дійсному модулю, що дорівнює нормі комплексного модуля.

Доцільно відзначити взаємозв'язок і вплив на процес функціонування СОІУ наступних основних властивостей МСЧ.

1. Властивість малоразрядності лишків МСЧ дозволяє суттєво підвищити надійність і швидкодію виконання модульних операцій, як за рахунок малоразрядності каналів обробки інформації (КОІ), так і за рахунок можливості ефективного застосування, на відміну від ПСЧ, табличної арифметики. Коли операції додавання, вирахування й множення виконуються практично за один такт, що значно підвищує швидкодію виконання модульних операцій.

Дана властивість дозволяє використати безліч різних принципів реалізації модульних операцій, що значно розширює перелік варіантів системотехнічних рішень, які застосовуються при створенні СОІУ.

2. Властивість незалежності лишків МСЧ дозволяє створювати СОІУ у вигляді набору незалежних, паралельно працюючих КОІ (окремих, "малих" КОІ, що функціонують за своїм певним модулем m_i в МСЧ, незалежно один від одного). Таким чином, СОІУ, що функціонує у МСЧ володіє модульністю конструкції, що дозволяє здійснювати технічне обслугову-

ування й усунення несправностей, не припиняючи процесу обробки інформації.

Помилки, що виникають за рахунок відмов (збоїв) у довільному КОІ, не "розмножуються" у сусідні канали (залишаються в межах одного лишку), що дає можливість підвищити вірогідність обробки інформації у МСЧ. При цьому, не важливо чи мала місце однократна чи багаторазова помилка або група помилок довжиною не більше $\lceil \log_2(m-1) \rceil + 1$ двійкових розрядів. Помилка, що виникла в КОІ по основі m_i , або остається у цьому каналі до кінця обчислень, або самоусувається в процесі подальших обчислень (наприклад, якщо після виникнення збою в лишку a_i проміжний результат множиться на число, що має нульову цифру по основі m_i). Таким чином, дана властивість МСЧ дозволяє реалізувати унікальну систему контролю й виправлення помилок у динаміці процесу обробки інформації при введенні мінімальної кодової надмірності, без зупинки обчислень, що істотно для систем, що функціонують у реальному часі.

3. Властивість рівноправності лишків полягає в наступному. Любий лишок a_i числа $A=(a_1, a_2, \dots, a_n)$ несе інформацію про все число, що дає можливість програмними методами замінити КОІ, що відмовив по модулю m_i на працездатний канал по модулю m_j ($m_i < m_j$) не перериваючи рішення завдання. Таким чином, СОІУ функціонуюча в МСЧ що має, наприклад, дві контрольних основи зберігає свою працездатність при відмові двох будь-яких КОІ. При виникненні відмов у третьому або четвертому каналах СОІУ продовжує виконувати програму обробки інформації, при деякому зниженні точності обчислень, тобто СОІУ має властивість поступової деградації із зберіганням основних технічних характеристик. Дана властивість визначає характерну рису функціонування СОІУ у МСЧ – один і той же пристрій обробки інформації (ПОІ), залежно від заданих вимог може мати різну надійність, точність обчислень і швидкодію в динаміці процесу обробки інформації, тобто в процесі рішення завдання можна варіювати надійністю, точністю обчислень і швидкодією.

Наприклад, нехай об'єкт G , заданий числовим кодом, що визначається набором основ $\{m_i\}$ МСЧ, $i = \overline{1, n+k}$ (описується набором $\{a_i\}$ лишків). Час виконання модульних операцій і точність вирішення залежать від кількості інформаційних основ n , а надійність (вірогідність) обчислень залежить від кількості контрольних основ k . Нехай у процесі обчислень виникла необхідність підвищити надійність обчислень. У цьому випадку, у реальному часі, відбувається перерозподіл основ МСЧ $\{a_i\}$, $i = \overline{1, n'+k'}$, при цьому $n+k = n'+k' = const$, $n' < n$, а $k' > k$. У цьому випадку зменшується точність обчислень і підвищується швидкодія виконання арифметичних операцій, які визначаються кількістю інформаційних основ n' .

Якщо виникла необхідність на окремій ділянці програми, що виконується збільшити точність рішення, то перерозподіл основ МСЧ відбувається в такий спосіб: $i = \overline{1, n'' + k''}$ ($n+k = n''+k'' = const$). У цьому випадку при підвищенні точності обчислень ($n'' > n$) зменшується вірогідність обчислень і швидкодія ($k'' < k$) рішення даного завдання.

Необхідно відзначити, що існуючі методи підвищення продуктивності обробки інформації й відмовостійкості функціонування, засновані на використанні двійкових ПСЧ, не завжди у повному обсязі задовольняють зростаючим вимогам до систем обробки інформації спеціального призначення, що викликано наступними обставинами.

У ПСЧ кількісне значення кожної цифри розряду залежить від її місця (позиції) у вихідному числі. Будь-яке число A зображується у вигляді послідовності цифр a_i заданої системи числення. У СОІУ найбільш просто реалізуються процеси виконання арифметичних і логічних операцій над операндами, що представлені у двійковій ПСЧ у вигляді $A = a_{\rho-1}2^{\rho-1} + a_{\rho-2}2^{\rho-2} + \dots + a_12 + a_0$, де $a_i = \overline{0, 1}$ ($i = \overline{0, \rho-1}$).

Приклад 6.1. Скласти у ПСЧ два операнди, що представлені двійковим кодом, $A_{10} = 1010$ і $B_6 = 0110$.

$$\begin{array}{r}
 A_{10} = 1\ 0\ 1\ 0 \\
 + \quad +\ +\ +\ + \\
 \hline
 A_6 = 0\ 1\ 1\ 0 \\
 A_{16} = 1\ 0\ 0\ 0\ 0.
 \end{array}$$

Основні труднощі при реалізації арифметичних операцій у ПСЧ полягають в організації процесу утворення й поширення цифр переносу між двійковими розрядами операндів, що обробляються. Наявність міжрозрядних зв'язків впливає на процес "розмноження" помилки. Тобто помилка, що виникла в одному двійковому розряді, у процесі переносу від молодших розрядів до старших, поширюється по всій довжині машинного слова. Алгоритмічний зв'язок у ПСЧ всіх двійкових розрядів операндів між собою обумовлює той факт, що одинична відмова (збій) схеми обробки інформації здатний викликати не однократну, а багаторазові помилки.

Також у ПСЧ час реалізації арифметичних операцій залежить від довжини розрядної сітки ПОІ, що в умовах сучасної тенденції розвитку СОІУ, спрямованої на збільшення довжини розрядної сітки, є стримуючим фактором підвищення продуктивності таких систем.

При цьому методи підвищення продуктивності СОІУ, що функціонують у ПСЧ, мають загальний недолік - неможливість розпаралелювати алгоритми, що підлягають розв'язанню на рівні елементарних операцій (мікрооперацій), що також обумовлено в першу чергу наявністю у ПСЧ міжрозрядних зв'язків в операндах, що підлягають обробці.

Опираючись на фундаментальні поняття й положення теорії порівнянь, була створена оригінальна система числення, що здатна усунути зазначені недоліки ПСЧ. У новій системі числення число (операнд) A представляється набором $\{a_i\}$ найменших лишків від послідовного ділення операнда A на сукупність $\{m_i\}$ взаємно попарно простих чисел, яка отримала назву модулярна система числення.

Відзначимо, що основи МСЧ зв'язані один з одним так, що вони вибираються певним чином і закріплюються постійними для даної МСЧ. Кожний лишок по модулю $\{m_i\}$ інформаційно незалежний від інших лишків, але в межах кожного лишку, при реалізації операцій обробки інформації, використовується ПСЧ (як правило, двійкова). Таким чином, МСЧ правильно визначити як особливу конструкцію кодових числових структур, тобто спеціальним образом закодований блок інформації.

Коди МСЧ є подальшим удосконаленням відомих у ПСЧ арифметичних багатолішкових кодів, які мають наступний вигляд

$$A'_k = (A_k, A_k(\text{mod } m_1), A_k(\text{mod } m_2), \dots, A_k(\text{mod } m_i), \dots, A_k(\text{mod } m_{n-1}), A_k(\text{mod } m_n)),$$

тобто.

$$A'_k = (A_k, a_1, a_2, \dots, a_n),$$

де $a_i = A_k - [A_k / m_i]m_i$.

При $\prod_{i=1}^n m_i \geq A_k$ сукупність лишків $\{a_i\}$ однозначно визначає операнд A_k і чисельне значення A_k стає не потрібним, що дозволяє реалізувати модульні операції по окремих незалежних каналах, оперуючи тільки із лишками $\{a_i\}$. Таке кодування чисел дозволяє створювати СОІУ, у яких обробка всіх розрядів числа (лишків a_i) здійснюється паралельно у часі. У цьому випадку узагальнена структурна схема ПОІ в МСЧ являє набір КОІ, що функціонують незалежно один від одного й паралельно у часі, причому кожний по своєму певному модулю m_i (рис. 6.1).

Можна виділити наступні основні принципи побудови паралельних підсистем обробки інформації СОІУ:

- модульність побудови;
- здатність системи до адаптації, до самонастроювання й самоорганізації;
- забезпечення необхідного рівня відмовостійкості, що виявляється у здатності СОІУ зберігати працездатний стан при виникненні відмов, за рахунок реконфігурації й виконання обмінних операцій.

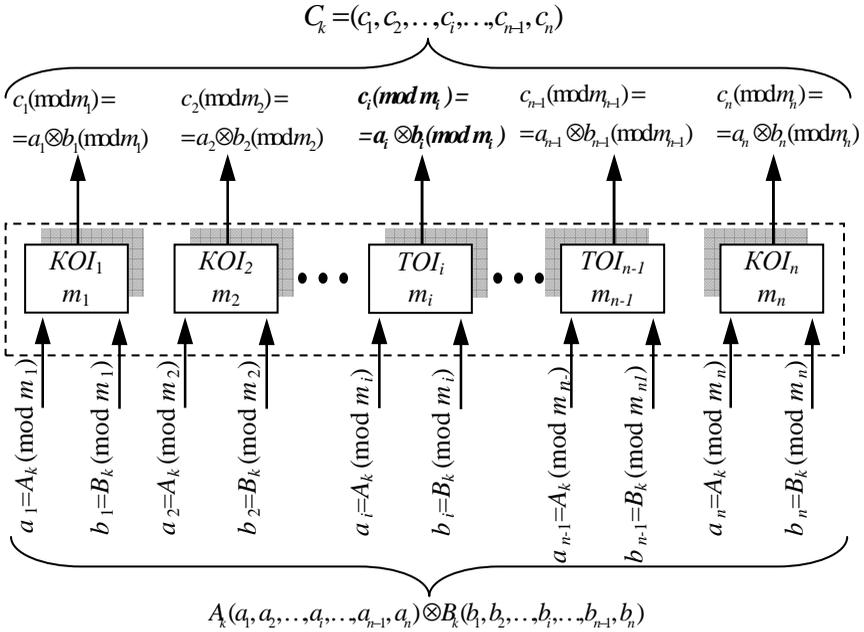


Рис. 6.1. Структурна схема ПОІ у МСЧ

Розпаралелювання процесу обробки інформації, з погляду технічної реалізації, може здійснюватися по-різному. У принципі розпаралелювання може бути здійснене на декількох рівнях. На рівні побудови фізичних і математичних моделей об'єктів або процесів, що дозволяють організувати паралельну обробку інформації. На рівні методу рішення. На рівні алгоритмів відомих методів. На рівні програм. На рівні арифметичних операцій. На рівні обміну інформацією або введення й представлення даних у СОІУ. Одним з найбільш перспективних напрямків у розробці високошвидкісних систем обробки інформації є перехід до розпаралелювання на рівні мікрооперацій, зокрема на основі застосування МСЧ.

Розглянемо, як приклад організації процесу паралельної обробки інформації у СОІУ трьохрівневу модель інформаційної технології (ІТ) що реалізується підсистемою обробки інформації СОІУ, яка функціонує у МСЧ. (рис. 6.2.). Зрозуміло, що основною метою, яка стоїть перед ІТ є одержання, у результаті переробки інформаційного ресурсу, якісного інформаційного продукту. Тому, інформаційну технологію що використовує модулярну систему числення можна представити як сукупність взаємозалежних інформаційних процесів, кожний з яких містить певний набір про-

цедур, які реалізуються за допомогою методів і алгоритмів обробки інформації в модулярній системі числення.

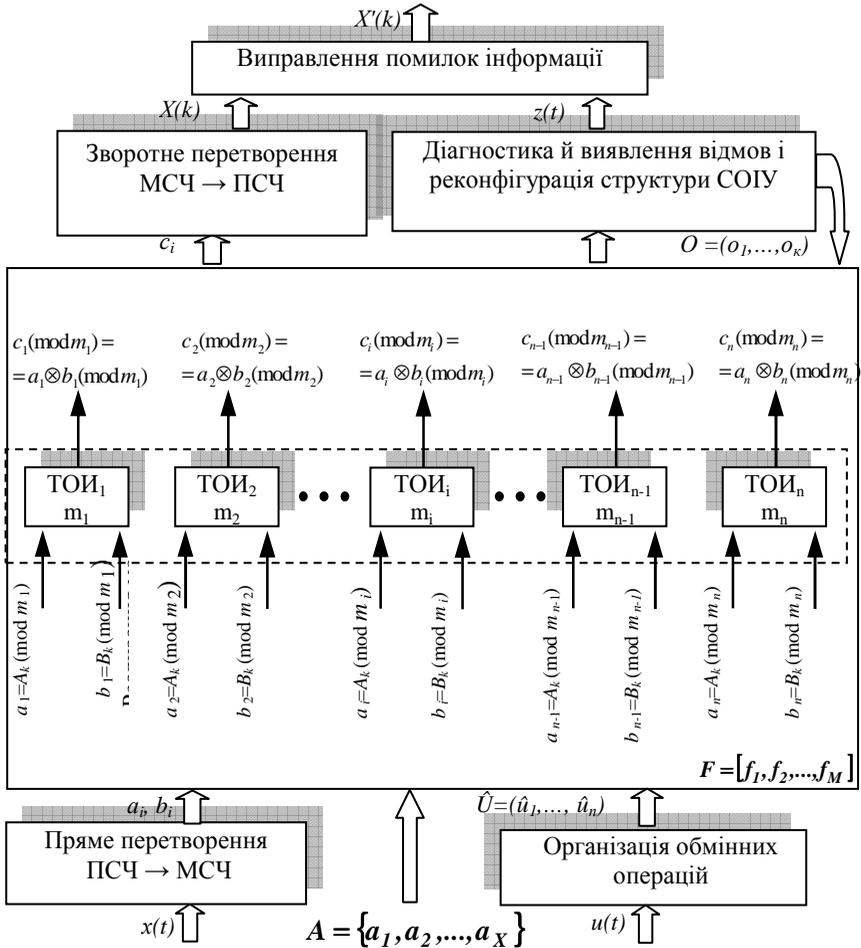


Рис. 6.2. Модель ІТ, що реалізується підсистемою обробки інформації СОІУ у МСЧ

Перший рівень є концептуальним, що визначає змістовний аспект ІТ. Другим є логічний рівень, що формується з концептуального шляхом виділення конкретної частини ІТ, її деталізації й формалізації. Для даного

випадку це безпосередньо підсистема обробки інформації, що функціонує у МСЧ. Даний рівень ІТ представляється комплексом взаємозалежних методів і моделей, які формалізують інформаційні процеси. На третьому, фізичному рівні розкривається програмно-апаратна реалізація ІТ. Тут математичні моделі й методи перетворюються в алгоритми, що визначають порядок дій по реалізації компонентів ІТ.

Відповідно до вихідного завдання $A = \{a_1, a_2, \dots, a_x\}$, що є набором процедур, які реалізуються підсистемою обробки інформації СОІУ, з використанням сукупності принципів, моделей, методів і алгоритмів $F = [f_1, f_2, \dots, f_M]$ реалізації арифметичних і логічних операцій, операцій контролю, діагностики й виправлення помилок у МСЧ, відбувається переробка первинної інформації $x(t)$ з метою одержання інформаційного продукту $X(k)$.

При цьому відповідно до програми функціонування СОІУ, по управляючих сигналах $u(t)$ здійснюється організація обмінних операцій між точною й вірогідною виконання процесів обробки інформації, з використанням сукупності моделей, методів і алгоритмів $\hat{U} = (\hat{u}_1, \dots, \hat{u}_n)$.

При виникненні помилок інформації, по сигналах корекції помилок $z(t)$, здійснюється корекція інформації $X(k)$. У результаті даної процедури одержуємо відкоректований інформаційний продукт $X'(k)$. При виявленні апаратних відмов ПОІ, відповідно до заданої програми, з використанням безлічі методів і алгоритмів $O = (o_1, \dots, o_n)$ здійснюється реконфігурація структури СОІУ, в динаміці процесу обробки інформації.

6.2. Основні властивості порівнянь

Ознайомимося з деякими властивостями порівнянь. Розглянемо безліч всіх натуральних чисел. Задамо, наприклад, число (модуль) $m_i = 5$. При діленні будь-якого натурального числа A на $m_i = 5$ може вийти наступна сукупність лишків $0, 1, 2, 3, 4$.

У цьому випадку вся безліч натуральних чисел, включаючи нуль, можна розбити на п'ять класів, включаючи в кожний клас числа, які при діленні на $m_i = 5$ дають той же самий лишок a_i . Класом $\overline{a_i}$ по даному модулю m_i будемо називати безліч всіх натуральних чисел, що порівнюються з деяким даним числом a_i . Вважається, що ці числа порівнянні між собою по модулю $m_i = 5$.

При цьому загальний алгоритм визначення лишку числа A по модулю m_i визначається як $a_i = A - [A/m_i] \cdot m_i$, де $[A/m_i]$ - ціла частина числа A/m_i , що його не переважає.

Відзначимо, що числа, які входять у класи $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}$, називаються відрахуваннями по модулю $m_i = 5$. Якщо з кожного класу \bar{a}_i взяти по одному відрахуванню, то їхня сукупність буде називатися *повною системою відрахувань* по модулю п'ять.

Приклад 6.2.

Визначити класи відрахувань по модулю $m_i=5$ серед натуральних чисел, включаючи нуль.

Таких класів буде п'ять $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}$:

$$\begin{aligned} \bar{0} & \{0, 5, 10, 15, 20, \dots\}, \\ \bar{1} & \{1, 6, 11, 16, 21, \dots\}, \\ \bar{2} & \{2, 7, 12, 17, 22, \dots\}, \\ \bar{3} & \{3, 8, 13, 18, 23, \dots\}, \\ \bar{4} & \{4, 9, 14, 19, 24, \dots\}. \end{aligned}$$

Приклад 6.3.

Визначити найменший позитивний лишок числа $A=17$ по модулю $m_i=5$.

Тому що $17 = 3 \cdot 5 + 2$, то $a_i=2$. Це можна записати у вигляді порівняння $17 \equiv 2 \pmod{5}$. При цьому загальний алгоритм визначення лишку числа A по модулю m_i визначається як

$$a_i = A - [A/m_i] \cdot m_i,$$

де $[A/m_i]$ - ціла частина числа A/m_i , що його не переважає.

Наприклад, $[0,3] = 0$; $[3,9] = 3$; $[5,1] = 5$; $[-3,4] = -4$ і т.п.

Приклад 6.4.

Визначити лишки від ділення числа $A = 26$ на числа $m_1=2, m_2=3, m_3=5$.

$$\begin{aligned} a_1 & = 26 - [26/2] \cdot 2 = 26 - 13 \cdot 2 = 0; & 26 & = 0 \pmod{2}; \\ a_2 & = 26 - [26/3] \cdot 3 = 26 - 8 \cdot 3 = 2; & 26 & = 2 \pmod{3}; \\ a_3 & = 26 - [26/5] \cdot 5 = 26 - 5 \cdot 5 = 1; & 26 & = 1 \pmod{5}. \end{aligned}$$

Приклад 6.5.

Визначити всі варіанти повних систем відрахувань по модулю $m_i = 5$. Класи відрахувань по модулю п'ять можна представити в загальному вигляді так:

$$\begin{aligned} &\bar{0} \{ \dots -10, -5, 0, 5, 10, \dots \}, \bar{1} \{ \dots -9, -4, 1, 6, 11, \dots \}, \\ &\bar{2} \{ \dots -8, -3, 2, 7, 12, \dots \}, \bar{3} \{ \dots -7, -2, 3, 6, 13, \dots \}, \\ &\bar{4} \{ \dots -6, -1, 4, 9, 14, \dots \}. \end{aligned}$$

Взявши з кожного класу по одному відрахуванню, складемо всі варіанти повних систем відрахувань по модулю п'ять:

0,1,2,3,4 – повна система найменших ненегативних відрахувань;

5,1,2,3,4 – повна система найменших позитивних відрахувань;

0,1,2,-2,-1 - повна система найменших, по абсолютній величині, відрахувань.

Як правило, повну систему відрахувань у МСЧ визначають із найменших позитивних чисел кожного класу \bar{a}_i відрахувань. У загальному виді повна система відрахувань по модулю m_i завжди містить сукупність таких чисел: **0,1,2,3,...,m_i-1**.

Коротко розглянемо дії над відрахуваннями. Арифметично скласти два відрахування a_i ($A \equiv a_i(\text{mod } m_i)$) й b_i ($B \equiv b_i(\text{mod } m_i)$) з повної системи відрахувань - це скласти їх за правилами додавання відрахувань $(a_i + b_i) \text{ mod } m_i$, тобто необхідно скласти відрахування a_i й b_i за загальними правилами додавання, а від суми $(a_i + b_i)$ визначити відрахування $(a_i + b_i) = c_i(\text{mod } m_i)$. Таблиця додавання по модулю п'ять (табл. 6.1) дає наочне уявлення про алгоритм виконання цієї операції.

Приклад 6.6.

Визначити суму наступних відрахувань по модулю п'ять: **0+1, 3+3, 3+4, 2+3, 4+1**.

Відповідно до даних табл. 6.1. визначимо: $(0+1) = 1(\text{mod } 5)$, $(3+3) = 1(\text{mod } 5)$, $(3+4) = 2(\text{mod } 5)$, $(2+3) = 0(\text{mod } 5)$, $(4+1) = 0(\text{mod } 5)$.

Таблиця 6.1

Таблиця складання по модулю 5

b_i	a_i				
	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Приклад 6.7.

Визначити різницю наступних відрахувань по модулю п'ять:

0 - 1, 3 - 3, 4 - 3, 2 - 3, 4 - 1.

Відповідно до даних табл. 6.2. визначимо:

$$(0 - 1) = 4 \pmod{5},$$

$$(3 - 3) = 0 \pmod{5},$$

$$(4 - 3) = 1 \pmod{5},$$

$$(2 - 3) = 4 \pmod{5},$$

$$(4 - 1) = 3 \pmod{5}.$$

Таблиця 6.2.

Таблиця віднімання

b_i	a_i				
	0	1	2	3	4
0	0	1	2	3	4
1	4	0	1	2	0
2	3	4	0	1	2
3	2	3	4	0	1
4	1	2	3	4	0

Приклад 6.8.

Визначити добуток відрахувань по *mod 5*: **0·1, 3·3, 4·3, 2·3, 4·1.**

Відповідно до даних табл. 6.3. визначимо:

$$0 \cdot 1 = 0 \pmod{5},$$

$$3 \cdot 3 = 4 \pmod{5},$$

$$3 \cdot 4 = 2 \pmod{5},$$

$$2 \cdot 3 = 1 \pmod{5},$$

$$4 \cdot 1 = 4 \pmod{5}.$$

Таблиця 6.3.

Таблиця множення

b_i	a_i				
	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Відомо, що відносини по модулю мають наступні властивості:

➤ - рефлексивності

$$\forall a_i (a_i \equiv a_i \pmod{m_i});$$

➤ - симетричності

$$\forall (a_i) \forall (b_i) (a_i \equiv b_i \pmod{m_i} \rightarrow b_i \equiv a_i \pmod{m_i});$$

➤ - транзитивності

$$\forall (a_i) \forall (b_i) \forall (c_i) (a_i \equiv b_i \pmod{m_i} \wedge b_i \equiv c_i \pmod{m_i} \rightarrow a_i \equiv c_i \pmod{m_i}).$$

Отже, класи відрахувань по модулю m_i володіють наступними властивостями.

Для додавання класів відрахувань: $\forall (\overline{a_i}) \forall (\overline{b_i}) (\overline{a_i + b_i} \equiv \overline{a_i} + \overline{b_i})$,

$$\forall (\overline{a_i}) \forall (\overline{b_i}) \forall (\overline{c_i}) ((\overline{a_i + b_i}) + \overline{c_i} \equiv \overline{a_i} (\overline{b_i + c_i})), \forall (\overline{a_i}) (\overline{a_i + 0} \equiv \overline{a_i}),$$

$$\forall (\overline{a_i}) \exists! (\overline{z_i}) (\overline{a_i} + \overline{z_i} \equiv 0).$$

Для перемноження класів відрахувань: $\forall (\overline{a_i}) \forall (\overline{b_i}) (\overline{a_i b_i} \equiv \overline{a_i} \overline{b_i})$,

$$\forall (\overline{a_i}) \forall (\overline{b_i}) \forall (\overline{c_i}) ((\overline{a_i b_i}) \overline{c_i} \equiv \overline{a_i} (\overline{b_i c_i})), \forall (\overline{a_i}) (\overline{a_i} 1 \equiv \overline{a_i}),$$

$$\forall (\overline{a_i}) \forall (\overline{b_i}) \forall (\overline{c_i}) ((\overline{a_i} (\overline{b_i} + \overline{c_i})) \equiv \overline{a_i} \overline{b_i} + \overline{a_i} \overline{c_i}).$$

На підставі розглянутих властивостей класу відрахувань введемо поняття непоозиційної МСЧ. Для цього задамо набір взаємно попарно простих чисел m_1, m_2, \dots, m_n , тобто найбільший загальний дільник (НЗД) будь-якої пари основ МСЧ дорівнює одиниці. Для подання числа A в МСЧ необхідно визначити набір таких відрахувань (лишків) $\{a_i\}$, щоб виконувалися наступні порівняння: $A = a_1 \pmod{m_1}$, $A = a_2 \pmod{m_2}$, ..., $A = a_n \pmod{m_n}$.

У діапазоні $[0, M)$, де $M = \prod_{i=1}^n m_i$, набір лишків a_i однозначно визначає число A у МСЧ у вигляді набору лишків $A_{MCC} = (a_1, a_2, \dots, a_n)$.

Приклад 6.9.

Нехай МСЧ задана основами $m_1 = 2$, $m_2 = 3$, $m_3 = 5$. Необхідно представити число $A = 26$ у заданій МСЧ.

Отримуємо $A_{MCC} = (a_1, a_2, a_3) = (0, 2, 1)$.

Тому що у СОІУ кожна цифра (кожний лишок a_i) кодується двійковим кодом, то одержимо $A_{MCC} = (a_1, a_2, a_3) = (0, 10, 001)$. Набір кодових слів для даної МСЧ представлений у табл. 6.4. Відзначимо, що при іншому наборі основ МСЧ операнд A буде представлятися іншою сукупністю лишків.

Для рішення завдання перекладу операндів із МСЧ у ПСЧ існує ряд методів. Розглянемо один з них.

Нехай $A_{MCC} = (a_1, a_2, \dots, a_n)$, тоді

$$A_{PCC} = \left(\sum_{i=1}^n a_i B_i \right) \bmod M = (a_1 B_1 + a_2 B_2 + \dots + a_n B_n) \bmod M,$$

де $B_i = \overline{m_i M / m_i}$,

$\overline{m_i}$ визначається як результат порівняння $\overline{m_i M / m_i} \equiv 1 \pmod{m_i}$.

Таблиця 6.4

Таблиця кодових слів у МСЧ

A	A у МСЧ			A	A у МСЧ		
	$m_1 = 2$	$m_2 = 3$	$m_3 = 5$		$m_1 = 2$	$m_2 = 3$	$m_3 = 5$
0	0	00	000	15	1	00	000
1	1	01	000	16	0	01	001
2	0	10	010	17	1	10	010
3	1	00	011	18	0	00	011
4	0	01	100	19	1	01	100
5	1	10	000	20	0	10	000
6	0	00	001	21	1	00	001
7	1	01	010	22	0	01	010
8	0	10	011	23	1	10	011
9	1	00	100	24	0	00	100
10	0	01	000	25	1	01	000
11	1	10	001	26	0	10	001
12	0	00	010	27	1	00	010
13	1	01	011	28	0	01	011
14	0	10	100	29	1	10	100

Приклад 6.10.

Нехай необхідно перевести число $A = (0, 2, 1)$ із МСЧ у ПСЧ, тоді

$$A_{PCC} = \left(\sum_{i=1}^n a_i b_i \right) \bmod M = (0 \cdot 15 + 2 \cdot 10 + 1 \cdot 6) \bmod 30 = 26,$$

де $B_1 = (1, 0, 0) = 15$, $B_2 = (0, 1, 0) = 10$, $B_3 = (0, 0, 1) = 6$,
 $M = 2 \cdot 3 \cdot 5 = 30$.

З алгоритму подання чисел у МСЧ, видно, що всі арифметичні операції у МСЧ виконуються незалежно й паралельно над однойменними розрядами (лишками), а структура операційного пристрою COIY представляєть-

ся у вигляді незалежних ПОІ, кожний з яких функціонує по своїй основі m_i МСЧ (рис. 6.3).

Додавання, вирахування й множення у МСЧ здійснюється по дуже простому алгоритму: ці операції модульні й виконуються незалежно по кожному модулю МСЧ у межах розрядної сітки $[0, M)$.

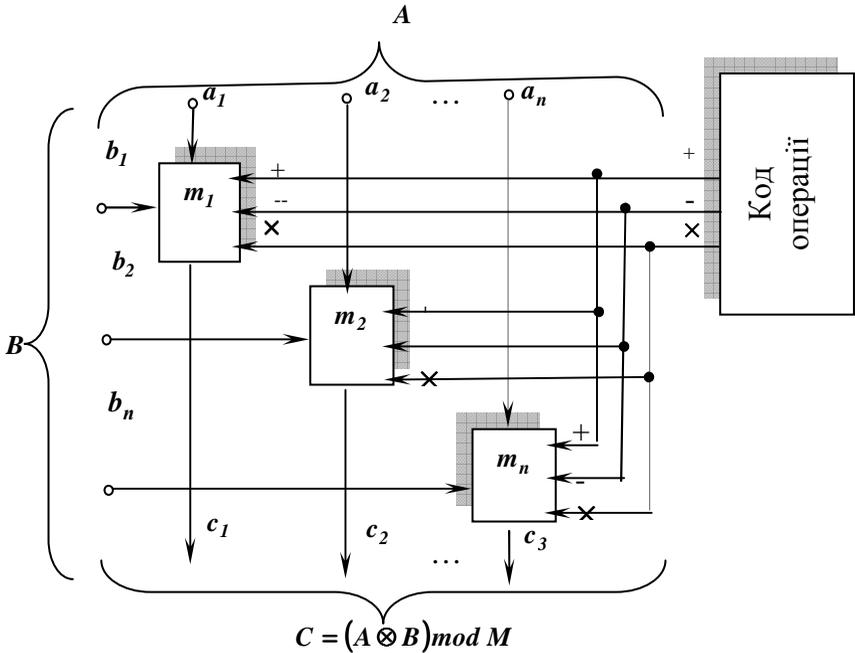


Рис. 6.3. Структура операційного пристрою COIU у МСЧ

Приклад 6.11.

Скласти два числа $A = (0,01,000)$, $B = (1,10,001)$. Результат даної операції має значення $C = (C_1, C_2, C_3) = (1,00,001)$,

де $C_1 = (0 + 1) = 1(\bmod 2)$, $C_2 = (01 + 10) = 00(\bmod 3)$,
 $C_3 = (000 + 001) = 001(\bmod 5)$.

Приклад 6.12.

Для тих же операндів визначити у МСЧ різницю чисел A та B . Результат даної операції приймає значення $C = (C_1, C_2, C_3) = (1,10,100)$

де $C_1 = (0 - 1) = 1(\bmod 2)$, $C_2 = (01 - 10) = 10(\bmod 3)$, $C_3 = (000 - 001) = 100(\bmod 5)$.

Приклад 6.13.

Визначити добуток $A \cdot B$ в МСЧ для операндів $A=(1,01,010)$, $B=(1,00,011)$. Результат даної операції приймає значення

$$C=(C_1, C_2, C_3)=(1,00,001),$$

де $C_1=(1 \cdot 1)=1(mod 2)$, $C_2=(01 \cdot 00)=00(mod 3)$, $C_3=(010 \cdot 011)=001(mod 5)$.

Позначаючи узагальнену арифметичну операцію через символ “*”, неважко показати алгоритм виконання арифметичних операцій у МСЧ у загальному виді. Нехай $A=(a_1, a_2, \dots, a_n)$, $B=(b_1, b_2, \dots, b_n)$, тоді $C = A \cdot B = ((a_1 \cdot a_2) mod m_1, (a_2 \cdot b_2) mod m_2, \dots, (a_n \cdot b_n) mod m_n)$.

6.3. Реалізація модульних операцій у МСЧ

Використання властивості малорозрядності лишків у поданні чисел у МСЧ дає можливість широкого вибору варіантів системотехнічних рішень при реалізації модульних операцій.

Сумматорний принцип (реалізується на базі малорозрядних двійкових суматорів). У ОП, що створені на базі малорозрядних суматорів кожний з розрядів числа обробляється незалежно, але час виконання всієї операції визначається часом, необхідним для одержання результату по найбільшій основі МСЧ. Відзначимо характерні недоліки властиві сумматорному варіанту реалізації арифметичних операцій:

- складність синтезу двійкових суматорів;
- великий час перетворення інформації для значних розрядних сіток СОІУ, що визначається максимальною основою МСЧ;
- складність реалізації операції множення;
- не ефективне використання двійкових елементів ОП СОІУ, внаслідок надмірності максимальних чисел, які можуть бути представлені суматорами, у порівнянні з величинами основ МСЧ;
- низька вірогідність обчислень за рахунок помилок, що виникають у процесі обчислень або в процесі переносів проміжних значень порозрядного підсумовування.

Прямий логічний принцип реалізації арифметичних операцій, ґрунтується на описі модульних операцій на рівні систем перемикальних функцій, за допомогою яких формуються значення двійкових розрядів результуючих відрахувань. Як елементна база для технічної реалізації даного принципу доцільно використовувати логічні матриці, що програмуються (ПЛМ), а також логічні інтегральні схеми, що програмуються (ПЛІС).

Принцип кільцевого зсуву (ПКЗ), заснований на використанні кільцевих регістрів зсуву (КРЗ). Особливість ПКЗ полягає в тому, що результат арифметичної операції $(a_i \pm \beta) mod m_i$ по довільному модулю МСЧ, зада-

ною сукупністю $\{m_j\}$, $j = \overline{1, n}$ основ, визначається тільки за рахунок послідовних циклічних зсувів заданої цифрової структури. Вихідна цифрова структура для кожного з модулів (основ) МСЧ представляється у вигляді змісту першого рядка (стовпця) таблиці модульного додавання (віднімання) $(a_i \pm \beta_i) \bmod m_i$ виду

$$P^{(m_i)} = \left[P_0(\alpha_0) \parallel P_1(\alpha_1) \parallel \dots \parallel P_{m_i-1}(\alpha_{m_i-1}) \right], \quad (6.1.)$$

де \parallel – знак операції конкатенації;

$P_k(\alpha_k)$ – k - розрядний двійковий код, що відповідає значенню α_k -го лишку $\alpha_k = \overline{0, m_i - 1}$ числа по модулю m_i .

Для заданого модуля $m_i = 5$ цифрова структура представиться у вигляді

$$P^{(5)} = \left[000 \parallel 001 \parallel 010 \parallel 011 \parallel 100 \right].$$

При технічній реалізації даного методу перший операнд a_i указує на номер α_{a_i} розряду $P_{a_i}(\alpha_{a_i})$ КРЗ, що визначає результат модульної операції по модулю m_i , а другий операнд β_i визначає кількість розрядів КРЗ ($\beta_i \cdot k$ - двійкових розрядів), на які необхідно зробити зсув вихідного (6.1.) умісту КРЗ відповідно до алгоритму.

Уміст розрядів КРЗ представиться у вигляді числових даних, наприклад першого рядка (стовпця) таблиці 6.5 (рис.6.4,а). На рисунку знаком \oplus позначено позитивний (проти годинникової стрілки) напрямок зсуву вмісту розрядів КРЗ. При цьому перший операнд a_i указує номер розряду КРЗ, уміст якого визначає результат даної операції, а другий операнд β_i вказує число зсувів умісту розрядів КРЗ (рис. 6.4. а, б, в).

Таблиця 6.5.

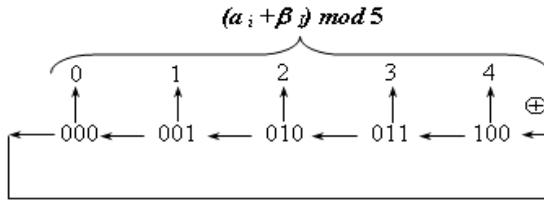
-Таблиця додавання двох чисел для $m_i = 5$

β_i	a_i				
	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

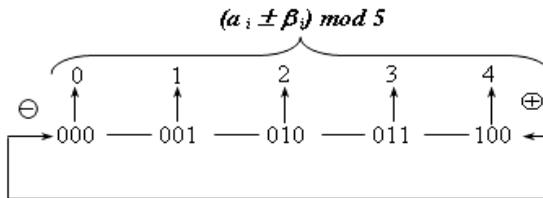
Уведемо поняття **оператора кільцевого зсуву** (ОКЗ), визначає величину (виражену в кількості розрядів, що зрушуються, КРЗ) і напрямок зрушення розрядів КРЗ, і позначається $k^{(z)}$, де

$$z = \begin{cases} +z & \text{— при позитивному напрямку зсуву умісту розрядів КРЗ;} \\ -z & \text{— при негативному (по годинниковій стрілці) напрямку зсуву умісту розрядів КРЗ;} \end{cases}$$

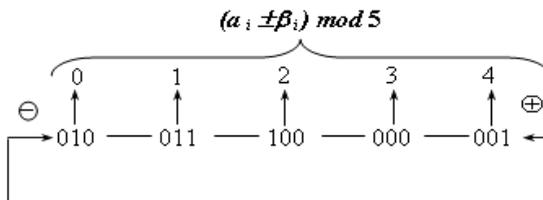
де z — показник оператора кільцевого зсуву (ПОКЗ).



а)



б)



в)

Рис. 6.4. Варіанти структур КРЗ для $m_i = 5$

Так, для операції модульного додавання ОКЗ має вигляд $k^{(+\beta_i)}$, при цьому час зсуву t_3 (що складає основний час t виконання операції) умісту розрядів КРЗ визначається виразом (вважасмо, що $t \approx t_3$) $t_3 = k \cdot \tau \cdot z$,

де $k = [\log_2 (m_n - 1)] + 1$ (m_n – модуль, по якому працює схема модульного додавання);

τ – час зсуву одного двійкового розряду (час спрацьовування одного тригера).

Для ПКЗ, використовуючи наступну тотожність

$$(a_i - \beta_i) \equiv [a_i + (m_n - \beta_i)] \bmod m_n ,$$

можна реалізувати операцію модульного вирахування $(a_i - \beta_i) \bmod m_n$.

У цьому випадку ОКЗ має вид $k^{+(m_n - \beta_i)}$.

Як видно, перевага ПКЗ у порівнянні з методами, заснованими на застосуванні двійкових суматорів, складається у відсутності міжразрядних переносів, що істотно підвищує вірогідність реалізації модульних операцій. Однак, час виконання модульних операцій порівняно великий, що знижує загальну ефективність застосування СОІУ у МСЧ.

Нейромержевий принцип реалізації позиційних операцій у МСЧ. Тривалий час вважалося, що нейронні мережі ефективні лише для вирішення так званих тяжкоформалізуємих і неформалізуємих завдань, що пов'язані з необхідністю включення в алгоритм рішення заходів процесу навчання на реальному експериментальному матеріалі. У теперішній час до цього класу завдань додається ще один клас завдань, які не потребують навчання на експериментальному матеріалі, але добре реалізуються у нейромержевому логічному базисі. Це у першу чергу завдання з яскраво вираженим паралелізмом: цифрова обробка сигналів і зображень у реальному часі, криптографічні перетворення, нейромержеві системи обробки даних та ін.

Логічний базис завдання визначає основний набір операцій, що виконуються у процесі деталізації алгоритму. Таким базисом для більшості завдань є процедура $\{\sum \overline{ax}\}$. До таких завдань відносяться: векторна алгебра, ортогональні перетворення сигналів, рішення диференціальних рівнянь, рівнянь Пуассона, Ейлера й ін.

Основу нейромержевого логічного базису становлять операції типу $\{\sum \overline{ax}, \text{sign}\}$, які максимально відповідають логічному базису основних завдань, що розв'язуються.

Табличний принцип (ТП) (на основі використання постійних запам'ятовувачих пристроїв (ПЗП)). Основні переваги табличного варіанту побудови ОП СОІУ у МСЧ:

- матричні схеми мають досить високу надійність, тому що реалізуються у вигляді компактних ПЗП;

- простота матричних схем і дешифраторів, що мають кількість виходів, яка відповідає основі МСЧ;
- висока швидкодія, результат операції може бути отриманий у момент надходження вхідних операндів, тобто за один такт, час виконання арифметичних операцій у МСЧ відповідає тактовій частоті СОІУ.

Тому розглянемо ТП більш докладно. Під табличною реалізацією арифметичних операцій $C_i = f(a_i, \beta_i)$ будемо розуміти організацію такої таблиці, у якій кожній комбінації вхідних величин a_i і β_i відповідає одне й тільки одне значення вихідної величини C_i . Нехай $[0, x)$ - діапазон зміни величини a_i , $[0, y)$ - діапазон зміни величини β_i , $[0, z)$ - діапазон зміни величини C_i .

Основні характеристики таблиці:

- $j = x^2 - z$ - надмірність таблиці;
- $\gamma_2 = \frac{z}{x^2} 100\%$ - коефіцієнт використання таблиці;
- $w = \frac{x^2}{z} 100\%$ - коефіцієнт надмірності таблиці.

У загальному випадку табличний операційний пристрій СОІУ для реалізації арифметичних операцій (в унітарному коді) являє собою двохходовий ПЗП. Для кожного із входів кількість вхідних шин для l -байтової ($8l$ двійкових розряду) СОІУ дорівнює 2^{8l} . При цьому загальна кількість логічних схем збігу "І" у вузлах ПЗП (що в основному й визначає загальну кількість устаткування табличного операційного пристрою СОІУ) дорівнює $V_{1\text{ПСЧ}} = 2^{8l} \times 2^{8l} = 2^{16l}$. Виходячи з формули, зрозуміло, що таблична реалізація цілочисельних модульних арифметичних операцій у ПСЧ доцільна тільки для значення $l=1$. Дійсно, у цьому випадку $V_1 = 2^{16} = 65536$, що є прийнятною кількістю устаткування для сучасного розвитку елементної бази. Однак, як відзначалося вище, тенденція розвитку засобів обробки цифрової інформації спрямована на збільшення довжини розрядної сітки СОІУ. Вже зараз пропонується до практичного використання СОІУ для $l=2$. У цьому випадку $V_{4\text{ПСЧ}} = 2^{32} \times 2^{32} = 2^{64}$ і $V_{8\text{ПСЧ}} = 2^{64} \times 2^{64} = 2^{128}$. Якщо врахувати, наприклад, що $2^{32} = 4294967296$, $2^{64} = 18446744073709551616$, то очевидно, що табличний метод реалізації арифметичних операцій у ПСЧ практично не можливо застосувати.

Інші, позитивні результати можна одержати, якщо застосувати МСЧ у СОІУ в якості системи числення. Дійсно, у загальному випадку, при реалізації алгоритмів модульної обробки інформації для табличного операцій-

ного пристрою COIU необхідно $V_{МСЧ} = \sum_{i=1}^n m_i^2$ схем збігу. Тоді для COIU у МСЧ із $l=4$ і $l=8$ відповідно маємо $V_{4МСЧ}=2397$ і $V_{8МСЧ}=13275$, що цілком прийнятно, якщо використати при реалізації арифметичних операцій додавання, вирахування й множення у МСЧ сучасну мікроелектронну елементну базу.

Розглянемо алгоритми реалізації модульних операцій, які дозволяють підвищити ефективність застосування табличної арифметики.

Нехай задана пара операндів $A = (a_1, \dots, a_n)$ і $B = (\beta_1, \dots, \beta_n)$ у МСЧ із попарно взаємно простими основами m_1, \dots, m_n . Необхідно реалізувати у табличному варіанті узагальнену модульну операцію $(A \otimes B) \bmod M$. Відповідно до правил виконання арифметичних операцій кожній парі лишків a_i і β_i ставиться у відповідність значення $(a_i \otimes \beta_i) \bmod m_i$. Таким чином, весь канал обчислювальної операції $(A \otimes B) \bmod M$ можна представити у вигляді n незалежних однотипних ПЗП.

Складемо таблицю із числових значень $a_i \beta_i \bmod m_i$ (табл. 6.6.).

Таблиця 6.6.

Узагальнена арифметична операція по довільному модулю

a	a_0	...	$\frac{a_{m-1}}{2}$	$\frac{a_{m+1}}{2}$...	a_{m-1}
b_0	$(a_0 \otimes b_0) \bmod m =$ $= c_{(0)0}$...	$(\frac{a_{m-1}}{2} \otimes b_0) \bmod m =$ $= c_{(\frac{m-1}{2})0}$	$(\frac{a_{m+1}}{2} \otimes b_0) \bmod m =$ $= c_{(\frac{m+1}{2})0}$...	$(a_{m-1} \otimes b_0) \bmod m =$ $= c_{(m-1)0}$
$b_{\frac{m-1}{2}}$	$(a_0 \otimes \frac{b_{m-1}}{2}) \bmod m =$ $= c_{0(\frac{m-1}{2})}$...	$(\frac{a_{m-1}}{2} \otimes \frac{b_{m-1}}{2}) \bmod m =$ $= c_{(\frac{m-1}{2})(\frac{m-1}{2})}$	$(\frac{a_{m+1}}{2} \otimes \frac{b_{m-1}}{2}) \bmod m =$ $= c_{(\frac{m+1}{2})(\frac{m-1}{2})}$...	$(a_{m-1} \otimes \frac{b_{m-1}}{2}) \bmod m =$ $= c_{(m-1)(\frac{m-1}{2})}$
$b_{\frac{m+1}{2}}$	$(a_0 \otimes \frac{b_{m+1}}{2}) \bmod m =$ $= c_{0(\frac{m+1}{2})}$...	$(\frac{a_{m-1}}{2} \otimes \frac{b_{m+1}}{2}) \bmod m =$ $= c_{(\frac{m-1}{2})(\frac{m+1}{2})}$	$(\frac{a_{m+1}}{2} \otimes \frac{b_{m+1}}{2}) \bmod m =$ $= c_{(\frac{m+1}{2})(\frac{m+1}{2})}$...	$(a_{m-1} \otimes \frac{b_{m+1}}{2}) \bmod m =$ $= c_{(m-1)(\frac{m+1}{2})}$
b_{m-1}	$(a_0 \otimes b_{m-1}) \bmod m =$ $= c_{0(m-1)}$...	$(\frac{a_{m-1}}{2} \otimes b_{m-1}) \bmod m =$ $= c_{(\frac{m-1}{2})(m-1)}$	$(\frac{a_{m+1}}{2} \otimes b_{m-1}) \bmod m =$ $= c_{(\frac{m+1}{2})(m-1)}$...	$(a_{m-1} \otimes b_{m-1}) \bmod m =$ $= c_{(m-1)(m-1)}$

Ця таблиця симетрична щодо діагоналей, вертикалі й горизонталі, що проходять між числами $(m_i - 1)/2$ й $(m_i + 1)/2$. Симетричність таблиці щодо лівої діагоналі визначається комутативністю операції множення, симетричність щодо правої діагоналі визначається тим, що $(m_i - a_i)(m_i - \beta_i) \equiv a_i \beta_i \pmod{m_i}$.

Симетричність щодо вертикалі й горизонталі визначається з умови кратності суми симетричних чисел $a_i \beta_i + a_i(m_i - \beta_i) \equiv 0 \pmod{m_i}$, $a_i \beta_i + \beta_i(m_i - a_i) \equiv 0 \pmod{m_i}$.

Використання основних властивостей МСЧ дозволяє для реалізації операції модульного множення $a_i \beta_i \pmod{m_i}$ мати числову інформацію тільки про восьму частину таблиці, але при цьому необхідно проводити попередній аналіз величин вхідних операндів a_i і β_i . Це збільшує час і технічну складність реалізації арифметичної операції.

Для найбільш ефективної реалізації операції $a_i \beta_i \pmod{m_i}$ застосовуються методи спеціального кодування, що дозволяють у чотири рази зменшити таблицю модульного множення. Розглянемо один з варіантів виконання операції модульного множення за допомогою коду інформаційного стиску (КІС).

Нехай дані вхідні операнди a_i й β_i . Значення $a_i(\beta_i)$, що лежать у діапазоні $[0, (m_i - 1)/2)$, можуть бути закодовані довільним способом, а значення $a_i(\beta_i)$, що лежать у діапазоні $[(m_i + 1)/2, m_i - 1)$, кодуються як $m_i - a_i$, $(m_i - \beta_i)$. Для відмінності діапазонів вводиться наступний індекс (ознака)

$$\gamma(\beta) = \begin{cases} 0, & \text{коли } 0 \leq a_i(\beta_i) \leq (m_i - 1)/2, \\ 1, & \text{коли } (m_i + 1)/2 \leq a_i(\beta_i) \leq m_i - 1. \end{cases}$$

Алгоритм визначення результату операції модульного множення за допомогою КІС наступний. Якщо задані два операнда в КІС $a_i = (\gamma_a, a'_i)$, $\beta_i = (\gamma_\beta, \beta'_i)$, то для того, щоб одержати добуток цих чисел по модулю m_i , досить знайти добуток $a'_i \beta'_i \pmod{m_i}$ і інвертувати його узагальнений індекс γ_i , у випадку, якщо γ_a відрізняється від γ_β , тобто $a_i \beta_i \pmod{m_i} = (\gamma_i, a'_i \beta'_i \pmod{m_i})$, де

$$\gamma = \begin{cases} \bar{\gamma}_i, & \text{коли } \gamma_a \neq \gamma_\beta, \\ \gamma_i, & \text{коли } \gamma_a = \gamma_\beta, \end{cases} \quad \text{і відповідно } a'_i = \begin{cases} a_i, & \text{коли } \gamma_a = 0, \\ m_i - a_i, & \text{коли } \gamma_a = 1. \end{cases}$$

При використанні даного алгоритму ПЗП, що реалізує операцію модульного множення, конструктивно зменшуються в чотири рази.

При виконанні арифметичної операції табличними методами в деяких випадках можливо додаткове зменшення устаткування за рахунок того, що будуватися не єдина таблиця для модульних операцій, а k більш дрібних таблиць, що дозволяють дати результати по кожному з k розрядів результату, де k - розрядність регістра, що необхідна для зберігання цифри по розглянутій основі.

Цікаві результати можна одержати, досліджуючи можливості реалізації однієї модульної операції за допомогою таблиць, що реалізують обратну їй операцію і навпаки.

$$[(\gamma_a, a'_i) + (\gamma_\beta, \beta'_i)] + \{[m_i - (\gamma_a, a'_i)] - (\gamma_\beta, \beta'_i)\} = 0 \pmod{m_i}, \quad (6.2)$$
де $a_i = (\gamma_a, a'_i)$, $\beta_i = (\gamma_\beta, \beta'_i)$ – вхідні операнди, що представлені у КІС.

Вираз (6.2) можна записати у вигляді

$$(\gamma_a, a'_i) + (\gamma_\beta, \beta'_i) = m_i - \{[m_i - (\gamma_a, a'_i)] - (\gamma_\beta, \beta'_i)\}. \quad (6.3)$$

З виразу (6.3) витікає, що для одержання результату операції модульного додавання у КІС досить знати результат операції модульного вирахування.

Розглянемо можливості процедури, що представлена виразом (6.3), для виконання операцій множення, додавання й вирахування. Алгоритм, що реалізує модульне додавання за допомогою таблиці для виконання операції модульного вирахування $(a'_i - \beta'_i) \pmod{m_i}$ можна представити у такий спосіб.

1. Зменшуване $a_i = (\gamma_a, a'_i)$ інвертується по модулю m_i , тобто $\bar{a}_i = ((\gamma_a + 1) \pmod{2}, a'_i)$. Віднімаємо (γ_β, β'_i) залишаємо без змін.

2. За допомогою ПЗП для модульного вирахування по вхідним операндам a'_i і β'_i визначається результат операції $(a'_i - \beta'_i) \pmod{m_i}$. Як і для алгоритму модульного множення, індекс результату операції формується у відповідності зі значеннями індексів відповідних операндів, тобто у відповідності зі значеннями $(\gamma_a + 1) \pmod{2}$ й γ_β , де

$$\gamma_i = \begin{cases} \bar{\gamma}, & \text{коли } (\gamma_a + 1) \pmod{2} \neq \gamma_\beta, \\ \gamma, & \text{коли } (\gamma_a + 1) \pmod{2} = \gamma_\beta. \end{cases}$$

Отже, результат операції буде мати вигляд $(\gamma_i(a'_i - \beta'_i) \pmod{m_i})$.

3. Інвертуючи цей результат по модулю m_i одержимо результат модульного додавання $((\gamma_i + 1) \pmod{2}, (a'_i - \beta'_i) \pmod{m_i})$, що схематично можна представити у вигляді

$$(a_i - \beta_i) \rightarrow [(m_i - a_i) - \beta_i] \rightarrow \{m_i - [(m_i - a_i) - \beta_i]\} \rightarrow (a_i + \beta_i).$$

Результат операції модульного вирахування за допомогою ПЗП, що реалізує операцію модульного додавання можна визначити з використанням наступного виразу, що отримано з (6.2)

$$(\gamma_a, a'_i) - (\gamma_\beta, \beta'_i) = \{(\gamma_a, a'_i) + [m_i - (\gamma_\beta, \beta'_i)]\}.$$

Схематично цей алгоритм можна представити в наступному вигляді

$$(a_i + \beta_i) \rightarrow [a_i + (m_i - \beta_i)] \rightarrow (a_i - \beta_i).$$

При обробці інформації в МСЧ виникає необхідність отримати зворотну мультиплікативну величини A_n^{-1} числа A (тобто $A \cdot A^{-1} = 1(\text{mod } M)$),

де $M = \prod_{i=1}^n m_i$. Так, зокрема, при реалізації операції ділення двох операндів A_1 і A_2 необхідно робити операцію модульного ділення над лишками операндів,

$$(a_{1i} / a_{2i}) \text{mod } m_i, \quad \text{де } A_1 = (a_{11}, a_{12}, \dots, a_{1i}, \dots, a_{1n}), \\ A_2 = (a_{21}, a_{22}, \dots, a_{2i}, \dots, a_{2n}), \text{ та } a_{1i} \equiv A_1(\text{mod } m_i), a_{2i} \equiv A_2(\text{mod } m_i).$$

Визначення $(A_1 / A_2) \text{mod } M$ ґрунтується на заміні операції ділення на операцію множення, де дільник A_2 замінюється на співмножник A_2^{-1} ,

$$A_1 / A_2 = A_1 \cdot \frac{1}{A_2} = A_1 A_2^{-1}, \quad \text{тобто виконується } n \text{ операцій}$$

$a_{1i} / a_{2i} = a_{1i} \cdot a_{2i}^{-1}(\text{mod } m_i)$. Таким чином, у МСЧ потрібно порівняти операнди виду $a_{2i} \cdot a_{2i}^{-1} \equiv 1(\text{mod } m_i)$. Це завдання існує й при реалізації операції перетворення чисел із МСЧ у ПСЧ і зворотно. Дійсно, визначення ортогональних базисів $\beta_i = \frac{M}{m_i}$ у МСЧ призводить до необхідності порівняння $\beta_i \equiv 1(\text{mod } m_i)$ по базі $\overline{m_i}$ ортогонального базису, тобто визначення величини $(M / m_i)^{-1}$.

Один з алгоритмів визначення зворотної мультиплікативної величини ґрунтується на застосуванні малої теореми Ферма, яка стверджує наступне, якщо p - просте число, і ціле a не ділиться на p , то $a^{p-1} \equiv 1(\text{mod } p)$ (або $a^{p-1} - 1$ ділиться на p). У відповідності, з даною теоремою отримано

$$a_{2i}^{m_i-1} \equiv 1(\text{mod } m_i), \text{ або}$$

$$a_{2i}^{-1} \equiv a_{2i}^{m_i-2}(\text{mod } m_i). \quad (6.4)$$

Вираз (6.4) є формулою для знаходження зворотної мультиплікативної величини числа при простому значенні m_i . Розглянемо приклади визначення $(a_{1i} / a_{2i}) \bmod m_i$.

Приклад 6.14.

Визначимо результат ділення числа $A_{21} = (1,0,1)$ на число $A_7 = (1,1,2)$ у МСЧ, заданої основами $m_1 = 2$, $m_2 = 3$, $m_3 = 5$, тобто знайдемо значення $A_{21} / A_7 \pmod{M}$.

Відповідно до викладеного $A_{21} / A_7 = A_{21} \cdot A_7^{-1}$. Для операнда A_7 визначимо значення A_7^{-1} . На підставі теореми Ферма визначимо для числа A_7^{-1} відповідні лишки $a_1^{-1} \equiv 1^0 \equiv 1 \pmod{2}$, $a_2^{-1} \equiv 1 \equiv 1 \pmod{3}$, $a_3^{-1} \equiv 2^3 \equiv 3 \pmod{5}$. Таким чином, отримуємо

$$A_{21} / A_7 = A_{21} \cdot A_7^{-1} = (1,0,1) \cdot (1,1,3) = (1,0,3) = A_3.$$

6.4 Реалізація немодульних операцій у МСЧ.

Існуючі методи виконання немодульних операцій, зокрема методи порівняння чисел у МСЧ є трудомісткими операціями. Даний недолік обумовлений значними часовими витратами, що викликані необхідністю перетворення операндів із МСЧ у позиційну систему числення й зворотно. Даний недолік можна усунути використовуючи, наприклад, алгоритми порівняння операндів у МСЧ, які засновані на принципі одержання й порівняння унітарного однорядового коду без попереднього перетворення операндів, що порівнюються з коду МСЧ у позиційний код і зворотно.

Нехай задана МСЧ упорядкованими $(m_i < m_{i+1})$ взаємно попарно простими натуральними числами (основами) m_1, m_2, \dots, m_n і нехай операнди, що порівнюються представлені у вигляді $A = (a_1, a_2, \dots, a_n)$, $B = (\beta_1, \beta_2, \dots, \beta_n)$.

При цьому передбачається, що вихідні операнди лежать у відповідних інтервалах $\left[\frac{j_1 M}{m_n}, \frac{(j_1 + 1) M}{m_n} \right)$ та $\left[\frac{j_2 M}{m_n}, \frac{(j_2 + 1) M}{m_n} \right)$, де $M = \prod_{i=1}^n m_i$.

Номер $j_k + 1$ інтервалу визначається як

$$j_k = \overline{\gamma_n m_n \pmod{m_n}},$$

де величина $\overline{m_n}$ є результатом вирішення порівняння $\overline{m_n M} / m_n \equiv 1 \pmod{m_n}$.

Якщо $j_1 \neq j_2$ то операція арифметичного порівняння може бути реалізована порівнянням номерів інтервалів, а саме: якщо $j_1 < j_2$, то $A < B$, якщо $j_1 > j_2$, то $A > B$. При $j_1 = j_2$ визначається номер $j_3 + 1$ інтервалу $\left[\frac{j_3 M}{m_n}, \frac{(j_3 + 1) M}{m_n} \right)$, у якому розташоване число $A - B$. Якщо

$0 \leq j_3 < (m_n + 1) / 2$, то $A < B$, а якщо $\frac{m_n + 1}{2} \leq j_3 < m_n$, то $A > B$.

Метод арифметичного порівняння чисел у МСЧ припускає перетворення чисел до виду $A^{(H)} = (0, 0, \dots, \gamma_n)$, що вимагає $n - 1$ тактів операції нулевизації. Крім цього необхідно зробити позиційне порівняння номерів $(j_1 + 1)$ і $(j_2 + 1)$ інтервалів влучення вихідних операндів A і B .

Розглянемо метод порівняння, що використовує арифметичні паралельні вираховування. Нехай операнди, що порівнюються можуть перебувати в

довільних інтервалах $[jm_i, (j + 1)m_i)$, де $j = \overline{1, N - 1}$ $\left(N = \prod_{\substack{k=1 \\ k \neq i}}^n m_k \right)$.

Вихідні операнди A та B приводяться до чисел, що кратні m_i , шляхом модульного вираховування наступного виду

$$A_{m_i} = A - a_i = (a_1^{(i)}, a_2^{(i)}, \dots, a_{i-1}^{(i)}, 0, a_{i+1}^{(i)}, \dots, a_n^{(i)}),$$

$$B_{m_i} = B - \beta_i = (\beta_1^{(i)}, \beta_2^{(i)}, \dots, \beta_{i-1}^{(i)}, 0, \beta_{i+1}^{(i)}, \dots, \beta_n^{(i)}),$$

де $a_i = (a'_1, a'_2, \dots, a_i, a'_n)$, $\beta_i = (\beta'_1, \beta'_2, \dots, \beta_i, \beta'_n)$.

Далі, за допомогою набору констант $0, m_i, 2m_i, \dots, (N - 1)m_i$, представлених за $(n - 1)$ -ю основою МСЧ $m_1, m_2, \dots, m_{i+1}, \dots, m_n$, здійснюється побудова однорядового коду у вигляді

$$K_n^{(n_A)} = \{z_N z_{N-1} \dots z_2 z_1\}, z_{n_A} = 0 \quad (z_l = 1; l = \overline{1, N}, l \neq n_A);$$

$$K_n^{(n_B)} = \{z'_N z'_{N-1} \dots z'_2 z'_1\}, z_{n_B} = 0 \quad (z'_l = 1; l = \overline{1, N}, l \neq n_B).$$

Алгоритм побудови однорядового коду в МСЧ можна представити в такий спосіб:

$$\left\{ \begin{array}{l} A_{m_1} - 0 = z_1, \\ A_{m_2} - m_i = z_2, \\ A_{m_i} - 2m_i = z_3, \\ \dots\dots\dots \\ A_{m_i} - \left(\prod_{\substack{\rho=1 \\ \rho \neq i}}^{n-1} m_\rho - 1 \right) m_i = z_N, \end{array} \right. \quad \left\{ \begin{array}{l} B_{m_i} - 0 = z'_1, \\ B_{m_i} - m_i = z'_2, \\ B_{m_i} - 2m_i = z'_3, \\ \dots\dots\dots \\ B_{m_i} - \left(\prod_{\substack{\rho=1 \\ \rho \neq i}}^{n-1} m_\rho - 1 \right) m_i = z_N. \end{array} \right.$$

У цьому випадку маємо $z_{n_A} = 0$, коли $A_{m_i} - n_A \cdot m_i = 0$;
 $z_{n_A} = 1$, коли $A_{m_i} \neq n_A \cdot m_i$;
 $z'_{n_B} = 0$, коли $B_{m_i} - n_B \cdot m_i = 0$;
 $z'_{n_B} = 1$, коли $B_{m_i} \neq n_B \cdot m_i$.

Геометрично дану процедуру порівняння можна пояснити наступним чином. Інтервал $\left[0, \prod_{i=1}^n m_i \right)$ розбивається на n відрізків. Вихідні операнди

A и B , шляхом вираховання констант виду $\prod_{\substack{\rho=1 \\ \rho \neq i}}^{n-1} m_\rho$, зміщують на лівий

край інтервалу їхнього влучення. Це рівнозначно приведенню операндів, що порівнюються до чисел, кратних основі m_i МСЧ. Виходячи із цього, точність W порівняння операндів залежить від величини основи, тобто $W = W(m_i)$.

Розглянемо алгоритм паралельних вирахувань із порівнянням лишків. Введемо операцію порівняння безпосередньо лишків a_n, β_n , по основі m_n . У цьому випадку результат порівняння, одночасно з результатом порівняння однорядового коду $K_N^{(n_A)}$ й $K_N^{(n_B)}$, буде визначатися з максимальною точністю W_{max} . Алгоритм визначення результату операції арифметичного порівняння може бути представлений як:

$$\begin{array}{l} \text{коли } n_A > n_B, \text{ то } A > B; \\ \text{коли } n_A < n_B, \text{ то } A < B; \text{ при цьому} \\ \text{коли } n_A = n_B, \end{array} \quad \left\{ \begin{array}{l} a_n = \beta_n, \text{ то } A = B, \\ a_n > \beta_n, \text{ то } A > B, \\ a_n < \beta_n, \text{ то } A < B. \end{array} \right.$$

Сутність даного алгоритму ґрунтується на проведенні порівняння не безпосередньо операндів A і B , а величин m_i і $\chi = (A - B) \bmod M = (\gamma_1, \gamma_2, \dots, \gamma_n)$.

У цьому випадку визначається значення $\chi_{m_i} = \chi - \gamma_1 = (0, \gamma'_2, \gamma'_3, \dots, \gamma'_n)$, де константи $\gamma_1 = (\gamma_1, \gamma'_2, \gamma'_3, \dots, \gamma'_n)$ та $\gamma_1 = (a_1 - \beta_1) \bmod m_1$ представлені в заданій МСЧ.

Тоді загальний алгоритм порівняння операндів представимо у вигляді

$$\begin{cases} A > B, & \text{коли } \chi_{m_i} \leq m_1; \\ A < B, & \text{коли } \chi_{m_i} > m_1; \\ A = B, & \text{коли } \chi_{m_i} = 0. \end{cases}$$

6.5. Модулярні обчислення

Існує досить велика кількість підходів до реалізації суматорів по модулю m_i . Розглянемо найбільш типові й прості схеми модулярного підсумовування (рис. 6.5.).

Перша з них обчислює модулярну суму $|x + y|_m$ за допомогою таблиці розміром $n \times 2^{2n}$, $n = \lceil \log_2(m) \rceil$. Для двох відповідних елементів просто вибирається відповідь із великої таблиці. Це рішення дуже гарно підходить для випадків, коли довжина слова мала, наприклад, $n \leq 4$. Для великих значень модулів, пам'ять таблиць була б значного розміру, тому інші схеми для виконання операції підсумовування виявляються в цьому випадку більше привабливими.

Наступне рішення ґрунтується на використанні суматора й одного ПЗП (таблиці), що містить всі можливі значення операції $|x + y|_m$. При цьому істотно скорочується розмір підстановочної таблиці з $n \times 2^{2n}$ до $n \times 2^{n+1}$, що дає можливість розширювати набір модулів якщо буде потреба застосування великого динамічного діапазону або надлишкових модульних каналів для корекції помилок.

Третє схемне рішення підсумовування є найпоширенішим у більшості випадків. У даному випадку використовуються два суматори й мультиплексор для вибору результату відповідно до виразу:

$$|x + y|_m = \begin{cases} x + y & 0 \leq x + y < m \\ x + y - m & m \leq x + y \end{cases}.$$

Перемножувачи (рис. 6.6.) обчислюють модулярний добуток $|x \cdot y|_m$ за допомогою наступної рівності (закон квадратів):

$$xy = \left(\frac{x+y}{2}\right)^2 - \left(\frac{x-y}{2}\right)^2, \quad (6.6)$$

де $0 \leq x, y < m$.

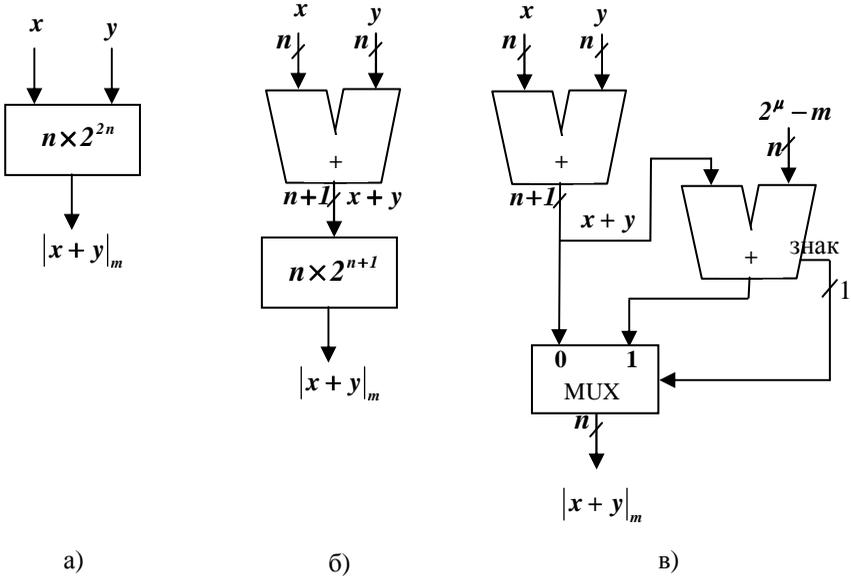


Рис. 6.5. Модулярне підсумовування. (а) - за допомогою великої таблиці; (б) - з попереднім звичайним підсумовуванням; (в) - без використання таблиць.

Модулярне множення з використанням виразу (6.6) можна записати у такий спосіб:

$$|xy|_m = \left| \Phi(s^+) - \Phi(s^-) \right|_m, \quad (6.7)$$

де $\Phi(s) = |s^2|_m$;

$$s^+ = \frac{x+y}{2} \quad \text{і відповідно} \quad s^- = \frac{x-y}{2},$$

і добуток $|xy|_m$ можна обчислювати по формулі:

$$|xy|_m = \left\| \frac{1}{4} \left| (x+y)^2 - (x-y)^2 \right| \right\|_m.$$

Існування операції ділення на 2 ставить під погрозу цілочисельність проміжних обчислень і, відповідно, правильність результату після використання таблиць підстановок. Проте Тейлором була доведена теорема, яка показує, що навіть коли при обчисленні (6.7) з'являться проміжні дробі, вони взаємно знищуються.

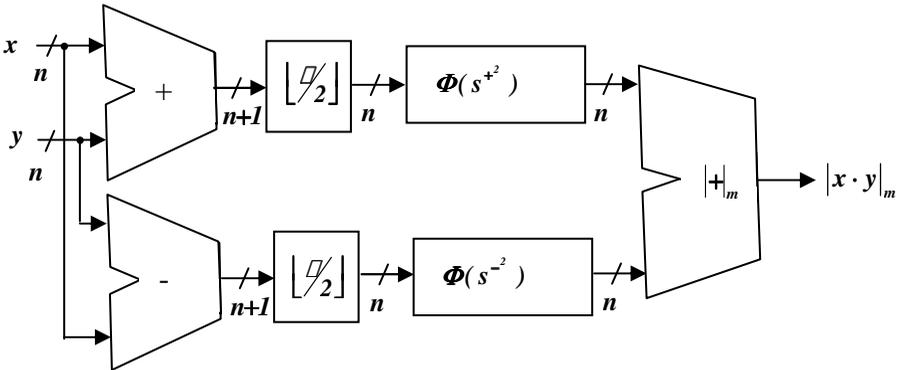


Рис. 6.6. Схема модулярного перемножувача по модулю m_i , що функціонує на підставі використання закону квадратів.

Розглянемо роботу перемножувача, що використовує арифметику покажчиків, який є альтернативною по складності й швидкості перемножувачам, які використовують закон квадратів. Їхнє використання обмежене простими модулями й ґрунтується на здійсненні перетворення в статичну форму, у якій перемноження може виконуватися більш швидко за допомогою операції підсумування.

Робота цього перемножувача ґрунтується на математичних властивостях полів Галуа $GF(p)$, де p - просте число. Всі ненульові елементи поля Галуа можуть бути отримані шляхом багаторазового піднесення до ступеня примітивного елемента g_j , що породжує поле $GF(p)$. Цю властивість полів Галуа можна використати для перемноження в $GF(m_j)$ завдяки використанню ізоморфізму між мультиплікативною групою $Q = \{1, 2, \dots, m-1\}$ по модулю m_j , і адитивною групою $I = \{0, 1, \dots, m-2\}$ по модулю $(m_j - 1)$.

Таким чином, множення двох чисел q_j і q_k можна робити обчислюючи модулярну суму відповідних покажчиків i_j і i_k , а потім проводячи зворотне перетворення зі статечного простору у первинний вид. Якщо один з операндів на вході перемножувача дорівнює нулю то в цьому випадку виходить нульовий результат добутку.

Ступеня i_j й i_k для q_j й q_k , відповідно, можуть бути заздалегідь визначені й поміщені в таблиці. Додавання ступенів виконує суматор по модулю $m_j - 1$. Зворотне перетворення зі статечного подання i_j й i_k у первинне q_j й q_k також може бути виконане за допомогою попередньо обчислених таблиць.

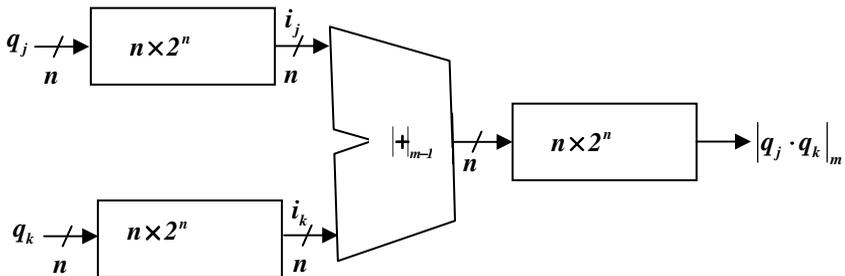


Рис. 6.7. Схема перемноження, заснованого на вирахуванні ступенів.

Приклад 6.15.

Розглянемо як приклад роботу цього перемножувача на прикладі перемноження двох чисел 14 і 28 по модулю 31. Тому що 31 - просте число то існує породжуючий елемент g , який дає можливість асоціювати кожний елемент мультиплікативної групи $Q = \{1, 2, \dots, 31\}$ з елементом адитивної групи $I = \{0, 1, \dots, 30\}$. Відповідність задається виразом $q_n = |g^n|_{31}$, де $g = 3$, і $q_n \in Q$, $i_n \in I$. У табл. 6.7. розрахована відповідність між елементами групи Q й відповідним ступенем з адитивної групи I . Ця таблиця в сутності і являє собою зміст таблиці розміром $2^5 \cdot 5$ прямого й зворотнього перетворення у перемножувачі, що зображено на рис. 6.7.

Розглянемо роботу перемножувача Галуа (рис. 6.7., рис. 6.8, табл. 6.7.) на прикладі перемноження $|14 \cdot 28|_{31}$. Отже $q_j = 14$ й $q_k = 28$, а добуток $|q_j q_k|_{31}$ отримується за рахунок підсумовування відповідних їм

елементів i_j і i_k , обраних з табл. 6.7. Таким чином, покажчики мають значення $i_j = 22$ й $i_k = 16$ і $|i_j + i_k|_{30} = 8$. Елементу $i_n = 8$ в табл. 6.7. відповідає $q_n = 20$, отже, $|14 \cdot 28|_{31} = 20$.

Таблиця 6.7.

Зміст таблиці для множення по модулю

q_n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
i_n	0	24	1	18	20	25	28	12	2	14	23	19	11	22	21
q_n	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
i_n	6	7	26	4	8	29	17	27	13	10	5	3	16	9	

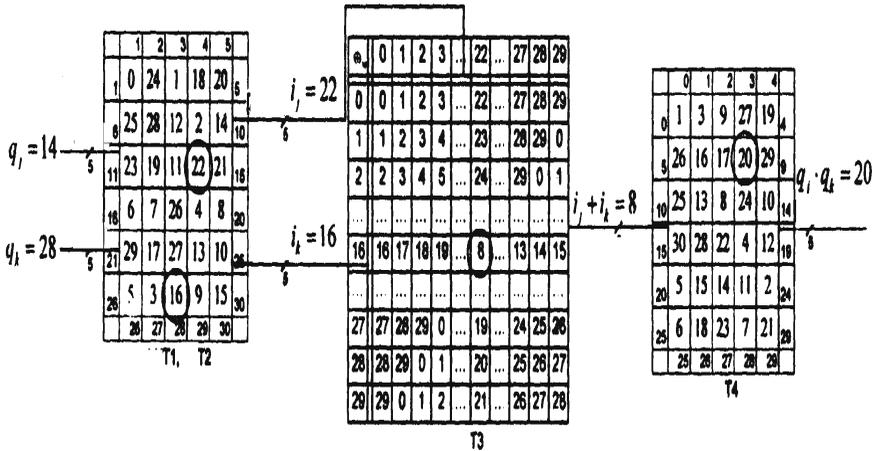


Рис. 6.8. Схема роботи 5-бітного перемножувача Галуа.

На рис. 6.8. показано, яким чином відбувається перемноження чисел 14 і 28 по модулю 31 за схемою, що зображена на рис. 6.7. Для спрощення дві таблиці 1 і 2 об'єднані в одну і являють собою таблиці, що переводять числа, що перемножуються в статечне подання відповідно до табл. 6.7., а в якості суматора виступає простий модулярний суматор, який зображений на рис. 6.5(а). Таблиця 3 виконує додавання по модулю 30, а таблиця 4 переводить результат зі статечного подання назад у первинний вигляд. Таблиця 4 являє собою табл. 6.7., тільки відсортовану по i_n . З рис. 6.8. видно, що значення, яке надійшло на вхід таблиці, розглядається як лінійна адреса елемента, що буде виданий на вихід таблиці.

6.6. Функціональне кодування

Навіть у тому випадку, коли МСЧ не надлишкова, відмова елементів, що відносяться до будь якого КОІ, не призводить до повного виходу СОІУ з ладу. Якщо встановлено факт появи помилки й вона локалізована, то, без несправного модуля із МСЧ, можна продовжувати обчислення при де якому зменшенні точності. Тому, застосовуючи для виявлення помилок, що виникають у ході рішення завдання, програмні методи контролю, можна забезпечити високу надійність СОІУ, що працюють у модулярної системі числення, не залучаючи практично ніякого додаткового устаткування.

Любий алгоритм можна розглядати як деяке відображення безлічі вхідних змінних x_1, \dots, x_m у безлічі вихідних змінних y_1, \dots, y_n , причому в якості змінних можуть використатися дійсні, цілі або булеві числа. Розширимо безліч вихідних змінних, додаючи функції y_{n+1}, \dots, y_{n+r} такі, що:

$$y_{n+i}(x_1, \dots, x_m) = \varphi_i(y_1, \dots, y_n), \text{ де } i = 1, 2, \dots, r.$$

Ці додаткові функції можуть бути використані для виявлення й виправлення помилок, що виникають у ході обчислення. Мова йде про використання таких коригувальних кодів, символами яких служать не числа, а досить складні функції.

Для таких вихідних функцій y_1, \dots, y_n які є лінійними щодо деякої базисної системи $v_1(x_1, \dots, x_m), \dots, v_s(x_1, \dots, x_m)$, можна записати

$$y_i(x_1, \dots, x_m) = \sum_{j=1}^s \lambda_{ij} v_j(x_1, \dots, x_m),$$

де $i = 1, 2, \dots, m$, причому всі змінні й коефіцієнти λ_{ij} відносяться до безлічі дійсних чисел.

Слід зазначити, що клас подібних функцій є досить широким, тому що в їхній склад входять будь-які аналітичні функції, для яких існують розкладання в статеchnі або тригонометричні ряди, а також функції, що є рішеннями лінійних диференціальних рівнянь.

Якщо функції y_1, \dots, y_n мають зазначену вище властивість, то додаткові змінні визначаються як лінійні комбінації вихідних функцій.

Для виявлення практично будь-яких помилок досить ввести лише одну додаткову змінну:

$$y_{n+1}(x_1, \dots, x_m) = -\sum_{i=1}^n y_i(x_1, \dots, x_m) = \sum_{j=1}^s \lambda_{n+1,j} v_j(x_1, \dots, x_m),$$

де $\lambda_{n+1,j} = -\sum_{i=1}^n \lambda_{ij}$, $j = 1, 2, \dots, s$.

При відсутності помилок повинне виконуватися наступна умова:

$$\sum_{i=1}^{n+1} y_i(x_1, \dots, x_m) = 0.$$

Однак через похибки, що обумовлені використанням кінцевих розкладань замість нескінченних, округленням при виконанні операції множення й т.д., точне виконання цієї рівності практично неможливо. Тому як контрольна умова використовують нерівність

$$\left| \sum_{i=1}^{n+1} y_i(x_1, \dots, x_m) \right| \leq \Delta,$$

де Δ - максимально припустима помилка, що може з'явитися в результаті підсумовування зазначених похибок.

Неважко переконатися в тому, що розглянутий код дозволяє виявляти будь-яку помилку, що виводить яку-небудь одну зі змінних y_1, \dots, y_{n+1} за межі границь, обумовлених припустимими похибками. Такого роду помилки називаються грубими. Крім того, можливе визначення будь-якої комбінації таких грубих помилок, сума яких по абсолютній величині більше, ніж Δ . Частка цих помилок від загального їхнього числа дорівнює $1 - \Delta/L$, де L - діапазон подання чисел у СОІУ. Оскільки $\Delta/L \approx 0$, можна вважати, що практично будь-які помилки, що виникають у процесі рішення завдання, можуть бути виявлені за допомогою подібного найпростішого функціонального коду.

При введенні додаткової функції збільшується загальний час розв'язання завдання. Однак для багатьох практичних завдань управління додаткова функція виходить досить простою і для її обчислення необхідно приблизно такий же час, що й для визначення кожної з вихідних функцій. При досить великому числі вихідних змінних додаткові витрати часу виявляються досить малими.

Приклад 6.16.

Як найпростіший приклад функціонального кодування можна розглянути завдання перетворення прямокутних координат:

$$y_1 = x_1 \sin \alpha + x_2 \cos \alpha; \quad y_2 = x_1 \cos \alpha + x_2 \sin \alpha.$$

Покладемо $y_3 = -(y_1 + y_2)$. Тоді, виконуючи елементарні тригонометричні перетворення, одержимо:

$$y_3 = -1,41[x_1 \cos(\pi/4 - \alpha) + x_2 \sin(\pi/4 - \alpha)].$$

При цьому виконується контрольна умова $|y_1 + y_2 + y_3| \leq \Delta$.

Функціональні коди дозволяють не тільки виявляти, але й виправляти помилки, що виникають у процесі розв'язання завдання. Якщо грубі помилки, що спотворюють окремі вихідні змінні, є незалежними, то для корек-

ції будь-яких t - кратних помилок досить використати $2t$ додаткових змінних. Причому основну частину цих помилок можна виправити при використанні лише $t+1$ додаткових змінних. Слід зазначити, що відмова якого-небудь із елементів СОІУ найчастіше призводить до перекручування всіх функцій, що обчислюють у ході розв'язання завдання. Тому коригувальні функціональні коди принципово не можуть застосовуватися для боротьби з подібними помилками й область їхнього застосування звичайно обмежується корекцією помилок, обумовлених випадковими збоями. У той же час навіть найпростіший функціональний код у сполученні із МСЧ дозволяє певною мірою боротися з помилками, викликаними відмовами елементів СОІУ.

Нехай у СОІУ використовується не надлишкова МСЧ з основами m_1, \dots, m_m й для контролю ходу розв'язання завдання до вихідних функцій y_1, \dots, y_n додається ще одна змінна y_{n+1} , така, що $\sum_{i=1}^{n+1} y_i = 0$. З появою помилки порушується контрольна умова:

$$\left| \sum_{i=1}^{n+1} y_i \right| \leq \Delta.$$

Для того щоб перевірити, чи не викликана помилка випадковим збоєм, завдання варто перерішати ще раз. Якщо й у цьому випадку контрольна умова не виконується, то для локалізації несправного модуля завдання вирішується знову, але вже в скороченій МСЧ, що отримується в результаті виключення одної з основ системи. Оскільки при цьому зменшується діапазон подання чисел, то відповідно збільшується помилка округлення. Отже, для МСЧ із виключеною основою m_i контрольна умова функціонального коду прийме вигляд:

$$\left| \sum_{i=1}^{n+1} y_i \right| \leq m_i \Delta.$$

При виключенні із МСЧ модуля, якому відповідає несправний елемент, контрольна умова завжди виконується.

Якщо ж виключений справний модуль m_j , то ймовірність виконання контрольної умови не перевищує величини $m_j m_i \Delta / M$ (тут $M = L$). Більше того, з огляду на той факт, що при будь-яких перекручуваннях символів по основі m_i мінімальна величина помилки дорівнює $(M / m_i) \square m_i \Delta$, можна стверджувати, що при виключенні справного модуля контрольна умова завжди виявиться порушеною.

Після локалізації несправної основи надалі СОІУ продовжує працювати у скороченій МСЧ, тобто зі зменшеною точністю. Тим часом несправний блок можна ремонтувати, а усунувши несправність, знову повернутися до обчислень у повній модулярній системі числення.

Звичайно при вирішенні багатьох завдань управління вихідні величини за час одного прорахунку змінюються незначно. Тому втрати часу, що затрачується на повторні рішення завдання, практично не впливають на характеристики системи управління.

Час пошуку несправного модуля можна сильно скоротити, якщо замість повторних рішень завдання у скороченій МСЧ проводити обчислення у повній модулярній системі числення, але використати основи m_{m-1} й m_m у якості контрольних. При цьому зменшується точність обчислень у $m_{m-1}m_m$ раз. Але це не має значення, тому що розв'язуване завдання виконує роль контрольного тесту. Якщо помилка носить досить загальний характер, то при виконанні перших же операцій не модульного типу вона буде виявлена й локалізована.

6.7. Контрольні питання

1. Охарактеризуйте властивість малорядності лишків МСЧ.
2. Охарактеризуйте властивість незалежності лишків МСЧ.
3. Охарактеризуйте властивість рівноправності лишків МСЧ.
4. Зобразить структурну схему пристрою обробки інформації у МСЧ.
5. Визначте класи відрахувань по модулю $m_i=7$ серед натуральних чисел, включаючи нуль.
6. Визначте лишки від ділення числа $A = 28$ на числа $m_1=2$, $m_2=3$, $m_3=5$.
7. Визначити суму наступних відрахувань по модулю п'ять: $3 + 1$, $3 + 2$, $3 + 4$, $2 + 3$, $4 + 2$.
8. Визначити різницю наступних відрахувань по модулю п'ять: $0 - 2$, $3 - 3$, $4 - 3$, $2 - 4$, $4 - 2$.
9. Охарактеризуйте табличний принцип виконання модульних операцій.
10. . Охарактеризуйте принцип кільцевого зсуву виконання модульних операцій.
11. Як виконати операцію модульного вирахування за допомогою ПЗП, що реалізує операцію модульного додавання?
12. Як виконується функціональне кодування у МСЧ?

Додатки

Додаток А

Приклади розв'язання завдань. Задачі для самостійного розв'язання

А.1. Приклади розв'язання практичних завдань

А.1.1. Тема: Основні поняття та визначення теорії ймовірностей

Мета: Повторення основних понять, визначень та теорем теорії ймовірностей

Контрольні питання:

1. Дайте визначення поняттям: подія, ситуація та випробування; випадкова, достовірна (вірогідна) та неможлива події; суміжні, несумісні та протилежні події; елементарні та складні події; рівноможливі події.

2. Дайте визначення ймовірності випадкової події. Привести формулу для визначення випадкової події A у залежності від загального числа n елементарних подій та числа m елементарних подій, які сприяють появі події A .

3. Визначити властивості ймовірності випадкової події.

4. Сформулювати теореми додавання ймовірностей для сумісних та несумісних подій.

5. Сформулювати теореми множення ймовірностей для залежних та незалежних подій.

6. Привести та пояснити формулу повної ймовірності.

7. Привести та пояснити формулу Байєса (ймовірність гіпотез).

Приклад А.1.

Нехай в урні знаходиться 10 білих та 6 чорних куль. Навмання одночасно беруть 5 куль.

Яка ймовірність $P(A)$ того, що серед 5 навмання взятих куль 3 є білими?

Розв'язання. Загальна можлива кількість наслідків випробувань дорівнює $n = C_{16}^5$. Кількість варіантів вибору трьох білих кульок дорівнює C_{10}^3 , а кількість варіантів вибору двох чорних кульок дорівнює C_6^2 . Множина m наслідків, яка сприяє появі події A , тобто появі 3 білих куль, дорівнює $m = C_{10}^3 \cdot C_6^2$. Таким чином знаходимо, що

$$P(A) = \frac{m}{n} = \frac{C_{10}^3 \cdot C_6^2}{C_{16}^5} = 0,4.$$

Приклад А.2.

Студент отримує залік за умовою що одержує оцінку не нижче 3.

Яка ймовірність $P(A)$ здати залік, якщо відомо, що студент може одержати оцінки: 5 (подія A_1), 4 (подія A_2) та 3 (подія A_3) з ймовірностями відповідно $P(A_1) = 0,1$; $P(A_2) = 0,2$ та $P(A_3) = 0,5$?

Розв'язання. Події A_1 , A_2 та A_3 несумісні. Тоді подія A (що студент отримає залік) буде мати вигляд $A = A_1 + A_2 + A_3$, а ймовірність отримання заліку, згідно з теоремою додавання ймовірностей, є

$$P(A) = P(A_1 + A_2 + A_3) = P(A_1) + P(A_2) + P(A_3) = 0,1 + 0,2 + 0,5 = 0,8.$$

Приклад А.3.

Нехай система складається з трьох агрегатів. Перший та другий агрегати дубльовані, тобто при відмові одного з них починає робити другий. Відмова системи настає тоді, коли одноразово відмовили перший та другий агрегати, або відмовив третій агрегат.

Визначити ймовірність $P(B)$ відмови всієї системи, коли ймовірність відмов першого, другого та третього агрегатів відповідно дорівнює

$$P(A_1) = P(A_2) = 0,2 \text{ та } P(A_3) = 0,1,$$

де: A_1 - подія відмови першого агрегату, A_2 - подія відмови другого агрегату, A_3 - подія відмови третього агрегату, а B - подія відмови всієї системи.

Розв'язання. Згідно з умовою приклада маємо складну подію B у вигляді $B = A_1 \cdot A_2 + A_3$.

Події A_1 , A_2 та A_3 сумісні і незалежні. Згідно з теоремами додавання та множення ймовірностей маємо:

$$\begin{aligned} P(B) &= P(A_1 \cdot A_2 + A_3) = P(A_1 \cdot A_2) + P(A_3) - P(A_1 A_2 A_3) = \\ &= P(A_1) \cdot P(A_2) + P(A_3) - P(A_1) \cdot P(A_2) \cdot P(A_3) = \\ &= 0,2 \cdot 0,2 + 0,1 - 0,2 \cdot 0,2 \cdot 0,1 = 0,04 + 0,1 - 0,004 = 0,136. \end{aligned}$$

Приклад А.4.

Кругова мішень складається з трьох зон: **I**, **II** та **III**. Ймовірність влучення в кожну з них при одному пострілі дорівнює відповідно **0,15**; **0,23** та **0,17**.

Знайти ймовірність $P(A)$ невлучення у мішень при одному пострілі.

Розв'язання. Нехай подія A - невлучення у мішень, тоді \bar{A} - подія влучення у мішень. Події A_1 , A_2 та A_3 - події невлучення відповідно у **I**, **II** та **III** зони мішені, а події \bar{A}_1 , \bar{A}_2 та \bar{A}_3 - події влучення. Події \bar{A}_1 , \bar{A}_2 та \bar{A}_3 несумісні, тоді $\bar{A} = \bar{A}_1 + \bar{A}_2 + \bar{A}_3$, а

$$\begin{aligned} P(\bar{A}) &= P(\bar{A}_1 + \bar{A}_2 + \bar{A}_3) = P(\bar{A}_1) + P(\bar{A}_2) + P(\bar{A}_3) = \\ &= 0,15 + 0,23 + 0,17 = 0,55. \end{aligned}$$

Події A і \bar{A} протилежні. В цьому випадку, згідно з теоремою додавання ймовірностей, маємо

$$P(A) = 1 - P(\bar{A}) = 1 - 0,55 = 0,45.$$

Приклад А.5.

На склад поступають двигуни з двох заводів. З першого заводу на склад поступає **80%** усіх двигунів, що знаходяться на складі, а з другого - **20%**. Перший завод на сто двигунів в середньому поставляє **90 %** справних, а другий - **95 %**.

Знайти ймовірність $P(A)$ того, що перший навання куплений на складі двигун є справний.

Розв'язання. Нехай:

A - подія, що куплений зі складу двигун справний;

H_1 - подія, що перший навання куплений зі складу двигун є двигун, вироблений на першому заводі;

H_2 - подія, що перший навання куплений зі складу двигун є двигун, вироблений на другому заводі;

A_1 - подію, що куплений зі складу двигун, вироблений на першому заводі, буде справним;

A_2 - подію, що куплений зі складу двигун, вироблений на другому заводі, буде справним.

Ймовірності вищезначених подій позначаються і дорівнюють відповідно: $P(H_1) = 0,8$; $P(H_2) = 0,2$; $P(A/H_1) = 0,9$; $P(A/H_2) = 0,95$.

Згідно з формулою повної ймовірності маємо

$$\begin{aligned} P(A) &= \sum_{i=1}^n P(H_i) \cdot P(A/H_i) = \sum_{i=1}^2 P(H_i) \cdot P(A/H_i) = \\ &= P(H_1) \cdot P(A/H_1) + P(H_2) \cdot P(A/H_2) = \\ &= 0,8 \cdot 0,9 + 0,2 \cdot 0,95 = 0,72 + 0,19 = 0,91. \end{aligned}$$

Приклад А.6.

За умовою приклада 5 знайти апостеріорні (післядослідні) ймовірності $P(H_i/A)$ того, що куплений зі складу справний двигун є двигун першого ($i = 1$) або другого ($i = 2$) заводу

Розв'язання. За формулою Байеса маємо

$$P(H_i/A) = \frac{P(H_i) \cdot P(A/H_i)}{\sum_{i=1}^n P(H_i) \cdot P(A/H_i)},$$

тобто

$$P(H_1/A) = \frac{P(H_1) \cdot P(A/H_1)}{\sum_{i=1}^2 P(H_i) \cdot P(A/H_i)} = \frac{0,8 \cdot 0,9}{0,91} = 0,7919;$$

$$P(H_2/A) = \frac{P(H_2) \cdot P(A/H_2)}{\sum_{i=1}^2 P(H_i) \cdot P(A/H_i)} = \frac{0,2 \cdot 0,95}{0,91} = 0,2088,$$

де: $\sum_{i=1}^2 P(A_i) \cdot P(H_i) = P(A) = 0,9$;

$P(A/H_1)$ - апостеріорна ймовірність того, що двигун, вироблений на першому заводі, справний (тобто $P(A/H_1) = P(A_1) = 0,9$);

$P(A/H_2)$ - апостеріорна ймовірність того, що двигун, вироблений на другому заводі, справний ($P(A/H_2) = P(A_2) = 0,95$).

Отже до купівлі двигуна апріорна (додослідна) ймовірність того, що двигун з другого заводу дорівнює $P(H_2) = 0,2$, а після того, як двигун купили, апостеріорна ймовірність дорівнює $P(H_2/A) = 0,2088$. Тобто за формулою Байєса ми дещо переоцінили ймовірність події H_2 ($P(H_2/A) > P(H_2)$).

Перевірка: $P(H_1/A) + P(H_2/A) = 0,7912 + 0,2088 = 1.$

A.1.2. Тема: кількісна оцінка ентропії та інформації (міра Р. Хартлі).

Мета: Придбати навички кількісної оцінки ентропії та інформації.

Контрольні питання:

1. Дайте визначення наступним поняттям: подія, ймовірність здійснення події; залежні, незалежні, спільні і неспільні події; повна група подій.

2. У чому сутність оцінки кількості інформації $I(X)$ за Р. Хартлі?

3. Від яких факторів залежить оцінка кількості інформації за Р. Хартлі?

4. Представити та пояснити формулу для визначення кількості інформації за Р. Хартлі.

5. Чим обумовлений вибір значення основи a логарифма при визначенні кількості інформації? У яких одиницях може вимірятися кількість інформації?

6. Навести вираз для визначення кількості інформації $I(X)$ у повідомленні з довжиною n розрядів.

7. Перелічити та пояснити всі основні властивості ентропії та інформації дискретних повідомлень.

8. Дайте визначення поняттю “один біт інформації”.

9. Що поєднує та чим принципово відрізняються поняття ентропії та інформації?

Приклад А.7.

Визначити максимальну кількість N повідомлень для кодової комбінації, що складається з n елементів, кожний з яких має m різних якісних ознак, для $n=10$ та $m=2$.

Розв’язання.

$$N = m^n = 2^{10} = 1024.$$

Приклад А.8.

Визначити максимально можливу ентропію $H(X)$ письмового повідомлення X , що складається з 10 символів (розрядів). Будемо рахувати, що загальна кількість букв російського алфавіту дорівнює 32.

Розв’язання. Загальна кількість N повідомлень дорівнює $N = m^n = 32^{10}$. Відповідно до міри Р. Хартлі, одержимо

$$H_{\max}(X) = \log_2 N = \log_2 32^{10} = \log_2 2^{50} = 50 \text{ (біт)}.$$

Приклад А.9.

Визначити кількість інформації $I(X)$ після одержання абонентом K повідомлень m -значного n -розрядного коду при $K = 2$, $n = 4$ і $m = 4$.

Розв’язання. Спочатку визначимо по Р. Хартлі кількість інформації $I_0(X)$, що міститься в одному повідомленні X

$$\begin{aligned} I_0(X) &= \log_2 N = \log_2 m^n = n \cdot \log_2 m = \\ &= 4 \cdot \log_2 4 = 4 \cdot \log_2 2^2 = 8 \log_2 2 = 8 \text{ (біт)}, \end{aligned}$$

де $N = m^n$ – кількість можливих комбінацій одного повідомлення.

У цьому випадку шукана величина кількості інформації дорівнює

$$I(X) = K \cdot I_0(X) = 2 \cdot 8 = 16 \text{ (біт)}.$$

А.1.3. Тема: Оцінка кількості ентропії та інформації у повідомленні (міра К. Шеннона)

Мета: Одержати навички розрахунку ентропії та інформації дискретних повідомлень

Контрольні питання:

1. Дайте визначення поняттям ентропія та інформація. У чому суть розходжень цих понять?

2. Навести та пояснити формулу для визначення кількості інформації за оцінкою К. Шеннона.

3. Пояснити вибір значення основи логарифма у формулі для оцінки кількості інформації.

4. Пояснити від яких змінних залежить значення кількості інформації при її оцінці за К. Шенноном.

5. Пояснити суть відмінностей в оцінці кількості інформації за критеріями Р. Хартлі та К. Шеннона.

6. Привести формулу для визначення часткової $I(x_i)$ та загальної $I(X)$ кількості інформації у повідомленні X . У якому випадку загальна кількість інформації $I(X)$ буде максимальною?

7. Пояснити вибір одиниці виміру ентропії та інформації.

Приклад А.10.

Нехай ансамбль ДДП представлено у вигляді

$$X = \begin{pmatrix} x_1 & x_2 \\ 0,4 & 0,6 \end{pmatrix}.$$

Необхідно визначити частинну $H(x_i)$ та і загальну $H(X)$ ентропії дискретного джерела повідомлень.

Розв'язання. Частинна ентропія $H(x_i)$ визначаються наступним чином:

$$H(x_1) = -\log_2 p(x_1), \text{ тобто } H(x_1) = -\log_2 0,4 = 1,32 \text{ (біт)}$$

$$H(x_2) = -\log_2 p(x_2) = -\log_2 0,6 = 0,74 \text{ (біт)}.$$

Загальна ентропія $H(X)$ дискретного джерела повідомлень дорівнює

$$H(X) = -\sum_{i=1}^n p(x_i) \cdot \log_2 p(x_i) = -\sum_{i=1}^2 p(x_i) \cdot \log_2 p(x_i) =$$

$$= -p(x_1) \cdot \log_2 p(x_1) - p(x_2) \cdot \log_2 p(x_2) = 0,53 + 0,44 = 0,97 \text{ (біт)}.$$

А.1.4. Тема: Метод перетворення неперервних сигналів у дискретні (теорема В.О. Котельникова).

Мета: Засвоєння методу перетворення неперервних сигналів у дискретні (цифрові).

Контрольні питання:

1 Пояснити логічний зв'язок між поняттями: інформація, повідомлення та сигнал.

2 Навести класифікацію повідомлень за характером їх зміни у часі.

3 Навести класифікацію повідомлень за можливою множиною значень (за рівнем).

4 Перелічити всі можливі методи представлення повідомлень.

5 Сформулюйте теорему В. О. Котельникова.

6 Пояснити причини переходу від аналогового до дискретного сигналу.

7 Перелічити та пояснити етапи перетворення неперервного сигналу у цифровий.

8 Пояснити сутність процесів дискретизації та квантування неперервних сигналів.

9 Дайте визначення поняттю «шум квантування».

10 Яким чином визначається кількість m рівнів квантування?

Приклад А.11.

Нехай є неперервний сигнал (функція часу) $U(t)$, обмежений смугою частот від 0 до $F_{max} = 1/2\Delta t$.

Необхідно сформувавти цифровий сигнал $U_{kv}(K \cdot \Delta t)$ ($K = \overline{0,6}$) для передачі його каналом зв'язку при кількості рівнів квантування $m = 8$ (зробити перетворення сигналу виду: аналог – код).

Розв'язання. Нехай вихідний вигляд неперервного сигналу $U(t)$ представлений на рис. А.1. Спочатку зробимо операцію дискретизації – перетворення функції $U(t)$ неперервного часу у функцію дискретного виду. Роль координат виконують миттєві значення функції, відлічені у визначені моменти $\Delta t = 1/2F_{max}$ часу. Далі зробимо операцію квантування – перетворення неперервної величини у величину, що має дискретну шкалу значень. Вона зводиться до заміни будь-якого миттєвого значення функції $U(t)$ одним із кінцевих заданої безлічі m дозволених значень – рівнями квантування.

На рис. А.1 миттєве значення $U(t)$ позначено горизонтальною рисою (—), а дискретне значення $U_{kv}(K \cdot \Delta t)$ – крапкою (•) ($K = 0, 1, 2, \dots$). Похибку квантування $\Delta_{kv} = |U(t) - U_{kv}(K \cdot \Delta t)|$ називають шумом квантування.

Якщо в даній крапці значення неперервної функції $U(t)$ знаходиться в інтервалі $[j, (j+1)]$, то воно чисельно визначається шляхом присвоєння найближчого за величиною одного з двох значень, що присвоєні кінцям j чи $j+1$ інтервалу, тобто $U_{kv}(K \cdot \Delta t) = j$ чи $U_{kv}(K \cdot \Delta t) = j+1$ ($j = \overline{0, m-1}$). Якщо $U(t) = [j + (j+1)]/2$, то величина $U_{kv}(K \cdot \Delta t)$ приймається рівною j , або $j+1$.

Так, наприклад, для першої ($K = 1$) риски, рис. А.1, чисельне значення неперервної функції $U(t)$ лежить в інтервалі $[3, 4]$. Таким чином значення $U_{kv}(K \cdot \Delta t)$ визначається величиною до найближчого цілого числа, тобто, $U_{kv}(\Delta t) = 3$.

Подібним чином для усіх восьми ($m = 8$) “рисок” функції $U(t)$ одержимо наступний цифровий код $U_{kv}(K \cdot \Delta t)$, для $K = \overline{0,6}$, у двійковому коді:

$$K = 0 - 1 (001); K = 1 - 3 (011); K = 2 - 5 (101); K = 3 - 7 (111); \\ K = 4 - 7 (111); K = 5 - 7 (111); K = 6 - 4 (100).$$

Таким чином, отримана шукана цифрова форма $U_k(K \cdot \Delta t)$ аналогового (неперервного) сигналу $U(t)$, що представляється на рис. А.2 у виді цифрової кодової комбінації.

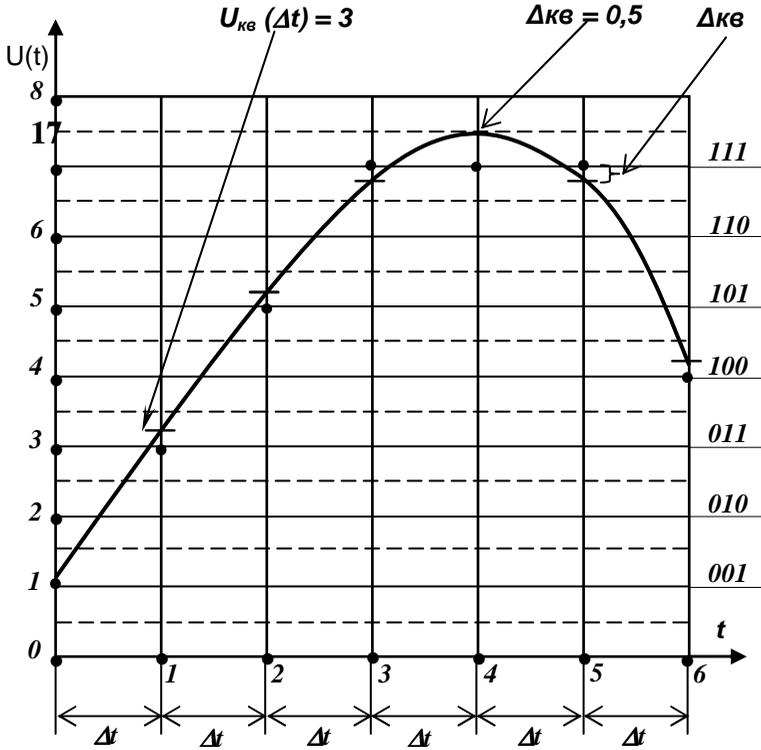


Рис. А.1 – Вихідна функція неперервного сигналу

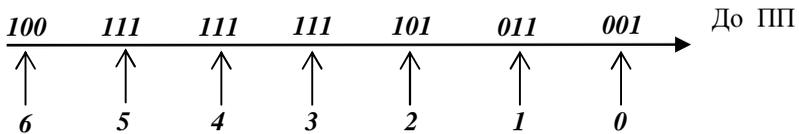


Рис. А.2 – Цифрова форма сигналу

А.1.5. Тема: Інформаційні характеристики дискретних джерел повідомлень.

Мета: Засвоєння основних інформаційних характеристик джерела дискретних повідомлень. Одержання навичок їх кількісної оцінки.

Контрольні питання:

- 1 Дайте визначення поняттю "модель джерела дискретних повідомлень".
- 2 Перелічити та пояснити основні інформаційні характеристики джерел дискретних повідомлень.
- 3 Що таке надмірність повідомлень? Як вона кількісно визначається?
- 4 Дайте визначення продуктивності джерела дискретних повідомлень.
- 5 Дайте визначення коефіцієнтів надмірності K_n та стиску K_c .
- 6 Дайте визначення поняттю абсолютної інформаційної недовантаженості. В яких одиницях вона вимірюється?
- 7 Привести формулу для визначення коефіцієнту інформаційної надмірності. В яких одиницях він вимірюється?

Приклад А.12.

Нехай алфавіт дискретного джерела повідомлень X складається з чотирьох букв, ймовірності появи яких дорівнюють відповідно: $p(x_1) = 0,5$; $p(x_2) = 0,25$; $p(x_3) = p(x_4) = 0,125$.

Необхідно визначити коефіцієнти K_n надмірності та K_c стиску.

Розв'язання. Відомо, що $K_n = 1 - H_n/H_o$ та $K_c = H_n/H_o$ (тобто $K_n = 1 - K_c$),

де: $H_o(X)$ – середня ентропія, що приходить на один елемент безнадлишкового повідомлення з S_o незалежними елементами (символами);

$H_n(X)$ – середня ентропія, що приходить на один елемент надлишкового повідомлення з S_n нерівноймовірними та взаємозалежними елементами.

При цьому, у загальному виді кількість інформації I джерела повідомлень дорівнює

$$I = S_o \cdot H_o(X) = S_n \cdot H_n(X).$$

Відомо, що

$$H_o(X) = -\sum_{i=1}^n p(x_i) \cdot \log p(x_i) = -\sum_{i=1}^4 p(x_i) \cdot \log_2 p(x_i) =$$

$$= -p(x_1) \cdot \log_2 p(x_1) - p(x_2) \cdot \log_2 p(x_2) - p(x_3) \cdot \log_2 p(x_3) - p(x_4) \cdot \log_2 p(x_4) = -4 \cdot p(x) \cdot \log_2 p(x) = -4 \cdot 1/4 \cdot \log_2 1/4 = 2(\text{біт}),$$

так як для безнадлишкового повідомлення виконується рівність $p(x) = p(x_1) = p(x_2) = p(x_3) = p(x_4) = 1/4$, то ентропія $H(X)$ повідомлення X буде максимальна і дорівнює $H_o(X)$.

Визначимо значення середньої ентропії

$$\begin{aligned}
 H_n(X) &= -\sum_{i=1}^4 p(x_i) \cdot \log_2 p(x_i) = \\
 &= -(0,5 \cdot \log_2 0,5 + 0,25 \cdot \log_2 0,25 + 0,125 \cdot \log_2 0,125 + \\
 &\quad + 0,125 \cdot \log_2 0,125) = 1,75 \text{ (біт)}.
 \end{aligned}$$

Таким чином одержимо

$$\begin{aligned}
 K_n &= 1 - H_n / H_0 = 1 - 1,75/2 = 1 - 0,875 = 0,125, \\
 K_c &= H_n / H_0 = 0,875.
 \end{aligned}$$

Приклад А.13.

Джерело дискретних повідомлень (яке визначає задану кількість вихідної інформації I) видає кодову комбінацію, що складається з $S_n = 12$ символів (букв). Відомо, що безнадлишкова комбінація, яка містить однакову кількість інформації I , складається з $S_0 = 10$ символів.

Визначити значення K_c і K_n .

Розв'язання. Відомо, що $K_c = S_0 / S_n$ і $K_n = 1 - S_0 / S_n$. Таким чином:

$$K_c = 10/12 = 0,83 \text{ і } K_n = 0,17.$$

Приклад А.14.

Використовуючи умову прикладу А.12 визначити кількість S_0 двійкових розрядів безнадлишкового повідомлення, що містить дану кількість інформації I . При цьому кількість S_n двійкових розрядів надлишкового повідомлення, що містить однакову кількість інформації I , дорівнює 20 .

Розв'язання. Скористаємося результатами розв'язання прикладу А.12. Так як

$$K_c = H_n / H_0 = S_0 / S_n = 0,875, \text{ тоді } S_0 = S_n \cdot 0,875 = 20 \cdot 0,875 = 17,5.$$

Отримане значення S_0 не може бути дробовим числом, тому округлимо його до найближчого найбільшого цілого. У цьому випадку кількість двійкових розрядів безнадлишкового повідомлення буде дорівнювати 18 .

Приклад А.15.

Дискретне джерело видає повідомлення у виді двійкового коду, що складається з $S_n = 30$ двійкових розрядів.

Потрібно визначити значення S_0 , якщо відомий коефіцієнт $K_n = 0,2$.

Розв'язання. На початку визначимо $K_c = 1 - K_n = 0,8$. З урахуванням, що $K_c = S_0 / S_n$, одержимо: $S_0 = S_n \cdot K_c = 30 \cdot 0,8 = 24$ (дв. розр.).

Приклад А.16.

Дискретне джерело інформації видає 20 одиниць інформації ($I = 20$ (біт)). Відомо, що $H_n(X) = 0,4$ (біт).

Визначити довжину S_n комбінації (двійкового коду) на виході джерела.

Розв'язання. Відомо, що $I = S_n \cdot H_n(X)$. Тому $S_n = I/H_n(X) = 20/0,4 = 50$ (дв. розр.), тобто довжина S_n кодової комбінації на виході джерела буде дорівнювати 50 двійковим розрядам.

Приклад А.17.

Дискретне джерело повідомлень видає за час $T_n = 10^6$ с, двійковими послілками, тривалістю $\tau = 10$ мс ($1\text{с} = 10^3$ мс), $I = 10^7$ біт інформації.

За який час T_0 та якою кількістю S_0 двійкових посилок можна передати той же обсяг інформації, якщо відповідною обробкою цілком усувається надмірність джерела? Визначити коефіцієнти K_n і K_c джерела.

Розв'язання. За умовою завдання заданий обсяг $I = 10^7$ (біт) інформації передається за допомогою S_n двійкових посилок, кількість яких визначається наступним чином:

$$S_n = T_n / \tau_i = 10^6 / 10 \cdot 10^{-3} = 10^8 \text{ (дв. розр.)}$$

Значення середньої ентропії визначається як

$$H_n(X) = I / S_n = 10^7 / 10^8 = 0,1 \text{ (біт)}$$

Якщо надмірність усунута, тоді кожен один двійковий символ двійкового дискретного джерела несе в собі $H_n(X) = 1$ (біт) інформації. У цьому випадку заданий обсяг інформації I передається за допомогою $S_0 = I/H_n(X) = 10^7/1 = 10^7$ (дв. розр.) за час $T_0 = S_0 \cdot \tau_i = 10^7 \cdot 10 \cdot 10^{-3} = 10^5$ с.

Значення коефіцієнта надмірності визначиться таким чином $K_n = 1 - S_0 / S_n = 1 - 10^7 / 10^8 = 1 - 0,1 = 0,9$.

Коефіцієнт стиску K_c визначиться на підставі відомого співвідношення $K_c = S_0/S_n = 10^7/10^8 = 0,1$ чи $K_c = 1 - K_n = 1 - 0,9 = 0,1$

А.1.6. Тема: Ентропія та інформація складних дискретних повідомлень.

Мета: Засвоєння основних властивостей ентропії та інформації складних дискретних повідомлень. Одержання навичок розрахунку ентропії та інформації.

Контрольні питання:

1 Дайте визначення та поясніть зміст наступних понять: ентропія складних повідомлень, умовна ентропія, частинна умовна ентропія, загальна умовна ентропія, спільна та взаємна ентропії.

2 Представте загальний вигляд матриці об'єднання для двох довільних ансамблів дискретних повідомлень X та Y .

3 Представте та поясніть формули для визначення наступних величин: загальної безумовної ентропії, частинної умовної ентропії та загальної умовної ентропії дискретних повідомлень.

4 Наведіть та поясніть вираз для визначення спільної ентропії двох повідомлень як функції від безумовної ентропії одного з повідомлень X та умовної ентропії іншого повідомлення Y .

5 Наведіть та поясніть вираз для визначення спільної ентропії для деякої безлічі повідомлень.

6 Поясніть всі основні властивості ентропії та інформації складних дискретних повідомлень.

7 Наведіть та поясніть формули для визначення взаємної ентропії та середньої кількості інформації.

8 Дайте геометричну інтерпретацію поняттю частинної умовної ентропії.

9 Перерахуйте властивості ентропії складних дискретних повідомлень.

10 Перерахуйте властивості інформації складних дискретних повідомлень.

11 Дайте геометричну інтерпретацію умовних ентропій.

12 Наведіть та поясніть формули для визначення умовних ентропій.

Приклад А.18.

Нехай задана матриця $P(x, y)$ об'єднання двох джерел дискретних повідомлень X та Y у вигляді

$X \backslash Y$	y_1	Y_2	$p(x_i)$
x_1	0,4	0	0,4
x_2	0,2	0	0,2
x_3	0,2	0,2	0,4
$p(y_j)$	0,8	0,2	

Необхідно визначити:

- а) загальні безумовні ентропії $H(X)$ і $H(Y)$;
- б) загальні умовні ентропії $H(X/Y)$ і $H(Y/X)$;
- в) спільну ентропію $H(Y, X)$;
- г) взаємну ентропію $H(X \cdot Y)$.

Розв'язання. Відповідно до даних матриці $P(x, y)$, за відомими формулами, визначимо шукані величини (одиниці виміру "біт" для зручності будемо надалі опускати)

$$\begin{aligned}
 H(X) &= -\sum_{i=1}^3 p(x_i) \log_2 p(x_i) = -[0,4 \log_2 0,4 + 0,2 \log_2 0,2 + \\
 &\quad + 0,4 \log_2 0,4] = 0,53 + 0,48 + 0,53 = 1,52;
 \end{aligned}$$

$$H(Y) = -\sum_{j=1}^2 p(y_j) \log_2 p(y_j) = -[0,8 \log_2 0,8 + 0,2 \log_2 0,2] = \\ = 0,26 + 0,46 = 0,72.$$

Для того, щоб обчислити значення

$$H(X/Y) = -\sum_{j=1}^2 p(y_j) \sum_{i=1}^3 p(x_i/y_j) \log_2 p(x_i/y_j),$$

попередньо необхідно визначимо сукупність наступних величин:

$$p(x_i/y_j) = \frac{p(x_i, y_j)}{p(y_j)} \quad \text{для } i = \overline{1,3} \text{ та } j = \overline{1,2}.$$

$$p(x_1/y_1) = \frac{0,4}{0,8} = 0,5; \quad p(x_1/y_2) = \frac{0}{0,2} = 0;$$

$$p(x_2/y_1) = \frac{0,2}{0,8} = 0,25; \quad p(x_2/y_2) = \frac{0}{0,2} = 0;$$

$$p(x_3/y_1) = \frac{0,2}{0,8} = 0,25; \quad p(x_3/y_2) = \frac{0,2}{0,2} = 1.$$

У цьому випадку одержимо

$$H(X/Y) = -\{0,8[0,5 \log_2 0,5 + 0,25 \log_2 0,25 + 0,25 \log_2 0,25] + \\ + 0,2[0 + 0 + 1 \log_2 1]\} = 0,8(0,5 + 0,5 + 0,5) = 0,8 \cdot 1,5 = 1,2.$$

Аналогічно обчислимо значення

$$H(Y/X) = -\sum_{i=1}^3 p(x_i) \cdot \sum_{j=1}^2 p(y_j/x_i) \log_2 p(y_j/x_i),$$

де: $p(y_j/x_i) = \frac{p(x_i, y_j)}{p(x_i)},$

$$p(y_1/x_1) = \frac{0,4}{0,4} = 1; \quad p(y_2/x_2) = \frac{0}{0,2} = 0;$$

$$p(y_2/x_1) = \frac{0}{0,4} = 0; \quad p(y_1/x_3) = \frac{0,2}{0,4} = 0,5;$$

$$p(y_1/x_2) = \frac{0,2}{0,2} = 1; \quad p(y_2/x_3) = \frac{0,2}{0,4} = 0,5.$$

Тоді:

$$H(Y/X) = -\{0,4(1 \log_2 1 + 0) + 0,2(1 \log_2 1 + 0) + \\ + 0,4(0,5 \log_2 0,5 + 0,5 \log_2 0,5)\} = 0,4 \cdot 0 + 0,2 \cdot 0 + 0,4 \cdot 1 = 0,4.$$

В остаточному підсумку отримуємо

$$\begin{aligned} H(X, Y) &= - \sum_{i=1}^n \sum_{j=1}^m p(x_i, y_j) \log_2 p(x_i, y_j) = \\ &= - \sum_{i=1}^3 \sum_{j=1}^2 p(x_i, y_j) \log_2 p(x_i, y_j) = 0,4 \log_2 0,4 + 0 + \\ &\quad + 0,2 \log_2 0,2 + 0 + 0,2 \log_2 0,2 + 0,2 \log_2 0,2 = \\ &\quad = 0,53 + 0 + 0,46 + 0 + 0,46 + 0,46 = 1,91. \end{aligned}$$

З метою перевірки отриманих результатів, обчислимо значення взаємної ентропії $H(X \cdot Y)$ за відомим, але різним, аналітичним співвідношенням:

$$\begin{cases} H(X \times Y) = H(X) - H(X/Y) = 1,52 - 1,2 = 0,32. \\ H(X \times Y) = H(Y) - H(Y/X) = 0,72 - 0,4 = 0,32. \\ H(X \times Y) = H(X, Y) - H(X/Y) - H(Y/X) = \\ = 1,91 - 1,2 - 0,4 = 0,31. \end{cases}$$

За підсумком розрахунків маємо:

$$\begin{aligned} H(X) &= 1,52; H(Y) = 0,72; H(X/Y) = 1,2; H(Y/X) = 0,4; \\ H(X, Y) &= 1,91; H(X \cdot Y) = 0,32. \end{aligned}$$

Перевірка підтверджує правильність розрахунків

1. $H(X, Y) = H(X) + H(Y/X) = 1,52 + 0,4 = 1,92.$

2. $H(X, Y) = H(Y) + H(X/Y) = 0,72 + 1,2 = 1,92.$

3. $H(X, Y) = H(X/Y) + H(Y/X) + H(X \cdot Y) = 1,2 + 0,4 + 0,32 = 1,92.$

Приклад А.19.

Нехай сигнали управління з виходу АСУ ТП у цифровій формі (у виді двійкового коду) надходять на вхід технологічного об'єкта управління (ТОУ) з ймовірностями появи сигналів x_1, x_0 , що відповідають значенням «1» та «0» рівними, відповідно, $p(x_1) = 0,6$; $p(x_0) = 0,4$. При цьому надходження кожного із символів взаємозалежно з наступними умовними ймовірностями $p(x_i/x)$ виду

$$\begin{cases} p(x_0 / x_0) = 0,1; \\ p(x_1 / x_1) = 0,1; \\ p(x_1 / x_0) = 0,9; \\ p(x_0 / x_1) = 0,9. \end{cases}$$

Ці ймовірності зручно представити у виді наступної таблиці

$x_j \backslash x_i$	x_0	x_1
x_0	0,1	0,9
x_1	0,9	0,1

Необхідно визначити ентропію $H(X)$ вхідної інформації.

Розв'язання.

$$\begin{aligned}
 H(X) &= -\sum_{i=0}^1 p(x_i) \sum_{j=0}^1 p(x_i/x_j) \log_2 p(x_i/x_j) = -\{p(x_0) \cdot \\
 &\cdot [p(x_0/x_0) \log_2 p(x_0/x_0) + p(x_0/x_1) \log_2 p(x_0/x_1)] + \\
 &+ p(x_1) [p(x_1/x_0) \log_2 p(x_1/x_0) + p(x_1/x_1) \log_2 p(x_1/x_1)] \} = \\
 &= 0,4(0,1 \log_2 0,1 + 0,9 \log_2 0,9) + 0,6(0,9 \log_2 0,9 + 0,1 \log_2 0,1) = \\
 &= 0,4(0,33 + 0,137) + 0,6(0,137 + 0,33) = 0,467 \text{ (біт)}.
 \end{aligned}$$

Таким чином, ентропія вхідної інформації ТОК дорівнює **0,467** (біт).

Приклад А.20.

Необхідно визначити середню кількість $I(X,Y)$ інформації у прийнятому повідомленні Y , щодо переданого X . Канал зв'язку описується матрицею $P(X,Y)$ спільних ймовірностей передачі x_i та прийому y_j елементів повідомлення.

$X \backslash Y$	y_1	y_2	y_3	$P(x_i)$
x_1	0,4	0,1	0	0,5
x_2	0	0,2	0,1	0,3
x_3	0	0	0,2	0,2
$P(y_j)$	0,4	0,3	0,3	

У цьому випадку елементами матриці $P(X,Y)$ є спільні ймовірності $P_{ij} = P(x_i, y_j)$.

Розв'язання. $I(X, Y) = H(X) - H(X/Y)$

$$\begin{aligned}
 H(X) &= -\sum_{i=1}^n p(x_i) \log_2 p(x_i) = -[p(x_1) \log_2 p(x_1) + \\
 &+ p(x_2) \log_2 p(x_2) + p(x_3) \log_2 p(x_3)] = \\
 &= -(0,5 \log_2 0,5 + 0,3 \log_2 0,3 + 0,2 \log_2 0,2) = 1,485 \text{ (біт)}
 \end{aligned}$$

Загальна умовна ентропія визначається виразом

$$\begin{aligned}
 H(X/Y) &= -\sum_{j=1}^m p(y_j) \sum_{i=1}^n p(x_i/y_j) \log_2 p(x_i/y_j) = \\
 &= -\{p(y_1)[p(x_1/y_1) \log_2 p(x_1/y_1) + p(x_2/y_1) \log_2 p(x_2/y_1) + \\
 &+ p(x_3/y_1) \log_2 p(x_3/y_1)] + p(y_2)[p(x_1/y_2) \log_2 p(x_1/y_2) + \\
 &+ p(x_2/y_2) \log_2 p(x_2/y_2) + p(x_3/y_2) \log_2 p(x_3/y_2)] + \\
 &+ p(y_3)[p(x_1/y_3) \log_2 p(x_1/y_3) + p(x_2/y_3) \log_2 p(x_2/y_3) + \\
 &+ p(x_3/y_3) \log_2 p(x_3/y_3)] \}
 \end{aligned}$$

За значеннями $p(x_i, y_j)$ знаходимо величини $p(x_i / y_j)$:

$$\left\{ \begin{aligned} p(x_i, y_j) &= p(x_i/y_j) \cdot p(y_j); \\ p(y_j, x_i) &= p(y_j/x_i) \cdot p(x_i), \end{aligned} \right.$$

$$p(x_1/y_1) = \frac{p(x_1, y_1)}{p(y_1)} = \frac{0,4}{0,4} = 1; \quad p(x_1/y_2) = \frac{p(x_1, y_2)}{p(y_2)} = \frac{0,1}{0,3} = 0,33;$$

$$p(x_2/y_1) = \frac{p(x_2, y_1)}{p(y_1)} = \frac{0}{0,4} = 0; \quad p(x_2/y_2) = \frac{p(x_2, y_2)}{p(y_2)} = \frac{0,2}{0,3} = 0,66;$$

$$p(x_3/y_1) = \frac{p(x_3, y_1)}{p(y_1)} = \frac{0}{0,4} = 0; \quad p(x_3/y_2) = \frac{p(x_3, y_2)}{p(y_2)} = \frac{0}{0,3} = 0$$

$$p(x_1/y_3) = \frac{p(x_1, y_3)}{p(y_3)} = \frac{0}{0,3} = 0; \quad p(x_2/y_3) = \frac{p(x_2, y_3)}{p(y_3)} = \frac{0,1}{0,3} = 0,33;$$

$$p(x_3/y_3) = \frac{p(x_3, y_3)}{p(y_3)} = \frac{0,2}{0,3} = 0,66.$$

Таким чином $H(X/Y) = 0,55$ (біт).

Середня кількість інформації прийнятий одержувачем буде дорівнювати

$$I(X/Y) = H(X) - H(X/Y) = 1,485 - 0,55 = 0,935 \text{ (біт)}.$$

А.2. Задачі для самостійного розв'язання

Задача 1.

Символи алфавіту мають m якісних ознак. Визначити максимальну кількість N повідомлень, що можна одержати для кодової комбінації з n елементів (розрядів). Варіанти завдань представлені у таблиці.

Таблиця А.2.1.

Варіанти завдань

Вар.	m	n	Вар.	m	n	Вар.	m	n
1	1	100	11	1	10	21	1	10
2	2	1	12	2	2	22	2	3
3	3	2	13	3	3	23	3	2
4	4	3	14	4	4	24	4	3
5	5	4	15	5	2	25	5	3
6	1	5	16	6	3	26	1	8
7	2	2	17	7	2	27	2	5
8	3	3	18	8	3	28	3	2
9	4	4	19	9	2	29	4	2
10	5	2	20	10	1	30	5	3

Задача 2.

Відповідно до умови задачі 1 визначити кількість інформації I в отриманому повідомленні за умови, що всі повідомлення рівноймовірні.

Задача 3.

За умови рівноймовірності та незалежності символів алфавіту, що складається з m елементів (букв), визначити середню ентропію $H(X)$ на один символ алфавіту. Варіанти завдань представлені у таблиці.

Таблиця А.2.2.

Варіанти завдань

Вар.	m	Вар.	m	Вар.	m	Вар.	m	Вар.	m
1	1	7	64	13	20	19	80	25	500
2	2	8	128	14	30	20	90	26	600
3	4	9	256	15	40	21	100	27	700
4	8	10	512	16	50	22	200	28	800
5	16	11	1024	17	60	23	300	29	900
6	32	12	10	18	70	24	400	30	1000

Задача 4.

Визначити максимально можливу ентропію $H(X)$ повідомлення X інформаційної системи, яке складається з трьох елементів (розрядів), кожний з яких може перебувати у чотирьох можливих станах.

Задача 5.

Визначити максимально можливу ентропію $H(X)$ повідомлення X , що складається з **10** розрядів, причому загальна кількість букв російського алфавіту рахується рівною **32**.

Задача 6.

Поле умовно розбите на **16** окремих ділянок. Необхідно визначити кількість інформації $I(X)$, що міститься у повідомлення X : на якому з **16** ділянок знаходиться працюючий комбайн, якщо відомо, що у даній момент часу ймовірність $P(X)$ перебування комбайна на будь-якій ділянці однакова.

Задача 7.

Чому дорівнює кількість інформації у повідомленні X , переданого у двійковому коді n – значною комбінацією (довжина повідомлення дорівнює n). Варіанти завдань представлені у таблиці.

Таблиця А.2.3.

Варіанти завдань

Вар.	n								
1	0	7	10	13	70	19	15	25	65
2	1	8	20	14	80	20	16	26	75
3	2	9	30	15	90	21	17	27	85
4	3	10	40	16	100	22	18	28	120
5	4	11	50	17	25	23	45	29	130
6	5	12	60	18	35	24	55	30	140

Задача 8.

Нехай мається ДДП, стани якого рівноймовірні, а об'єм $\{a_i\}$ алфавіту дорівнює m_a . Визначити кількість інформації, що приходяться на один ($n = 1$) символ повідомлення.

Задача 9.

Визначити кількість інформації I при одержанні абонентом K повідомлень рівномірного m – значного n – розрядного коду.

Варіанти завдань представлені у таблиці.

Таблиця А.2.4.

Варіанти завдань

Вар.	K	m	n	Вар.	K	m	n
1	1	1	10	16	4	8	4
2	2	2	5	17	5	16	5
3	3	4	5	18	6	32	6
4	4	8	10	19	7	64	7
5	5	16	5	20	8	128	8
6	10	32	1	21	9	512	9
7	5	4	2	22	10	1024	10
8	10	8	1	23	11	1	11
9	20	16	1	24	12	2	12
10	20	4	1	25	13	4	13
11	40	8	4	26	14	8	14
12	100	2	2	27	15	16	15
13	1	1	1	28	16	4	16
14	2	2	2	29	17	8	17
15	3	4	3	30	18	1024	18

Задача 10.

а). Визначити приватну інформацію $I(x_i)$, що міститься у повідомленні x_i першого зустрічного студента: «У мене сьогодні день народження!», за умови, що в році 365 днів.

б). Визначити повну інформацію $I(X)$ від повідомлення, що з'ясовує чи є сьогоднішній день днем народження першого зустрічного студента?

Задача 11.

У вихідному повідомленні A джерела дискретних повідомлень, складеного на підставі використання алфавіту з m якісними ознаками, міститься n двійкових розрядів. Визначити приватну ентропію $H(x_i)$ на один елемент a_i повідомлення A , а також загальну ентропію $H(A)$ усього повідомлення, при заданих ймовірностях $P(a_i)$ появи елементів a_i повідомлення. Варіанти завдань представлені у таблиці.

Варіанти завдань

Вар.	P_1	P_2	P_3	P_4	n	Вар.	P_1	P_2	P_3	P_4	n
1	0,6	0,25	0,05	0,1	20	16	0,7	0,1	0,1	0,1	5
2	0,25	0,25	0,25	0,25	10	17	0,1	0,1	0,7	0,1	10
3	0,3	0,3	0,3	0,1	5	18	0,2	0,1	0,6	0,1	20
4	0,3	0,1	0,1	0,5	4	19	0,3	0,1	0,5	0,1	30
5	0,3	0,2	0,1	0,4	3	20	0,4	0,1	0,4	0,1	1
6	0,3	0,1	0,2	0,4	2	21	0,5	0,1	0,3	0,1	2
7	0,4	0,1	0,2	0,3	1	22	0,6	0,1	0,2	0,1	3
8	0,5	0,1	0,2	0,2	5	23	0,7	0,1	0,1	0,1	4
9	0,6	0,1	0,2	0,1	10	24	0,8	0,05	0,05	0,1	5
10	0,1	0,1	0,1	0,7	20	25	0,1	0,6	0,1	0,2	6
11	0,2	0,1	0,1	0,6	30	26	0,2	0,5	0,1	0,2	7
12	0,3	0,1	0,1	0,5	40	27	0,3	0,4	0,1	0,2	8
13	0,4	0,1	0,1	0,4	50	28	0,4	0,3	0,1	0,2	9
14	0,5	0,1	0,1	0,3	60	29	0,5	0,2	0,1	0,2	10
15	0,6	0,1	0,1	0,2	100	30	0,6	0,1	0,1	0,2	15

Задача 12.

Розв'язати задачу 11 за умови, що поява всіх m ознак рівноймовірна.

Задача 13.

Визначити кількісну залежність між величинами, що визначають одиниці виміру кількості інформації: біт, ніт, діт.

$$1 \text{ біт} = \begin{cases} -\delta i m, \\ -ni m. \end{cases} \quad 1 \text{ діт} = \begin{cases} -\delta i m, \\ -ni m. \end{cases} \quad 1 \text{ ніт} = \begin{cases} -\delta i m, \\ -\delta i m. \end{cases}$$

Задача 14.

Порівняти ентропії двох ансамблів X та Y ДДП

$$X = \begin{pmatrix} 10 & 20 & 3,5 & 15 \\ 0,25 & 0,25 & 0,25 & 0,25 \end{pmatrix}; \quad Y = \begin{pmatrix} 0,1 & 0,15 & 16 & 105 \\ 0,25 & 0,25 & 0,25 & 0,25 \end{pmatrix}.$$

Задача 15.

Визначити ентропію системи, що описується дискретною випадковою величиною X з наступним рядом розподілу ймовірностей цих величин: $p(x_1) = p(x_2) = p(x_3) = p(x_4) = 0,01$; $p(x_5) = 0,96$.

Задача 16

Визначити загальну ентропію джерела дискретних повідомлень з наступним ансамблем

$$X = \begin{pmatrix} x_1 & x_2 \dots & x_i \dots & x_m \\ p_1 & p_2 \dots & p_i \dots & p_m \end{pmatrix}.$$

Варіанти завдань представлені в таблиці.

Таблиця А.2.6.

Варіанти завдань

Вар.	p ₁	p ₂	p ₃	p ₄	Вар.	p ₁	p ₂	p ₃	p ₄
1	0,1	0,1	0,3	0,5	16	0,8	0,1	0,05	0,05
2	0,1	0,1	0,1	0,7	17	0,7	0,2	0,05	0,05
3	0,1	0,1	0,7	0,1	18	0,6	0,3	0,05	0,05
4	0,1	0,1	0,2	0,6	19	0,5	0,4	0,05	0,05
5	0,1	0,1	0,4	0,4	20	0,6	0,15	0,15	0,1
6	0,2	0,1	0,1	0,6	21	0,6	0,2	0,1	0,1
7	0,3	0,1	0,1	0,5	22	0,5	0,3	0,1	0,1
8	0,4	0,1	0,1	0,4	23	0,6	0,1	0,15	0,15
9	0,5	0,1	0,1	0,3	24	0,5	0,1	0,2	0,2
10	0,6	0,1	0,1	0,2	25	0,4	0,2	0,2	0,2
11	0,7	0,1	0,1	0,1	26	0,3	0,2	0,2	0,2
12	0,25	0,25	0,25	0,25	27	0,15	0,15	0,2	0,5
13	0,9	0,05	0,05	0	28	0,15	0,15	0,15	0,55
14	0,8	0,05	0,05	0,1	29	0,4	0,4	0,1	0,1
15	0,7	0,05	0,05	0,2	30	0,3	0,3	0,3	0,1

Задача 17.

Двійкове (символи a_1, a_2) дискретне джерело інформації A виробляє перший символ a_1 з ймовірністю P .

Визначити приватну кількість інформації $J(a_i)$ у a_1 і a_2 , а також загальну ентропію $H(A)$ джерела при заданому значенні P .

Варіанти завдань представлені в таблиці.

Таблиця А.2.7.

Варіанти завдань

Вар.	P	Вар.	P	Вар.	P	Вар.	P	Вар.	P	Вар.	P
1	0,1	6	0,6	11	0	16	0,15	21	0,95	26	0,06
2	0,2	7	0,7	12	0,01	17	0,35	22	0,02	27	0,07
3	0,3	8	0,8	13	0,25	18	0,65	23	0,03	28	0,08
4	0,4	9	0,9	14	0,45	19	0,75	24	0,04	29	0,09
5	0,5	10	1	15	0,55	20	0,85	25	0,05	30	0,21

Задача 18.

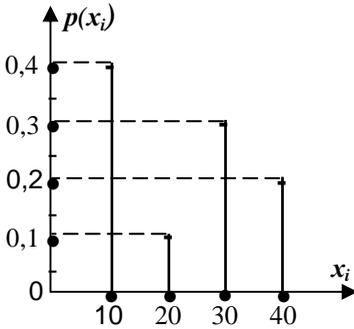


Рис. А.1.

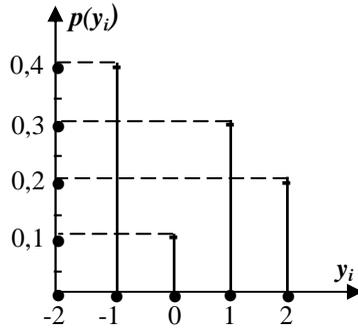


Рис. А.2.

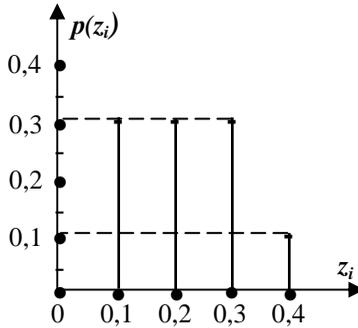


Рис. А.3.

Задача 23.

Нехай X і Y є два дискретних джерела повідомлень та $Z = X + Y$.
Визначити умовну ентропію $H(Z/X)$, якщо:

- а) X та Y незалежні;
- б) X та Y залежні.

Задача 24.

Джерело A виробляє двійкові символи a_1 та a_2 з безумовними та умовними ймовірностями відповідно

$$p(a_1), p(a_2), p(a_1/a_1), p(a_2/a_1), p(a_1/a_2), p(a_2/a_2).$$

Визначити середню умовну ентропію $H(A)$ джерела. Варіанти завдань представлені у таблиці.

Таблиця А.2.7.

Варіанти завдань

Вар.	$p(a_1)$	$p(a_1/a_1)$	$p(a_2/a_1)$	$p(a_1/a_2)$	$p(a_2/a_2)$
1	0,2	0,4	0,6	0,15	0,85
2	0,1	0,1	0,9	0,1	0,9
3	0,3	0,2	0,8	0,2	0,8
4	0,4	0,3	0,7	0,4	0,6
5	0,5	0,5	0,5	0,1	0,9
6	0,6	0,6	0,4	0,2	0,8
7	0,7	0,7	0,3	0,3	0,7
8	0,8	0,8	0,2	0,4	0,6
9	0,9	0,9	0,1	0,5	0,5
10	0,1	0,1	0,9	0,6	0,4
11	0,1	0,2	0,8	0,7	0,3
1	0,2	0,3	0,7	0,8	0,2
13	0,3	0,4	0,6	0,9	0,1
14	0,4	0,5	0,5	1	0
15	0,5	0,6	0,4	0	1
16	0,1	0,1	0,9	0,1	0,9
17	0,2	0,2	0,8	0,3	0,7
18	0,3	0,3	0,7	0,5	0,5
19	0,4	0,4	0,6	0,7	0,3
20	0,5	0	0	0	0
21	0,5	0,5	0,5	0,5	0,5
22	0,5	0,5	0,5	0,9	0,1
23	0,6	0,6	0,4	0,2	0,8
24	0,7	0,7	0,3	0,4	0,6
25	0,8	0,8	0,2	0,6	0,4
26	0,9	0,9	0,1	0,8	0,2
27	0,1	0,2	0,8	0,7	0,3
28	0,9	0,2	0,8	0,75	0,25
29	0,1	0,2	0,8	0,8	0,2
30	0,5	0,2	0,8	0,85	0,15

Задача 25.

Нехай дана матриця де $P_{ij} = p(x_i, y_j)$ об'єднання двох джерел повідомлень X та Y .

Таблиця А.2.8

Матриця об'єднання

X \ Y	Y					
		y ₁	y ₂	...	y _m	P(x _i)
x ₁		P ₁₁	P ₁₂	...	P _{1m}	P(x ₁)
x ₂		P ₂₁	P ₂₂	...	P _{2m}	P(x ₂)
...		P _{ij} = (x _i , y _j)
x _n		P _{n1}	P _{n2}	...	P _{nm}	P(x _n)
P(y _j)		P(y ₁)	P(y ₂)	...	P(y _m)	

При цьому:

$$p(x_i) = \sum_{j=1}^m p_{ij}, \text{ для } i = \overline{1, n};$$

$$p(y_j) = \sum_{i=1}^n p_{ij}, \text{ для } j = \overline{1, m}.$$

Необхідно визначити:

- а) загальні безумовні ентропії $H(X)$ та $H(Y)$;
- б) загальні умовні ентропії $H(X/Y)$ та $H(Y/X)$;
- в) спільну ентропію $H(X, Y)$;
- г) взаємну ентропію $H(X \cdot Y)$.

По відомих співвідношеннях перевірити правильність проведених розрахунків.

У таблиці А.2.9 приведені варіанти завдань для розв'язання задачі 25, а в таблиці 3 представлені загальні позначення матриці об'єднання $P_i = p(x_i, y_j)$.

Таблиця А.2.9

Варіанти завдань

Вар.	P ₁₁	P ₁₂	P ₁₃	P ₂₁	P ₂₂	P ₂₃	P ₃₁	P ₃₂	P ₃₃
1	0,1	0,5	0	0,2	0,2	0	0	0	0
2	0,2	0,4	0	0,1	0,3	0	0	0	0
3	0,1	0,2	0	0,1	0,6	0	0	0	0
4	0,2	0,3	0	0,3	0,2	0	0	0	0
5	0,1	0,4	0	0,4	0,1	0	0	0	0
6	0,15	0,35	0	0,35	0,15	0	0	0	0
7	0,1	0,1	0,3	0,3	0,1	0,1	0	0	0
8	0,4	0,4	0	0,1	0	0,1	0	0	0
9	0,1	0,1	0,3	0,2	0,2	0,1	0	0	0

Вар.	P_{11}	P_{12}	P_{13}	P_{21}	P_{22}	P_{23}	P_{31}	P_{32}	P_{33}
10	0,4	0,4	0,1	0,05	0,05	0	0	0	0
11	0,2	0,1	0,1	0,1	0,4	0,1	0	0	0
12	0,3	0,3	0,2	0,1	0,05	0,05	0	0	0
13	0,1	0,2	0,3	0,25	0	0,15	0	0	0
14	0,1	0,1	0,3	0,25	0,1	0,15	0	0	0
15	0,1	0,3	0,2	0,25	0	0,15	0	0	0
16	0,2	0,2	0,2	0,4	0	0	0	0	0
17	0,1	0,1	0,1	0,5	0,1	0,1	0	0	0
18	0,4	0,2	0,2	0,1	0,1	0	0	0	0
19	0,1	0,2	0,3	0,25	0	0,15	0	0	0
20	0,4	0,1	0	0	0,2	0,1	0	0	0,2
21	0,1	0,1	0,1	0	0,3	0	0	0,2	0,2
22	0,1	0,05	0,15	0	0,3	0	0	0,2	0,2
23	0,05	0,15	0,1	0	0,3	0	0	0,2	0,2
24	0	0,1	0,2	0,1	0,3	0	0,1	0	0,2
25	0,1	0	0,2	0,1	0,3	0	0	0,1	0,2
26	0,05	0,05	0,2	0	0,3	0,1	0,15	0	0,15
27	0,1	0,1	0,1	0,1	0,1	0,2	0,2	0	0,1
28	0,2	0	0,1	0,1	0,1	0,2	0,2	0	0,1
29	0,2	0,05	0,05	0,2	0,1	0,1	0,05	0	0,25
30	0,1	0,2	0	0	0,3	0	0	0,2	0,2

Таблиця А.2.10

Таблиця позначень

$\begin{matrix} Y \\ X \end{matrix}$	y_1	y_2	y_3	P_i
x_1	P_{11}	P_{12}	P_{13}	$P(x_1)$
x_2	P_{21}	P_{22}	P_{23}	$P(x_2)$
x_3	P_{31}	P_{32}	P_{33}	$P(x_3)$
P_j	$P(y_1)$	$P(y_2)$	$P(y_3)$	$\begin{matrix} 1 \\ 1 \end{matrix}$

Задача 26.

Нехай відомі безумовні ентропії $H(X)$ та $H(Y)$. Визначити, у яких межах буде змінюватися умовна ентропія $H(Y / X)$ при зміні умовної ентропії $H(X / Y)$ у максимально можливих межах. Вихідні дані представлені у таблиці.

Таблиця А.2.11

Варіанти завдань

Вар.	$H(X)$	$H(Y)$	Вар.	$H(X)$	$H(Y)$	Вар.	$H(X)$	$H(Y)$
1	0,1	1	11	7,5	10	21	7	10
2	1	1	12	8	10	22	8	10
3	1,5	2	13	10	10	23	9	10
4	2	2	14	11	15	24	15	20
5	3	5	15	12	15	25	60	10
6	3,5	5	16	15	15	26	70	100
7	4	5	17	20	30	27	80	100
8	4,5	5	18	25	30	28	90	100
9	5	5	19	30	30	29	100	100
10	6	10	20	50	100	30	1	100

Задача 27.

Сигнали управління з виходу автоматизованої системи управління технологічними процесами (АСУ ТП) у цифровій формі (у виді двійкового коду) надходять на вхід технологічного об'єкта управління автоматизованого технологічного комплексу (ТОУ АТК) з ймовірностями появи сигналів, що відповідають значенням «1» та «0», рівними відповідно, $p(x_1) = 0,6$ та $p(x_0) = 0,4$. При цьому надходження кожного із символів «1» та «0» взаємозалежно наступними співвідношеннями $p(x_i / x_j)$ для $i, j = \overline{0,1}$; $p(x_1) + p(x_0) = 1$; де: $p(x_i / x_j)$ – умовні ймовірності появи вхідних символів «0» та «1». (див. табл. А.2.12).

Таблиця А.2.12

Варіанти завдань

Вар.	$p(x_1)$	$p(x_0/x_0)$	$p(x_1/x_0)$	$p(x_1/x_1)$	$p(x_0/x_1)$
1	0,1	0,1	0,9	0,1	0,9
2	0,2	0,2	0,8	0,1	0,9
3	0,3	0,3	0,7	0,1	0,9
4	0,4	0,4	0,6	0,1	0,9
5	0,5	0,5	0,5	0,5	0,5
6	0,6	0,3	0,7	0,3	0,7
7	0,7	0,4	0,6	0,3	0,7
8	0,8	0,1	0,9	0,3	0,7
9	0,9	0,4	0,6	0,5	0,5
10	0,9	0,3	0,7	0,5	0,5

Вар.	$p(x_i)$	$p(x_0/x_0)$	$p(x_1/x_0)$	$p(x_1/x_1)$	$p(x_0/x_1)$
11	0,8	0,1	0,9	0,5	0,5
12	0,7	0,1	0,9	0,1	0,9
13	0,8	0,1	0,9	0,5	0,5
14	0,6	0,2	0,8	0,1	0,9
15	0,4	0,1	0,9	0,2	0,8
16	0,3	0,2	0,8	0,2	0,8
17	0,4	0,8	0,2	0,8	0,2
18	0,7	0,4	0,6	0,4	0,6
19	0,2	0,6	0,4	0,6	0,4
20	0,1	0,3	0,7	0,7	0,3
21	0,8	0,7	0,3	0,3	0,7
22	0,3	0,5	0,5	0,1	0,9
23	0,1	0,5	0,5	0,1	0,9
24	0,9	0,5	0,5	0,9	0,1
25	0,4	0,4	0,6	0,4	0,6
26	0,9	0,6	0,4	0,3	0,7
27	0,1	0,6	0,4	0,3	0,7
28	0,7	0,4	0,6	0,7	0,3
29	0,5	0,4	0,6	0,2	0,8
30	0,6	0,1	0,9	0,1	0,9

Необхідно визначити ентропію $H(X)$ вхідної інформації.

Задача 28.

Параметр X , що вимірюється може приймати два значення x_0 та x_1 з рівною ймовірністю $p(x_0) = p(x_1)$. Внаслідок обмеженої точності системи контролю можливі помилки виміру виду $x_0 \rightarrow x_1$ та $x_1 \rightarrow x_0$, тобто замість x_0 може бути зафіксовано значення x_1 та навпаки, замість значення x_1 - отримана величина x_0 . Умовні ймовірності $p(x_i / x_j)$ таких подій однакові і дорівнюють значенням $0,01$.

Потрібно визначити кількість інформації $I(X)$, одержуване оператором АСУ ТП при проведенні контролю.

Задача 29.

Відповідно до вихідних даних варіантів задачі 25 визначити середня кількість інформації $I(X)$ при прийомі повідомлення по каналу, що задано матрицею $P(X,Y)$ спільних ймовірностей передачі та прийому елементів повідомлення. У цьому випадку елементами p_{ij} матриці є спільні ймовірності появи елементів x_i на виході джерела інформації та елементів y_j на вході приймача інформації.

Таблиця А.2.13

Таблиця позначень

$X \backslash Y$	y_1	y_2	...	y_m	$p(x_i) = \sum_{j=1}^m p(x_i, y_j)$
x_1	p_{11}	p_{12}	...	p_{1m}	
x_2	p_{21}	p_{22}	...	p_{2m}	
...			p_{iJ}		
x_n	p_{n1}	p_{n2}		p_{nm}	

Задача 30.

Відповідно до результатів теореми В.А. Котельникова, за заданим значенням m та Δt , необхідно сформувавши цифровий вид сигналу (цифровий код) для передачі його по каналу зв'язку.

Варіанти завдань представлені у таблиці та на рис. 1 – 6.

Таблиця А.2.14

Таблиця позначень

Вар.	Рис.	Графік функції	Вар.	Рис.	Графік функції
1	1	I	16	4	I
2	1	II	17	4	II
3	1	III	18	4	III
4	1	IV	19	4	IV
5	1	V	20	4	V
6	2	I	21	5	I
7	2	II	22	5	II
8	2	III	23	5	III
9	2	IV	24	5	IV
10	2	V	25	5	V
11	3	I	26	6	I
12	3	II	27	6	II
13	3	III	28	6	III
14	3	IV	29	6	IV
15	3	V	30	6	V

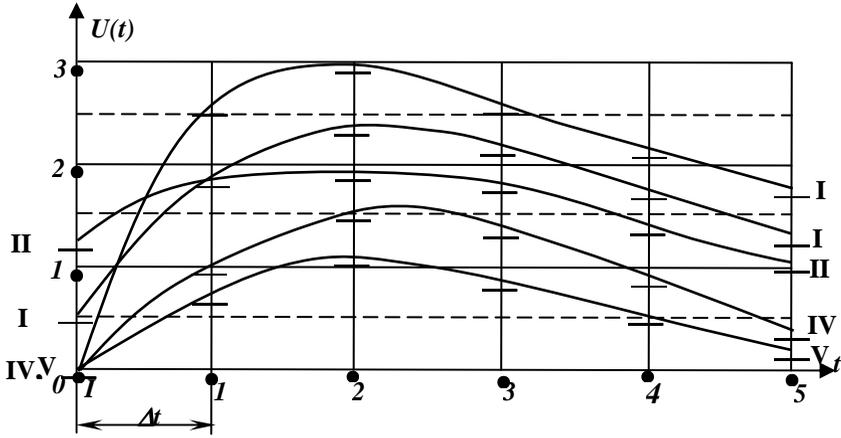


Рис. А.4. – Варіанти завдань

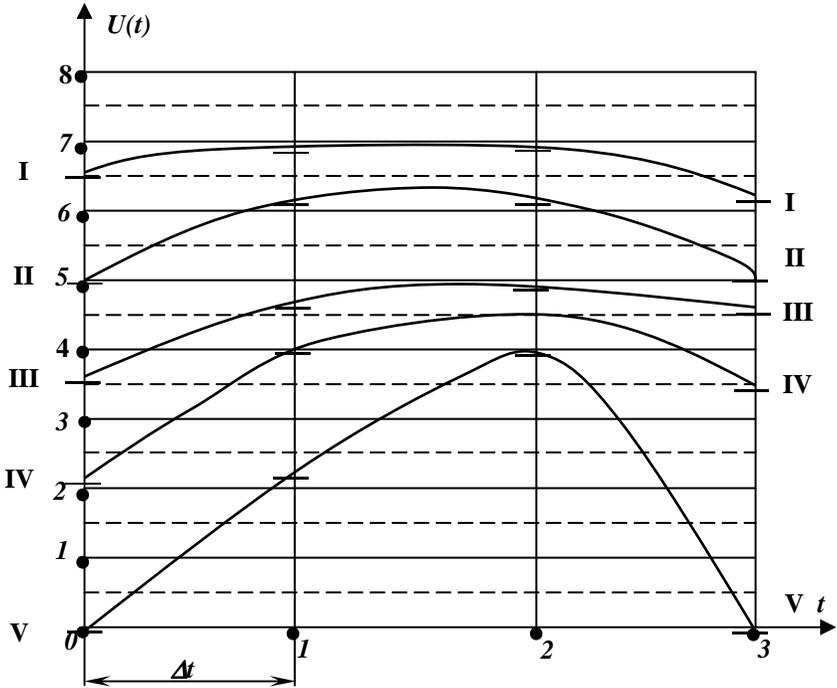


Рис. А.5. – Варіанти завдань

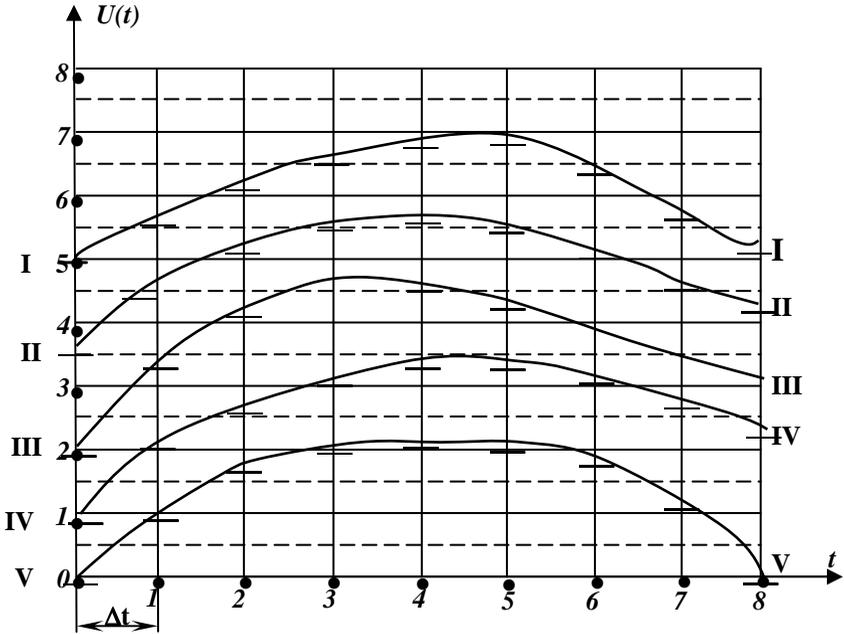


Рис. А.6. – Варіанти завдань

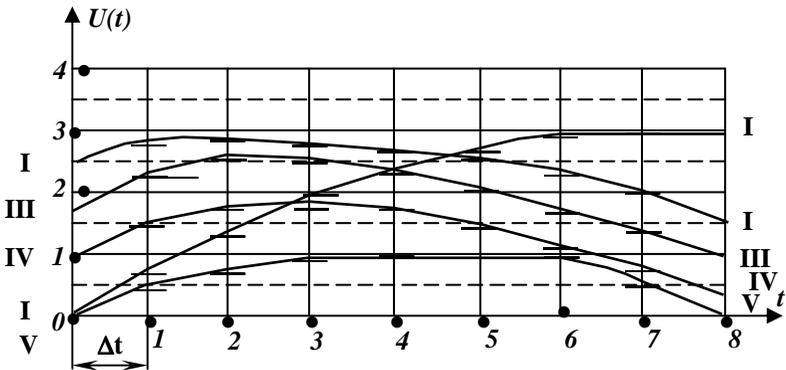


Рис. А.7. – Варіанти завдань

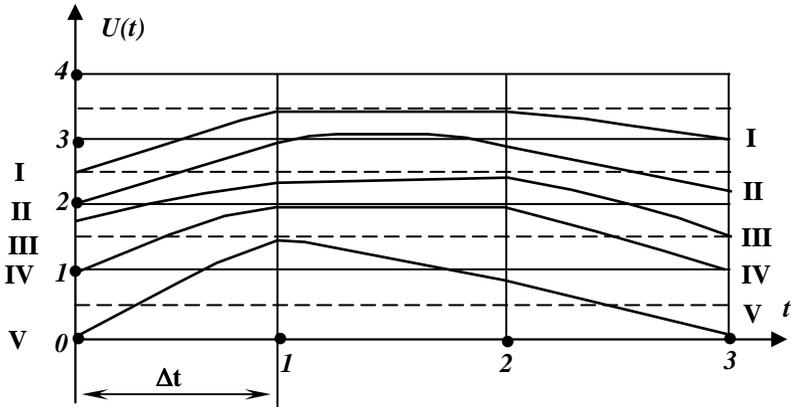


Рис. А.8. – Варіанти завдань

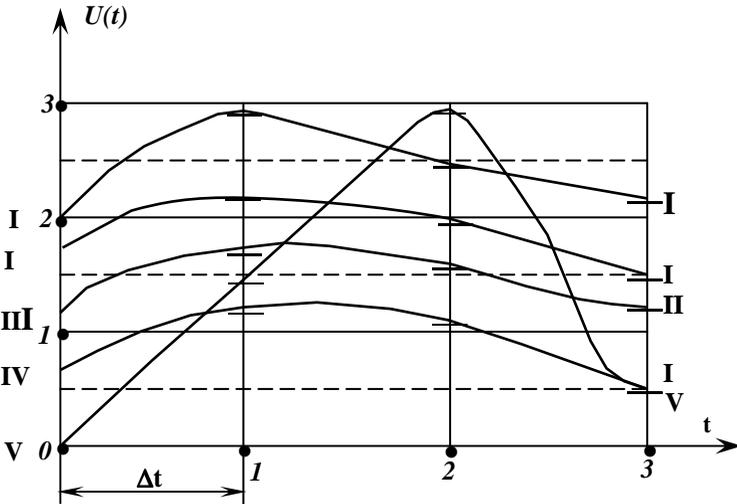


Рис. А.9. – Варіанти завдань

Задача 31.

Дискретне джерело інформації видає I одиниць інформації, при цьому середня ентропія, що приходиться на один елемент надлишкового повідомлення S_n дорівнює $H_n(x)$.

Відповідно до варіанта завдання (таблиця) знайти довжину S_n двійкового коду на виході джерела.

Таблиця позначень

Вар.	I	$I_n(X)$	Вар.	I	$I_n(X)$	Вар.	I	$I_n(X)$
1	2	0,1	11	20	0,2	21	10	0,1
2	4	0,2	12	25	0,4	22	20	0,2
3	8	0,3	13	30	0,6	23	30	0,3
4	10	0,4	14	40	0,8	24	40	0,4
5	20	0,5	15	50	0,2	25	50	0,5
6	25	0,6	16	60	0,4	26	60	0,6
7	30	0,7	17	70	0,6	27	15	0,7
8	5	0,8	18	80	0,8	28	25	0,1
9	10	0,9	19	90	0,9	29	35	0,2
10	15	1	20	100	0,1	30	50	0,3

Задача 32.

Стаціонарне джерело видає за час $T = 10^6 c$ двійковими послілками тривалості $\tau = 10$ мс $I = 10^6$ біт інформації. За який час та якою кількістю двійкових послілок можна передати такий самий об'єм I інформації, якщо відповідною обробкою цілком усунуто надмірність джерела? Визначити коефіцієнти надмірності та стиску джерела.

Задача 33.

Показати, що максимальна кількість інформації, яка міститься у квантованому телевізійному сигналі, що відповідає одному телевізійному кадру при 625 рядках розкладання, дорівнює $I = 2,083 \cdot 10^6$ біт. При цьому сигнал, що відповідає одному рядку зображення, є послідовність із 833 (при співвідношенні сторін кадру 4/3) статистично незалежних випадкових по амплітуді імпульсів, кожний з яких з рівною ймовірністю приймає лише одне з 16 значень. Знайти надмірність телевізійного сигналу, якщо фактично кадр зображення з 16 градаціями рівнів ($m = 16$) містить $9,37 \cdot 10^5$ біт.

Задача 34.

Згідно з одержаними експериментальними даними значень безумовних ймовірностей появи у тексті букв російського, українського та англійського алфавітів (додатки Г, Д та Е) знайти ентропію джерела інформації, що видає тексти з цих букв, при відсутності статичних зв'язків між буквами. Також обчислити надмірність джерела, що видає російські, українські та англійські тексти, обумовлену нерівноймовірністю вибору букв, а також і їх статистичними зв'язками, якщо по експериментальним даним ентропія джерела дорівнює $H(X) = 1$ біт/буква.

Задача 35.

Після усунення статистичних зв'язків між символами збільшений ал-

фавіт характеризується 8 символами, ймовірності яких наведені у таблиці.

Таблиця А.2.16

Таблиця позначень

Номер символу	Ймовірність	Код	n
1	0,6	1	1
2	0,2	10	2
3	0,1	100	3
4	0,04	1000	4
5	0,025	10000	5
6	0,015	100000	6
7	0,01	1000000	7
8	0,01	10000000	8

Показати, що використання нерівномірного двійкового коду, зазначеного у таблиці дозволяє майже цілком усунути надмірність. Крім цього визначити коефіцієнти K_c та K_n .

Задача 36.

Визначити диференційну ентропію $h(x)$ неперервного сигналу x , який має експоненційний закон розподілу з функцією щільності ймовірності для $x > 0$

$$f(x) = \frac{1}{a} \cdot e^{-\frac{x}{a}}$$

Задача 37.

Визначити ентропію неперервного джерела інформації, якщо миттєві значення повідомлення розподілені за нормальним законом для $\sigma_x = 10$, де σ_x - дисперсія.

Задача 38.

Визначити диференційну ентропію вимірів величини X в межах $[a, 2a]$, якщо її значення розподілено за рівномірним законом.

Додаток Б

Таблиця Б.1

Двійкові логарифми чисел від 1 до 128

x	$\log_2 x$						
1	0,0000	33	5,04439	65	6,02237	97	6,59991
2	1,0000	34	5,08746	66	6,04439	98	6,61471
3	1,5849	35	5,12928	67	6,06609	99	6,62936
4	2,0000	36	5,16993	68	6,08746	100	6,65386
5	2,3219	37	5,20945	69	6,10852	101	6,65821
6	2,5849	38	5,24793	70	6,12928	102	6,67242
7	2,8073	39	5,28540	71	6,14975	103	6,68650
8	3,0000	40	5,32193	72	6,16992	104	6,70044
9	3,1699	41	5,35755	73	6,18982	105	6,71425
10	3,3219	42	5,39232	74	6,20945	106	6,72792
11	3,4594	43	5,42626	75	6,22882	107	6,74147
12	3,5849	44	5,45943	76	6,24793	108	6,75489
13	3,7004	45	5,49185	77	6,26679	109	6,76818
14	3,8073	46	5,52356	78	6,28540	110	6,78136
15	3,9068	47	5,55459	79	6,30378	111	6,79445
16	4,0000	48	5,58496	80	6,32193	112	6,80732
17	4,0874	49	5,61471	81	6,33985	113	6,82018
18	4,1699	50	5,64386	82	6,35755	114	6,83289
19	4,2479	51	5,67242	83	6,37504	115	6,84549
20	4,3219	52	5,70044	84	6,39232	116	6,85798
21	4,3923	53	5,72792	85	6,40939	117	6,87036
22	4,4594	54	5,75489	86	6,42626	118	6,88264
23	4,5235	55	5,78136	87	6,44294	119	6,89482
24	4,5849	56	5,80735	88	6,45943	120	6,90689
25	4,6438	57	5,83289	89	6,47573	121	6,91886
26	4,7004	58	5,85798	90	6,49185	122	6,93074
27	4,7548	59	5,88264	91	6,50779	123	6,94252
28	4,8073	60	5,90689	92	6,52356	124	6,95420
29	4,8579	61	5,93074	93	6,53916	125	6,96578
30	4,9068	62	5,95420	94	6,55459	126	6,97728
31	4,9542	63	5,97728	95	6,56986	127	6,98869
32	5,0000	64	6,00000	96	6,5849	128	7,00000

Додаток В

Таблиця В. 1

Значення двійкових логарифмів чисел виду $-p \log_2 p$

p	$-\log_2 p$	$-p \log_2 p$	H	$-q \log_2 q$	$-\log_2 q$	q
0,0005	10,965784	0,005483	0,006204	0,000721	0,000722	0,9995
0,0010	9,965784	0,009966	0,011408	0,001442	0,001443	0,9990
0,0015	9,380882	0,014071	0,016234	0,002162	0,002166	0,9985
0,0020	8,965784	0,017932	0,020814	0,002882	0,002888	0,9980
0,0025	8,643956	0,021610	0,025212	0,003602	0,003611	0,9975
0,0030	8,380882	0,025142	0,029464	0,004322	0,004335	0,9970
0,0035	8,158429	0,028555	0,033595	0,005041	0,005058	0,9965
0,0040	7,965784	0,031863	0,037622	0,005759	0,005782	0,9960
0,0045	7,795859	0,035081	0,041559	0,006477	0,006507	0,9955
0,0050	7,643856	0,038219	0,045415	0,007195	0,007232	0,9950
0,0055	7,506353	0,041285	0,049198	0,007913	0,007957	0,9945
0,0060	7,380822	0,044285	0,052915	0,008630	0,008682	0,9940
0,0065	7,265345	0,047225	0,056572	0,009347	0,009408	0,9935
0,0070	7,158429	0,050109	0,060172	0,010063	0,010134	0,9930
0,0075	7,058894	0,052942	0,063721	0,010780	0,010861	0,9925
0,0080	6,955784	0,055726	0,067222	0,011495	0,011588	0,9920
0,0085	6,878321	0,058466	0,070676	0,012211	0,012315	0,9915
0,0090	6,795859	0,061163	0,074088	0,012926	0,013043	0,9910
0,0095	6,717857	0,063820	0,077460	0,013640	0,013771	0,9905
0,0100	6,643856	0,066439	0,080793	0,014355	0,014500	0,9900
0,0110	6,506353	0,071570	0,087352	0,015782	0,015958	0,9890
0,0120	6,380822	0,076570	0,093778	0,017208	0,017417	0,9880
0,0130	6,265345	0,081449	0,100082	0,018633	0,018878	0,9870
0,0140	6,158429	0,086218	0,106274	0,020056	0,020340	0,9860
0,0150	6,058894	0,090883	0,112361	0,021477	0,021804	0,9850
0,0160	5,965784	0,095453	0,118350	0,022897	0,023270	0,9840
0,0170	5,878321	0,099931	0,12248	0,024316	0,024737	0,9830
0,0180	5,795859	0,104325	0,130059	0,025733	0,026205	0,9820
0,0190	5,717857	0,108639	0,135788	0,027149	0,027675	0,9810
0,0200	5,643856	0,112877	0,141441	0,028563	0,029146	0,9800
0,0210	5,573467	0,117043	0,147019	0,029976	0,030619	0,9790
0,0220	5,506353	0,121140	0,152527	0,031388	0,032094	0,9780
0,0230	5,442222	0,125171	0,157969	0,032797	0,033570	0,9770
0,0240	5,380822	0,129140	0,163346	0,034206	0,035047	0,9760
0,0250	5,321928	0,133048	0,168661	0,035513	0,036526	0,9750

p	$-\log_2 p$	$-p \log_2 p$	H	$-q \log_2 q$	$-\log_2 q$	q
0,0260	5,265345	0,136899	0,173917	0,037018	0,038006	0,9740
0,0270	5,210897	0,140694	0,179116	0,038422	0,039488	0,9730
0,0280	5,158428	0,144436	0,184216	0,040972	0,040972	0,9720
0,0290	5,107803	0,148126	0,189352	0,041226	0,042457	0,9710
0,0300	5,058894	0,151767	0,194392	0,042625	0,043943	0,9700
0,0310	5,011588	0,155359	0,199382	0,044023	0,045431	0,9690
0,0320	4,965784	0,158905	0,204325	0,045420	0,046921	0,9680
0,0330	4,921390	0,162406	0,209220	0,046815	0,048412	0,9670
0,0340	4,878321	0,165863	0,214071	0,048208	0,049904	0,9660
0,0350	4,836501	0,169278	0,218878	0,049600	0,051399	0,9650
0,0360	4,795859	0,172651	0,223642	0,050991	0,052895	0,9640
0,0370	4,756331	0,175984	0,228364	0,052380	0,054392	0,9630
0,0380	4,717857	0,179279	0,233046	0,053767	0,055891	0,9620
0,0390	4,680382	0,182535	0,237688	0,055153	0,057392	0,9610
0,0400	4,643856	0,185754	0,242292	0,056553	0,058894	0,9600
0,0410	4,608232	0,188938	0,246858	0,057921	0,060397	0,9590
0,0420	4,573467	0,192086	0,251388	0,059303	0,061902	0,9580
0,0430	4,539519	0,195199	0,255882	0,060683	0,063409	0,9570
0,0440	4,506353	0,198280	0,260341	0,062061	0,064917	0,9560
0,0450	4,473931	0,201327	0,264765	0,063438	0,066427	0,9550
0,0460	4,442222	0,204342	0,269156	0,064814	0,067939	0,9540
0,0470	4,411195	0,207326	0,273514	0,066188	0,069452	0,9530
0,0480	4,380822	0,210279	0,277840	0,067560	0,070967	0,9520
0,0490	4,351074	0,213203	0,282134	0,068931	0,072483	0,9610
0,0500	4,321928	0,216096	0,286397	0,070301	0,074001	0,9500
0,0520	4,265345	0,221798	0,294833	0,073035	0,077041	0,9480
0,0530	4,237864	0,224607	0,290007	0,074400	0,078564	0,9470
0,0540	4,210897	0,227388	0,303152	0,075763	0,070078	0,9460
0,0550	4,184425	0,230143	0,307268	0,077125	0,081614	0,9450
0,0560	4,158429	0,232872	0,311357	0,078485	0,083141	0,9440
0,0570	4,132894	0,235575	0,315419	0,079844	0,084670	0,9430
0,0580	4,107803	0,238253	0,319454	0,081201	0,086201	0,9420
0,0590	4,083141	0,240905	0,323462	0,082557	0,087733	0,9410
0,0600	4,058894	0,243534	0,327445	0,083911	0,089267	0,9400
0,0625	4,000000	0,250000	0,337290	0,087290	0,093109	0,9375
0,0650	3,943416	0,256322	0,346981	0,090659	0,096962	0,9350
0,0675	3,888969	0,262505	0,356524	0,094019	0,100824	0,9325
0,0700	3,936501	0,268555	0,365924	0,097369	0,104698	0,9300

p	$-\log_2 p$	$-p \log_2 p$	H	$-q \log_2 q$	$-\log_2 q$	q
0,0725	3,785875	0,274476	0,375185	0,100709	0,108581	0,9275
0,0750	3,736966	0,280272	0,384312	0,104039	0,112475	0,9250
0,0775	3,689660	0,285949	0,393308	0,107360	0,116379	0,9225
0,0800	3,643856	0,291508	0,402179	0,110671	0,120294	0,9200
0,0825	3,599462	0,296956	0,410227	0,113972	0,124220	0,9175
0,0850	3,556393	0,302293	0,419556	0,117263	0,128156	0,9150
0,0875	3,514573	0,307525	0,428070	0,120544	0,132104	0,9125
0,0900	3,473931	0,312654	0,436470	0,123816	0,136062	0,9100
0,0925	3,434402	0,317682	0,444760	0,127078	0,140030	0,9075
0,0950	3,395929	0,322613	0,452943	0,130329	0,144010	0,9050
0,0975	3,358454	0,327449	0,461020	0,133571	0,148001	0,9025
0,1000	3,321928	0,332193	0,468986	0,136803	0,152003	0,9000
0,1025	3,286304	0,336846	0,476871	0,140024	0,156016	0,8975
0,1050	3,251539	0,341412	0,484648	0,143236	0,160040	0,8950
0,1075	3,217591	0,345891	0,492329	0,146438	0,164076	0,8925
0,1100	3,184425	0,350287	0,499916	0,149629	0,168123	0,8900
0,1125	3,152003	0,354600	0,507411	0,152811	0,172181	0,8875
0,1150	3,120294	0,358834	0,514816	0,155982	0,176251	0,8850
0,1175	3,089267	0,362989	0,522132	0,159143	0,180332	0,8825
0,1200	3,058894	0,367067	0,529361	0,162294	0,184425	0,8800
0,1225	3,029146	0,371070	0,536505	0,165434	0,188529	0,8775
0,1250	3,000000	0,375000	0,543564	0,168564	0,192645	0,8750
0,1275	2,911431	0,378857	0,550542	0,171684	0,196773	0,8725
0,1300	2,943416	0,382644	0,557438	0,174794	0,200913	0,8700
0,1325	2,915936	0,386361	0,564255	0,177893	0,205064	0,8675
0,1350	2,888969	0,390011	0,570993	0,180982	0,209228	0,8650
0,1375	2,862496	0,393593	0,577654	0,184061	0,213404	0,8625
0,1400	2,836501	0,397110	0,584239	0,187129	0,217591	0,8600
0,1425	2,810966	0,400563	0,590749	0,190186	0,221791	0,8575
0,1450	2,785875	0,403952	0,597185	0,193233	0,226004	0,8550
0,1475	2,761213	0,407279	0,603549	0,196270	0,230228	0,8525
0,1500	2,736966	0,410545	0,609840	0,199295	0,234465	0,8500
0,1525	2,713119	0,413751	0,616061	0,203311	0,238715	0,8475
0,1550	2,689660	0,416897	0,622213	0,205315	0,142977	0,8450
0,1575	2,666576	0,419986	0,628295	0,208309	0,247251	0,8425
0,1600	2,643856	0,423017	0,634310	0,211293	0,251539	0,8400
0,1625	2,621488	0,425992	0,640257	0,214265	0,255839	0,8375

p	$-\log_2 p$	$-p \log_2 p$	H	$-q \log_2 q$	$-\log_2 q$	q
0,1650	2,599462	0,428911	0,646138	0,217227	0,260152	0,8350
0,1675	2,577767	0,431776	0,651954	0,220178	0,264678	0,8325
0,1700	2,556393	0,434587	0,657705	0,223168	0,268817	0,8300
0,1725	2,535332	0,437345	0,663392	0,226047	0,273169	0,8275
0,1750	2,514573	0,440050	0,669016	0,228966	0,277534	0,8250
0,1775	2,494109	0,442704	0,674577	0,231873	0,281912	0,8225
0,1800	2,473931	0,445308	0,680077	0,234769	0,286304	0,8200
0,1825	2,454032	0,337861	0,685516	0,237655	0,290709	0,8175
0,1850	2,434403	0,450365	0,690894	0,240529	0,295128	0,8150
0,1875	2,415037	0,452820	0,696212	0,243393	0,299560	0,8125
0,1900	2,395929	0,455226	0,701471	0,246245	0,304006	0,8100
0,1925	2,377070	0,457586	0,706672	0,249086	0,308466	0,8075
0,1950	2,358454	0,459899	0,711815	0,251916	0,312939	0,8050
0,1975	2,340075	0,462165	0,716900	0,254735	0,317427	0,8025
0,2000	2,321928	0,464386	0,721928	0,257542	0,321928	0,8000
0,2050	2,286304	0,468692	0,731816	0,262124	0,330973	0,7250
0,2100	2,251539	0,472883	0,741483	0,268660	0,340075	0,7900
0,2150	2,217591	0,476782	0,750932	0,274151	0,349235	0,7850
0,2200	2,184425	0,480573	0,760167	0,279594	0,358454	0,7800
0,2250	2,152003	0,484201	0,769193	0,284992	0,367732	0,7750
0,2300	2,120294	0,487668	0,778011	0,290344	0,377070	0,7700
0,2350	2,089267	0,490978	0,786626	0,295648	0,386468	0,7650
0,2400	2,058894	0,494134	0,795040	0,300906	0,395929	0,7600
0,2450	2,029146	0,497141	0,803257	0,306116	0,405451	0,7550
0,2500	2,000000	0,500000	0,811278	0,311278	0,415037	0,7500
0,2550	1,971431	0,502715	0,819107	0,316392	0,424688	0,7450
0,2600	1,943416	0,505288	0,826746	0,321458	0,434403	0,7400
0,2650	1,915936	0,507723	0,834198	0,326475	0,444184	0,7350
0,2700	1,888969	0,510022	0,841465	0,331443	0,454032	0,7300
0,2750	1,862496	0,512187	0,848548	0,336362	0,463947	0,7250
0,2800	1,836501	0,514220	0,855451	0,341230	0,473931	0,7200
0,2850	1,810966	0,516125	0,862175	0,346049	0,483985	0,7150
0,2900	1,785875	0,517904	0,868721	0,350817	0,494109	0,7100
0,2950	1,761213	0,519558	0,875093	0,355535	0,504305	0,7050
0,3000	1,736966	0,521090	0,881291	0,360201	0,514573	0,7000
0,3050	1,713119	0,522501	0,887317	0,364816	0,524915	0,6950
0,3100	1,689660	0,523795	0,893173	0,369379	0,535332	0,6900
0,3150	1,665576	0,524972	0,898861	0,373890	0,545824	0,6850

p	$-\log_2 p$	$-p \log_2 p$	H	$-q \log_2 q$	$-\log_2 q$	q
0,3200	1,643856	0,526034	0,904381	0,378347	0,556393	0,6800
0,3250	1,621488	0,526984	0,909736	0,382752	0,567041	0,6750
0,3300	1,599462	0,527822	0,914926	0,387104	0,577767	0,6700
0,3350	1,577767	0,528552	0,919953	0,391402	0,588574	0,6650
0,3400	1,556393	0,529174	0,924819	0,395645	0,599462	0,6600
0,3450	1,535332	0,529689	0,929523	0,399834	0,610043	0,6550
0,3500	1,514573	0,530101	0,934068	0,403967	0,621488	0,6500
0,3550	1,494109	0,530409	0,938454	0,408046	0,632629	0,6450
0,3600	1,473931	0,530615	0,942683	0,412068	0,643856	0,6400
0,3650	1,454032	0,530722	0,946755	0,416034	0,655157	0,6350
0,3700	1,434403	0,530729	0,950672	0,419943	0,666576	0,6300
0,3750	1,415037	0,530639	0,954434	0,423795	0,678072	0,6250
0,3800	1,395929	0,530453	0,958042	0,427589	0,689660	0,6200
0,3850	1,377070	0,530172	0,961497	0,431323	0,701342	0,6150
0,3900	1,358454	0,529797	0,965800	0,435002	0,713119	0,6100
0,3950	1,340075	0,529330	0,967951	0,438621	0,724993	0,6050
0,4000	1,321928	0,528771	0,970951	0,442179	0,736966	0,6000
0,4050	1,304006	0,528122	0,973800	0,445678	0,749038	0,5950
0,4100	1,286304	0,527385	0,976500	0,449116	0,761213	0,5900
0,4150	1,268817	0,526559	0,979051	0,452493	0,773491	0,5850
0,4200	1,251539	0,525645	0,981454	0,455808	0,785875	0,5800
0,4250	1,234464	0,524648	0,983708	0,459061	0,798366	0,5750
0,4300	1,217591	0,523564	0,985815	0,462251	0,810966	0,5700
0,4350	1,200913	0,522397	0,987775	0,465378	0,823677	0,5650
0,4400	1,184425	0,521147	0,989588	0,468441	0,836501	0,5600
0,4450	1,168123	0,519815	0,991254	0,471439	0,849440	0,5550
0,4500	1,152003	0,518401	0,992774	0,474373	0,862496	0,5500
0,4550	1,136062	0,516908	0,994149	0,477241	0,875672	0,5450
0,4600	1,120294	0,515335	0,995378	0,480043	0,888969	0,5400
0,4650	1,104697	0,513684	0,996462	0,482778	0,902389	0,5350
0,4700	1,089267	0,511956	0,997402	0,485446	0,915936	0,5300
0,4750	1,074001	0,510150	0,998196	0,488046	0,929611	0,5250
0,4800	1,058894	0,508269	0,998846	0,490577	0,943416	0,5200
0,4850	1,043943	0,506313	0,999351	0,493038	0,957356	0,5150
0,4900	1,029156	0,504282	0,999711	0,495430	0,971431	0,5100
0,4950	1,014500	0,502177	0,999928	0,497751	0,985645	0,5050
0,5000	1,000000	0,500000	1,000000	0,500000	1,000000	0,5000

Додаток Д

Таблиця Д.1

Розподіл ймовірностей появи літер російського алфавіту

Літера	p_i	$-\log_2 p_i$	$-p_i \log_2 p_i$	Літера	p_i	$-\log_2 p_i$	$-p_i \log_2 p_i$
Аа	0,062	4,000	0,249	Рр	0,040	4,643	0,185
Бб	0,014	6,158	0,086	Сс	0,045	4,473	0,201
Вв	0,038	4,717	0,179	Тт	0,053	4,237	0,238
Гг	0,013	6,265	0,081	Уу	0,021	5,573	0,117
Дд	0,025	5,321	0,133	Фф	0,002	8,965	0,018
Ее	0,072	3,785	0,273	Хх	0,009	6,795	0,061
Ёё	0,020	5,643	0,113	Цц	0,004	7,965	0,031
Жж	0,007	7,158	0,050	Чч	0,012	6,380	0,076
Зз	0,016	5,965	0,095	Шш	0,006	7,380	0,044
Ии	0,062	4,000	0,249	Щщ	0,003	8,380	0,025
Йй	0,010	6,643	0,066	Ъъ	0,014	6,158	0,086
Кк	0,028	5,158	0,144	Ыы	0,016	5,965	0,095
Лл	0,035	4,836	0,169	Ьь	0,014	6,158	0,086
Мм	0,026	5,265	0,136	Ээ	0,003	8,380	0,025
Нн	0,053	4,237	0,238	Юю	0,006	7,380	0,044
Оо	0,090	3,473	0,313	Яя	0,018	5,795	0,104
Пп	0,023	5,442	0,125	Пробіл	0,175	2,514	0,440

Додаток Е

Таблиця Е.1

Розподіл ймовірностей появи літер українського алфавіту

Літера	p_i	$\log_2 p_i$	$-p_i \log_2 p_i$	Літера	p_i	$\log_2 p_i$	$-p_i \log_2 p_i$
Аа	0,071	3,936	0,270	Нн	0,079	3,643	0,289
Бб	0,008	6,955	0,56	Оо	0,082	3,599	0,296
Вв	0,059	4,083	0,240	Пп	0,030	5,058	0,152
Гг	0,005	7,643	0,038	Рр	0,045	4,473	0,201
Ґґ	0,001	0,965	0,010	Сс	0,031	5,011	0,155
Дд	0,022	5,506	0,121	Тт	0,047	4,411	0,207
Ее	0,051	4,321	0,297	Уу	0,041	4,608	0,189
Єє	0,0007	10,965	0,007	Фф	0,009	9,965	0,061
Жж	0,003	8,380	0,025	Хх	0,010	6,643	0,066
Зз	0,040	4,643	0,186	Цц	0,008	6,955	0,056
Ии	0,081	3,643	0,0294	Чч	0,021	5,543	0,117
Іі	0,072	3,785	0,273	Шш	0,008	6,955	0,056
Її	0,005	7,643	0,038	Щщ	0,005	7,643	0,038
Йй	0,0009	9,965	0,009	Ь	0,0246	5,321	0,890
Кк	0,025	5,321	0,133	Юю	0,007	7,158	0,050
Лл	0,007	7,158	0,050	Яя	0,019	5,717	0,109
Мм	0,037	4,756	0,176	Пробіл	0,172	2,543	0,437

Додаток Ж

Таблиця Ж. 1

Розподіл ймовірностей появи літер англійського алфавіту

Літера	p_i	$\log_2 p_i$	$-p_i \log_2 p_i$	Літера	p_i	$\log_2 p_i$	$-p_i \log_2 p_i$
Aa	0,063	4,000	0,251	Oo	0,065	3,943	0,256
Bb	0,011	6,506	0,072	Pp	0,018	5,795	0,104
Cc	0,023	5,442	0,125	Qq	0,001	9,965	0,010
Dd	0,035	4,836	0,169	Rr	0,054	4,210	0,227
Ee	0,105	3,251	0,341	Ss	0,052	4,265	0,222
Ff	0,023	5,442	0,125	Tt	0,072	3,785	0,273
Gg	0,011	6,506	0,072	Uu	0,023	5,442	0,125
Hh	0,047	4,411	0,207	Vv	0,008	6,955	0,056
Ii	0,055	4,184	0,230	Ww	0,012	6,380	0,077
Jj	0,001	9,965	0,010	Xx	0,001	9,965	0,010
Kk	0,003	8,380	0,025	Yy	0,012	6,380	0,077
Ll	0,029	5,107	0,148	Zz	0,001	9,965	0,010
Mm	0,021	5,573	0,117	Пробіл	0,2	2,321	0,464
Nn	0,059	4,083	0,241				

Додаток К

Загальнонаукові поняття та визначення теорії інформації

Вірогідність інформації - information trustworthiness. Властивість підсистеми контролю і захисту інформації (КЗІ), що характеризує ступінь відповідності (у межах заданої точності) реальних інформаційних одиниць (символів, знаків, записів, повідомлень, документів та ін.) їхньому значенню і полягає в здатності забезпечити відсутність помилок переробки інформації, тобто не допустити зниження цінності інформації при прийнятті управлінських рішень, перекручувань, і ін. через недосконалість організації процесу передачі інформації, недосконалість алгоритмів, ненадійної роботи, збоїв і несправностей СПІ (ЕОМ), помилок операторів.

Гомоморфізм інформації - information homomorphism. Властивість змістовної інформації досить повно відображати дійсність, представлену інформаційними масивами великого обсягу, за допомогою малого числа інформаційних одиниць (символів) на основі відповідних моделей агрегування (типу «багато чого в одному»). Формально-технічна складова кумулятивності інформації.

Ентропія - entropy. 1. Міра розмаїтості (непорядкованості) станів складних систем (ситуацій), що характеризує ймовірність визначеного стану системи серед безлічі можливих її станів. 2. Кількісна міра синтаксичної (структурно-статистичної) і логіко-селективної інформації. 3. Кількісна міра можливості вибору.

Захищеність інформації - protection of information. Властивість функціональної підсистеми контролю і захисту змістовної інформації, що характеризує ступінь захищеності інформаційних масивів, що полягає в здатності не допускати випадкового або цілеспрямованого перекручування чи руйнування, розкриття або модифікації інформаційних масивів в інформаційній базі.

Імитостійкість інформації - information steadfastness to imitation. Властивість підсистеми КЗІ, що характеризує ступінь захищеності інформації від інфільтрації (упровадження) масивів, що імітують авторизовані (зарєєстровані) інформаційних масивів (ІМ), і що полягає в здатності не допустити нав'язування дезінформації і порушення нормального функціонування ергасистеми.

Інформатика - computer science. Область знання, що вивчає процеси формування (рецепції, генерації, виміру), інтерпретації (перетворення, пошуку, представлення, реорганізації) і комунікації (передачі, збереження) інформації, а також процеси розв'язання проблем створення, впроваджен-

ня і використанні інформаційної техніки й інформаційної технології у всіх сферах цілеспрямованої діяльності.

Інформаційна система - informative system. Система, у якій утворюючі елементи і їхні відносини (зв'язки) є інформаційними.

Інформаційне середовище - informative environment. Безліч інформаційних об'єктів (систем) і зв'язків між ними, інформаційні засоби і технології, власне інформація, а також організаційної і юридичної структури.

Інформаційні міри і показники - informative models and indexes. Математичні моделі, призначені для оцінювання (виміру) кількості інформації й ефективності функціонування і застосування ергасистем. Відомі міри кількості інформації структурної (Н. Вінера і К. Шеннона, А. Колмогорова, А. Шилейко і В. Кочнева й ін.) і кількості інформації змістовної (Н. Моїсеєва, Р. Хартлі, Ю. Шрейдера й ін.). Міри використовуються як компоненти показників.

Інформаційний ресурс - informative resource. Сукупність запасів змістовної інформації (інформаційно-змістовний ресурс) і можливостей структурної інформації (інформаційно-структурний ресурс) ергасистеми.

Інформаційний перетворювач - informative processor. Елемент, у якому реалізоване тотожне перетворення параметрів середовища якої-небудь фізико-хімічної природи в параметри впливів чи сигналів установленого виду. Причому значення інформативного параметра вихідного сигналу чи відповідає миттєвому значенню параметрів середовища (датчик), або дискретно змінюється при досягненні значень параметра середовища встановлених рівнів (*сигналізатор*).

Ітерація - iteration. Процедура, заснована на багаторазовому повторенні послідовності операцій, при якому на кожному наступному кроці використовуються результати попередніх, що забезпечує в кінцевому рахунку розв'язання вихідної задачі.

Кількість інформації структурно-статистична - міра зміни розмаїтості (зменшення невизначеності) ситуації, унаслідок того, що стає відомим результат іншої ситуації. У процесі взаємодії (об'єднання) об'єктів відбувається збільшення інформації, яке дорівнює зменшенню статистичної ентропії: $I = -H - H(S, Y) - H(S) - H(Y)$, де: $H(S)$, $H(Y)$ - значення статистичних ентропій систем S , Y до їхньої взаємодії;

$H(S, Y)$ - значення ентропії системи, що виникла в результаті взаємодії складових.

Кількість інформації комбінаторна - логарифм повного числа елементів кінцевої безлічі.

Кількість інформації алгоритмічна - міра зміни складності відновлення числової послідовності s при завданні (визначенні) числової послі-

довності y , що містить частковий опис слова s , рівна мінімальній довжині записаної у вигляді двійкової послідовності z програми, що дозволяє побудувати числову послідовність s , маючи у своєму розпорядженні числову послідовність при цьому $I(s, y) = A(s) - A(s/y)$.

Кількість взаємної інформації структурно-статистичне (що міститься в системі Y щодо системи S) - міра зменшення ступеня невизначеності системи S , що виникає в результаті зняття невизначеності зі зв'язаної з нею системи Y :

$$I(S^n/Y^m) = H(S^n) - H(S^n/Y^m) = \sum_{s^n} \sum_{y^m} P(s^n, y^m) \log [P(s^n, y^m)/P(s^n)P(y^m)]$$

(дискретний випадок);

$$I(S^n, Y^m) = h(S^n) - h(S^n/Y^m) = \int \int_{s^n Y^m} w(s^n, y^m) \log [w(s^n, y^m)/w(s^n)w(y^m)] ds^n dy^m$$

(неперервний випадок).

Кількість інформації семантична (що міститься в інформаційному масиві, повідомленні) - міра зміни індивідуального (системного, загальнолюдського) тезауруса під впливом вхідного інформаційного масиву.

Кількість інформації структурна - міра інформаційної насиченості (інформаційно-структурного ресурсу) об'єкта (системи), тобто кількості і розмаїтості взаємодіючих один з одним неоднорідних елементів об'єкта.

Комунікаційна (зв'язна) інформація - communicate information. Сукупність зведень (знань) про конкретний процес взаємодії в ансамблі матеріальних об'єктів (систем), що міститься в статистичних структурах заданої безлічі інформаційних масивів (повідомлень), що сприймається одержувачем (людиною-оператором й ін.) і використовується ним (з обліком його індивідуального чи загальносистемного тезауруса - накопичених знань) для визначення стану джерела інформації. Різновид змістовної інформації.

Комплекс - complex. Сукупність (обхват) явищ, предметів, властивостей, що складають одне ціле. Відрізняється від системи (об'єднання) відсутністю властивостей цілісності і відносин взаємопідпорядкування між складовими його елементами.

Конфіденційність інформації - information confidence. Статус, наданий інформаційним масивам і погоджений між організацією чи особою, що надають ІМ, і організаціями, що одержують їх. При цьому під таємністю інформації розуміється право організацій і окремих осіб вирішувати, які ІМ вони бажають розділити з іншими, а які - сховати від інших, це поняття вживається стосовно організацій чи окремої людини.

Кумулятивність інформації - information cumulativeness. Властивість змістовної інформації, укладеної в масиві невеликого обсягу, досить повно

відображати дійсність.

Перешкодостійкість інформації - information hindrance-stability. Властивість підсистеми КЗІ, що характеризує ступінь стійкості реальних інформаційних масивів до дії незначних перешкод і полягає в здатності забезпечити відсутність трансформації символів (синтаксична перешкодостійкість на основі контролю перетворень ІМ) і перекручування смислового значення ІМ, що переробляються (семантична перешкодостійкість на основі логічного контролю перетворень, надлишкового кодування ІМ та ін.).

Перешкодозахищеність інформації - information hindrance-defence. Властивість підсистеми КЗІ, що характеризує ступінь живучості інформаційних масивів (ІМ) і полягає в здатності забезпечити виконання хоча б мінімального встановленого обсягу цільових і функціональних задач ергасистеми в умовах зовнішніх руйнуючих впливів .

Повнота інформації - information wholeness. Властивість змістовної інформації забезпечувати раціональне (оптимальне) управління об'єктом.

Сигнал - signal. Сукупність залежної від часу величини - несучого впливу, призначеного для передачі інформації та яке асоціюється з фізичним явищем (подією), і інформацією, що переноситься.

Скритність інформації - information reticence. Властивість підсистеми КЗІ, що характеризує ступінь маскуванню інформації і полягає в здатності протистояти розкриттю змісту інформаційних масивів переданого ІМ і установленню факту передачі ІМ по каналах.

Цінність інформації - information value. Значимість інформації, обумовлена способом динамічного відображення безлічі її якісних властивостей і кількісних характеристик на безліч можливих керуючих рішень, що ведуть до досягнення цілей управління.

Якість інформації - information quality. Сукупність властивостей змістовної інформації, що характеризує ступінь її відповідності потребам (цілям, цінностям) користувачів. Виділяють внутрішню якість (властиву власне інформації і яка зберігається при її переносі в іншу ергасистему) і зовнішню (властиву інформації, що використовується тільки у визначеній ергасистемі,).

Література

1. Батаєв О. П. Теорія електричного зв'язку ("Основи теорії інформації та кодування") / О. П. Батаєв, В. Й. Піддубняк. Навчальний посібник, ч.5. Харків: УкрДАЗТ, 1999. – 355 с.
2. Блейхут Р. Теорія та практика кодів, що контролюють помилки. – М.: Світ, 1986. – 436 с.
3. Дмитрієв В. І. Прикладна теорія інформації. – М.: Вища школа., 1989. – 320 с.
4. Жураковський Ю. П. Передача інформації у ГАП: Навчальний посібник. – К.: "Вища школа", 1991. – 210 с.
5. Зюко А. Г. Теорія передачі сигналів / А. Г. Зюко, Д. Д. Кловський, М. В. Назаров, Л. М. Финк – М.: Связь, 1980. – 288 с.
6. Ігнатов В. А. Теорія інформації та передачі сигналів: Підручник для вузів. – М.: Радіо та зв'язок, 1991. – 264 с.
7. Касами Т. і ін. Теорія кодування. – М.: Світ, 1978. – 520 с.
8. Кловський Д. Д. Теорія передачі сигналів в задачах / Д. Д. Кловський, В. А. Шилкін – М.: Связь, 1978. – 252 с.
9. Кловський Д. Д. Теорія електричного зв'язку. Збірник вправ / Д. Д. Кловський, В. А. Шилкін: Навчальний посібник для вузів. – М.: Радіо та зв'язок, 1990. – 280 с.
10. Ключко В. І. Методи та засоби захисту інформації від помилок у АСУ.– МО СРСР, 1980. – 256 с.
11. Краснобаєв В. А.. Теорія інформації. / В. А. Краснобаєв, І. О. Фурман: Конспект лекцій. – Харків. ХДТУСГ, 2004. – 94 с.
12. Краснобаєв В. А. та ін. Задачі кодування у АСУ. – Харків.: МО СРСР, 1990. – 156 с.
13. Краснопоєсовський А. С. Теорія інформації та кодування. Харків, ХАІ, 1976. – 80 с.
14. Кузьмін І. В. Основи теорії інформації і кодування / І. В. Кузьмін, В. А. Кедрус – К.: Вища школа, 1986. – 238 с.
15. Леонтьєв В. К. Теорія кодування. – М.: Зв'язок, 1977. – 120 с.
16. Никитин Г. І. Помехоустойчивые циклические коды: Учеб. пособие. – Санкт-Петербург. – СПбГУАП, 2003. – 33 с.
17. Панфілов І. П., Підвищення перешкодостійкості каналів зв'язку АСУТП. / І. П. Панфілов, М. Т. Козаченко – К.: Техніка, 1991. – 160 с.
18. Питерсон У. Коды, исправляющие ошибки / У. Питерсон, Э. Уэлдон; пер. с англ. – М.: Мир, 1976. – 600 с.
19. Поставний В. І. Теорія передачі сигналів. – М.: МО СРСР. – 1985, ПВВКИУ РВ. – 264 с.
20. Рад Б. Я. Теорія інформації. – Л.: Изд. БРЕШУ, 1978. – 230 с.

21. Скляров В. С. Математические модели информационных систем. – ХВВКИУРВ, 1988. – 480 с.
22. Солодов А. В. Теорія інформації та її застосування до задач автоматичного керування і контролю. – М.: Наука, 1967. – 240 с.
23. Сорока Л. С. Теорія інформації та кодування / Л. С. Сорока, О. В. Северінов, О. С. Жученко: Навч. посібник. – Х.: ХУПС, 2007. – 186 с.
24. Стратонович Р. Л. Теорія інформації. – М.: Сов. радіо, 1975. – 424 с.
25. Темників Ф. Е., Афонін В. А., Дмитриєв В. И. Теоретичні основи інформаційної техніки. – М.: Енергія, 171. – 424 с.
26. Хартлі Р. Передача інформації // Теорія інформації та її додатки. – М.: Наука, 1959. – 350 с.
27. Хеммінг Р. Теорія кодування і теорія інформації. – М.: Радіо і зв'язок, 1983. – 460 с.
28. Цимбал В. П. Основи теорії інформації та кодування. Київ, “Вища школа”, 1973. – 234 с.
29. Черенга В.С. Розрахунок та проектування технічних засобів обміну та передачі інформації: / В. С. Черенга, В. А. Василенко, В. Н. Бондарєв. Навчальний посібник для вузів. – М.: Вища школа, 1990. – 120 с.
30. Шварцман В. О. Теорія передачі дискретної інформації / В. О. Шварцман, Г. А. Ємельянов. – М.: Зв'язок, 1979. – 230 с.
31. Шульгин В. И. Основы теории передачи информации. Ч. 2. Помехоустойчивое кодирование: Учеб. пособие. – Харьков: Нац. аэрокосм. ун-т «ХАИ », 2003. – 87 с.

НАВЧАЛЬНЕ ВИДАННЯ

*Барсов Валерій Ігорович
Краснобаєв Віктор Анатолійович
Барсова Зоя Валеріївна
Тиртишніков Олексій Іванович,
Авдєєв Іван Віталійович*

Теорія інформації та кодування

підручник

Відповідальний за випуск – Барсов В.І.
Комп'ютерна верстка та технічне редагування – Барсова З. В.

Друк RISO

Ум. друк. арк. 18,6

Тираж 30 прим. Замовлення № 932 від 8.11.2011 року

Поліграфічний центр
Полтавського національного технічного університету
Імені Юрія Кондратюка
36011, Полтава, Першотравневий проспект,24

Свідоцтво про внесення суб'єкта видавничої справи до Державного
реєстру видавців, виготовників і розповсюджувачів видавничої літератури

Серія ДК №3130 від 06.03.2008 року