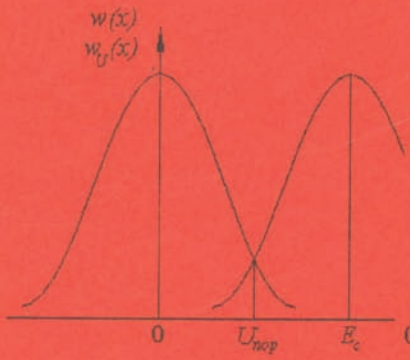
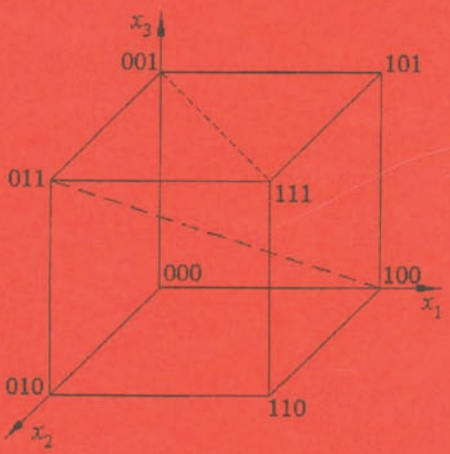
А.Я. Кулик, С.Г. Кривогубченко

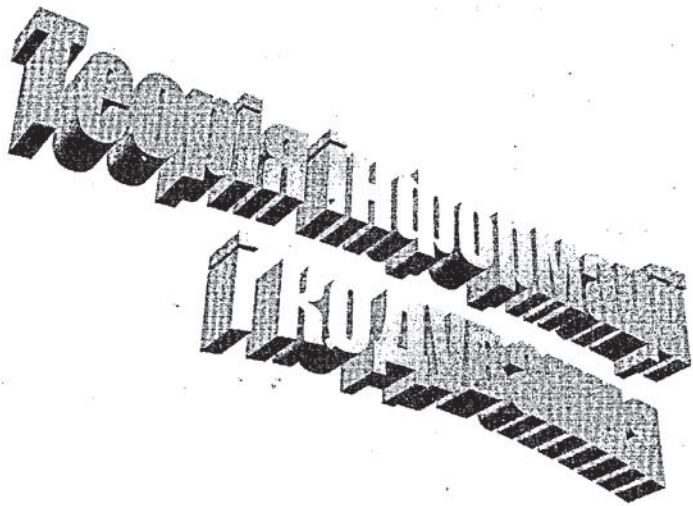
Теорія інформації і кодування





Вінниця ВНТУ 2008

Міністерство освіти і науки України
Вінницький національний технічний університет



Затверджено Вченою радою Вінницького національного технічного університету як навчальний посібник для студентів напряму підготовки „Системна інженерія" спеціальності „Системи управління і автоматики". Протокол № 8 від "24" січня 2008 р.

Вінниця ВНТУ 2008

УДК 621.3

К 90

Рецензенти:

О.В. Поджаренко, доктор технічних наук, професор

І.В. Гребеннік, доктор технічних наук, професор

В.М. Дубовой, доктор технічних наук, професор

Рекомендовано до видання Вченою радою Вінницького національного технічного університету Міністерства освіти і науки України

К 90 **Кулик А.Я., Кривогубченко С.Г., Теорія інформації і кодування** / Навчальний посібник. – Вінниця: ВНТУ, 2008. - 145 с.

Посібник присвячений розгляду теорії інформації і кодування. Призначений для однойменного курсу та аналогічних вищих навчальних закладів технічного напрямку.

УДК 621.3

Зміст

Вступ

Однією з найважливіших науково-технічних проблем на сучасному етапі є створення комп'ютерних систем управління різного функціонального призначення. Процеси контролю та управління нерозривно пов'язані з інтенсивним обміном інформацією між окремими складовими частинами систем, причому обсяги інформації, що підлягають передаванню, та швидкості обміну даними постійно зростають. Все більші вимоги висуваються до вірогідності передавання інформації. Аналогічні проблеми стоять і під час побудови та експлуатації як розподілених інформаційно-вимірювальних систем, так і комп'ютерних мереж. З урахуванням різноманітності використовуваних ліній та каналів зв'язку, проблема передавання інформації стає достатньо складною і потребує спеціальних заходів, що вирішують весь комплекс задач.

Необхідність детального аналізу системи або мережі вимагає визначення фізичних та статистичних параметрів каналів зв'язку, побудови їх математичної моделі, а також узгодження із джерелом передавання. З цим нерозривно пов'язані задачі побудови оптимальних кодів для передавання інформації за відсутності шуму, використання ефективних кодів для забезпечення необхідної завадозахищеності під час передавання інформації реальними каналами з шумом тощо.

Пропонований навчальний посібник охоплює коло питань, пов'язаних з теоретичними основами передавання інформації в комп'ютерних системах та мережах, і призначений для підготовки фахівців напряму 6.050201 „Системна інженерія" спеціальності „Системи управління і автоматики".

Розділ 1 написаний А.Я. Куликом, розділ 2 – С.Г. Кривогубченком, розділ 3 написаний у співавторстві – С.Г. Кривогубченком висвітлені питання щодо систем числення, кодування без визначення помилок та згорткового кодування, а Куликом А.Я. – всі інші.

1. Перетворення інформації в комп'ютерних системах та мережах

1.1 Комп'ютерні системи та мережі

Терміни „комп'ютерні системи" та „комп'ютерні мережі" сформувались останнім часом і стандартами не регламентовані. Вони підкреслюють спорідненість (за певними ознаками) структур процесорних засобів, призначених для збирання та оброблювання інформації. Так, всі сучасні системи будуються з використанням мікропроцесорних засобів, а це, в свою чергу, передбачає використання типових модулів, що призначаються для виконання певних чітко окреслених функцій. Вони можуть входити до складу комп'ютера або розроблятись для використання у мікропроцесорних контролерах. Їх перелік, в основному, є незмінним і передбачає оброблювання уніфікованих сигналів за допомогою стандартних модулів (АЦП або таймер в залежності від інформативного параметра), зберігання даних у модулі пам'яті тощо, не кажучи вже про стандартний набір модулів, які забезпечують працездатність системного блока персонального комп'ютера.

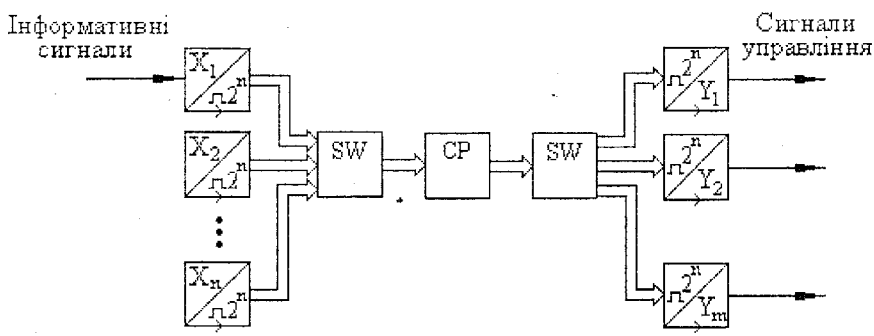


Рисунок 1.1 – Узагальнена структура комп'ютерної системи

Відмінність структур комп'ютерних систем визначається їх функціональним призначенням. Інформаційно-вимірювальні системи будуються для збирання та оброблювання інформації, тому їх структура обмежується модулем визначення параметрів сигналів і процесорним блоком з

пам'яттю для зберігання та оброблювання даних. Інформаційно-консультативні системи будуються на базі процесорного блока з розвиненими периферійними пристроями для введення запиту, його оброблювання та виведення необхідної інформації. Автоматизовані системи управління крім модулів, необхідних для побудови ІВС, вимагають введення блоків формування сигналів управління (підсилювачі потужності, ЦАП, таймер тощо) в залежності від виконавчих пристроїв. Під час детального розроблювання конкретної системи можуть здійснюватися певні варіювання структур (наприклад, вводитися один чи декілька зворотних зв'язків), але перелік уніфікованих апаратних модулів лишається практично незмінним. Основне навантаження під час побудови системи припадає на розроблення алгоритмічного і програмного забезпечення.

Для розподілених систем прийнятне все висловлене вище, але особливого значення набуває процес передавання інформації. Суто інформаційні системи призначаються для циркулярного виведення інформації і передбачають використання симплексного режиму (передавання інформації лише в один бік, як у системах телебачення чи радіомовлення). Адресне опитування давачів або каналів у розподілених інформаційно-вимірювальних системах та автоматизованих системах управління вимагає використання напівдуплексного режиму (передавання інформації в обидва боки, але по черзі). Комп'ютерні мережі потребують задіяння повнодуплексного режиму (одночасне передавання інформації в обидва боки). Таким чином, в узагальненому вигляді з урахуванням певних припущень з точки зору передавання інформації різниця між розподіленими системами і комп'ютерними мережами не така вже й суттєва.

В усіх випадках реалізується адресний вибір об'єкта (передавача чи приймача), в усіх випадках використовується уніфікований набір апаратних модулів, в усіх випадках метою обміну інформацією є її вірогідне передавання з максимально ефективним використанням каналу зв'язку. Оскільки передавання даних каналом зв'язку найбільш ефективно здійснюється в послідовному форматі, то необхідні перетворювачі паралельного коду на послідовний та навпаки, а також пристрої узгодження передавача та приймача з каналом зв'язку.

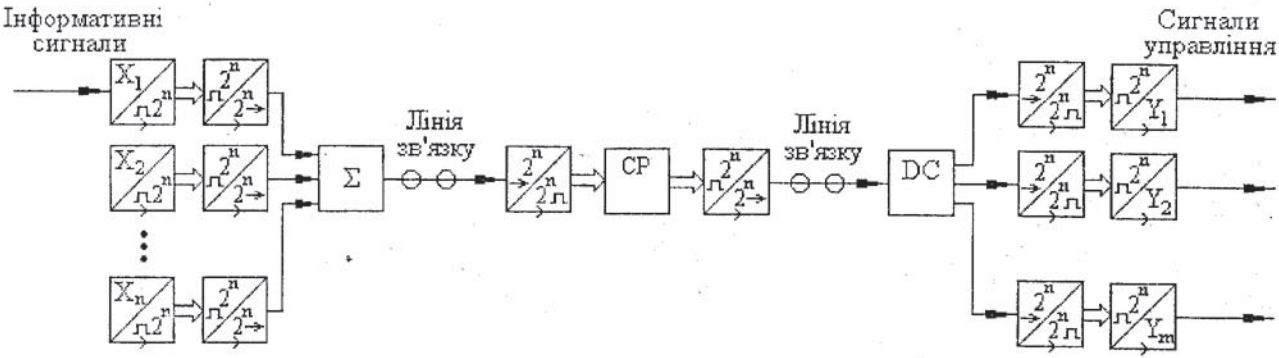


Рисунок 1.2 – Узагальнена структура розподіленої комп'ютерної системи

Канал зв'язку – сукупність технічних засобів та тракту для передавання повідомлення на відстань незалежно від інших каналів в лінії зв'язку.

Лінія зв'язку – сукупність кінцевої апаратури та фізичного середовища, якими здійснюється передавання сигналів від передавача до приймача.

Для максимально ефективного використання кожна лінія зв'язку може бути використана для утворення багатьох каналів з незалежним передаванням повідомлень і, крім засобів обміну даними, вміщує також середовище передавання (дроти, кабелі, світловоди тощо).

При розгляді розподілених інформаційних систем необхідно мати на увазі, що з точки зору користувача режим передавання є симплексним (як у прикладі телевізійної системи), але з точки зору розробника необхідно забезпечувати зворотний зв'язок і отримувати певну інформацію про якість зв'язку, умови передавання, ну, а як мінімум, – чи доходять взагалі передавані дані до пункту призначення. Для цього необхідно реалізовувати напівдуплексний або дуплексний режим в залежності від функціонального призначення створюваної системи, її швидкодії та особливостей побудови. Структура, наведена на рис. 1.2, також піддається варіюванню в залежності від перерахованих умов. Якщо вони дозволяють, то можна суттєво скоротити апаратні витрати, подаючи сигнали зі вхідних перетворювачів безпосередньо на ключ і поставивши після нього один перетворювач паралельного коду на послідовний. Аналогічно змінюється і блок формування сигналів управління.

Література

1. Советов Б.Я. Теория информации (теоретические основы передачи информации в АСУ) / Учебн. пос. – Л.: Изд-во Ленингр. ун-та, 1977. – С. 5 – 34.
2. Васюра А.С., Кривогубченко С.Г., Кулик А.Я., Компанець М.М., Худолій О.І. Техніка передавання аналогової та дискретної інформації / Навч. посібн. – Вінниця: ВДТУ, 1998. – С. 6 – 10.
3. Квєтний Р.Н., Компанець М.М., Кривогубченко С.Г., Кулик А.Я. Основи техніки передавання інформації / Підручник. – Вінниця: Універсум-Вінниця, 2002. – С. 10 – 14.

1.2 Інформація. Її властивості та етапи перетворення в комп'ютерних системах

Існує дуже багато означень терміна „інформація", серед яких можна виділити пояснювальні, термодинамічні, концептуальні, філософські, машинні, енциклопедичні, юридичні тощо. Але більшість з них не віддзеркалює її основних властивостей та призначення. Найбільш прийнятним для комп'ютерних систем є класичне означення, наведене нижче.

Інформація – змістовні відомості (дані), що втілюються в повідомленні, попередньо невідомі людині чи машині, яка це повідомлення отримує.

Це означення чітко характеризує основні властивості інформації, без яких інформація перетворюється на дані, що обробляються системою або зберігаються нею. ***Змістовність*** даних передбачає, що вони формуються, обробляються, передаються, зберігаються тощо з певною метою, яка визначається функціональним призначенням системи і побажанням людини, яка з цією системою працює. Є маса даних, які споживачу просто непотрібні, тому вони не є інформацією. ***Втілення*** інформації у повідомленні визначає форми її існування – статичну (у вигляді записів на папері, стрічці, диску, фотопапері тощо) та динамічну (під час її передавання). Потрібно зауважити, що процес фізичного перевезення чи пересування носія інформації (листа, магнітної стрічки, диска, касети тощо) не відносять до динамічної форми існування інформації. Якщо дані передаються каналом зв'язку, то у кожній точці каналу під час передавання процес змінюється в часі і так само змінюється вплив зовнішніх факторів на сигнали, що несуть в собі інформацію. При фізичному перевезенні цього не відбувається, хоча дані, що зафіксовані на носії, теж підпадають під вплив зовнішніх факторів і можуть руйнуватися з часом. Таким чином, статичною цю форму можна назвати відносно, більш точно – квазистатичною. Інформація, що зберігається на носії, може зчитуватись, передаватись, знов записуватись, тобто вона може багаторазово переходити з однієї форми іс-

нування в іншу. ***Новизна*** даних для споживача теж є необхідною умовою, оскільки відомі йому дані інформацією не є.

Перелік операцій, які забезпечують перетворення інформації в комп'ютерній системі, визначається функціональним призначенням цієї системи. В загальному вигляді можна виділити певні етапи. Першим з них є ***підготовка інформації***. В залежності від конкретної системи вона може здійснюватися автоматично або автоматизовано. Так, для інформаційно-вимірювальних систем або автоматизованих систем контролю етап підготовки полягає у перетворенні сигналів давачів на нормалізовані та у їх оцифровуванні, що може бути здійснено в автоматичному режимі без участі людини. Інформаційно-консультативні системи вимагають введення запиту та його перетворення за допомогою доступного процесору алфавіту. Здебільшого це здійснюється за участі людини, тому перша фаза реалізується вручну, а друга – автоматично. Метою цього етапу є введення інформації до системи, а також її підготовка до подальшого перетворення та оброблювання.

Наступним етапом є ***збирання*** інформації, яке в будь-якому випадку пов'язано з ***передаванням***, оскільки здійснюється з територіально рознесених об'єктів, контролерів, терміналів, постів тощо. Ці два етапи нерозривно пов'язані ще й тому, що їх метою є доставка первинних даних до центрального процесора для подальшого оброблювання. Етап забезпечується кодуванням даних, їх втіленням у відповідні сигнали та передаванням вибраними каналами зв'язку.

Кодування – встановлення відповідності між елементом даних і сукупністю символів, яка називається кодовою комбінацією.

Кодування даних може здійснюватися з метою їх захисту від завад, криптографічного закриття, стиснення або вирішення комплексу перерахованих задач.

Під час передавання формуються спеціальні сигнали, тому на приймальному боці необхідно використовувати відповідні технічні засоби, які забезпечують виявлення сигналів за певними алгоритмами та їх декодування для перетворення у необхідний для центрального процесора вигляд.

Оброблювання інформації здійснюється центральним процесором у відповідності з функціональним призначенням системи і розробленими алгоритмами. Під час оброблювання та після нього обов'язковим етапом є ***зберігання***, а у випадку необхідності – ***архівація*** даних. Доцільність останньої визначається необхідним терміном зберігання інформації. При цьому виникають задачі класифікації та систематизації наявної інформації, вирішення яких вимагає формування одного чи декількох банків даних, що, в свою чергу, передбачає ефективну організацію та пошук інформаційних масивів для збереження необхідної швидкодії комп'ютерної системи.

Системи автоматизованого управління різних типів передбачають формування відповідних сигналів для корегування параметрів системи чи об'єктів. Практично ця задача вирішується на етапі підготовки даних з тією різницею, що її реалізує центральний процесор. Він забезпечує ***виведення*** інформації з використанням операцій кодування та передавання. Виведення інформації може здійснюватися на виконавчі агрегати, на засоби відображення або комплексно. При цьому в кожному випадку дані повинні бути подані у відповідному форматі, що знов-таки забезпечується центральним процесором. Кінцеве обладнання являє собою необхідні цифрові або цифро-аналогові перетворювачі для формування нормованих сигналів, які забезпечують необхідні функції системи: регулювання, управління, контроль, індикацію тощо.

Незалежно від етапу перетворення оброблюваним даним властиві певні характеристики, які визначаються призначенням та особливостями функціонування комп'ютерної системи. Мета перетворення визначає відповідний етап і всі характеристики, що йому притаманні.

Формат визначається середовищем передавання, фізичною природою сигналів тощо. В свою чергу, це вимагає певного апаратного і програмного забезпечення, спроможного працювати з наперед визначеним оптимальним форматом даних.

Надлишковість може бути природною або штучною. Природна пов'язана з періодичністю введення даних, лінгвістичною структурою мови тощо. Штучна надлишковість вводиться для забезпечення захисту від впливу завад і дозволяє зберегти вірогідність інформації під час передавання, хоча суттєво знижує швидкодію або енергетичні показники систе-

ми. Таким чином, задача зводиться до вибору балансу між вірогідністю передавання та ефективністю використання каналу зв'язку. Природну надлишковість варто і необхідно зменшувати, а штучну – вводити обґрунтовано, забезпечуючи оптимальне вирішення поставленої задачі.

Час перетворення є однією з основних характеристик функціонування комплексу технічних засобів. Часові затримки, визначені ним, викликають старіння інформації і зниження її цінності. Особливо це виявляється у випадках необхідності забезпечення оперативного управління та регулювання. Таким чином, і в цьому випадку необхідно шукати баланс між ефективністю процесу перетворення і часом затримки.

Вірогідність – одна з основних характеристик інформації на будь-якому етапі її перетворення. Вона визначає ступінь довіри до неї під час прийняття рішення, а виходячи з цього – і ступінь ефективного функціонування комп'ютерної системи в цілому.

Таким чином, наявність декількох етапів перетворення інформації ускладнює комп'ютерну систему, але дозволяє підвищити її ефективність з урахуванням того, що системою в цілому і на кожному етапі інформація поставляється своєчасно і вірогідно.

Література

1. Советов Б.Я. Теория информации (теоретические основы передачи информации в АСУ) / Учебн. пос. – Л.: Изд-во Ленингр. ун-та, 1977. – С. 5 – 34.
2. Васюра А.С., Кривогубченко С.Г., Кулик А.Я., Компанець М.М., Худолій О.І. Техніка передавання аналогової та дискретної інформації / Навч. посібн. – Вінниця: ВДТУ, 1998. – С. 23.
3. Квєтний Р.Н., Компанець М.М., Кривогубченко С.Г., Кулик А.Я. Основи техніки передавання інформації / Підручник. – Вінниця: Універсум-Вінниця, 2002. – С. 55.

1.3 Інформаційні потоки в комп'ютерних системах і мережах

Розглянуті вище узагальнені засади побудови комп'ютерних систем та мереж показують мету, з якою формується локальна або ієрархічна ме-

режа обміну інформацією, що є зовнішньою відносно джерел та користувачів інформації. Необхідними умовами її побудови та експлуатації є:

- підтримання заданих необхідних імовірнісно-часових характеристик доведення інформації до користувача;
- обслуговування інформаційних потоків у вузлах перетинання, об'єднання або розгалуження інформаційних потоків;
- забезпечення необхідних параметрів сигналів, якими здійснюється перенесення інформації у каналах зв'язку.

Виходячи з вищевикладеного локальну або ієрархічну комп'ютерну мережу в загальноприйнятому розумінні можна розглядати як автоматизовану систему управління інформаційними потоками, для якої прийнятні класичні моделі і методи аналізу та синтезу АСУ. При цьому в комп'ютерній системі або мережі виникають зовнішні впливи збурення за рахунок завад, які проявляються у вигляді спотворення складових інформаційних потоків або відмов при низькій імовірності прийняття інформації. Ці впливи мають випадковий характер і можуть описуватись певними імовірнісними закономірностями.

В часовому аспекті інформація, що циркулює в системі або в мережі, являє собою інформаційний потік, що визначається моментами появи окремих повідомлень. Часто цей потік має випадковий характер і описується статистичними моделями. В залежності від розглядуваного режиму (статичний або динамічний) ці моделі повинні пов'язувати між собою як імовірнісні, так і часові параметри або характеристики.

Для повного аналізу та синтезу системи або мережі в цілому необхідно враховувати як імовірність безпомилкового передавання інформації каналами зв'язку (захист від впливу завад), так і ймовірнісні оцінки безпомилкової роботи програмного та апаратного забезпечення (їх надійність). Вирішення цих задач можна суттєво спростити, якщо використовувати уніфіковані технічні засоби, характеристики яких стандартизовані.

Аналізуючи структуру багатоканальної комп'ютерної системи або мережі можна виділити в ній вузли, які забезпечують введення, видачу та комутацію інформації. Ці вузли пов'язуються між собою каналами зв'язку. Таким чином можна побудувати графову модель системи або мережі. Управління потоками можна здійснювати методами комутації потоків, каналів або комбінованим.

Метод комутації каналів призначений для встановлення фізичного з'єднання між джерелом і користувачем інформації, після чого побудований канал використовується лише для обміну між відповідними передавачем та приймачем. При бажанні використати цей канал іншими джерелами необхідно очікувати завершення обміну (або хоча б перерви) для можливості перекомутації каналу. Класична теорія автоматичного управління передбачає наявність відмов в обслуговуванні запитів. В даному випадку відмова означає затримку інформації в часі, що може призвести до втрати її цінності, оскільки старіння інформації практично визначає неможливість її використання для забезпечення управління.

Більш перспективним, хоча і більш складним, є випадок, коли немає жорсткого закріплення каналу зв'язку за приймачем та передавачем, а передавання здійснюється ланцюгом від одного вузла до іншого шляхом комутації повідомлень або їх пакетів. При цьому кожному з них присвоюється адреса, яка визначає маршрут проходження повідомлення. Зайнятість каналу зв'язку вимагає забезпечення зберігання повідомлення, яке ставиться в чергу і передається при вивільненні каналу.

Метод комутації пакетів є перспективним для реальних сучасних комп'ютерних мереж різного функціонального призначення, розгалуженості та рівня. В першу чергу це пояснюється тим, що в кожній з них використовуються лінії зв'язку різної природи – радіоканали, оптоволокно, дротові кабелі типу „витої пари", телефонні модеми тощо з різними статичними та динамічними характеристиками. Це вимагає зміни швидкості передавання під час переходу з вузла на вузол, зміни співвідношення сигнал/шум за рахунок різного впливу завад на різні види ліній та каналів зв'язку, а часто і зміни умов кодування, якщо інші заходи виявляються недієвими. В проміжних вузлах (центрах) комутації необхідно забезпечувати зберігання повідомлень, що надійшли низькошвидкісними каналами; розбирання пакетів на повідомлення для їх переадресування різними каналами; сортування повідомлень; збирання повідомлень у пакети, які мають однакові адреси і функціональне призначення; видачу скомпонованих пакетів каналами, тобто забезпечувати оптимальне управління інформаційними потоками. Метод комутації повідомлень дозволяє також забезпечувати пріоритетне обслуговування окремих повідомлень, які є особливо важливими для виконання функцій системи або мережі, в зв'язку з чим менш

важливі повідомлення затримуються, а пріоритетні обробляються поза чергою. Легко побачити, що реалізація вказаного методу потребує не лише значно більшого обсягу обладнання для кожного вузла, але і якісно іншої його побудови з необхідністю інтелектуалізації. В окремих випадках можливе використання комбінації методів.

Узагальнений граф комп'ютерної мережі з комутацією пакетів наведений на рис. 1.3. Інформація повинна надходити від джерела повідомлення до користувача крізь вузли комутації (в даному випадку повідомлень). Надходження інформації від джерела здійснюється відповідно до її появи і зазвичай не синхронізовано із управлінням вузлів комутації.

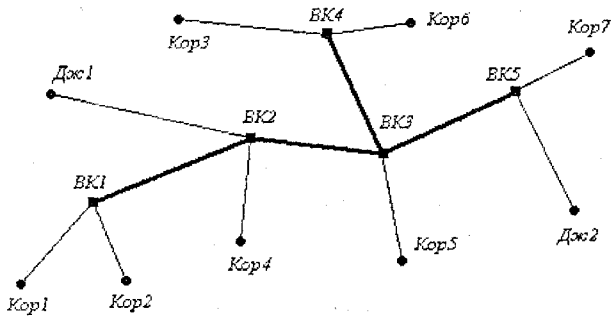


Рисунок 1.3 – Узагальнений граф комп'ютерної мережі з комутацією пакетів:
Дж – джерело повідомлень,
Кор – користувач повідомлення,
ВК – вузол комутації

Крім того, часто необхідно здійснювати циклічне опитування готовності джерел та користувачів. При цьому вимагають вирішення задачі зменшення часу опитування, розбиття джерел користувачів на групи з метою оптимізації імовірнісно-часових характеристик процесу опитування і обміну інформацією в цілому. Повідомлення у вузлах комутації зберігаються у вигляді блоків і за певним алгоритмом, в залежності від засад побудови комп'ютерної мережі, передаються високошвидкісним каналом, який з'єднує між собою вузли. Їх кількість визначається функціональним призначенням системи чи мережі, її територіальним розташуванням, розгалуженістю функціональних підрозділів, ієрархією підпорядкування рівнів, вимогами безпеки тощо, тому в окремих випадках інформація може проходити крізь декілька вузлів до моменту її надходження до користува-

ча. Для зв'язку користувачів та джерел з комутаційними вузлами зазвичай використовуються низькошвидкісні канали, побудовані на виділених або ущільнених лініях зв'язку.

Для забезпечення заданої якості функціонування системи або мережі доводиться здійснювати оптимізацію за декількома окремими або одним універсальним критерієм, які докладно розглянуті у відповідній літературі. При цьому обов'язково необхідно враховувати повний час оброблювання інформації, який вміщує час опитування готовності, час передавання, час оброблювання та інші складові, в тому числі і час затримки, пов'язаний із збиранням та розбиранням пакетів повідомлень, оскільки він може бути досить значним для кожного з вузлів.

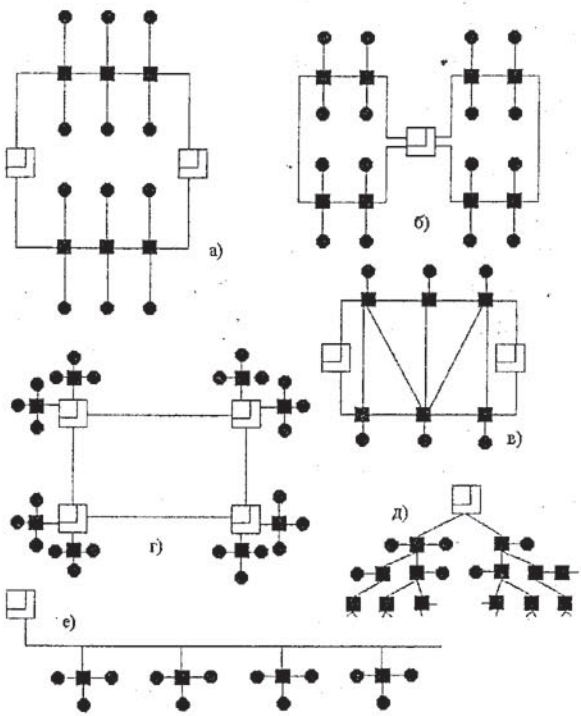


Рисунок 1.4 – Види структур систем та мереж:
а) – петльова (коміркова); б) – двопетльова;
в) – розподілена; г) – радіально-петльова;
д) – ієрархічна (деревоподібна); е) – лінійна

Топологія комп'ютерної системи або мережі визначається структурою використовуваних ліній зв'язку. Варіанти структур наведені на рис. 1.4. Петльова або коміркова структура мережі передбачає наявність одного каналу зв'язку, який проходить замкненим колом крізь всі вузли та зв'язкові процесори, які підключені до деяких вузлів чи центрів комутації. Перевагою цієї мережі є те, що пошкодження каналу не призводить до руйнування мережі. Деколи

формують мережу з дво- або багатопетльовою структурою. Радіально-петльова структура являє собою комбінацію радіальної та петльової структур. Мережі з розподіленою структурою вміщують центри комутації, які з'єднуються не менше як з двома іншими центрами. Ця мережа є найбільш мобільною завдяки багатьом варіантам маршрутів зв'язку і вчасній реакції на пошкодження окремих частин мережі.

Ієрархічна або деревоподібна структура найбільш часто зустрічається в реальних умовах. Лінійна структура є найбільш простою серед усіх, але має невелику надійність. Джерела інформації в системі чи мережі створюють інформаційні потоки, управління якими здійснюють один або декілька зв'язкових процесорів.

В залежності від типу та структури технічних засобів можливі декілька моделей інформаційних потоків. Найчастіше зустрічається регулярний потік, що характеризується частотою появи повідомлень в часі. Більш загальним є випадковий потік, який описується пуасонівською моделлю, з якої неважко визначити імовірність виникнення заданої кількості повідомлень за фіксований проміжок часу. Але всі моделі вимагають експериментальних досліджень і оцінки статистичних властивостей системи чи мережі, після чого розрахунок характеристик можна здійснити аналітично або методом моделювання.

Література

1. Советов Б.Я. Теория информации (теоретические основы передачи информации в АСУ) / Учебн. пос. – Л.: Изд-во Ленингр. ун-та, 1977. – С. 5 – 34.
2. Васюра А.С., Кривогубченко С.Г., Кулик А.Я., Компанець М.М., Возняк О.М. Мікропроцесорні засоби передавання інформації / Навч. посібн. – Вінниця: ВДТУ, 1998. – С. 31 – 35.
3. Квєтний Р.Н., Компанець М.М., Кривогубченко С.Г., Кулик А.Я. Основи техніки передавання інформації / Підручник. – Вінниця: Універсум-Вінниця, 2002. – С. 246 – 249.

1.4 Перетворення неперервних сигналів на дискретні

Передавання повідомлень здійснюється неперервними та дискретними сигналами. Неперервні сигнали являють собою неперервні функції часу з безмежною кількістю проміжних точок.

Дискретне повідомлення має кінцеву кількість значень. Передавання та зберігання дискретних повідомлень математично відповідає передаванню та зберіганню кінцевого набору символів і може бути зведене до передавання та зберігання послідовності чисел.

Пізніше буде показано, що для передавання неперервних повідомлень без похибки потрібен канал зв'язку з необмеженою пропускною здатністю. На практиці завжди передавання повідомлень здійснюється з обмеженими спектром частот та точністю, оскільки всі канали мають обмежену пропускну здатність.

Якщо неперервне повідомлення має обмежений спектр частот, то воно завжди може бути передано своїми значеннями в окремі моменти часу, тобто перетворене на дискретне за часом, що складається з послідовного у часі ряду значень.

Можливість такої заміни вперше була обгрунтована в 1933 році В.А. Котельніковим та сформульована у вигляді теореми: „Якщо функція $x(t)$ не вміщує в собі частот, вищих за f_{max}, то вона повністю визначається своїми миттєвими значеннями у моменти часу, що лежать у віддаленні один від одного на $1/2f_{max}$". В деякій літературі її називають ще ***теоремою відрахунків.***

Нехай сигнал, що описується неперервною функцією часу $x(t)$, має обмежений спектр, є кусково-неперервним і має обмежену кількість екстремумів (задовольняє умови Діріхле), тобто перетворення Фур'є:

$$S(j\omega) = \int_{-\infty}^{\infty} x(t) \cdot e^{-j\omega t} dt, \qquad (1.1)$$

задовольняє умову:

$$S(j\omega) = 0, \text{ якщо } |\omega| > \omega_{max}.$$

При визначенні сигналу інтегралом Фур'є інтегрування можна окреслити значеннями $-\omega_{max}$ та ω_{max}, тобто:

$$x(t) = \frac{1}{2\pi} \int_{-\omega_{max}}^{\omega_{max}} S(j\omega) \cdot e^{j\omega t} d\omega \ . \qquad (1.2)$$

Розглянувши спектральну функцію (1.1) як функцію частоти, період якої дорівнює $2\omega_{max}$, можна розкласти цю функцію в ряд Фур'є на інтервалі $[-\omega_{max}, \omega_{max}]$:

$$S(j\omega) = \sum_{k=-\infty}^{\infty} C_k \cdot e^{\frac{jk\omega}{\omega_{max}}} \ , \qquad (1.3)$$

де коефіцієнти розкладу:

$$C_k = \frac{1}{2\omega_m} \int_{-\infty}^{\infty} S(j\omega) \cdot e^{-\frac{jk\omega}{\omega_m}} d\omega \ . \qquad (1.4)$$

Порівнюючи вирази (1.4) та (1.2), можна помітити, що вони збігаються до постійного множника $\Delta t = \pi / \omega_{max}$, якщо прийняти $t = -k\Delta t$. Тоді:

$$C_k = \frac{\pi}{\omega_{max}} x(-k\Delta t) \ . \qquad (1.5)$$

Підставивши (1.5) в (1.3), можна одержати:

$$S(j\omega) = \sum_{k=-\infty}^{\infty} \frac{\pi}{\omega_{max}} \cdot x(-k\Delta t) \cdot e^{\frac{jk\omega}{\omega_{max}}} \ . \qquad (1.6)$$

Підставивши тепер (1.6) у (1.2):

$$x(t) = \frac{1}{2\pi} \int_{-\omega_{max}}^{\omega_{max}} e^{j\omega t} \sum_{k=-\infty}^{\infty} \frac{\pi}{\omega_{max}} \cdot x(-k\Delta t) \cdot e^{\frac{jk\omega}{\omega_{max}}} d\omega = \frac{1}{2\omega_{max}} \sum_{k=-\infty}^{\infty} x(k\Delta t) \int_{-\omega_{max}}^{\omega_{max}} e^{j\omega(t-k\Delta t)} d\omega \ . \qquad (1.7)$$

Зміна знака k може бути здійснена тому, що додавання функції здійснюється за всіма негативними і позитивними значеннями k. Після обчислення інтегралу:

$$\int_{-\infty}^{\infty} e^{j\omega(t-k\Delta t)} d\omega = \frac{2\sin\omega(t-k\Delta t)}{t-k\Delta t} \tag{1.8}$$

функція $x(t)$ має вигляд:

$$x(t) = \sum_{k=-\infty}^{\infty} x(k\Delta t) \frac{\sin\omega_{\max}(t-k\Delta t)}{\omega_{\max}(t-k\Delta t)} . \tag{1.9}$$

Інтерполяційний ряд (1.9) має назву ***ряду Котельникова***. Цей вираз показує, що неперервна функція $x(t)$ з обмеженим спектром може бути точно подана відрахунками функції $x(kt)$, що взяті через рівні інтервали:

$$\Delta t_{\max} = \frac{1}{2f_{\max}} = \frac{\pi}{\omega_{\max}} . \tag{1.10}$$

З виразу (1.9) зрозуміло, що функція $x(t)$ є сумою множників, один з яких - ***вибірка функції***, а інший - ***функція відрахунків***:

$$\varphi(t) = \frac{\sin\omega_{\max}(t-k\Delta t)}{\omega_{\max}(t-k\Delta t)} . \tag{1.11}$$

Функція відрахунків $\sin x/x$ (1.11) має певні властивості:

- сягає максимуму (одиниці) в моменти часу $t = k\Delta t$;
- дорівнює нулю в моменти часу $t = (k + n)\Delta t$, де n - будь-яке ціле число;
- ортогональна на нескінченному інтервалі часу.

Фізичний сенс перетворень полягає в тому, що кожен член ряду (1.9) являє собою відгук ідеального фільтра нижніх частот з граничною частотою зрізу $f_{\max}$ на дуже короткий імпульс, що виникає в момент часу $k\Delta t$, і має площину, яка дорівнює миттєвому значенню функції $x(t)$.

Цікавою властивістю ряду є те, що його значення в момент часу $k\Delta t$ визначається тільки k-тим членом ряду, тому що інші члени ряду в цей час обертаються на нуль.

Таким чином, неперервне повідомлення зводиться до сигналу у вигляді послідовності імпульсів, амплітуда яких дорівнює значенню початкової функції, що перетворюється на дискретну в інтервали часу $k\Delta t$, а інтервали між імпульсами складають $\Delta t = 1/2f_{max}$. Для перетворення дискретної функції на неперервну необхідно включити ідеальний фільтр нижніх частот з частотою зрізу f_{max}.

Описуваний процес перетворення неперервного повідомлення на дискретне за часом має назву ***дискретизації за часом***.

Процес перетворення неперервної функції на дискретну за рівнем носить назву ***квантування*** і полягає в тому, що у діапазоні неперервних значень функції $x(t)$ вибирається кінцева кількість значень функції, розподілених, наприклад, у всьому діапазоні рівномірно. У будь-який момент часу значення функції замінюється найближчим дискретним за рівнем. Функція при цьому набуває східчастого вигляду.

Крок квантування за рівнем - різниця між сусідніми дискретними значеннями функції.

Для рівномірного квантування крок $h_{кв}$ постійний.

$$h_{кв} = \frac{x_{max} - x_{min}}{q-1}, \qquad (1.12)$$

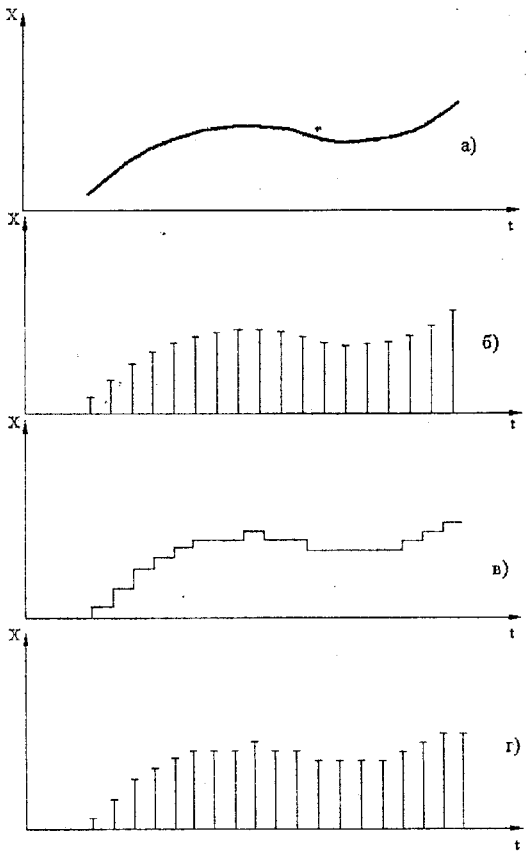
де q - кількість кроків квантування.

Абсолютне значення похибки квантування визначається значенням половини кроку квантування $\Delta_{кв} = h_{кв}/2$.

Таким чином, повідомлення та сигнали можуть бути чотирьох типів (рис. 1.5) – неперервні (а), дискретні зі часом та неперервні за рівнем (б), неперервні за часом та квантовані за рівнем (в), дискретні (г).

Для реальних систем використання теореми Котельнікова викликає два принципових припущення – вважається, що реальні сигнали $x(t)$ мають обмежений частотний спектр, хоча вони завжди обмежені за часом і тому мають нескінченний спектр. В реальних системах відкидають вищі гармо-

ніки, обмежуючись тими, на які припадає найбільша частина енергії сигналу – дискретизований реальний сигнал на приймальному боці пропускають крізь фільтри нижніх частот. При цьому він відновлюється досить приблизно, оскільки реальні фільтри не можуть точно відтворити функцію відрахунків (з необмеженою тривалістю в часі і негативними значеннями самого часу). Для покращання якості фільтрів їх роблять активними зі змінними параметрами.



а – неперервний; б – дискретний за часом і неперервний за рівнем; в – неперервний за часом та квантований за рівнем; г – дискретний.

Рисунок 1.5 – Типи сигналів

Література

1. Кузьмин И.В., Кедрус В.А. Основы теории информации и кодирования / Учебн. пос. – К.: Выща школа, 1986. – С. 54 – 56.
2. Квєтний Р.Н., Компанець М.М., Кривогубченко С.Г., Кулик А.Я. Основи техніки передавання інформації / Підручник. – Вінниця: Універсум-Вінниця, 2002. – С. 40 – 46.
3. Васюра А.С., Кривогубченко С.Г., Кулик А.Я., Компанець М.М., Худолій О.І. Техніка передавання аналогової та дискретної інформації / Навч. посібн. – Вінниця: ВДТУ, 1998. – С. 40 – 46.

2. Інформаційні характеристики процесу передавання

2.1 Одиниці вимірювання інформації

Існує багато означень терміна „інформація", кожне з яких висвітлює її певні властивості, тому і підхід до змістовності інформації визначає одиниці її вимірювання. ***Статистична теорія*** оцінює інформацію з точки зору невизначеності, яка знімається після отримання інформації. При цьому не приділяється увага семантичному змісту даних, а враховується лише розподіл імовірностей окремих часток даних і будуються характеристики, які дозволяють кількісно оцінити вміст інформації в цих частках. ***Семантична теорія*** враховує, в основному, цінність інформації, її корисність. Це дозволяє пов'язати кількість і цінність інформації з параметрами її старіння, а відповідно і з ефективністю функціонування системи чи мережі. ***Структурна теорія*** враховує структуру побудови окремих інформаційних масивів, при цьому за одиницю інформації приймаються певні елементарні одиниці – кванти, а кількість інформації визначається простим підрахунком квантів у масиві даних.

Таким чином, вимірювання інформації, а відповідно і вибір необхідної теорії, визначаються метою підрахунку її кількості. З урахуванням сформульованого означення терміна „інформація" і для оцінювання характеристик її передавання доцільно користуватися саме статистичною теорією.

Перша спроба ввести міру інформації була зроблена в 1927 році Р. Хартлі (Англія). Він запропонував і обґрунтував кількісну міру, яка дозволяє порівнювати спроможність різних систем передавати інформацію. Ця міра підходить також для систем зберігання інформації, тому вона є відправною точкою для створення теорії інформації.

Природною вимогою, що її висувають до інформаційної міри, є вимога адитивності, тобто кількість інформації, що може бути збережена у двох однакових комірках, повинна бути вдвічі більшою за ту, що зберігається в одній з них.

Якщо одна комірка для зберігання інформації має m можливих станів, то дві таких комірки будуть мати m^2 можливих станів, а n однакових

комірок – m^n можливих станів. Це стосується і кількості можливих повідомлень. Якщо символ може прийняти значення „0" або „1", то з одного символу можуть бути одержані 2 повідомлення, з двох символів – 4, з трьох – 8 тощо. Таким чином, кількість можливих повідомлень визначається кількістю символів, що входять до слова, n та кількістю можливих станів символу m: m^n. Саме тому Р. Хартлі ввів логарифмічну міру інформаційної ємності:

$$C = \log m \ . \tag{2.1}$$

Така міра задовольняє вимогу адитивності. Ємність засобу, що складається з n комірок і має m^n станів, дорівнює ємності однієї комірки, помноженій на їх кількість:

$$C = \log\left(m^n\right) = n \cdot \log m \ . \tag{2.2}$$

За одиницю вимірювання інформаційної ємності вибрана двійкова одиниця - ***біт*** (binary digit - двійковий знак), що дорівнює ємності однієї комірки з двома можливими станами. Інформаційна ємність C у двійкових одиницях в загальному випадку визначається як:

$$C = k_a \cdot \log_2 m \ , \tag{2.3}$$

де k_a - коефіцієнт, що залежить від основи системи числення a.

При використанні для зберігання інформації десяткових комірок більш зручно користуватись десятковими логарифмами. В цьому випадку:

$$K_{10} = \log_2 10 \approx 3{,}32 \ ,$$

тобто одна десяткова комірка за інформаційною ємністю дорівнює 3,32 двійковим. Одиниця вимірювання кількості інформації в цьому випадку – ***діт***.

Якщо від джерела інформації каналом зв'язку передається повідомлення про подію, апріорна імовірність якої на передавальному боці дорівнювала $p_{пер}$, то після приймання повідомлення апостеріорна імовірність цієї події для приймача інформації дорівнює $p_{пр}$. Збільшення кількості інформації з урахуванням логарифмічної міри складає:

$$\Delta I = \log\left(\frac{p_{пр}}{p_{пер}}\right) = \log p_{пр} - \log p_{пер} \ . \qquad (2.4)$$

Для ідеального каналу зв'язку (без завад та спотворень) приймання інформації є вірогідною подією, тобто імовірність $p_{пр}$ обертається на одиницю:

$$\Delta I_i = -\log p_{пер} \ . \qquad (2.5)$$

Чим меншою буде імовірність $p_{пер}$, тим більшою буде невизначеність результату, тобто тим більша кількість інформації повинна вміщуватися у прийнятому повідомленні.

Значення $p_{пер}$ знаходиться у межах $0 < p_{пер} < 1$, тобто ΔI завжди позитивна величина.

Якщо припустити, що може передаватися n_a символів S_a, що відповідають події A, n_b символів S_b, що відповідають події B, тощо, а всього m різних символів. Символи S_a, S_b тощо являють собою алфавіт з різних m символів. Сума всіх символів g складає:

$$g = n_a + n_b + \ldots \ . \qquad (2.6)$$

Згідно з (2.5) приймання символу S_a дає кількість інформації:

$$\Delta I = -\log p_a \, , \qquad (2.7)$$

де p_a – імовірність події A.

Тоді у n_a символах міститься кількість інформації $n_a \cdot (-\log p_a)$. Загальна кількість інформації:

$$I_g = \left(-n_a \cdot \log p_a - n_b \cdot \log p_b - \ldots\right) = -\sum_{i=1}^{m} n_i \cdot \log p_i \ . \qquad (2.8)$$

Вираз для визначення середньої кількості інформації, що припадає на один символ, можна отримати, розділивши (2.8) на g:

$$I_1 = -\sum_{i=1}^{m} \frac{n_i}{g} \cdot \log p_i \ . \qquad (2.9)$$

У (2.9) відношення n_i/g (при $i = a$) є апріорною імовірністю появи символу S_a для великих значень n_i та g, n_b/g - імовірність появи символу S_b тощо. Тоді:

$$\lim_{g\to\infty}\left(\frac{n_i}{g}\right) = p_i \,. \tag{2.10}$$

При цьому сума імовірностей:

$$p_a + p_b + \ldots = 1, \tag{2.11}$$

оскільки одна з усіх m подій A, B, ... відбувається обов'язково (повна імовірність подій).

Таким чином, можна отримати вираз для середньої кількості інформації на один символ:

$$I_1 = -\sum_{i=1}^{m} p_i \cdot \log p_i \,, \tag{2.12}$$

де p_i - імовірність i-того символу.

Формула (2.10) виражає теорему К. Шеннона, згідно з якою, середня кількість інформації, що припадає на один символ, отримала назву ***ентропії*** H і визначається з формули:

$$H_* = -\sum_{i=1}^{m} p_i \cdot \log p_i \,. \tag{2.13}$$

Ентропія являє собою логарифмічну міру безладдя стану джерела повідомлень і характеризує середній степінь невизначеності стану цього джерела. Отримання інформації – процес розкриття невизначеності.

В інформаційних системах невизначеність знижується за рахунок прийнятої інформації, тому чисельно ентропія H дорівнює кількості інформації I, тобто є кількісною мірою інформації.

Доцільно проаналізувати її певні властивості. Ентропія завжди додатна. Для детермінованих повідомлень вона дорівнює нулю. Якщо одне з

повідомлень є вірогідним ($p_n = 1$), то імовірність всіх інших дорівнює нулю ($p_0, p_1, \ldots, p_{n-1}, p_{n+1}, \ldots = 0$). Якщо всі m різних станів джерела рівноімовірні, то ентропія максимальна:

$$H_{\max} = -\sum_{i=1}^{m} \frac{1}{m} \cdot \log \frac{1}{m} = \log m \,. \qquad (2.14)$$

В цьому окремому випадку кількісна міра Шеннона збігається з мірою Хартлі. Якщо повідомлення нерівноімовірні, то середня кількість інформації, що вміщується в одному повідомленні, буде меншою.

При використанні двійкової системи з рівними імовірностями виникнення „0" та „1", згідно із формулою Шеннона:

$$H = -0{,}5 \cdot \log_2 0{,}5 - 0{,}5 \cdot \log_2 0{,}5 = 1 \,.$$

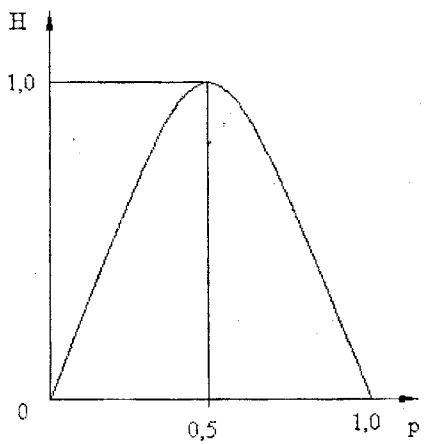


Рисунок 2.1 – Ентропія H для двох можливих станів з імовірностями p_1 та $(1 - p_1)$

Ентропія, а разом з нею і кількість інформації, дорівнюють нулю у випадках, коли $p_1 = 0$, або $p_1 = 1$. Графік ентропії наведено на рис. 2.1.

Іноді використовується параметр ***„питома ентропія"***, який характеризує ентропію на один використовуваний символ алфавіту. Така оцінка зручна для порівняння різних джерел.

Розповсюджуючи означення ентропії на повідомлення, що мають неперервний характер, необхідно знати їх щільність розподілу імовірності $w(x)$. Вона характеризує імовірність потрапляння неперервної величини x в інтервал dx. Неперервне повідомлення відзначається нескінченно великим набором елементів x_k. Ці елементи вибираються з постійним інтервалом Δx,

їх кількість кінцева і елементи мають вигляд $x_1, x_2, ..., x_k, ..., x_K$. Тоді ентропія буде визначатися

$$H = -\sum_{k=1}^{K} p(x_k) \cdot \log_2 p(x_k) . \qquad (2.15)$$

Для елемента x_k імовірність появи $p(x_k)$ можна знайти з розподілу $w(x)$ при $x = x_k$ з урахуванням зони дискретизації елемента Δx у вигляді $p(x_k) = w(x_k) \cdot \Delta x$:

$$H = -\sum_{k=1}^{K} w(x_k) \cdot \Delta x \cdot \log_2 w(x_k) - \sum_{k=1}^{K} w(x_k) \cdot \Delta x \cdot \log_2 \Delta x . \qquad (2.16)$$

Оскільки повідомлення має неперервний характер, то $\Delta x \to 0$, $K \to \infty$. Тоді

$$H = -\int_{-\infty}^{\infty} w(x) \log_2 w(x) dx - \int_{-\infty}^{\infty} w(x) \log_2 \Delta x dx = -\int_{-\infty}^{\infty} w(x) \log_2 \left(w(x) \cdot \Delta x\right) dx . \qquad (2.17)$$

При $\Delta x \to 0$, з урахуванням $\int_{-\infty}^{\infty} w(x) dx = 1$, можна отримати

$$H = -\int_{-\infty}^{\infty} w(x) \log_2 w(x) dx - \log_2 \Delta x . \qquad (2.18)$$

Оскільки кількість інформації визначається, в основному, першою складовою, то часто розраховують ***приведену відносну ентропію***

$$H_n = -\int_{-\infty}^{\infty} w(x) \log_2 w(x) dx . \qquad (2.19)$$

Визначено, що $H_{n.\max} = \log_2 \left(\sigma \sqrt{2\pi e}\right)$.

Література

4. Кузьмин И.В., Кедрус В.А. Основы теории информации и кодирования / Учебн. пос. – К.: Вища школа, 1986. – С. 115 – 117.

5. Васюра А.С., Кривогубченко С.Г., Кулик А.Я., Компанець М.М., Худолій О.І. Техніка передавання аналогової та дискретної інформації / Навч. посібн. – Вінниця: ВДТУ, 1998. – С. 23 – 29.
6. Квєтний Р.Н., Компанець М.М., Кривогубченко С.Г., Кулик А.Я. Основи техніки передавання інформації / Підручник. – Вінниця: Універсум-Вінниця, 2002. – С. 55 – 60.
7. Женко Л.А. Теория передачи сигналов на железнодорожном транспорте / Учебн. пос. – Самара: СамГАПС, 2005. – С. 66 – 69.
8. Теория электрической связи [Электронный ресурс]– Режим доступу: http://www.mtuci.ru/cde/courses/tes/testoc.html

2.2 Передавання інформації ідеальним каналом без завад

Ємність каналу – гранична швидкість передавання інформації цим каналом:

$$C = \lim_{T \to \infty} \left(\frac{\log g}{T} \right), \tag{2.20}$$

де g – кількість елементарних інформативних повідомлень, що передається за час T.

Якщо сигнали передаються зі швидкістю S імпульсів за секунду, тобто:

$$S = \frac{1}{\tau}, \tag{2.21}$$

де τ – час передавання одного імпульсу;

то за час T можна передати n імпульсів:

$$n = \frac{T}{\tau} = ST. \tag{2.22}$$

Для двійкового каналу, що пропускає лише елементарні сигнали «0» та «1», максимальна кількість комбінацій елементарних сигналів, яка може бути передана за час T, складає:

$$g = 2^n = 2^{ST} \ . \tag{2.23}$$

Тоді ємність цього каналу визначається:

$$C = \lim_{T \to \infty} \left(\frac{\log_2 g}{T} \right) = \frac{\log_2 2^{ST}}{T} = S \ , \tag{2.24}$$

тобто, чим меншою буде тривалість імпульсу $\tau = 1/S$, тим більшою буде ємність каналу *C*. Для недвійкового каналу:

$$g = m^{ST} \ , \tag{2.25}$$

де m - кількість символів у алфавіті;

і ємність каналу:

$$C = \lim_{T \to \infty} \left(\frac{\log g}{T} \right) = \frac{\log \left(m^{ST} \right)}{T} = S \cdot \log m \ . \tag{2.26}$$

Ємність каналу зв'язку *C* може бути виражена у бітах на символ. Якщо до входу каналу підключене джерело повідомлень з ентропією на символ, що дорівнює ємності каналу зв'язку, то джерело інформаційно узгоджене з каналом. Якщо ентропія джерела менша, ніж ємність каналу, то ємність каналу використовується не повністю (канал інформаційно недовантажений).

Узгодження джерела з каналом є досить складною справою і реалізується за допомогою статистичного кодування. К. Шеннон показав, що інформаційне узгодження, яке досягається статистичним кодуванням, аналогічне енергетичному узгодженню внутрішнього опору електричного генератора з навантаженням за допомогою трансформатора для передавання від генератора максимальної потужності. Тут мається на увазі узгодження джерела з каналом зв'язку за допомогою кодувального пристрою з метою максимального використання ємності каналу.

У своїй фундаментальній праці К. Шеннон навів приклад. Нехай бінарним каналом ємністю 1 біт/символ передається послідовність символів):

$$0010000000110000000000000000000\,.$$

Ентропія цієї послідовності складає:

$$H = -0{,}1 \cdot \log 0{,}1 - 0{,}9 \cdot \log 0{,}9 \approx 0{,}5 \text{ (біт/символ)}\,.$$

Таким чином ємність каналу удвічі більша за ентропію, тобто канал не узгоджений із джерелом. Статистичне кодування дозволяє збільшити ентропію, скоротивши довжину повідомлення. Оскільки при цьому збільшується ентропія, то збільшується і питома інформаційна вага повідомлення (співвідношення "кількість інформації/символ"). Послідовність символів розбивається на групи з трьох елементів. Після цього можна підрахувати імовірність можливих сполучень. Групам з великою імовірністю присвоюються короткі комбінації нерівномірного двійкового коду без розподільних знаків. У табл. 2.1 наведені можливі групи послідовностей з трьох елементів, їх імовірності та присвоєний їм код. Нова послідовність кодів буде мати вигляд:

$$1100011110000000\,.$$

Таблиця 2.1 - Статистичне кодування

Кодова послідовність	Імовірність	Присвоєне значення
000	$0{,}9^3 = 0{,}729$	0
001	$0{,}9^2 \cdot 0{,}1 = 0{,}081$	110
010	$0{,}9^2 \cdot 0{,}1 = 0{,}081$	101
100	$0{,}9^2 \cdot 0{,}1 = 0{,}081$	011
110	$0{,}9 \cdot 0{,}1^2 = 0{,}009$	11100
101	$0{,}9 \cdot 0{,}1^2 = 0{,}009$	11101
011	$0{,}9 \cdot 0{,}1^2 = 0{,}009$	11110
111	$0{,}1^3 = 0{,}001$	11111

Сформована послідовність складається з 16 елементів і її ентропія близька до 1 біт/символ. Сформована кодова послідовність може бути на приймальному боці декодована однозначно. Але вказаний принцип кодування має цілий ряд недоліків:

- вимагає певної інформації про те, які повідомлення будуть передані;
- викликає досить великі затримки в режимі реального часу;
- може погіршувати завадозахищеність системи.

У комп'ютерній системі обов'язково наявне джерело. Воно періодично формує дискретне повідомлення X_0, яке кодувальним пристроєм перетворюються на кодову комбінацію X. При цьому необхідно пов'язати властивості сформованої кодової комбінації та початкового повідомлення, що можна зробити за допомогою ентропії. ***Ентропія повідомлення*** (середня кількість інформації, що вміщується у повідомленні) буде визначатися

$$H(X_0) = -\sum_{j=1}^{D} p(x_{0,j}) \cdot \log_2 p(x_{0,j}) \quad \left[\frac{біт}{повідомлення}\right]. \qquad (2.27)$$

Відповідно ***ентропія кодової комбінації***, тобто кількість інформації, що вміщується в одному символі кодової комбінації, становить

$$H(X) = -\sum_{j=1}^{K} p(x_j) \cdot \log_2 p(x_j) \quad \left[\frac{біт}{символ}\right]. \qquad (2.28)$$

Так, якщо передаються чотири рівноймовірнісних повідомлення двійковим кодом 00, 01, 10, 11, то ентропія повідомлення

$$H(X_0) = -\sum_{j=1}^{4} \frac{1}{4} \cdot \log_2 \frac{1}{4} = 2 \ (біт/повідомлення),$$

а ентропія кодової комбінації

$$H(X) = -\sum_{j=1}^{2} \frac{1}{2} \cdot \log_2 \frac{1}{2} = 1 \ (біт/символ),$$

тобто кожний символ кодової комбінації несе один біт інформації.

Якщо розділити $H(X_0)$ на $H(X)$, то можна отримати оптимальну кількість елементів коду

$$\frac{H(X_0)}{H(X)} = k_0 . \qquad (2.29)$$

Виконання умови (2.29) показує, що код вибраний оптимально, інакше код є надлишковим і він не є оптимальним для каналу без шуму. Оптимальність коду передбачає, що символи в ньому зустрічаються з рівною імовірністю.

Все вищевикладене є справедливим лише для випадків взаємної незалежності символів у повідомленнях та самих повідомлень джерела. На практиці частіше зустрічаються джерела, в яких імовірність появи символу визначається тим які символи були сформовані раніше. При цьому вводять обмеження за тривалістю кореляційної функції в часі. В таких випадках користуються математичним описом джерела у вигляді ланцюга Маркова. Щоб описати джерело із взаємно залежною появою окремих символів, необхідно знати імовірності, що визначають всю множину станів, і для кожного g-го стану знайти його імовірність p_g. Тоді можуть бути знайдені імовірності $p_g(x_k)$ появи k-го символу для g-го стану джерела. Середня кількість інформації на один символ для цього випадку визначається ентропією

$$H_g = -\sum_{k=1}^{K} p_g(x_k) \cdot \log_2 p_g(x_k). \qquad (2.30)$$

Якщо можлива поява K різних символів та l можливих станів кодера, то ентропія кодової комбінації

$$H(X) = -\sum_{g=1}^{l}\sum_{k=1}^{K} p_g \cdot p_g(x_k) \cdot \log_2 p_g(x_k). \qquad (2.31)$$

Потрібно відзначити, що наявність імовірнісних зв'язків викликає зменшення ентропії.

Для порівняння різних пристроїв використовують такий параметр, як надлишковість, для чого порівнюють дійсну ентропію з максимально можливою. Зрозуміло, що максимально можливій ентропії відповідає мак-

симум інформації, що передається одним символом. В свою чергу, він відповідає рівномірному розподілу імовірності появи дискретних символів, тобто існує при $p(x_k) = 1/K$. В цьому випадку $H_{max} = \log_2 K$. Надлишковість джерела можна визначити як

$$R = 1 - \frac{H(X)}{H_{max}(X)} = 1 - \frac{H(X)}{\log_2 K}. \qquad (2.32)$$

Наявність надлишковості у передавачі пов'язана, з одного боку, із імовірнісними залежностями між появою символів, а з другого – із нерівномірним законом розподілу імовірностей їх появи. Для збільшення ентропії необхідно намагатися будувати передавач із взаємно незалежними символами при рівноймовірності їх появи.

Сукупність символів, що видаються передавачем до каналу зв'язку, складає певне повідомлення. При використанні кодів із усіма можливими сполученнями кількість можливих повідомлень $M = K^n$. Якщо кожне повідомлення складається з n елементів, то за рахунок адитивності кількість інформації, що її містить повідомлення дорівнює сумі за всіма елементами. Для найпростішого випадку $H(X_0) = n \cdot H(X)$. Надлишковість, що характерна для кожного символу коду, пропорційно розподіляється і на повідомлення. Якщо максимум інформації, яку вміщує повідомлення, становить $H_{max}(X_0) = \log_2 M$, то зрозуміло, що він виникає при наявності максимуму для кожного символу кодової комбінації

$$H_{max}(X_0) = n \cdot H_{max}(X) = n \cdot \log_2 K. \qquad (2.33)$$

Надлишковість повідомлення

$$R_n = 1 - \frac{H(X_0)}{H_{max}(X_0)} = 1 - \frac{n \cdot H(X)}{n \cdot H_{max}(X)} = 1 - \frac{H(X)}{H_{max}(X)} = R. \qquad (2.34)$$

Таким чином, надлишковість у випадку зміни алфавіту не змінюється, але зі збільшенням довжини повідомлення виникає ефект декореляції окремих символів і знищення взаємних зв'язків між ними. Для джерела без надлишковості ентропія повідомлення є максимальною і складає $\log_2 K$.

Якщо передавач формує рівноймовірні взаємно незалежні послідовності довжиною n таким чином, що $M_{\min} = K^n$, то такі послідовності є ***типовими*** і для будь-якої з них $p(x_{0,j}) = 1/K^n$. Звідси $H_{\max}(X) = \log_2 p(x_{0,j})/n$. При цьому загальна кількість типових послідовностей довжиною n із збільшенням довжини асимптотично наближається до $M_{\min} = 2^{-n \cdot H_{\max}(X)}$. Фізично типова послідовність характеризує оптимальне використання кожного символу в коді і серед усіх можливих співвідношення типових можна визначити як

$$\frac{M_{\min}}{M} = 2^{-n(H_{\max}(X) - H(X))}. \qquad (2.35)$$

Зрозуміло, що при достатньо великій довжині n значення $H(X)$ наближається до $H_{\max}(X)$ і всі можливі послідовності будуть типовими.

Література

4. Советов Б.Я. Теория информации (теоретические основы передачи информации в АСУ) / Учебн. пос. – Л.: Изд-во Ленингр. ун-та, 1977. – С. 55 – 58.
5. Васюра А.С., Кривогубченко С.Г., Кулик А.Я., Компанець М.М., Худолій О.І. Техніка передавання аналогової та дискретної інформації / Навч. посібн. – Вінниця: ВДТУ, 1998. – С. 29 – 33.
6. Квєтний Р.Н., Компанець М.М., Кривогубченко С.Г., Кулик А.Я. Основи техніки передавання інформації / Підручник. – Вінниця: Універсум-Вінниця, 2002. – С. 61 – 64.
7. Теория электрической связи [Электронный ресурс]– Режим доступу: http://www.mtuci.ru/cde/courses/tes/testoc.html

2.3 Передавання інформації каналом із завадами

Завади або шуми в каналі зв'язку суттєво ускладнюють передавання інформації. На приймальному боці немає впевненості, що той чи інший елемент повідомлення прийняті саме в тому вигляді, в якому вони були передані. Тому під час передавання інформації каналом із завадами виникають дві проблеми:

- підвищення ефективності передавання;
- підвищення вірогідності (завадозахищеності) передавання.

Ці проблеми до певної міри протилежні.

Якщо за рахунок впливу шуму був прийнятий елемент повідомлення j в той час, як був переданий елемент i, то збільшення інформації можна визначити як

$$\Delta I_{ij} = \log_2 \frac{1}{p_i} - \log_2 \frac{1}{p_j(i)} = \log_2 \frac{p_j(i)}{p_i} , \qquad (2.36)$$

де p_i – апріорна імовірність передавання елемента i;

$p_j(i)$ – умовна імовірність приймання елемента j в той час, як був переданий елемент i.

Якщо шуми досить великі $\left(p_j(i) = p_i, \Delta I = \log_2 1 = 0\right)$, повідомлення, що приймається, не вміщує інформації і приймання його не змінює початкових знань. За умови відсутності шуму: $p_j(i) = 1$, якщо $i = j$; або $p_j(i) = 0$, якщо $j \neq i$. В цьому випадку:

$$\Delta I = \log_2 \frac{1}{p_i} = -\log_2 p_i . \qquad (2.37)$$

Пропускна здатність каналу являє собою максимальну кількість інформації, яка цим каналом може бути передана. Для каналу з шумами (у двійкових одиницях на символ) вона дорівнює середньому за всіма i та j значенню приросту інформації:

$$C = \sum_{j,i} p_i \cdot p_j(i) \cdot \Delta I_{ij} = H_i - H_j(i) = H_j - H_i(j) , \qquad (2.38)$$

де $H_i = -\sum_i p_i \cdot \log p_i$ – ентропія джерела;

$H_j = -\sum_j p_j \cdot \log p_j$ – ентропія повідомлень на приймальному боці;

$$\left.\begin{aligned} H_i(j) &= \sum_{i,j} p_i \cdot p_i(j) \cdot \log p_i(j) \\ H_j(i) &= \sum_{i,j} p_j \cdot p_j(i) \cdot \log p_j(i) \end{aligned}\right\} - \text{умовні ентропії.}$$

Для каналу з шумами швидкість передавання інформації (у бітах за секунду):

$$v = SR_c \,, \tag{2.39}$$

де S - кількість символів, що передаються за секунду.

$$R_c = H_i - H_j(i). \tag{2.40}$$

Тоді:

$$v = S \cdot (H_i - H_j(i)) \,. \tag{2.41}$$

Якщо швидкість передавання інформації каналу складає 1000 біт/с, а дія завад викликає помилку в 1% символів, то за умови, що імовірності передавання „0" та „1" однакові, ентропія є максимальною $H = 1$ (біт/символ). Імовірність того, що під час передавання «0» приймається «1» складає $p_1(0) = 0{,}01$. Відповідно до цього інші умовні імовірності будуть $p_0(0) = 0{,}99$; $p_0(1) = 0{,}01$; $p_1(1) = 0{,}99$. Розраховані ентропії складають: $H_i = 1$, $H_i(j) = H_j(i) = 0{,}081$. Згідно з (2.36) швидкість передавання інформації каналом із шумами:

$$C = 1000 \cdot (1 - 0{,}081) = 919 \text{ (біт/с)} \,.$$

Таким чином швидкість передавання інформації під впливом шуму зменшується більш стрімко ніж кількість правильно переданих символів. На рис. 2.2 наведений графік залежності ємності бінарного каналу з шумами від імовірності спотворення елементів. К. Шеннон довів, що якщо ентропія джерела інформації не перевищує пропускної здатності каналу, тобто $H \le C$, то існує код, який забезпечує передавання інформації каналом із шумами з якою завгодно малою частотою помилок, або з якою завгодно малою невірогідністю. При $H > C$ такого коду не існує, тобто передавання без помилок неможливе.

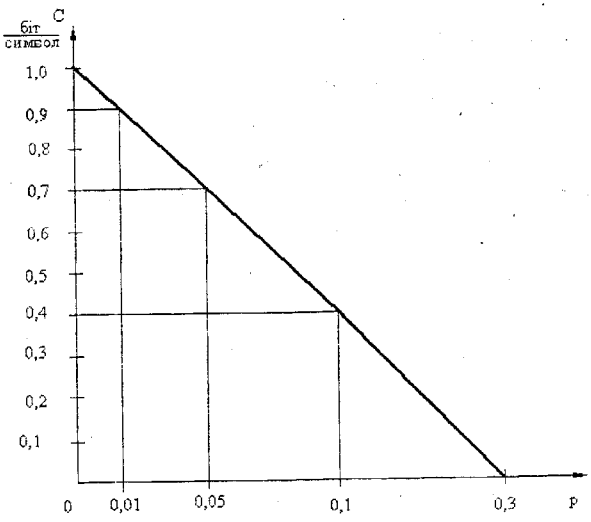


Рисунок 2.2 – Залежність ємності бінарного каналу від імовірності спотворення сигналів

Якщо в каналі діє нормально розподілений сигнал зі значенням $U_c = \sqrt{D_c} = \sqrt{P_c}$, причому D_c – дисперсія сигналу, тобто його потужність P_c, то цей сигнал можна описати вектором, довжина якого залежить і від значення потужності завади $U_\xi = \sqrt{D_\xi} = \sqrt{P_\xi}$. Кількість відрахунків сигналу, які може розрізнити приймач, приблизно можна визначити

$$N = \frac{U_c + U_\xi}{U_\xi} = \frac{\sqrt{D_c} + \sqrt{D_\xi}}{\sqrt{D_\xi}}. \qquad (2.42)$$

Оскільки сигнал і завада незалежні, то сума їх дисперсій дорівнює дисперсії суми

$$N = \frac{\sqrt{D_c + D_\xi}}{\sqrt{D_\xi}} = \sqrt{1 + \frac{P_c}{P_\xi}}. \qquad (2.43)$$

Ентропія джерела, тобто середня кількість інформації, що переноситься кожним відрахунком сигналу $H = \log_2 N = \log_2 \sqrt{1 + P_c / P_\xi}$. У відповідності із теоремою Котельнікова відрахунки неперервного сигналу необхідно здійснювати з частотою $f_в = 2f_{c.max}$ [відрахунків/с]. Для забезпечення проходження сигналу каналом зв'язку їй повинна відповідати верхня частота смуги каналу $f_k = f_{c.max}$. Таким чином максимальна швидкість переда-

вання інформації каналом чи пропускна здатність неперервного каналу становить:

$$C_k = f_k \cdot H = 2f_k \cdot \log_2 \sqrt{1+\frac{P_c}{P_\xi}} = f_k \cdot \log_2\left(1+\frac{P_c}{P_\xi}\right), \qquad (2.44)$$

де f_k – смуга частот каналу;

P_c – середня потужність сигналу;

P_ξ – середня потужність білого шуму.

Формула (2.44) називається ***формулою Шеннона***. Вона показує, що пропускна здатність каналу залежить як від смуги пропускання каналу f_k, так і від співвідношення сигнал/шум $h^2 = P_c / P_\xi$. Потужність завади визначається питомою потужністю (потужністю, яка відповідає 1 Гц смуги частот) та смугою частот каналу $P_\xi = G_0 \cdot f_k$. Питома потужність завади зростає із збільшенням f_k, а потужність інформативного сигналу як вузькосмугового процесу лишається незмінною, тобто при збільшенні смуги частот настає межа збільшення $C_{k.\max} = f_k \cdot \log_2 e \cdot \ln\left(1+P_c/(G_0 \cdot f_k)\right)$. Це означає, що смугу частот доцільно обмежувати величиною $f_{k.\max} = P_c / G_0$ [Гц].

Другий важливий висновок з формули Шеннона полягає в тому, що пропускна здатність каналу стає максимальною у випадку нормального розподілу сигналу, коли при заданій потужності диференціальна ентропія h інформативного сигналу є максимальною. Оскільки флуктуаційна завада завжди розподілена нормально, то пропускна здатність каналу буде максимальною, якщо як носій використовується нормальний стаціонарний випадковий процес типу білого шуму.

Таким чином, можна передавати інформацію, якщо швидкість передавання інформації не перевищує максимальної швидкості каналу. Для випадку, коли $P_c >> P_\xi$, у формулі (2.44) одиницею можна знехтувати:

$$C_k = f_k \cdot \log_2\left(\frac{P_c}{P_\xi}\right). \qquad (2.45)$$

Максимальна пропускна здатність двійкового дискретного каналу визначається як $C_{k.bin} = 2f_{c.max}$ [біт/с]. При збільшенні основи коду пропускна здатність дискретного каналу наближається до пропускної здатності неперервного каналу, яка, в свою чергу, збільшується при зростанні h. Максимальна кількість інформації, яка може бути передана за час T:

$$V_{\max} = f_m \cdot T \cdot \log_2\left(\frac{P_c}{P_\xi}\right). \qquad (2.46)$$

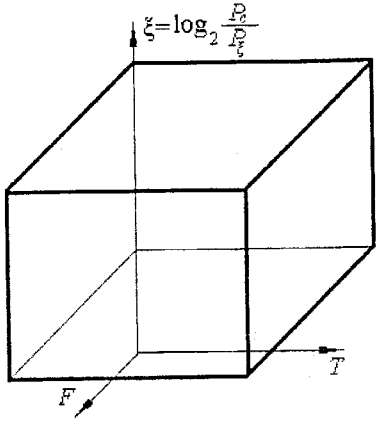


Рисунок 2.3 – Об'єм сигналу

В неперервних каналах зв'язку із завадами швидкість передавання також обмежується.

Оскільки ця величина може бути подана у вигляді паралелепіпеда, то вона отримала назву ***об'єму сигналу***. Таким чином можна змінювати окремі параметри сигналу, не змінюючи його об'єм (рис. 2.3). Якщо до виразу (2.39) підставити потенційні можливості каналу передавання (час, на який канал надається користувачу, виділену йому смугу частот і максимальну потужність сигналу, що може передаватися каналом), то параметр характеризуватиме ємність каналу. Для передавання сигналу каналом зв'язку необхідно щоб об'єм сигналу був не менший, ніж ємність каналу, тобто потрібно виконання умови:

$$V_c \le V_k. \qquad (2.47)$$

Якщо названа умова не виконується, то сигнал передати цим каналом зв'язку неможливо. Може статися, що умова (2.48) виконується, але смуга частот, на яку розрахований канал, менша за смугу частот сигналу, або час, який виділено на передавання інформації, менший, ніж необхідно, тобто умова (2.47) розпадається на систему:

$$\begin{cases} F_c \le F_k \\ T_c \le T_k \\ h_c^2 \le h_k^2 \end{cases}. \qquad (2.48)$$

Одним з найбільш розповсюджених способів перетворення сигналу є варіювання величинами F_c та T_c за їх незмінним добутком. Потужність сигналу, як правило, не збільшується. При цьому можна забезпечити багаторазове передавання повідомлення, тобто забезпечити перерозподіл ресурсів між потужністю сигналу та часом його передавання. Аналогічно можна вчиняти подовжуючи кодову комбінацію з метою збільшення завадозахищеності.

При моделюванні дискретний канал в більшості випадків подають у вигляді графа, у вузлах якого знаходяться символи, що передаються і приймаються, а дуги чи ребра віддзеркалюють взаємні імовірності перетворення символів під час їх передавання каналом зв'язку (рис. 2.4).

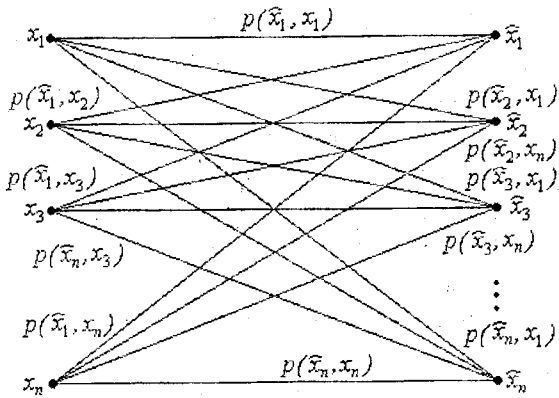


Рисунок 2.4 – Модель каналу зв'язку у вигляді графа

Імовірності переходів, що пов'язують прийняті та передані символи можуть бути подані у вигляді матриці умовних імовірностей (2.48). Імовірності, що розташовані по діагоналі, характеризують правильність приймання символів і повинні мати найбільші значення відносно інших. Всі імовірності за будь-яким рядком або стовпцем описують повну групу подій, тому їх сума повинна дорівнювати одиниці.

$$\mathbf{P} = \begin{Vmatrix} p(\hat{x}_1, x_1) & p(\hat{x}_2, x_1) & p(\hat{x}_3, x_1) & \dots & p(\hat{x}_n, x_1) \\ p(\hat{x}_1, x_2) & p(\hat{x}_2, x_2) & p(\hat{x}_3, x_2) & \dots & p(\hat{x}_n, x_2) \\ p(\hat{x}_1, x_3) & p(\hat{x}_2, x_3) & p(\hat{x}_3, x_3) & \dots & p(\hat{x}_n, x_3) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ p(\hat{x}_1, x_n) & p(\hat{x}_2, x_n) & p(\hat{x}_3, x_n) & \dots & p(\hat{x}_n, x_n) \end{Vmatrix}. \qquad (2.49)$$

Імовірності, що входять до матриці каналу **P**, можуть бути функціями часу, що властиво практично всім реальним каналам зв'язку. Наявність динаміки у зміні вірогідностей призводить до нестаціонарності каналу. Для аналізу таких каналів використовуються моделі стаціонарних, тобто нестаціонарний канал розглядається як сукупність квазістаціонарних, для чого визначається їх множина та оцінюються імовірності знаходження каналу для кожного з цих станів.

З урахуванням певних обмежень (короткий час передавання, висока швидкість тощо) окремі конкретні канали зв'язку можна вважати стаціонарними, переходячи від аналізу динамічних режимів до аналізу квазістатичних, припускаючи що за достатньо короткий час передавання умови суттєво змінитися не можуть, а імовірності канальної матриці – постійні.

Імовірності, що входять до канальної матриці, можуть залежати від попередньо переданих значень символів. Для розрахунку та оцінювання якості передавання інформації каналами з пам'яттю використовується математичний апарат ланцюгів Маркова, а такі канали називаються ***марківськими***. Для марківського каналу властиве існування певної кількості станів, для кожного з яких складається відповідна матриця імовірностей. Тоді кількість можливих матриць каналу з пам'яттю відповідає кількості вибраних станів S і можна знайти імовірності, осереднені за можливими станами. В цьому випадку

$$p(\hat{x}_i, x_j) = \sum_{s=1}^{S} p_s \cdot p_s(\hat{x}_i, x_j), \qquad (2.50)$$

де $p_s(\hat{x}_i, x_j)$ – імовірність появи символу $\hat{x}_i$ за умови, що був переданий сигнал x_i, а канал знаходився у стані s;

p_s – імовірність знаходження каналу в стані s.

Додаткові умови спрощення можна отримати під час розгляду імовірностей, що входять до рядків та стовпців матриці **P**. Якщо імовірності, що складають рядок матриці, є перестановками одних і тих самих чисел, то канал є ***симетричним за входом***. Якщо це саме стосується імовірностей, що складають стовпець матриці, то канал ***симетричний за виходом***. Виконання обох умов забезпечує ***симетричність каналу за входом і виходом***. Модель симетричного дискретного каналу зв'язку є найбільш простою, і описання каналу даною моделлю дозволяє достатньо швидко отримати кінцеві результати за характеристиками каналу зв'язку. Так, матриця двійкового симетричного каналу має вигляд

$$\mathbf{P} = \begin{Vmatrix} q & p \\ p & q \end{Vmatrix}, \tag{2.51}$$

де p – імовірність спотворення символу під час передавання каналом зв'язку;

$q = 1 - p$ – імовірність безпомилкового передавання символу.

Для покращення властивостей двійкового симетричного каналу може бути введена зона стирання при ідентифікації прийнятого символу. Тоді матриця набуває вигляду

$$\mathbf{P}_c = \begin{Vmatrix} 1-p-p_{cm} & p & p_{cm} \\ p & 1-p-p_{cm} & p_{cm} \end{Vmatrix}, \tag{2.52}$$

де p_{cm} – імовірність стирання прийнятого символу.

Чисельні значення імовірностей, що характеризують канал зв'язку, можуть бути знайдені, якщо відомі принцип побудови приймача та параметри завади. В найпростішому випадку, коли параметри каналу постійні і завади можна вважати стаціонарними, результатом буде модель дискретного, а іноді симетричного каналу без пам'яті.

Таким чином, граф, що віддзеркалює дискретний канал, є моделлю реального каналу зв'язку, за допомогою якої можна визначати основні характеристики каналу, які пов'язують його параметри з параметрами передавача, а іноді і приймача. Це дає можливість оцінити не лише можливість

передавання необхідної кількості інформації цим каналом, але й визначити оптимальні режими та параметри передавання.

Якщо всі імовірності, що входять до матриці **P**, крім діагональних, дорівнюють нулю, то модель описує канал без завад (ідеальний). Основною проблемою під час аналізу каналів без шуму є вибір оптимального коду, який за своїми властивостями узгоджується із джерелом інформації і має найменшу середню довжину. Для реальних каналів із завадами основною задачею є передавання інформації із максимальним завантаженням каналу зв'язку при заданій вірогідності передавання.

Потрібно відзначити, що за певних умов та при правильному виборі параметрів приймача використання каналу зі стиранням дозволяє зменшити імовірність помилки під час приймання інформації, хоча для цього також можуть використовуватися інші методи (лінійна та нелінійна фільтрація сигналів).

Література

4. Советов Б.Я. Теория информации (теоретические основы передачи информации в АСУ) / Учебн. пос. – Л.: Изд-во Ленингр. ун-та, 1977. – С. 61 – 67.
5. Кузьмин И.В., Кедрус В.А. Основы теории информации и кодирования / Учебн. пос. – К.: Выща школа, 1986. – С. 145 – 151.
6. Квєтний Р.Н., Компанець М.М., Кривогубченко С.Г., Кулик А.Я. Основи техніки передавання інформації / Підручник. – Вінниця: Універсум-Вінниця, 2002. – С. 64 – 69.
7. Теория электрической связи [Электронный ресурс]– Режим доступу: http://www.mtuci.ru/cde/courses/tes/testoc.html

2.4 Особливості побудови приймача

Передумови побудови приймача полягають в тому, що:

- якщо завади, з яких необхідно виділяти сигнал, мають взаємокореляційну з інформативним сигналом функцію, рівень якої значно менший від максимального значення автокореляційної функції інформативного сигналу, то такий сигнал може бути виділений шляхом обчислення прийнятої суміші сигналу та завади, а також завади з опорною копією

інформативного сигналу, навіть якщо інформативний сигнал повністю замаскований завадою;

- якщо як завади виступають аналогічні інформативному сигнали, але з іншим носієм, то за рахунок кореляційного оброблювання можна виділити необхідний адресований сигнал; це пов'язано з тим, що автокореляційна функція адресованого сигналу має значну амплітуду без зсуву і малі амплітуди при часовому зсуві τ, а взаємокореляційна функція адресованого сигналу та фонових має лише малі амплітуди на всій часовій осі;
- якщо високі амплітуди автокореляційної функції інформативного сигналу згруповані навколо нуля часової осі, то спектр його достатньо широкий, тому можна попередньо обробити прийнятий сигнал вузькосмуговими фільтрами і вирізати пошкоджені ділянки спектра до кореляційного оброблювання.

Але автокореляційна функція інформативного сигналу не може впливати на завадозахищеність каналу на фоні завади типу білого шуму.

На вхід приймача протягом інтервалу часу (0, τ) надходить сигнал $\hat{x}(t)$. Задача полягає у прийнятті рішення щодо наявності на вході приймача адитивної суміші інформативного сигналу $x(t)$ та шуму $\xi(t)$: $\hat{x}(t) = x(t) + \xi(t)$ чи наявності лише шуму за відсутності інформативного сигналу $\hat{x}(t) = \xi(t)$. Структура сигналу вважається повністю відомою, а шум – білим з відомою двобічною спектральною щільністю $N_0/2$. За критерій оптимального приймання приймають максимум імовірності правильної ідентифікації сигналу при заданому рівні імовірності помилки. Алгоритм роботи оптимального приймача Котельнікова складає два етапи:

- ✓ обчислення кореляційного інтеграла прийнятого сигналу $\hat{x}(t)$ та опорної копії структури сигналу $x_0(t)$ на інтервалі можливої реєстрації сигналу $R = \int_0^T \hat{x}(t) \cdot x_0(t) \cdot dt$;
- ✓ порівняння обчисленого інтегралу R з пороговим значенням. Якщо $R > R_{пор}$, то приймається рішення щодо наявності інформативного сигналу, в іншому випадку вважається, що на вході приймача присутній лише шум. Значення $R_{пор}$ визначається імовірністю помилки ідентифі-

кації, тобто вибирається таким, щоб за відсутності сигналу імовірність перевищення порогу не перевищувала б задану.

Кореляційна функція R при наявності сигналу буде мати вигляд

$$R = \int_0^T \hat{x}(t) \cdot x_0(t) \cdot dt = \int_0^T (x(t) + \xi(t)) \cdot x_0(t) \cdot dt = \int_0^T x(t) \cdot x_0(t) \cdot dt + \int_0^T \xi(t) \cdot x_0(t) \cdot dt =$$

$$= E_c + \xi, \qquad (2.53)$$

де $E_c = \int_0^T x(t) \cdot x_0(t) \cdot dt = \int_0^T x^2(t) \cdot dt$ – енергія інформативного сигналу $x(t)$ на інтервалі $(0, T)$;

$\xi = \int_0^T \xi(t) \cdot x_0(t) \cdot dt$ – випадкова величина.

Вираз (2.53) показує, що результат обчислення кореляційного інтеграла є сумою детермінованої складової енергії сигналу E_c та випадкової складової, що визначається опорним сигналом та шумом. Ця випадкова складова являє собою кореляційний інтеграл за відсутності інформативного сигналу на вході приймача ($x(t) = 0$). Тому величина ξ та кореляційний інтеграл R за відсутності сигналу статистично еквівалентні.

Інтервал інтегрування $(0, T)$ доцільно розбити на множину інтервалів ΔT_i. Тоді, з урахуванням властивості адитивності,

$$\xi = \sum_i \int_{\Delta T_i} \xi(t) \cdot x_0(t) \cdot dt = \sum_i \xi_i . \qquad (2.54)$$

де $\xi_i = \int_{\Delta T_i} \xi(t) \cdot x_0(t) \cdot dt$ – інтервальний інтеграл по i-тій ділянці інтервалу $(0, T)$.

Для аналізу можна вважати функцію інформативного сигналу $x(t)$ неперервною в часі, тоді з урахуванням теореми про середнє значення, інтервальний інтеграл

$$\xi_i = \int_{\Delta T_i} \xi(t) \cdot x_0(t) \cdot dt = x_0(t_i) \cdot \int_{\Delta T_i} \xi(t) \cdot dt = x_0(t_i) \cdot \lambda_i , \qquad (2.55)$$

де $\lambda_i = \int_{\Delta T_i} \xi(t) \cdot dt$ – інтеграл від білого шуму на інтервалі тривалістю ΔT_i.

Інтеграл від функції білого шуму являє собою нормально розподілену випадкову величину із нульовим середнім і дисперсією $D_\xi = {}^{N_0}\!/_2 \cdot T$. Відповідно дисперсія величин λ_i дорівнює $D_{\lambda_i} = {}^{N_0}\!/_2 \cdot \Delta T_i$. Кожний з інтервальних інтегралів ξ_i являє собою добуток детермінованого числа $x(t_i)$ на випадкову величину λ_i, тому дисперсія випадкової величини ξ_i дорівнює дисперсії випадкової величини λ_i, помноженої на квадрат детермінованої величини $x(t_i)$:

$$D_{\xi_i} = x_0^2(t_i) \cdot D_{\lambda_i} = x_0^2(t_i) \cdot \frac{N_0}{2} \cdot \Delta T_i. \qquad (2.56)$$

Оскільки випадкова величина ξ є сумою незалежних випадкових величин ξ_i, то дисперсія випадкової величини є сумою дисперсій складових:

$$D_\xi = \sum_i D_{\xi_i} = \frac{N_0}{2} \cdot \sum_i x_0^2(t_i) \cdot \Delta T_i. \qquad (2.57)$$

Оскільки завада являє собою білий шум, тобто може змінюватися нескінченно швидко в межах якого завгодно малого інтервалу, вираз (2.57) залишається справедливим при $\Delta T_i \to 0$. Замінивши суму інтегралів по i на інтеграл по інтервалу $(0, T)$, можна отримати

$$D_\xi = \frac{N_0}{2} \cdot \int_0^T x_0^2(t) \cdot dt, \qquad (2.58)$$

але інтеграл, що входить до складу (2.58), являє собою енергію опорного сигналу $x_0(t)$ і тотожного йому на інтервалі очікування $(0, T)$ інформативного сигналу $x(t)$. Тому дисперсія випадкової складової ξ в кореляційному інтегралі дорівнює

$$D_\xi = E \cdot \frac{N_0}{2}. \qquad (2.59)$$

Математичне сподівання завади ξ дорівнює нулю, а згідно з центральною граничною теоремою вона розподілена за нормальним законом. Таким чином, кореляційний інтеграл R при наявності сигналу є сумою детермінованої величини E та нормально розподіленої із нульовим математичним сподіванням та дисперсією $E \cdot N_0/2$ випадкової величини ξ. Тому і кореляційний інтеграл R при наявності сигналу являє собою нормально розподілену випадкову величину із математичним сподіванням E та дисперсією $E \cdot N_0/2$. За відсутності сигналу кореляційний інтеграл R має нульове математичне сподівання та дисперсію $E \cdot N_0/2$, тобто статистично еквівалентний випадковій величині ξ.

Відомості про щільність розподілу імовірності кореляційного інтеграла дозволяють вибрати поріг $E_{пор}$, який забезпечує задану імовірність помилки ідентифікації $p_{пом}$, яка дорівнює

$$p_{пом}(R) = \sqrt{2\pi D_\xi} \cdot \int_{E_{пор}}^{\infty} \exp\left(-\frac{R^2}{2D_\xi}\right) dR. \qquad (2.60)$$

Цей інтеграл є стандартним ***інтегралом Лапласа*** або ***інтегралом імовірності***, який підстановкою $x = R/\sigma_\xi$ можна привести до вигляду

$$p_{пом} = \Phi\left(\frac{E_{пор}}{\sigma_\xi}\right) = \sqrt{2\pi} \cdot \int_{\frac{E_{пор}}{\sigma_\xi}}^{\infty} \exp\left(-\frac{x^2}{2}\right) dx. \qquad (2.61)$$

Цей самий інтеграл можна визначити через ***функцію Крампа***

$$p_{пом} = \Phi\left(\frac{E_{пор}}{\sigma_\xi}\right) = 1 - \mathrm{K}\left(\frac{E_{пор}}{\sigma_\xi}\right) = 1 - \sqrt{2\pi} \cdot \int_{-\infty}^{\frac{E_{пор}}{\sigma_\xi}} \exp\left(-\frac{x^2}{2}\right) dx. \qquad (2.62)$$

Як видно з виразів (2.61) та (2.62) $\Phi(x) + \mathrm{K}(x) = 1$. Функції Лапласа і Крампа є табличними і можуть легко визначатися. Величину порога $E_{пор}$ доцільно визначати в одиницях σ_ξ. Відомо, що імовірність відхилення від ма-

тематичного сподівання на величину 3σ для випадкової величини, розподіленою за нормальним законом, приблизно дорівнює 0,003, а для 5σ ця імовірність становить вже $3 \cdot 10^{-7}$. З урахуванням особливостей побудови передавальних пристроїв (уніполярний або біполярний режим) для першого з випадків імовірність ще зменшується вдвічі, оскільки помилку може викликати лише перевищення порогового рівня завадою тільки однієї полярності. Таким чином поріг ідентифікації сигналу у вигляді $E_{пор}/\sigma_\xi$ залежить лише від імовірності помилки і не залежить від енергії сигналу та спектральної щільності шуму, хоча сам параметр σ_ξ від них залежить.

Наявність на вході приймача інформативного сигналу зсовує розподіл кореляційного інтеграла R вправо на величину енергії сигналу E. Імовірність правильної ідентифікації сигналу також можна визначити через функцію Лапласа

$$p_{пр} = \Phi\left(\frac{E_{пор} - E_c}{\sigma_\xi}\right) = \sqrt{2\pi} \cdot \int_{\frac{E_{пор}-E_c}{\sigma_\xi}}^{\infty} \exp\left(-\frac{x^2}{2}\right) dx \qquad (2.63)$$

та через функцію Крампа

$$p_{пр} = \Phi\left(\frac{E_{пор} - E_c}{\sigma_\xi}\right) = 1 - \mathrm{K}\left(\frac{E_c - E_{пор}}{\sigma_\xi}\right) = 1 - \sqrt{2\pi} \cdot \int_{-\infty}^{\frac{E_c-E_{пор}}{\sigma_\xi}} \exp\left(-\frac{x^2}{2}\right) dx. \qquad (2.64)$$

Таким чином, імовірність ідентифікації інформативного сигналу оптимальним приймачем на фоні білого шуму при заданій імовірності помилки не залежить від форми сигналу, а визначається виключно співвідношенням сигнал/шум E_c/N_0. Кореляційні властивості сигналу при цьому мають значення лише в сенсі засад, сформульованих на початку підрозділу.

Література

1. Автокорреляционная функция радиосигнала и безразличие к ней АЗПП „Мошкарец" [Электронный ресурс] / Дыбенко К. – Режим доступу: http://jamwar.h10.ru.corr.htm

2. Кузьмин И.В., Кедрус В.А. Основы теории информации и кодирования / Учебн. пос. – К.: Выща школа, 1986. – С. 34 – 44.

2.5 Оцінювання швидкості передавання інформації та пропускної здатності каналу зв'язку

Сформульована вище основна задача процесу передавання інформації вимагає визначення максимального завантаження каналу зв'язку при заданій вірогідності приймання. Вираз (2.38) показує яка невизначеність знімається приймачем за винятком тієї частки, яку вносить завада. З урахуванням позначень, прийнятих для описуваних каналів зв'язку, доцільно цей вираз подати у вигляді

$$I = H(\hat{X}) - H(\hat{X}/X). \tag{2.65}$$

Ентропія приймача $H(\hat{X})$ залежить від статистики надходження символів з каналу зв'язку. Реалізація принципу взаємно однозначного кодування передбачає $H(\hat{X}) = H(X)$. Умовна ентропія $H(\hat{X}/X)$ також залежить від характеристик джерела, але значно суттєвішими виявляються характеристики каналу зв'язку та вибраний алгоритм кодування.

Оскільки для будь-якого каналу необхідно забезпечити передавання максимальної кількості інформації, тому важливими характеристиками є співвідношення, які визначають її граничну кількість.

Дискретний канал зв'язку без шуму характеризується тим, що $H(\hat{X}/X) = 0$. Тоді

$$I = H(\hat{X}) = -\sum_{j=1}^{K_x}\sum_{i=1}^{K_{\hat{x}}} p(x_j)\cdot \log_2\left(p(x_i)\cdot p(\hat{x}_i/x_j)\right) = -\sum_{i=1}^{K_{\hat{x}}} p(\hat{x}_i)\cdot \log_2 p(\hat{x}_i). \tag{2.66}$$

Якщо вважати символи на виході каналу рівноімовірними, то $p(\hat{X}) = 1/K_{\hat{x}}$, а пропускна здатність каналу

$$C = H_{\max}(\hat{X}) = -K_{\hat{x}}\cdot\frac{1}{K_{\hat{x}}}\cdot\log_2\frac{1}{K_{\hat{x}}} = \log_2 K_{\hat{x}}. \tag{2.67}$$

Для ***дискретного каналу із шумом без стирання*** справедливо $K_x = K_{\hat{x}} = K$. Тоді

$$I = H(\hat{X}) - H(\hat{X}/X) = -\sum_{j=1}^{K}\sum_{i=1}^{K} p(x_j)\cdot p(\hat{x}_i/x_j)\cdot \log_2\left(p(x_j)\cdot p(\hat{x}_i/x_j)\right) + \\ + \sum_{j=1}^{K}\sum_{i=1}^{K} p(x_j)\cdot p(\hat{x}_i/x_j)\cdot \log_2 p(\hat{x}_i/x_j). \qquad (2.68)$$

Якщо розглянути найпростіший випадок – K-ого симетричного каналу, то $p = \sum_{i=1}^{K} p(\hat{x}/x)$, а $p(\hat{x}/x) = p/(K-1)$ при $i \neq j$ – імовірність спотворення символу та $p(\hat{x}/x) = 1 - p = q$ при $i = j$ – імовірність його безпомилкового передавання. Пропускна здатність цього каналу зв'язку

$$I = H_{\max}(\hat{X}) - H_{\min}(\hat{X}/X). \qquad (2.69)$$

$H(\hat{X})$ буде максимальним, якщо символи рівноімовірні, тобто $p(\hat{x}_i) = 1/K$. Тоді

$$H_{\max}(\hat{X}) = -\sum_{j=1}^{K} p(\hat{x}_j)\cdot \log_2 p(\hat{x}_j) = \log_2 K. \qquad (2.70)$$

Якщо і символи, які видаються джерелом до каналу зв'язку рівноімовірні, то відповідно і $p(x_i) = 1/K$. Тоді

$$H(\hat{X}/X) = \sum_{j=1}^{K}\sum_{i=1}^{K} p(x_j)\cdot p(\hat{x}_i/x_j)\cdot \log_2 p(\hat{x}_i/x_j) = \\ = K\cdot\frac{1}{K}\cdot\left(q\cdot\log_2 q + (K-1)\cdot\frac{p}{K-1}\cdot\log_2\frac{p}{K-1}\right) = \\ = -q\cdot\log_2 q - p\cdot\log_2\frac{p}{K-1}. \qquad (2.71)$$

Підставивши (2.70) та (2.71) до (2.69), можна отримати

$$C = \log_2 K + q \cdot \log_2 q + p \cdot \log_2 \frac{p}{K-1} \left[\frac{біт}{символ}\right]. \qquad (2.72)$$

Фізично пропускна здатність показує потенційно можливу кількість інформації, яка може бути передана одним символом, якщо імовірність його спотворення становить p. Якщо взяти до уваги швидкість передавання $v \left[символів/с\right]$, то

$$C_0 = C \cdot v_{\max} = C \cdot \frac{1}{T_{0.\min}} = C \cdot F_k \left[\frac{біт}{с}\right]. \qquad (2.73)$$

З урахуванням отриманих співвідношень інформативний сигнал приймача

$$I_c = I_0 - I_\xi = F \cdot T \cdot \log_2 (P_c + P_\xi) - F \cdot T \cdot \log_2 P_\xi = F \cdot T \cdot \log_2 \left(1 + \frac{P_c}{P_\xi}\right), \qquad (2.74)$$

що цілком відповідає отриманим раніше співвідношенням. З урахуванням питомої потужності завади, розглянутої вище, і співвідношення

$$\frac{P_c}{P_\xi} = \frac{E_c}{F_k \cdot T_k \cdot P_\xi}, \qquad (2.75)$$

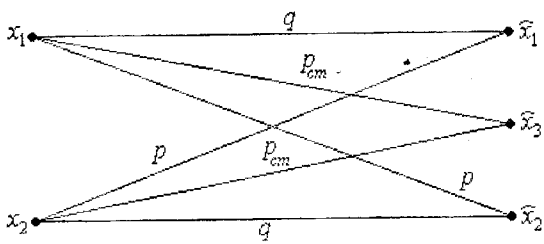


Рисунок 2.5 – Граф двійкового каналу зв'язку

визначивши добуток $F_k \cdot T_k = B$ як ***базу сигналу*** каналу зв'язку, можна отримати

$$C = B \cdot \log_2 \left(1 + \frac{E_c}{B \cdot G_0}\right). \qquad (2.76)$$

Для ***дискретного каналу із стиранням*** введення зони невизна-

ченості не ліквідує спотворення символу, а лише зменшує його імовірність. Якщо символи джерела повідомлення рівноімовірні, то для двійкової системи граф буде мати вигляд, поданий на рис. 2.5. Імовірність безпомилкового передавання $q = 1 - p - p_{cm}$. Для цього випадку

$$p(\hat{x}_1) = p(x_1)\cdot p(\hat{x}_1/x_1) + p(x_2)\cdot p(\hat{x}_1/x_2) = \frac{q}{2} + \frac{p}{2} = \frac{1-p_{cm}}{2} = p(\hat{x}_2), \qquad (2.77)$$

$$p(\hat{x}_3) = p(x_1)\cdot p(\hat{x}_3/x_1) + p(x_2)\cdot p(\hat{x}_3/x_2) = \frac{p_{cm}}{2} + \frac{p_{cm}}{2} = p_{cm}, \qquad (2.78)$$

$$H(\hat{X}) = -\sum_{i=1}^{3} p(x_i)\cdot \log_2 p(\hat{x}_i) = -2\cdot \frac{1-\frac{p_{cm}}{2}}{2}\cdot \log_2 \frac{1-p_{cm}}{2} - p_{cm}\cdot \log_2 p_{cm} =$$
$$= (1-p_{cm})\cdot\left(1 - \log_2(1-p_{cm}) - p_{cm}\cdot \log_2 p_{cm}\right). \qquad (2.79)$$

Умовна ентропія

$$H(\hat{X}/X) = \sum_{j=1}^{2}\sum_{i=1}^{3} p(x_j)\cdot p(\hat{x}_j/x_i)\cdot \log_2 p(\hat{x}_j/x_i) =$$
$$= -2\cdot \frac{q\cdot \log_2 q + p\cdot \log_2 p + p_{cm}\cdot \log_2 p_{cm}}{2} =$$
$$= q\cdot \log_2 q + p\cdot \log_2 p + p_{cm}\cdot \log_2 p_{cm}. \qquad (2.80)$$

Тоді

$$C = (1-p_{cm})\cdot\left(1 - \log_2(1-p_{cm})\right) + q\cdot \log_2 q + p\cdot \log_2 p. \qquad (2.81)$$

Якщо підставити $p_{cm} = 0$, то можна отримати пропускну здатність для каналу без стирання. Введення зони стирання знижує пропускну здатність каналу зв'язку, якщо рівень завад низький ($C \to (1-p_{cm})$ для $p = 0$). Канал зі стиранням доцільно організовувати, якщо вдається забезпечити $p << p_{cm}$.

Література

1. Советов Б.Я. Теория информации (теоретические основы передачи информации в АСУ) / Учебн. пос. – Л.: Изд-во Ленингр. ун-та, 1977. – С. 73 – 77.
2. Кузьмин И.В., Кедрус В.А. Основы теории информации и кодирования / Учебн. пос. – К.: Вища школа, 1986. – С. 120 – 129.

2.6 Наближення швидкості передавання інформації до пропускної здатності каналу зв'язку

До складу пропускної здатності згідно (2.67) входять дві складові: $H(\hat{X})$ та $H(\hat{X}/X)$, виходячи з чого можливі два методи підвищення швидкості передавання до потенційного значення пропускної здатності каналу.

Максимальне значення безумовної ентропії прийнятих символів $H_{\max}(\hat{X})$ можна отримати, забезпечуючи їх рівноімовірність, якщо джерело повідомлення цього забезпечити не може.

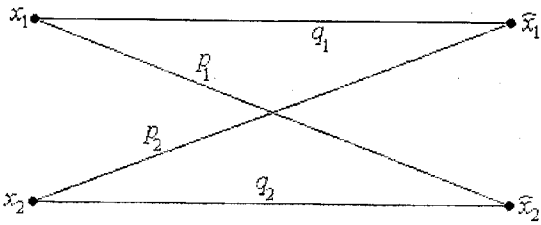


Рисунок 2.6 – Граф двійкового несиметричного каналу зв'язку

Для двійкового несиметричного каналу (рис. 2.6) ентропія $H(\hat{X})$ набуває максимального значення $H_{\max}(\hat{X})=1$ за умови $p_1(\hat{X})=p_2(\hat{X})$, тобто

$$p(x_1)\cdot p(\hat{x}_1/x_1)+p(x_2)\cdot p(\hat{x}_1/x_2)=p(x_1)\cdot p(\hat{x}_2/x_1)+p(x_2)\cdot p(\hat{x}_2/x_2)=$$
$$=p(x_1)\cdot q_1+p(x_2)\cdot p_2=p(x_1)\cdot p_1+p(x_2)\cdot q_2, \qquad (2.82)$$

звідки імовірності спотворення символу та безпомилкового приймання:

$$p_1=\frac{1}{2}+\frac{p(x_2)}{p(x_1)}\left(p_2-\frac{1}{2}\right), \qquad (2.83)$$

$$q_1=\frac{1}{2}+\frac{p(x_2)}{p(x_1)}\left(\frac{1}{2}-p_2\right). \qquad (2.84)$$

З отриманих виразів видно, що за умови рівноімовірності вхідних символів $p(x_1) = p(x_2)$ виконується $p_1 = p_2$, тобто максимум ентропії забезпечується для симетричного каналу. Якщо вхідні символи приймача нерівноімовірні $p(x_1) \neq p(x_2)$, то забезпечення умови $p_1 = p_2$ можна здійснити вибором порогів ідентифікації символів. Їх чисельне значення можна встановити, якщо відомі закони розподілу завади та завади і сигналу.

Другим методом є забезпечення мінімуму умовної ентропії $H(\hat{X}/X)$, яка визначається

$$H(\hat{X}/X) = -\sum_{j=1}^{K}\sum_{i=1}^{K} p(x_j)\cdot p(\hat{x}_i/x_j)\cdot \log_2 p(\hat{x}_i/x_j) =$$
$$= -p(x_1)\cdot(p_1\cdot\log_2 p_1 + q_1\cdot\log_2 q_1) - p(x_2)\cdot(p_2\cdot\log_2 p_2 + q_2\cdot\log_2 q_2) =$$
$$= p(x_1)\cdot H_1 + p(x_2)\cdot H_2, \qquad (2.85)$$

де $H_1 = p_1\cdot\log_2 p_1 + q_1\cdot\log_2 q_1$ – ентропія передавання символу x_1;

$H_2 = p_2\cdot\log_2 p_2 + q_2\cdot\log_2 q_2$ – ентропія передавання символу x_2;

Якщо символи x_1 та x_2 рівноімовірні, то залежності $H_1(p_1)$ та $H_2(p_2)$ відповідають рис. 2.1. За цієї умови $H(\hat{X}/X) = (H_1 + H_2)/2$. Оскільки умовна ентропія показує інформаційний внесок завади, то робочу точку p_0 необхідно вибирати поблизу нуля. Для оцінювання залежності умовної ентропії $H(\hat{X}/X)$ від імовірностей p_1 та p_2 доцільно розкласти функції H_1 і H_2 в ряд Тейлора в околі точки p_0, обмежуючись першими двома членами:

$$H_1 = H_0 + \Delta p_1\cdot\left.\frac{dH_1}{dp}\right|_{p=p_0} \text{ та } H_2 = H_0 + \Delta p_2\cdot\left.\frac{dH_2}{dp}\right|_{p=p_0}, \qquad (2.86)$$

звідки

$$H(\hat{X}/X) = H_0 + \frac{\Delta p_1 + \Delta p_2}{2}\cdot\left.\frac{dH}{dp}\right|_{p=p_0}. \qquad (2.87)$$

Оскільки похідна dH/dp додатна в точці p_0, то необхідно забезпечити максимум приросту $\Delta p_1 + \Delta p_2$, який виникає при зміні порогу ідентифікації сигналу в приймачі. При передаванні інформації каналом із шумом розподіл завади при відсутності сигналу $w(x)$ та спільний розподіл інформативного сигналу амплітудою U_c і завади $w_U(x)$ можуть бути для випадків симетричності та несиметричності. В першому з них (рис. 2.7):

$$p_1 = p(\hat{x}_2/x_1) = p(1/0) = \int_X^{\infty} w(x)dx, \qquad (2.88)$$

$$p_2 = p(\hat{x}_1/x_2) = p(0/1) = \int_{-\infty}^{X} w_U(x)dx. \qquad (2.89)$$

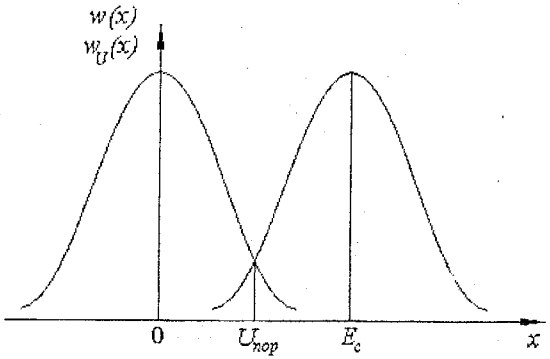


Рисунок 2.7 – Функції розподілу імовірностей для випадку симетричності

При збільшенні порога ідентифікації, тобто зсуві величини X вправо, $\Delta p_1 < 0$, а $\Delta p_2 > 0$. Оскільки $|\Delta p_2| > |\Delta p_1|$, то $\Delta p = \Delta p_1 + \Delta p_1 > 0$, тобто умовна ентропія збільшується. При зменшенні X, $\Delta p_2 < 0$, а $\Delta p_1 > 0$, а оскільки $|\Delta p_1| > |\Delta p_2|$, то $\Delta p = \Delta p_1 + \Delta p_1 > 0$, тобто і в цьому випадку умовна ентропія збільшується. Її мінімум визначається точками перетину кривих розподілу $w(x)$ та $w_U(x)$.

Якщо інформативні символи передаються прямокутними імпульсами, а в каналі наявний нормальний шум, то, як показано вище,

$$w(x) = \frac{1}{\sqrt{2\pi\sigma_\xi}} \cdot \exp\left(-\frac{x^2}{2\sigma_\xi^2}\right), \qquad (2.90)$$

$$w_U(x) = \frac{1}{\sqrt{2\pi\sigma_\xi}} \cdot \exp\left(-\frac{(x-U_c)^2}{2\sigma_\xi^2}\right). \qquad (2.91)$$

В цьому випадку поріг ідентифікації потрібно вибирати на рівні половини амплітуди інформативного сигналу $X = U_c/2$.

Несиметричність розподілів (рис. 2.8) властива реальним ситуаціям, коли на вході приймача використовуються смугові фільтри, закон розподілу завади відрізняється від нормального, а також іншим.

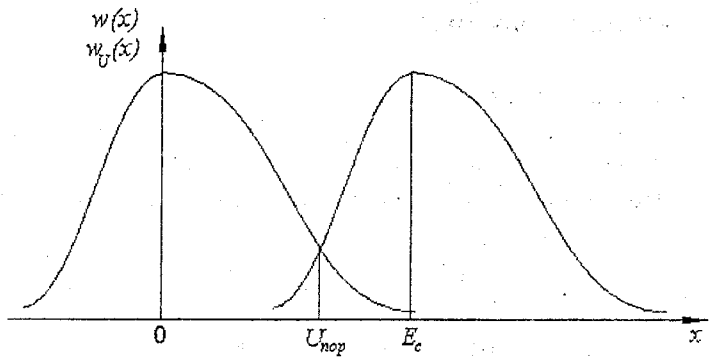


Рисунок 2.8 – Функції розподілу імовірностей
для випадку несиметричності

Але і в цьому випадку необхідно поріг ідентифікації вибирати за точкою перетинання кривих розподілу $w(x)$ та $w_U(x)$.

Література

1. Советов Б.Я. Теория информации (теоретические основы передачи информации в АСУ) / Учебн. пос. – Л.: Изд-во Ленингр. ун-та, 1977. – С. 77 – 81.
2. Кузьмин И.В., Кедрус В.А. Основы теории информации и кодирования / Учебн. пос. – К.: Вища школа, 1986. – С. 120 – 129.
3. Теория электрической связи [Электронный ресурс]– Режим доступу: http://www.mtuci.ru/cde/courses/tes/tes.oc.html

3 Методи кодування

3.1 Системи числення

Методика побудови кодів тісно пов'язана з відповідними системами числення. Побудова системи числення залежить від її основи, тобто кількості цифр, з яких можна одержати будь-яке число.

Так, десяткова система базується на цифрах від 0 до 9, двійкова – 0 та 1, вісімкова – від 0 до 7, шістнадцяткова – на цифрах від 0 до 9 та літерах A, B, C, D, E, F. В табл. 3.1 наведено співвідношення чисел у різних системах числення.

Таблиця 3.1 - Співвідношення чисел

Десяткова	Двійкова	Вісімкова	Шістнадцяткова
0	0000	00	00
1	0001	01	01
2	0010	02	02
3	0011	03	03
4	0100	04	04
5	0101	05	05
6	0110	06	06
7	0111	07	07
8	1000	10	08
9	1001	11	09
10	1010	12	0A
11	1011	13	0B
12	1100	14	0C
13	1101	15	0D
14	1110	16	0E
15	1111	17	0F
16	10000	20	10

Системи числення визначають коди на всі сполучення. Найбільше десяткове число, яке можна представити n-розрядним числом у системі числення з основою a, дорівнює $(a^n - 1)$. При цьому для його подання необхідно по a різних цифр на кожний розряд, тобто $в = n \cdot a$ цифр. В той самий час кількість чисел, які можна представити в системі з основою a, розташовуючи по $в$ цифр, визначається $a^{в/n}$. Вона сягає максимуму за умови рівності a експоненті e, що вказує, що для кодування найбільш привабливою буде трійкова система, а двійкова – трохи гіршою. Всі інші системи числення значно програють у продуктивності побудови кодів.

Література

1. Кодирование информации. Двоичные коды / под ред. Березюка Н.Т. – Харьков: Издательство при Харьковском государственном университете, 1978. – С. 5 – 7.
2. Тутевич В.Н. Телемеханика. – М.: Высшая школа, 1985. – С. 50 – 55.
3. Компьютеры / под ред. Хелмса Г.- М.: Мир, 1986, т. 1. – С. 49 – 53.
4. Васюра А.С. та ін. Техніка передавання дискретної інформації. – Вінниця: ВДТУ, 1998. – С. 56 – 57.

3.2 Класифікація кодів

В сучасних комп'ютерних системах здійснюється передавання дискретної інформації, що забезпечується формуванням відповідних дискретних сигналів, які відрізняються за однією або декількома ознаками. Виходячи з цього, набір елементів коду розглядають як ***алфавіт***, а їх певні сукупності – як ***кодові комбінації***.

Код – множина символів в деякому алфавіті, поставлена у взаємно однозначну відповідність з початковою множиною символів.

Кодування – встановлення відповідності між елементом початкових даних і кінцевою сукупністю символів, що називається кодовою комбінацією.

Перетворення повідомлень на кодові комбінації дозволяє забезпечити:

- передавання необхідної кількості різних повідомлень за допомогою комбінації з n елементів, які мають l кодових ознак;
- узгодження параметрів каналу зв'язку і повідомлень, що ним передаються;
- підвищення вірогідності передавання повідомлень;
- раціональне використання лінії зв'язку з урахуванням розподілу на канали;
- часткове або повне криптографічне закриття інформації.

Вибір методів кодування, які забезпечують виконання перерахованих задач, є складною проблемою, розв'язання якої залежить від обсягу повідомлення, що передається; параметрів каналу зв'язку; необхідної вірогідності передавання; можливостей апаратної та програмної реалізації тощо. Але основним показником є досягнення максимальної ефективності використання каналу при забезпеченні заданої вірогідності.

На рис. 3.1 наведені основні характеристики, за якими формуються кодові комбінації. Одиничний (число-імпульсний) код характеризується наявністю лише одного елемента, а кодові комбінації відрізняються їх кількістю. Кодові комбінації двійкового коду відзначаються наявністю двох інформативних елементів, а якщо їх більше двох, то код – багатопозиційний. Кількість використовуваних елементів називається ***основою коду***.

За кількістю розрядів кодові комбінації можуть мати їх постійну кількість (рівномірні коди) або неоднакову, коли довжина кожної комбінації вибирається залежно від зовнішніх чинників. Прикладом побудови нерівномірного коду може бути оптимальний, побудований для узгодження джерела і каналу зв'язку (п. 2.2).

В залежності від використовуваної кількості кодових комбінацій можуть бути побудовані коди, де задіяні всі можливі комбінації при заданій кількості розрядів (***коди на всі сполучення***), або коди, які використовують їх лише частково.

Для передавання інформації можуть використовуватися різні ознаки посилань інформативних сигналів (амплітуда, полярність, частота, фаза, тривалість), але в сучасних системах використовуються і комбіновані методи (амплітуда + фаза), які забезпечують передавання одним імпульсом двох, трьох або чотирьох бітів (вісім градацій фази та дві амплітудні). Зрозуміло, що це суттєво підвищує швидкість передавання.

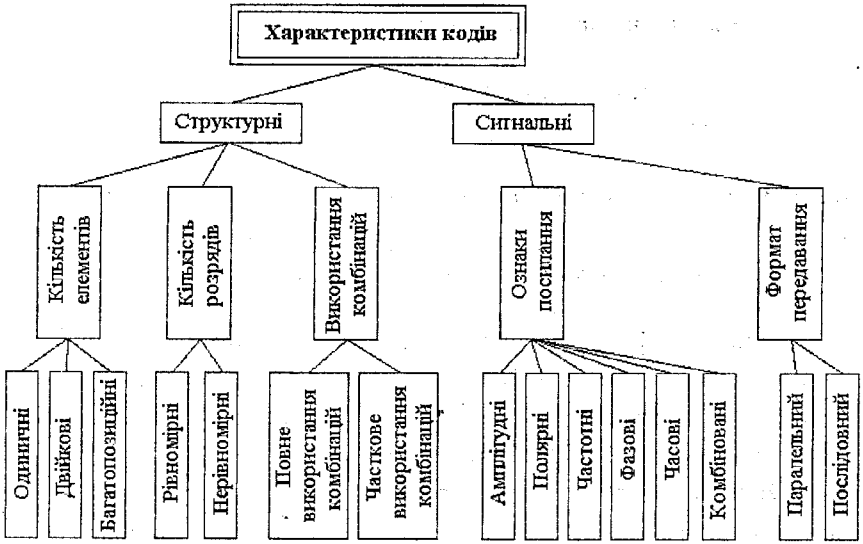


Рисунок 3.1 – Характеристики кодів

У послідовному форматі як всі елементи, так і кодові комбінації передаються каналом зв'язку послідовно в часі. При паралельному форматі кожному розряду виділяється окрема лінія і передавання здійснюється одночасно.

В наш час найбільш ефективними вважаються трійкові коди (0, –1, +1), хоча найчастіше використовують двійкові. Це пов'язано з розвиненим математичним апаратом двійкової логіки, її використанням у комп'ютерній техніці та простотою реалізації.

Література

1. Кодирование информации. Двоичные коды / под ред. Березюка Н.Т. – Харьков: Издательство при Харьковском государственном университете, 1978. – С. 32 – 36.
2. Тутевич В.Н. Телемеханика. – М.: Высшая школа, 1985. – С. 47 – 53.
3. Васюра А.С. та ін. Техніка передавання дискретної інформації. – Вінниця: ВДТУ, 1998. – С. 56.

3.3 Кодова метрика Хеммінга. Теоретичні засади виправлення помилок при використанні кодів

З курсу вищої математики вже відомі використані нижче терміни та означення.

Арифметичний n-вимірний лінійний простір F^n над полем F – множина всіх наборів $\mathbf{X} = (x_1, ..., x_n)$, $x_i \in F$ довжини n, які називають ***векторами лінійного простору*** (елементи x_i – ***координати вектора***).

Це означення передбачає виконання двох операцій:

- ✓ додавання: сумою векторів $\mathbf{X} = (x_1, ..., x_n)$ та $\mathbf{Y} = (y_1, ..., y_n)$ є такий вектор $\mathbf{Z} = (z_1, ..., z_n)$, що $z_i = x_i + y_i$, тобто при додаванні векторів відбувається додавання відповідних координат;
- ✓ множення на константу: добуток вектора $\mathbf{X} = (x_1, ..., x_n)$ на число $\alpha \in F$ визначається як вектор $\mathbf{Z} = (z_1, ..., z_n)$ такий, що $z_i = \alpha \cdot x_i$, тобто при множенні вектора на число з поля кожна координата множиться на це число.

Нульовим вектором у просторі F^n є вектор $\mathbf{0} = (0, ..., 0)$. Якщо скалярний добуток векторів $(\mathbf{X}, \mathbf{Y}) = x_1 \cdot y_1 + \ldots + x_n \cdot y_n = 0$, то вектори $\mathbf{X}$ та $\mathbf{Y}$ є ортогональними. Якщо для кожної пари векторів $\mathbf{X}$ та $\mathbf{Y}$ лінійного простору визначено число $d(\mathbf{X}, \mathbf{Y})$, яке задовольняє умови:

$d(\mathbf{X}, \mathbf{Y}) > 0$ при $x_i \neq y_i$ та $d(\mathbf{X}, \mathbf{X}) = 0$ для будь-якого $\mathbf{X}$;

$d(\mathbf{X}, \mathbf{Y}) = d(\mathbf{Y}, \mathbf{X})$;

$d(\mathbf{X}, \mathbf{Z}) \leq d(\mathbf{X}, \mathbf{Y}) + d(\mathbf{Y}, \mathbf{Z})$ для будь-яких $\mathbf{X}, \mathbf{Y}, \mathbf{Z}$,

то для цього лінійного простору введена метрика. Так, у речовинному n-вимірному арифметичному просторі R^n можна ввести метрику, визначивши відстань $d(\mathbf{X}, \mathbf{Y})$ між цими векторами як $d(\mathbf{X}, \mathbf{Y}) = \sum_{i=1}^{n} |x_i - y_i|$. Для цього простору відома евклідова метрика

$$d(\mathbf{X}, \mathbf{Y}) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2}. \qquad (3.1)$$

В теорії двійкового кодування основну роль відіграє лінійний арифметичний простір $GF(2^n)$ над полем з двох елементів $GF(2) = \{0, 1\}$. Згідно з означенням, простір $GF(2^n)$ складається з n наборів, які вміщують нулі та одиниці. Таким чином, кожна n-розрядна двійкова кодова комбінація являє собою вектор у просторі $GF(2^n)$. Хеммінг визначив відстань $d(\mathbf{X}, \mathbf{Y})$ у просторі $GF(2^n)$ як кількість позицій, у яких координати векторів $\mathbf{X}$ та $\mathbf{Y}$ не збігаються. Така відстань задовольняє вищевказані умови і є природною мірою різниці між двома n-розрядними кодовими комбінаціями, що зображаються векторами $\mathbf{X}$ та $\mathbf{Y}$. Ця метрика лінійного простору $GF(2^n)$ отримала назву ***метрики Хеммінга.*** В теорії кодування важливу роль відіграє число $d(0, \mathbf{X}) = w(\mathbf{X})$, яке називається ***вагою кодової комбінації*** X. Таким чином, вага $w(\mathbf{X})$ дорівнює кількості координат вектора $\mathbf{X}$, які відрізняються від нуля. Відстань Хеммінга, згідно з операцією додавання векторів $d(\mathbf{X} + \mathbf{Z}, \mathbf{Y} + \mathbf{Z}) = d(\mathbf{X}, \mathbf{Y})$, для будь-яких векторів $\mathbf{X}, \mathbf{Y}, \mathbf{Z} \in GF(2^n)$, а відповідно $d(\mathbf{X}, \mathbf{Y}) = w(\mathbf{X} + \mathbf{Y})$ для будь-яких $\mathbf{X}$ та $\mathbf{Y}$.

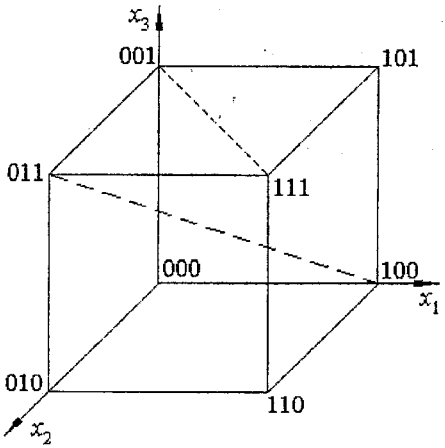


Рисунок 3.2 – Геометрична модель тирозрядного двійкового коду

Часто вектори n-вимірного простору $GF(2^n)$ зображують у вигляді вершин правильного багатогранника із одиничними ребрами, кожна вершина якого визначає набір одиниць та нулів. На рис. 3.2 зображена тривимірна модель двійкового коду, для якої відстань Хеммінга між векторами $\mathbf{X}$ та $\mathbf{Y}$ визначається як найкоротший шлях, який пролягає ребрами куба і з'єднує відповідні вершини.

Характеристикою помилок, що виникають в дискретному каналі, може виступати вектор $\mathbf{e}$, який записується у вигляді вектора тієї самої розрядності, що й кодові комбінації. Нулі в координатах вектора $\mathbf{e}$ показують, що спотворення у відповідних позиціях не відбуваються. Таким чином, вага вектора

$w(\mathbf{e})$ характеризує кратність помилок g. Прийнята кодова комбінація $\hat{X}$ отримується додаванням переданої кодової комбінації X із вектором помилки за модулем 2: $\hat{X} = X \oplus e$. Для того, щоб одна з дозволених кодових комбінацій не перетворювалась на іншу, необхідно щоб відстань Хеммінга між дозволеними комбінаціями була тим більшою, чим більша кратність помилок g. Оскільки відстані між дозволеними кодовими комбінаціями неоднакові, найбільш критичною буде найменша для даного коду відстань, яку за Хеммінгом називають ***кодовою відстанню***. Чим більшою є кодова відстань d, тим прийнята кодова комбінація буде схожою більше на передану, ніж на будь-яку іншу з дозволених. Найбільш простою є ситуація для двійкового симетричного каналу без пам'яті, для якого імовірність помилки кратності g визначається формулою Бернуллі

$$p_g = C_n^g \cdot p^g \cdot q^{n-g}, \tag{3.2}$$

де p – імовірність спотворення елементарного сигналу.

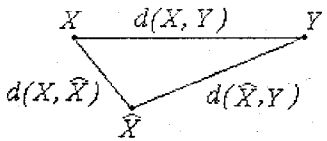


Рисунок 3.3 – Корегувальна здатність коду

Оскільки $p < 0{,}5$, імовірність $(g + 1)$-кратної помилки менша від імовірності g-кратної при $g < n/2$, тому в першу чергу необхідно виявляти і вилучати помилки малої кратності.

Якщо передана кодова комбінація X, а прийнята $\hat{X}$ (рис. 3.3), а при цьому пройшла t-кратна помилка, то $d(X, Y) = t$. Будь-яка інша дозволена комбінація даного коду Y пов'язана із переданою і прийнятою правилом трикутника

$$d(\hat{X},Y) \geq d(X,Y) - d(\hat{X},X) = d(X,Y) - t. \tag{3.3}$$

Якщо для будь-якої комбінації $d(\hat{X},Y) > 0$, то помилка (прийняття кодової комбінації Y) завжди визначається. Виходячи з цього необхідною і достатньою умовою визначення всіх t-кратних помилок є виконання умови $d(\hat{X},X) - t > 0$, а з урахуванням визначення кодової відстані, $d > t$. Для виправлення всіх t-кратних помилок необхідно і достатньо, щоб

$d(\hat{X},X) > d(\hat{X},X) = t$ або $d > 2t$. Для одночасного виявлення r і виправлення s помилок обов'язковою умовою є

$$d \geq r + s + 1 \ (r \geq s). \qquad (3.4)$$

Вже згадані коди на всі сполучення мають кодову відстань $d = 1$, тому виявляти і виправляти помилки вони не можуть.

Розглядаючи кодову комбінацію $\hat{X}$ як спотворену помилками під час передавання каналом зв'язку кодову комбінацію X з вектором помилок $\mathbf{e}$, можна отримати $\hat{\mathbf{X}} = \mathbf{X} + \mathbf{e}$, а з урахуванням умови $d(\mathbf{X}, \mathbf{Y}) = w(\mathbf{X} + \mathbf{Y})$

$$d(\hat{X},X) = w(X \oplus X) = w(X \oplus X \oplus e) = w(e), \qquad (3.5)$$

тобто відстань між прийнятою і переданою кодовими комбінаціями дорівнює вазі вектора помилки. Оскільки для симетричного каналу без пам'яті імовірність помилки (перетворення кодової комбінації X на кодову комбінацію Y) зменшується зі збільшенням відстані $d(\mathbf{X}, \mathbf{Y})$ або ваги $w(\mathbf{e})$ помилки, формування кодових комбінацій необхідно здійснювати таким чином, щоб між будь-якою парою кодових комбінацій відстань була максимальною.

Найменша імовірність помилки ідентифікації прийнятої кодової комбінації забезпечується використанням критерію максимальної правдоподібності: кожна прийнята кодова комбінація $\hat{X}$ ототожнюється з тією кодовою комбінацією, для якої виконується умова максимальної апостеріорної імовірності $p(X/\hat{X}) = p(\hat{X}/X)$. Для дискретних каналів без пам'яті при $p < 0{,}5$ ця умова відповідає принципу ідентифікації за мінімумом відстані Хеммінга. Оскільки найбільш імовірні помилки малої кратності, то доцільно ототожнювати прийняту кодову комбінацію з тією дозволеною, яка відрізняється найменше (має найменшу відстань Хеммінга). Реалізація цього алгоритму наведена на рис. 3.4. Він передбачає зберігання приймачем всього переліку кодових слів і здійснення їх перебору з метою визначення $\mathbf{e}_{min}$. Ця процедура для сучасних технічних засобів не є складною, враховуючи їх високу обчислювальну продуктивність. Використання ж мікропроцесорних засобів передбачає байтовий формат даних джерела,

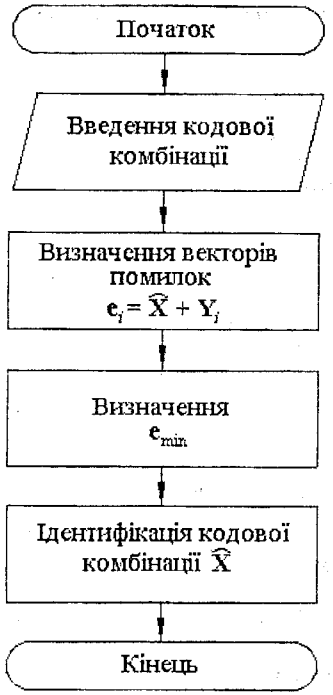


Рисунок 3.4 – Ідентифікація кодової комбінації

тобто кількість кодових комбінацій навряд чи перевищує 256 для більшості алгоритмів кодування.

Разом з тим, забезпечення високої вірогідності передавання інформації вимагає реалізації заходів організаційного і технічного характеру для покращення характеристик і параметрів каналів зв'язку (зменшення впливу завад), а також аналогічних заходів, спрямованих на покращення роботи приймача (збільшення об'єму сигналу та використання ефективніших методів передавання), аналізу і використання необхідних методів виявлення та виправлення помилок у прийнятій інформації. Для розв'язання третьої задачі використовують, в основному, три методи, які базуються на збільшенні надлишковості:

- використання кодів, що виправляють помилки;
- багаторазове передавання кодових комбінацій;
- синхронне передавання кодових комбінацій декількома каналами.

Використовують також їх комбінації, наприклад використання завадозахищених кодів та їх неодноразове передавання.

Під час передавання корегувальні коди використовують для виявлення та виправлення помилок. Швидкість передавання при цьому визначається співвідношенням кількості інформаційних символів k та загальною кількістю символів у кодовій комбінації n

$$C_p = C_n \cdot \frac{k}{n}, \tag{3.6}$$

тобто підвищення надлишковості зменшує швидкість передавання. Аналогічні співвідношення справедливі і для фізичної швидкості передавання v_p. Збільшення надлишковості може полягати також у створенні додаткових енергетичних рівнів, що теж знижує потенційну швидкість передавання.

При неоднократному передаванні кожна кодова комбінація передається декілька разів, а приймач здійснює порівняння прийнятих символів і здійснює ідентифікацію кожного з них мажоритарним методом (голосуванням). Відповідно, для прийняття рішення кількість передавань кожної кодової комбінації повинна бути непарною. Таким чином при триразовому передаванні інформації правильне рішення можливе, коли всі рази кодова комбінація прийнята правильно з імовірністю $p_{пр} = q^{3n}$ або коли вона правильно прийнята двічі, імовірність чого при незалежності символів складає $p_{пр} = C_3^2 \cdot q^{2n} \cdot p^n$. В останньому випадку взятий критичний випадок мінімальної імовірності, коли всі n розрядів один раз прийняті неправильно, що дає мінімальне значення $p_{пр}$. В загальному випадку при r-кратному повторюванні n-розрядної кодової комбінації імовірності помилок визначаються

$$p_{пом.r} = 1 - q^{r \cdot n} - \sum_{t=1=1}^{i=j=\frac{r+1}{2}} \sum_{j=r-1}^{t=\frac{r-1}{2}} C_r^j \cdot q^{(r-i)k} \cdot \left(1 - q^k\right)^i . \qquad (3.7)$$

Так, при $n = 5$, $r = 3$, $p_0 = 10^{-2}$ $p_{пом.1} = 1 - (1 \div 10^{-2})^5 \approx 5 \cdot 10^{-2}$, а $p_{пом.3} = 1 - (1 \div 10^{-2})^{15} - 5 \cdot (1 \div 10^{-2})^{10} \cdot ((1 \div 10^{-2})^5) \approx 7 \cdot 10^{-3}$, тобто при триразовому повторенні імовірність помилки знижується приблизно в 7 разів порівняно з одноразовим передаванням. Разом з тим швидкість передавання відповідно знижується в r разів.

Метод синхронного передавання кодових комбінацій декількома каналами за алгоритмом роботи, принципом ідентифікації прийнятої комбінації і можливостями аналогічний вже розглянутому за умови незалежності помилок в різних каналах. Це дозволяє скоротити час передавання, але за умови зберігання об'єму сигналу збільшується кількість каналів. Крім цього, умова незалежності помилок вимагає розташування каналів в різних лініях зв'язку, а також збільшення паузи між передаваннями окре-

мих блоків даних. Таким чином, виграш виявляється значно меншим, ніж здається, а програмні і апаратні витрати зростають дуже суттєво.

Комбінація методу багаторазового передавання з використанням надлишкового коду полягає в тому, що кожна комбінація передається r разів, а ті з них, у яких виявлені помилки, витираються з пам'яті. Імовірність правильного приймання кодової комбінації $p_{пр.п}^{(r)}$ та невизначеної помилки $p_{нв.п}^{(r)}$ відповідно дорівнюють

$$p_{пр.п}^{(r)} = p_{пр.п} \cdot \frac{1 - p_{в.п}^{r}}{1 - p_{в.п}}, \tag{3.8}$$

$$p_{нв.п}^{(r)} = p_{нв.п} \cdot \frac{1 - p_{в.п}^{r}}{1 - p_{в.п}}, \tag{3.9}$$

де $p_{пр.п}$ – імовірність правильного приймання n-розрядної кодової комбінації при одноразовому передаванні;

$p_{в.п}$ – імовірність виявлення помилки у n-розрядній кодовій комбінації при одноразовому передаванні;

$p_{нв.п}$ – імовірність невизначеної помилки у n-розрядній кодовій комбінації при одноразовому передаванні.

Швидкість передавання інформації для таких систем визначається виразом

$$C_p = C_n \cdot \frac{k}{r \cdot n}, \tag{3.10}$$

тобто швидкість додатково знижується за рахунок надлишковості кодової комбінації.

Задачу побудови надлишкового коду можна сформулювати залежно від мети передавання інформації, призначення комп'ютерної системи та інших чинників:

- при заданих кількості кодових комбінацій N та їх довжині n сформувати код з найбільшим значенням кодової відстані d, тобто код, який забезпечує максимальну завадозахищеність при заданій надлишковості;
- при заданих кількості кодових комбінацій N та кодовій відстані d знайти код мінімальної довжини n, тобто код який забезпечує мінімальну надлишковість при заданій завадозахищеності;

- при заданих довжині кодових комбінацій n та кодової відстані d побудувати код з найбільшою кількістю кодових комбінацій N, тобто код, який забезпечує максимальну ефективність при заданій завадозахищеності тощо.

На жаль, до теперішнього часу не існує алгоритмів розв'язання, які давали б чітку відповідь на поставлену задачу і дозволяли б згідно з розробленою методикою вибирати алгоритм кодування і формувати кодові комбінації, а також пов'язувати між собою вказані параметри. Так, Хеммінг запропонував співвідношення

$$N \le \frac{2^n}{\sum_{i=0}^{\text{int}(d)} C_n^i}, \tag{3.11}$$

де int(d) – операція округлення до меншого цілого значення.

Коди, для яких нерівність (3.11) обертається на рівність, називають ***щільно спакованими***. Такі коди характеризують третю з перерахованих вище задач, оскільки мають максимальну кількість комбінацій серед всіх, що виправляють t помилок. Сама нерівність (3.11) отримала назву ***нижньої межі (оцінки) Хеммінга***. Вона не означає, що існує код із заданими кількістю кодових комбінацій N та кодовою відстанню d, а те, що при невиконанні умови коду точно не існує.

У випадку

$$N \ge \frac{2^n}{\sum_{i=0}^{d-2} C_{n-1}^i} \tag{3.12}$$

при заданих довжині кодових комбінацій n та кодової відстані d існує код з кількістю кодових комбінацій не менше N. Вираз (3.12) отримав назву ***верхньої межі (оцінки) Варшамова***. Інша верхня оцінка, запропонована Гілбертом:

$$N \ge \frac{2^n}{\sum_{i=0}^{d-1} C_n^i}. \tag{3.13}$$

Так само не вирішена задача побудови коду із заданою корегувальною здатністю за рахунок внесення такої надлишковості, яка забезпечила б кодову відстань не менше d. Існує лише ряд верхніх та нижніх меж (оцінок), які визначають кількість перевірних символів m:

Хеммінга – $m \geq \log_2\left(1+\sum_{i=1}^{\frac{d-1}{2}} C_n^i\right)$; (3.14)

Плоткіна – $m \geq 2d-2-\log_2 d$; (3.15)

Елайєса – $m \geq \log_2 C_n^j - \log_2 d$, де $j = 0{,}5 \cdot n \cdot \left(1-\sqrt{1-\frac{2\cdot(d-1)}{2}}\right)$; (3.16)

Варшамова-Гілберта – $m \geq \log_2\left(1+\sum_{i=1}^{d-1} C_n^i\right)$. (3.17)

Експериментально доведено що найближчі значення дає оцінка Варшамова-Гілберта. Для кодів з $d = 3$ отримано точне співвідношення між кількістю перевірних символів m та довжиною коду n:

$$m \geq \log_2(n+1). \tag{3.18}$$

Імовірність приймання n-розрядної кодової комбінації з s та більше помилками (оцінка Пуртова) необхідна для розрахунку імовірності, що забезпечується завадозахищеними кодами і системами передавання дискретної інформації, але ця формула не може використовуватися для каналів з незалежними помилками:

$$p(s,n) = n^{1-\alpha} \cdot p \cdot \prod_{i=2}^{s} \frac{\left(\frac{i-1}{n}\right)^{1-\alpha} - \frac{i-1}{n}}{\left(\frac{i}{n}\right)^{1-\alpha} - \frac{i-1}{n}}, \tag{3.19}$$

де α – коефіцієнт, який враховує групування помилок і залежить від видів каналу і модуляції, $\alpha = 0{,}32 \div 0{,}6$.

Література

1. Кодирование информации. Двоичные коды / под ред. Березюка Н.Т. – Харьков: Издательство при Харьковском государственном университете, 1978. – С. 32 – 36.

2. Тутевич В.Н. Телемеханика. – М.: Высшая школа, 1985. – С. 62 – 65.
3. Васюра А.С. та ін. Техніка передавання дискретної інформації. – Вінниця: ВДТУ, 1998. – С. 63.
4. Шварцман В.О., Емельянов Г.А. Теория передачи дискретной информации. – М.: Связь, 1979. – С. 250 – 254, 262 – 270.
5. Квєтний Р.Н., Компанець М.М., Кривогубченко С.Г., Кулик А.Я. Основи техніки передавання інформації / Підручник. – Вінниця: Універсум-Вінниця, 2002. – С. 192.
6. Кузьмин И.В., Ключко В.И., Литвин В.А. Кодирование и декодирование в информационных системах. – К.: Выща школа, 1985. – С. 7 – 11.

3.4 Класифікація двійкових кодів

Для систематизації можна ввести класифікацію кодів за функціональними ознаками (рис. 3.5).

Рисунок 3.5 – Класифікація двійкових кодів за функціональними ознаками

Так всі коди можна розділити на:

- коди загального призначення;
- спеціалізовані;
- коди для передавання інформації.

До першої групи відносять двійкові, двійково-десяткові, код Грея тощо. До другої можна включити різноманітні штрих-коди, семисегментний, ASCII і т.п. Третю утворюють коди, призначені, в основному, для використання в системах та

пристроях передавання інформації.

З точки зору передавання інформації коди можна розділити на:

⇨ коди, які не визначають помилок;

⇨ коди, які визначають помилки;

⇨ коди, які виправляють помилки,

а з точки зору етапів передавання – на ***коди підготовки даних*** та ***канальні***.

Треба зазначити, що цей розподіл досить умовний, оскільки код може використовуватися не лише для класифікації та визначення предмета або чисельного значення вимірюваної величини, але й для передавання інформації до бази даних після відповідного перетворення формату.

На сьогоднішній день відома велика кількість кодів, призначених для передавання інформації. Їх досить складно систематизувати внаслідок великої кількості їх індивідуальних ознак. Тому доцільно використати визначені вище структурні характеристики. Всі коди можна розділити на дві самостійні групи (рис. 3.6).

До першої відносять коди, які використовують всі можливі комбінації, – ***коди на всі сполучення***, які ще називають ***простими*** або ***первинними***. З назви вже зрозуміло, що такі коди є безнадлишковими. До другої групи можна віднести коди, які використовують лише певну частину всіх можливих комбінацій – надлишкові. Та частина комбінацій, що відповідає умовам кодової відстані, не використовується для перетворення початкового повідомлення.

Обидві групи кодів, в свою чергу, поділяються на ***рівномірні***, всі кодові комбінації яких мають постійну кількість розрядів, та ***нерівномірні***, які вміщують кодові комбінації із різною кількістю розрядів. Серед надлишкових кодів нерівномірні не знайшли широкого використання внаслідок складності їх технічної реалізації.

Надлишкові коди можна розділити на два класи – неперервні та блокові. В ***неперервних*** процес кодування та декодування має неперервний характер. У ***блокових*** кожному повідомленню відповідає кодова комбінація (блок з n символів), причому блоки кодуються незалежно один від одного.

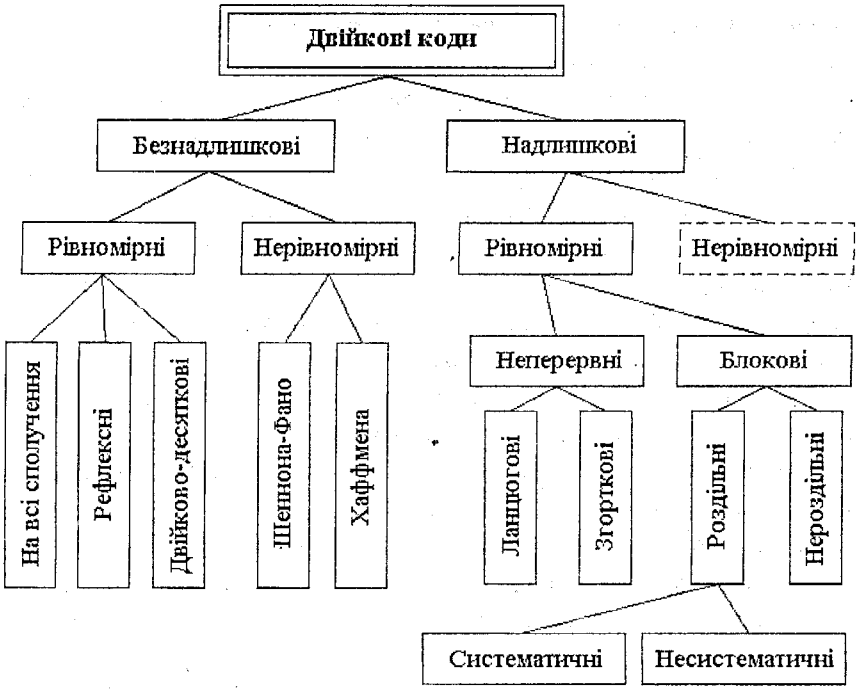


Рисунок 3.6 – Класифікація двійкових кодів за структурними ознаками

В деяких з таких кодів серед всіх розрядів кодової комбінації можна чітко виділити ***інформаційні***, призначені для вміщення даних початкового повідомлення, та ***контрольні***, призначені для визначення та виправлення помилок. Такі коди називають ***роздільними***. Як назва також використовується їх позначення, тому їх ще називають ***(n, k)-кодами***, причому, n визначає загальну кількість розрядів, а k – кількість інформаційних. ***Нероздільні*** коди не мають чіткого розподілу на інформаційні та контрольні розряди.

Серед роздільних блокових кодів можна також виділити несистематичні та систематичні. У ***несистематичних*** контрольні розряди, призначені для перевірки, являють собою суми підблоків з l розрядами, на які розділена послідовність інформаційних. До таких кодів належать коди Бергера. Найбільший клас розділимих блокових кодів складають ***систе-***

матичні, у яких перевірні символи є результатом лінійних операцій над інформаційними (всіма або частково).

Серед систематичних кодів окремою групою можна виділити ***циклічні***, які, крім всіх властивостей систематичних кодів, мають ще одну – якщо кодова комбінація належить коду, то циклічна перестановка символів формує кодову комбінацію, яка також належить цьому коду.

Оскільки у світі наукова робота зі створення нових алгоритмів кодування для вирішення нових задач продовжується, то не можна вважати наведену класифікацію універсальною. Прикладом цього є турбо-коди, публікації про які з'явились протягом останніх п'яти років.

Порівняння кодів, зазвичай, здійснюється за їх основними параметрами, що ілюструє їх різні кількісні та якісні показники. Ці параметри використовуються при виборі кодів, призначених для передачі, зберігання та оброблювання інформації: довжина коду; основа коду; потужність коду; повне число кодових комбінацій; кількість інформаційних символів; кількість перевірних символів; надлишковість коду; швидкість передавання; вага кодової комбінації; кодова відстань; вагова характеристика коду; імовірність невизначеної помилки; оптимальність коду; коефіцієнт помилкових переходів.

Довжина коду n – кількість розрядів (символів), що складають кодову комбінацію.

Основа коду a – кількість імпульсних ознак, використовуваних у кодових комбінаціях, що відрізняються одна від одної. Для випадку двійкових кодів $a = 2$. У двійкових кодах для визначення імпульсних ознак використовують цифри 0 та 1.

Потужність коду N_p – кількість кодових комбінацій (робочих кодових слів), використовуваних для передавання повідомлень.

Повна кількість кодових комбінацій N – число всіх можливих комбінацій, що дорівнює a^n (для двійкових кодів $N = 2^n$).

Кількість інформаційних символів k – кількість символів (розрядів) кодової комбінації, призначених для передачі саме повідомлення. Зрозуміло, що $N_p = a^n$, а для двійкового коду – $N_p = 2^n$.

Кількість перевірних символів m – кількість символів (розрядів) кодової комбінації, необхідних для корегування помилок. Цей параметр характеризує абсолютну надлишковість коду.

У теорії кодування під ***надлишковістю коду*** R розуміють відносну надлишковість, яка дорівнює відношенню кількості перевірних символів до довжини коду: $R = m/n$. Для більш загального випадку ця формула може бути зведена до вигляду

$$R = 1 - \frac{\log_m N_p}{\log_m N}. \qquad (3.20)$$

Швидкість передавання кодових комбінацій – відношення кількості інформаційних символів до довжини коду $C = k/n$. Оскільки $n = k + m$, то $C = 1 - R$.

Вага кодової комбінації (коду) w – кількість одиниць у кодовій комбінації. Наприклад, кодова комбінація 101100110 характеризується довжиною коду $n = 9$ і вагою $w = 5$.

Кодова відстань d – мінімальна кількість однойменних розрядів з різними символами.

Вагова характеристика коду $W(w)$ – кількість кодових комбінацій вагою w. Наприклад, для коду, що містить кодові комбінації 00000, 01110, 10101 і 11011, вагова характеристика $W(0) = 1$, $W(3) = 2$, $W(4) = 1$, тобто даний код складається з одного кодового слова ваги 0, двох слів ваги 3 і одного слова ваги 4.

Імовірність невизначеної помилки $p_{нв}$ – це ймовірність такої події, при якій прийнята кодова комбінація відрізняється від переданої, а властивості даного коду не дозволяють визначити факт наявності помилки.

Оптимальність коду – властивість такого коду, який забезпечує найменшу ймовірність невизначення помилки серед всіх кодів тієї ж довжини n і надлишковості R.

Коефіцієнт помилкових переходів

$$K_n(d) = \frac{1}{N_p} \sum_{i=1}^{N} \frac{N_{p.i}}{C_n^d}, \qquad (3.21)$$

де $N_{p.i}(d)$ – кількість робочих кодових комбінацій, що відстоять від i-тої кодової комбінації на відстань Хеммінга d;

характеризує частку помилок кратності d, яка не визначається. Для систематичних кодів всі кодові слова мають однаковий розподіл відстаней Хеммінга від інших слів, тому розподіл кодових відстаней для будь-якого слова можна визначити, використовуючи вагову характеристику систематичного коду. Коефіцієнт помилкових переходів у цьому випадку

$$K_n(w)=\frac{W(w)}{C_n^w}. \qquad (3.22)$$

Література

1. Кодирование информации. Двоичные коды / под ред. Березюка Н.Т. – Харьков: Издательство при Харьковском государственном университете, 1978. – С. 36 – 38.
2. Шварцман В.О., Емельянов Г.А. Теория передачи дискретной информации. – М.: Связь, 1979. – С. 270 – 272.
3. Квєтний Р.Н., Компанець М.М., Кривогубченко С.Г., Кулик А.Я. Основи техніки передавання інформації / Підручник. – Вінниця: Універсум-Вінниця, 2002. – С. 192.
4. Кузьмин И.В., Кедрус В.А. Основы теории информации и кодирования / Учебн. пос. – К.: Выща школа, 1986. – С. 78 – 79.

3.5 Коди без визначення помилок

До таких кодів відносять різні за функціональним призначенням коди, характерною властивістю яких є $d=1$.

Особливістю цього типу кодів є те, що у їх складі наявні кодові комбінації, які відрізняються одна від одної лише одним розрядом. Типовим кодом є двійковий. Коди зведені до табл. 3.2.

Кодові комбінації ***двійкового коду на всі сполучення*** відповідають запису натурального ряду чисел у двійковій системі числення.

Кодові комбінації ***одиничко-десяткового (число-імпульсного) коду*** відрізняються кількістю одиниць. Кожен розряд десяткового числа записується у вигляді відповідного числа одиниць. В такому випадку розря-

ди розподіляються по інтервалах. Якщо з одинично-десяткового нерівномірного коду одержати рівномірний додачею нулів до рівного числа розрядів, то сформується число-імпульсний код.

Таблиця 3.2 – Завадонезахищені коди

Символ	Двійковий	Двійково-десятковий *8.4.2.1*	Двійково-десятковий *4.2.2.1*	Код Грея	ASCII	Одинично-десятковий
0	0000	0000 0000	0000 0000	0000	30	0
1	0001	0000 0001	0000 0001	0001	31	1
2	0010	0000 0010	0000 0010	0011	32	11
3	0011	0000 0011	0000 0101	0010	33	111
4	0100	0000 0100	0000 0110	0110	34	1111
5	0101	0000 0101	0000 1001	0111	35	11111
6	0110	0000 0110	0000 1010	0101	36	111111
7	0111	0000 0111	0000 1101	0100	37	1111111
8	1000	0000 1000	0000 1110	1100	38	11111111
9	1001	0000 1001	0000 1111	1101	39	111111111
10	1010	0001 0000	0001 0000	1111	31 30	1111111111
11	1011	0001 0001	0001 0001	1110	31 31	1111111...11
12	1100	0001 0010	0001 0010	1010	31 32	11 ... 11
13	1101	0001 0011	0001 0101	1011	31 33	11 ... 111
14	1110	0001 0100	0001 0110	1001	31 34	11 ... 1111
15	1111	0001 0101	0001 1001	1000	31 35	11 ... 11111

Для побудови ***двійково-десяткового коду*** кожний розряд десяткового числа записується у вигляді комбінації двійкового коду. Вони бувають декількох типів з різними вагами розрядів - *8.4.2.1, 4.2.2.1, 2.4.2.1* (де кожна цифра означає вагу розряду у десятковій системі) тощо, але найчастіше використовуються *8.4.2.1.* та *4.2.2.1.*

Їх різновидом є ***самодоповнювальні*** двійково-десяткові коди, у яких при інвертуванні цифр в усіх розрядах утворюється доповнення до дев'ятки кодованої десяткової цифри. До цих кодів належать код Айкена 2-4-2-1 та код з надлишковістю 3 з вагою розрядів 8-4-2-1, зведені до табл. 3.3. Необхідність у таких кодах визначається заміною операції віднімання

Таблиця 3.3 – Самодоповнювальні коди

Символ	Код Айкена	Код з надлишковістю 3
0	0000	0011
1	0001	0100
2	0010	0101
3	0011	0110
4	0100	0111
5	1011	1000
6	1100	1001
7	1101	1010
8	1110	1011
9	1111	1100

операцією додавання у процесорних системах, яка виконується в оберненому чи додатковому машинних кодах. Зручність наведених кодів полягає в тому, що двійково-десятковий код цифри, яка є доповненням до дев'ятки, знаходиться інверсією значень розрядів, але код з надлишковістю 3 вимагає додаткової операції віднімання надлишку.

Двійково-десяткові коди відрізняються певною надлишковістю $R = 1 - {\log_2 10}/{\log_2 16} = 0{,}2$.

Код ASCII використовується у комп'ютерній техніці і базується на шістнадцятковій системі числення. Кожному з символів відповідає двозначний десятковий код.

Код Грея називають відбитим (рефлексним) і використовують для виготовлення кодувальних дисків та кодувальних масок.

У двійковому коді деякі кодові комбінації, що розташовані поряд, розрізняються декількома розрядами. Таким чином, у випадку зчитування може виникнути велика похибка (0111 – 1000). Для уникнення цього використовують коди, в яких, при переході від одного числа до іншого, комбінація змінюється лише в одному розряді, і, таким чином, зміна в будь-якому розряді може дати похибку на 1.

Код Грея формується складанням за модулем 2 комбінації із такою самою, але зсунутою вправо на один розряд. Під час складання найменший розряд другого доданка відкидається.

Декодування здійснюється за правилом: цифра старшого розряду не змінюється, а кожна наступна інвертується стільки разів, скільки їй передує одиниць у коді Грея.

Література

1. Кодирование информации. Двоичные коды / под ред. Березюка Н.Т. – Харьков: Издательство при Харьковском государственном университете, 1978. – С. 43 – 60.
2. Васюра А.С., Кривогубченко С.Г., Кулик А.Я. та ін. Техніка передавання дискретної інформації. – Вінниця: ВДТУ, 1998. – С. 57 – 60.
3. Квєтний Р.Н., Компанець М.М., Кривогубченко С.Г., Кулик А.Я. Основи техніки передавання інформації / Підручник. – Вінниця: Універсум-Вінниця, 2002. – С. 188 – 189.
4. Кузьмин И.В., Кедрус В.А. Основы теории информации и кодирования / Учебн. пос. – К.: Выща школа, 1986. – С. 74 – 78.

3.6 Методи статистичного кодування

Враховуючи статистичні якості джерела повідомлення можна мінімізувати середню кількість двійкових символів, що необхідні для позначення однієї літери повідомлення.

Кодування за ***алгоритмом Шеннона-Фано*** здійснюється таким чином:

⇒ літери алфавіту виписуються в порядку зменшення імовірностей появи;

⇒ потім вони розділяються на дві групи таким чином, щоб суми імовірностей були приблизно однаковими. Всім літерам першої половини першим символом надається "1", другої – "0". Кожна з груп розділяється на підгрупи і алгоритм повторюється;

⇒ процес продовжується до тих пір, поки у кожній підгрупі не залишиться одна літера.

Таким чином, найбільш імовірні комбінації передаються меншою кількістю символів. Але ця методика не приводить до однозначного формування коду, тому що під час розбиття можна зробити більшою за імовірністю як верхню, так і нижню половину.

Приклад формування кодових комбінацій за алгоритмом Шеннона-Фано.

№ дії	***Імовірність***	Поділ на групи	Кодові комбінації
1	0,3	0 0	00
2	0,2	0 1	01
3	0,15	1 0 0	100
4	0,12	1 0 1	101
5	0,08	1 1 0 0	1100
6	0,07	1 1 0 1	1101
7	0,04	1 1 1 0	1110
8	0,3	1 1 1 1 0	11110
9	0,01	1 1 1 1 1	11111

Для двійкового коду методика кодування за ***алгоритмом Хаффмена*** зводиться до того, що:

⇒ літери алфавіту виписуються до основного стовпця в порядку зменшення імовірностей;

⇒ дві останні літери об'єднуються до однієї допоміжної, якій присвоюється сумарна імовірність;

⇒ всі імовірності розташовуються в порядку зменшення, а дві останніх об'єднуються;

⇒ процес повторюється до тих пір, поки не буде одержано один символ з імовірністю 1;

⇒ якщо в результаті об'єднання одержується імовірність, значення якої вже наявне в таблиці на попередніх кроках, то остання імовірність записується нижче.

Після об'єднання імовірностей складається кодове дерево таким чином, що з точки, імовірність якої складає 1, гілки розходяться за її складовими, причому гілка, яка веде до більшої складової, позначається "1", гілка, що веде до меншої складової, позначається "0". Процес продовжується до тих пір, поки не будуть одержані початкові імовірності. Якщо гілки

мають однакову імовірність, то "одиницею" позначається більш розгалужена з них.

Таким чином кодові комбінації складають:

1 – 00	5 – 1100	9 – 11111
2 – 01	6 – 1101	
3 – 100	7 – 1110	
4 – 101	8 – 11110	

Приклад формування кодових комбінацій за алгоритмом Хаффмена.

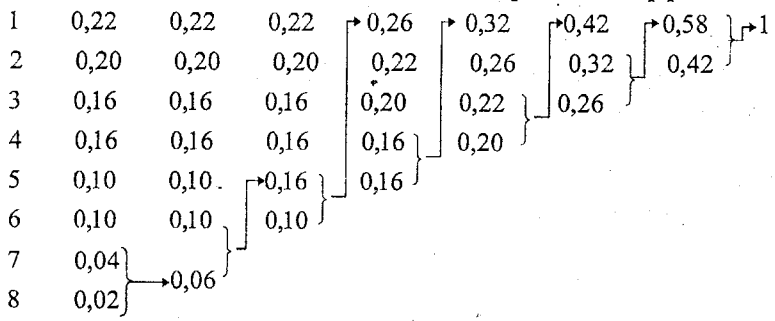


Рисунок 3.7 – Розподіл імовірностей

Для даної комбінації складається кодове дерево:

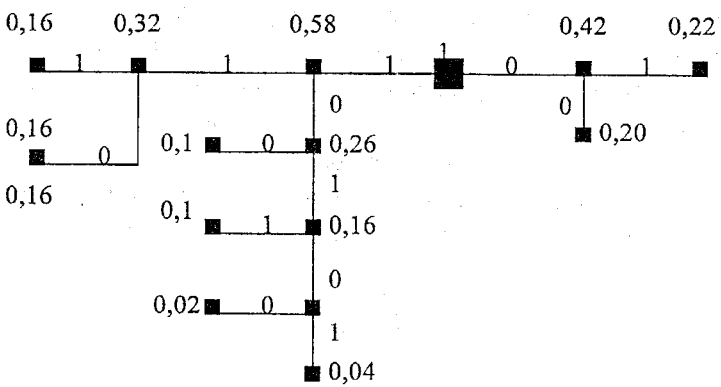


Рисунок 3.8 – Кодове дерево

Враховуючи наявність чітких правил об'єднання імовірностей та кодування шляхів, можна зауважити, що цей метод ліквідує неоднозначність кодування.

Література

1. Кодирование информации. Двоичные коды / под ред. Березюка Н.Т. – Харьков: Издательство при Харьковском государственном университете, 1978. – С. 60 – 63.
2. Васюра А.С., Кривогубченко С.Г., Кулик А.Я. та ін. Техніка передавання дискретної інформації. – Вінниця: ВДТУ, 1998. – С. 71 – 74.
3. Квєтний Р.Н., Компанець М.М., Кривогубченко С.Г., Кулик А.Я. Основи техніки передавання інформації / Підручник. – Вінниця: Універсум-Вінниця, 2002. – С. 200 – 203.

3.7 Коди з визначенням помилок

Ці коди можна розділити на дві групи:

⇒ коди, що побудовані шляхом зменшення кількості використовуваних комбінацій;

⇒ коди, які використовують усі можливі сполучення, але до них за певним алгоритмом додаються контрольні символи.

Код з постійною кількістю одиниць у комбінаціях (код з постійною вагою) має декілька модифікацій. Найчастіше використовуються ***п'ятирозрядний код з двома одиницями*** та ***семирозрядний код з трьома одиницями***. Правильність приймання визначається шляхом підраховування кількості одиниць. Ці коди не дозволяють визначити помилку в тому випадку, коли одна з одиниць перетворюється на нуль, а нуль перетворюється на одиницю (таке спотворення називається ***зміщенням***). Кількість можливих кодових комбінацій визначається правилами комбінаторики:

$$n_{2-5} = C_5^2 = \frac{5!}{2!3!} = 10$$

$$n_{3-7} = C_7^3 = \frac{7!}{3!4!} = 35$$

Розподільний код являє собою різновид коду з постійною вагою, що дорівнює одиниці. У будь-якій кодовій комбінації вміщується лише одна одиниця.

Код з перевіркою на парність формується таким чином, що до інформаційних розрядів додається ще один контрольний так, щоб загальна кількість одиниць у слові була парною. Таким чином, до кодової комбінації дописуються 0, якщо кількість одиниць у ній парна, та 1, якщо – непарна.

Під час приймання перевіряється кількість одиниць у слові. Якщо вона непарна, то під час передавання виникла помилка.

За цим же принципом будується код з ***перевіркою на непарність,*** який є модифікацією вищезгаданого, але одиниця у контрольному розряді формується у випадку парної кількості одиниць в інформаційних розрядах.

У деяких випадках формуються ***коди з перевіркою на парність*** та ***непарність за нулем***. Вони відрізняються тим, що в інформаційних розрядах підраховується кількість не одиниць, а нулів.

Код з кількістю одиниць, кратною трьом, формується таким чином. що до k інформаційних розрядів додається два додаткових контрольних символи. Вони мають такі значення, щоб сума одиниць в слові (з урахуванням контрольних розрядів) була кратною трьом.

Цей код дозволяє визначати поодинокі помилки та встановлювати парну кількість помилок одного типу (зміна 0 на 1).

Алгоритм побудови ***коду з подвоєнням елементів (кореляційного)*** полягає в тому, що кожний елемент двійкового коду на всі сполучення передається двома символами. Одиниця перетворюється на 10, а нуль – на 01. Таким чином, цей код вміщує вдвічі більше елементів, ніж початковий. Код не фіксує помилки тільки у випадку зміщення.

Під час формування ***інверсного коду*** для збільшення завадостійкості до k інформаційних розрядів додається ще m контрольних за правилами:

- якщо у початковій комбінації парна кількість одиниць, то комбінація, що додається, повторює початкову;
- якщо у початковій комбінації непарна кількість одиниць, то комбінація, що додається, є інверсною до початкової.

Цей код називають також ***кодом з повторюванням та інверсією***, на

відміну від ***коду з повторюванням***, де інформаційна комбінація додається такою самою в усіх випадках.

Література

1. Кодирование информации. Двоичные коды / под ред. Березюка Н.Т. – Харьков: Издательство при Харьковском государственном университете, 1978. – С. 88 – 94.
2. Васюра А.С., Кривогубченко С.Г., Кулик А.Я. та ін. Техніка передавання дискретної інформації. – Вінниця: ВДТУ, 1998. – С. 60 – 62.
3. Квєтний Р.Н., Компанець М.М., Кривогубченко С.Г., Кулик А.Я. Основи техніки передавання інформації / Підручник. – Вінниця: Універсум-Вінниця, 2002. – С. 190 – 191.

3.8 Теоретичні засади побудови кодів з визначенням помилок

Нехай комбінація $a_1 \ldots a_k b_1 \ldots b_m$, де a_i – інформаційні, а b_i – контрольні символи, є дозволеною комбінацією систематичного (n, k)-коду. В систематичних кодах перевірні розряди є лінійною комбінацією інформаційних, тобто значення будь-якого перевірного розряду $b_i = \alpha_{i1} \cdot a_1 \oplus \alpha_{i2} \cdot a_2 \oplus \ldots \oplus \alpha_{ik} \cdot a_k$, де $\alpha_{i1} \ldots \alpha_{ik}$ – числа, які дорівнюють 0 або 1.

Складемо за модулем 2 дві дозволені кодові комбінації систематичного коду:

$$a_1 \ldots a_k b_1 \ldots b_m \oplus a_1' \ldots a_k' b_1' \ldots b_m' = (a_1 \oplus a_1') \ldots (a_k \oplus a_k')(b_1 \oplus b_1') \ldots (b_m \oplus b_m'). \qquad (3.23)$$

Неважко побачити, що

$$(b_i \oplus b_i') = \alpha_{i1} a_1 \oplus \ldots \oplus \alpha_{ik} a_k \oplus \alpha_{i1} a_1' \oplus \ldots \oplus \alpha_{ik} a_k' = \\ = \alpha_{i1}(a_1 \oplus a_1') \oplus \ldots \oplus \alpha_{ik}(a_k \oplus a_k'). \qquad (3.24)$$

Таким чином, перевірні розряди суми за модулем 2 двох дозволених комбінацій утворюються за тим самим правилом, що й для кожної дозволеної комбінації. Звідси, сума двох дозволених комбінацій систематичного коду також є дозволеною комбінацією. Дана обставина дає можливість визначити всі дозволені кодові комбінації, маючи у своєму розпорядженні лише

обмежену їх кількість. Для цього дані вихідні комбінації вибираються за певними правилами:

- всі вихідні комбінації повинні бути різні;
- нульова комбінація не повинна входити до числа початкових;
- всі вихідні комбінації повинні бути лінійно незалежні, тобто повинна виконуватись умова $\alpha_1 a_1 \oplus ... \oplus \alpha_k a_k \neq 0$ для всіх значень α_i за винятком $\alpha_1 = \alpha_2 = ... = \alpha_k = 0$;
- кожна початкова кодова комбінація, як і будь-яка ненульова дозволена, повинна містити кількість одиниць не менше d;
- кодова відстань між будь-якими парами початкових комбінацій не повинна бути менше d. Підібрані певним чином k початкових кодових комбінацій однозначно визначають систематичний код. Ці комбінації записують у вигляді матриці $\mathbf{G_{nk}}$, що складається з k рядків та n стовпців. Така матриця називається ***утворювальною***:

$$\mathbf{G_{nk}} = \begin{Vmatrix} a_{11} & \dots & a_{1k} & b_{11} & \dots & b_{1m} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{k1} & \dots & a_{kk} & b_{k1} & \dots & b_{km} \end{Vmatrix}. \qquad (3.25)$$

Утворювальна матриця може бути представлена двома підматрицями – інформаційною та перевірною. Кількість стовпців інформаційної підматриці дорівнює k, кількість стовпців перевірної підматриці дорівнює m:

$$\mathbf{G_{nk}} = \left\| \begin{matrix} a_{11} & \dots & a_{1k} \\ \cdot & \cdot & \cdot \\ a_{k1} & \dots & a_{kk} \end{matrix} \right\| \left\| \begin{matrix} b_{11} & \dots & b_{1m} \\ \cdot & \cdot & \cdot \\ b_{k1} & \dots & b_{km} \end{matrix} \right\|. \qquad (3.26)$$

Теорією та практикою встановлено, що за інформаційну підматрицю зручно брати одиничну матрицю канонічної форми $\mathbf{E}_k$:

$$\mathrm{E}_k = \begin{Vmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & 1 \end{Vmatrix}, \qquad (3.27)$$

яка має k стовпців і k рядків. Перевірна підматриця $\mathbf{B_{mk}}$ будується шляхом добору різних m-розрядних комбінацій, що задовольняють умови:

- кількість одиниць у рядку повинна бути не меншою $d-1$;
- сума за модулем 2 двох будь-яких рядків не повинна мати менше $d-2$ одиниць.

При дотриманні перерахованих умов будь-яку утворювальну матрицю систематичного коду можна привести до вигляду

$$\begin{Vmatrix} 1 & 0 & \dots & 0 & b_{11} & \dots & b_{1m} \\ 0 & 1 & \dots & 0 & b_{21} & \dots & b_{2m} \\ . & . & . & . & . & . & . \\ 0 & 0 & \dots & 1 & b_{k1} & \dots & b_{km} \end{Vmatrix},$$

причому контрольні кодові комбінації b_i вибираються у відповідності з наведеними правилами. Оскільки перша комбінація – нульова, інші – рядки утворювальної матриці, то недостатні формують додаванням за модулем два всіх сполучень рядків утворювальної матриці.

Для побудови кодів необхідно алгоритмізувати знаходження перевірних розрядів кодової комбінації за інформаційним. Алгоритм утворення перевірних символів за допомогою матриці $\mathbf{G_{nk}}$ за відомими інформаційними може бути записаний у вигляді

$$\begin{cases} b_1 = b_{11} \cdot a_1 \oplus b_{21} \cdot a_2 \oplus \dots \oplus b_{k1} \cdot a_k \\ b_2 = b_{12} \cdot a_1 \oplus b_{22} \cdot a_2 \oplus \dots \oplus b_{k2} \cdot a_k \\ \vdots \\ b_m = b_{1m} \cdot a_1 \oplus b_{2m} \cdot a_m \oplus \dots \oplus b_{km} \cdot a_k \end{cases} . \qquad (3.28)$$

Для кожної конкретної матриці $\mathbf{G_{nk}}$ існує єдина система перевірок, які визначаються за правилом: у першу перевірку разом з перевірним розрядом b_1 входять інформаційні розряди, які відповідають одиницям першого стовпця підматриці $\mathbf{B_{mk}}$, у другу – входять другий перевірний розряд b_2 та інформаційні розряди, що відповідають одиницям другого стовпця підматриці $\mathbf{B_{mk}}$, тощо. Кількість перевірок дорівнює кількості перевірних розрядів коду (кількості стовпців підматриці $\mathbf{B_{mk}}$).

Дещо зручніше перевірні рівняння формувати за допомогою так званої перевірної матриці **H**, що складається з m рядків та n стовпців. Утворюється перевірна матриця в такий спосіб. Спочатку будується одинична матриця $\mathbf{E}_m$, після чого до неї зліва дописується підматриця $\mathbf{D}_{km}$, що містить k стовпців і m рядків, причому кожний її рядок відповідає стовпцю перевірних розрядів підматриці $\mathbf{B}_{mk}$ утворювальної матриці $\mathbf{G}_{nk}$, тобто $\mathbf{D}_{km} = (\mathbf{B}_{mk})^T$:

$$\mathbf{D}_{km} = \begin{Vmatrix} b_{11} & b_{21} & b_{31} & \dots & b_{k1} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ b_{1m} & b_{2m} & b_{3m} & \dots & b_{km} \end{Vmatrix}. \qquad (3.29)$$

Відповідно перевірна матриця матиме вигляд

$$\mathbf{H} = \|\mathbf{D}_{km}; \mathrm{E}_m\| = \begin{Vmatrix} b_{11} & b_{21} & \dots & b_{k1} & 1 & 0 & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ b_{1m} & b_{2m} & \dots & b_{km} & 0 & 0 & \dots & 1 \end{Vmatrix}. \qquad (3.30)$$

За її допомогою операція кодування здійснюється дуже просто. Позиції, зайняті одиницями в i-му рядку підматриці $\mathbf{D}_{km}$, визначають ті інформаційні розряди, які повинні приймати участь у формуванні i-го перевірного розряду.

Виходячи з вищевикладеного матричного подання кодів, можна зробити певні висновки:

- утворювальна матриця $\mathbf{G}_{nk}$ дозволяє подати весь набір кодових комбінацій у дуже зручній і компактній формі. За допомогою цієї матриці досить просто побудувати будь-яку кодову комбінацію за відомими інформаційними символами, тобто представити безнадлишкове повідомлення у закодованому даним кодом вигляді;
- перевірна матриця $\mathbf{H}_{nm}$ найчастіше використовується для побудови кодувальних і декодувальних пристроїв, оскільки вона визначає алгоритм знаходження перевірних розрядів за інформаційними символами. Крім цього, дана матриця дуже зручна для визначення місця помилки у кодовій комбінації.

Існує два основних методи виправлення помилок. Перший метод базується на використанні кодів-супутників. У цьому випадку будується кодова таблиця, в першому рядку якої розташовуються всі кодові слова V_i. Другий рядок таблиці заповнюється векторами, отриманими в результаті додавання за модулем два кодових слів першого рядка з вектором e_1, вага якого $w = 1$, а одиниця розташована в першому розряді. Третій рядок таблиці – результат додавання за модулем два кодових слів першого рядка з вектором e_2, вага якого $w = 1$, а одиниця вміщується у другому розряді. Аналогічно діють доти, поки не будуть додані з кодовими словами всі вектори e вагою $w = 1$ з одиницями в кожному з n розрядів. Потім додаються за модулем два вектори e_1 вагою $w = 2$ з послідовним перекриттям всіх можливих розрядів.

Вага вектора e_j визначає кількість помилок, що виправляються. Це ілюструється табл. 3.4. Таким чином, для кожного кодового слова V_i існує своя група кодів-супутників, розташованих у відповідному стовпці. Всі коди-супутники робочих кодових комбінацій зберігаються в пам'яті мікропроцесорної системи, і у випадку приймання комбінації, що збігається з одним з кодів супутників, спотворена комбінація розшифровується як початкова робоча комбінація, до якої входить даний код-супутник.

Таблиця 3.4 – Формування кодів-супутників

e	V_1	V_2	…	V_{2^k-1}
e_1	$e_1 \oplus V_1$	$e_1 \oplus V_{21}$	…	$e_1 \oplus V_{2^k-1}$
e_2	$e_2 \oplus V_1$	$e_2 \oplus V_2$	…	$e_2 \oplus V_{2^k-1}$
…	…	…	…	…
e_{2^m-1}	$e_{2^m-1} \oplus V_1$	$e_{2^m-1} \oplus V_2$	…	$e_{2^m-1} \oplus V_{2^k-1}$

Якщо код виправляє одну помилку з чотирма робочими комбінаціями 01001, 01110, 10010, 10101, то достатньо побудувати коди-супутники, що відрізняються від вихідних кодових комбінацій на e_j, із $w = 1$. Використовуючи табл. 3.4, можна отримати табл. 3.4, а. Завдяки складеним кодам-супутникам прийнята, наприклад, комбінація 10111 розшифрується як початкова 10101.

Такий метод виправлення помилок вимагає великих програмних та апаратних витрат, особливо при довгих кодових комбінаціях, оскільки кількість комірок пам'яті стає надзвичайно великою. Тому на практиці роз-

повсюджений інший метод виправлення помилок, при якому використовуються перевірні співвідношення, записані на підставі перевірної матриці **H**.

Таблиця 3.4, а – Формування кодів-супутників

e		***01001***	***01110***	***10010***	***10101***
e_1	00001	01000	01111	10011	10100
e_2	00010	01011	01100	10000	10111
e_3	00100	01101	01010	10110	10001
e_4	01000	00001	00110	11010	11101
e_5	10000	11001	11110	00010	00101

При цьому перевірка кодової комбінації на приймальному боці виконується шляхом зіставлення прийнятих контрольних розрядів кодової комбінації та контрольних розрядів, обчислених на підставі прийнятих інформаційних. Їхня сума за модулем два називається ***синдромом***. Характерною властивістю синдрому є його незалежність від виду передаваної комбінації. Він повністю визначається помилками, що спотворили прийняту комбінацію. Між комбінацією синдрому і комбінацією, що викликала помилку, немає взаємно однозначної відповідності – саме тому синдрому відповідає 2^k різних комбінацій помилок. Так, нульовому синдрому відповідає нульова комбінація помилок, а також $(2^k - 1)$ комбінацій помилок, що збігаються з дозволеними кодовими комбінаціями (невизначені помилки). Лише одна з комбінацій помилок, що відповідають нульовому синдрому, може бути виправлена кодом. При цьому за кожним синдромом закріплюється така комбінація, що може бути виправлена, поява якої в каналі найбільш імовірна.

Оскільки синдром є сумою за модулем 2 контрольних розрядів кодової комбінації та контрольних розрядів, обчислених за прийнятими інформаційними символами, то він збігається з комбінацією результатів перевірки на парність, обумовлених перевірною матрицею **H**.

Якщо контрольний символ, обчислений за інформаційними, позначити b_i', а перевірний символ прийнятої кодової комбінації – b_i, то синдром, наприклад для (7, 4)-коду з перевірною матрицею

$$\mathbf{H}=\begin{Vmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ a_1 & a_2 & a_3 & a_4 & b_1 & b_2 & b_3 \end{Vmatrix} \tag{3.31}$$

має вигляд

$$\begin{cases} b_1 \oplus b_1^{'} = S_1 \\ b_2 \oplus b_2^{'} = S_2 \\ b_3 \oplus b_3^{'} = S_3 \end{cases}, \tag{3.32}$$

де $\begin{cases} b_1^{'} = a_2 \oplus a_3 \oplus a_4 \\ b_2^{'} = a_1 \oplus a_3 \oplus a_4 \\ b_3^{'} = a_1 \oplus a_2 \oplus a_4 \end{cases}$.

Звідси можна визначити синдром шляхом розв'язання рівнянь

$$\begin{cases} a_2 \oplus a_3 \oplus a_4 \oplus b_1 = S_1 \\ a_1 \oplus a_3 \oplus a_4 \oplus b_2 = S_2 \\ a_1 \oplus a_2 \oplus a_4 \oplus b_3 = S_3 \end{cases}. \tag{3.33}$$

Нехай помилка діє в першому розряді (комбінація помилки 1000000). Застосуємо до цієї комбінації перевірки (3.33):

$$\begin{cases} a_2 \oplus a_3 \oplus a_4 \oplus b_1 = 0 \oplus 0 \oplus 0 \oplus 0 = 0 \\ a_1 \oplus a_3 \oplus a_4 \oplus b_2 = 1 \oplus 0 \oplus 0 \oplus 1 = 1 \\ a_1 \oplus a_2 \oplus a_4 \oplus b_3 = 1 \oplus 0 \oplus 0 \oplus 0 = 1 \end{cases}.$$

Це означає, що дія помилки в першому розряді визначає синдром 011. Аналогічно можна визначити види синдромів за умови дії всіх інших можливих однократних помилок. Їх доцільно звести до таблиці вигляду 3.5. З неї за розрахованим синдромом одразу можна визначити спотворений розряд. Для визначення помилок можуть використовуватися всі комбінації двійкового коду, окрім нульової. Таким чином кількість контрольних символів при виправленні однократних помилок визначається нерівністю $2^m - 1 \geq n$ або $2^m - 1 \geq C_n^1$.

Для виправлення не лише поодиноких, але й двократних помилок необхідно виконання умови $2^m - 1 \geq C_n^1 + C_n^2$. Або в загальному вигляді

$$2^m - 1 \geq C_n^1 + C_n^2 + ... + C_n^s, \qquad (3.34)$$

де s – кількість помилок, що виправляються кодом, який збігається з наведеною вище оцінкою Хеммінга.

Таблиця 3.5 – Синдроми

Комбінація помилки	Спотворений розряд	Синдром
1000000	1	011
0100000	2	101
0010000	3	110
0001000	4	111
0000100	5	100
0000010	6	010

Але якщо для виправлення поодинокої помилки достатньо просто сформувати синдроми, що дозволяють однозначно визначити місце помилки в комбінації, то для виправлення подвійних, потрійних і т.д. помилок, а також для виправлення пакетів помилок побудова синдромів достатньо складна. Дотепер в літературі не описаний метод, який дозволив би побудувати систематичний код для виправлення безлічі помилок. Розроблені методи побудови синдромів для кодів, призначених для виправлення подвійних, потрійних, а також пакетів помилок довжини $l \leq 3$. У табл. 3.6 наведені синдроми для коду, що виправляє подвійні помилки, а в табл. 3.7 – для коду, що виправляє потрійні помилки. У табл. 3.8 подані синдроми 30-розрядного коду, що виправляє пакети помилок довжини $l \leq 3$.

За цими таблицями можна знайти синдроми подвійних та потрійних помилок шляхом додавання за модулем два синдромів, у розрядах яких відбулися помилки. Наприклад, для коду, що виправляє подвійні помилки, отриманий синдром 00 0001 1111. Згідно з табл. 3.6 можна знайти, що даний результат отримується лише шляхом додавання за модулем два 5-го та 6-го розрядів, тобто спотворені п'ятий і шостий розряди кодової комбінації.

Таблиця 3.6 – Синдроми коду для виправлення подвійних помилок

Розряд коду	Синдром	Розряд коду	Синдром	Розряд коду	Синдром
1	00 0000 0001	11	00 0110 1010	21	01 1011 1101
2	00 0000 0010	12	00 1000 0000	22	10 0000 0000
3	00 0000 0100	13	00 1001 0110	23	10 0001 1001
4	00 0000 1000	14	00 1011 0101	24	10 0010 1101
5	00 0000 1111	15	00 1101 1011	25	10 0101 0010
6	00 0001 0000	16	00 1110 1101	26	10 1000 0011
7	00 0010 0000	17	00 1111 0111	27	11 0010 0011
8	00 0011 0011	18	01 0000 0000	28	110101 1111
9	00 0100 0000	19	01 0001 0111	29	11 1110 0110
10	00 0101 0101	20	01 0010 1001		

Таблиця 3.7 – Синдроми коду для виправлення потрійних помилок

Розряд коду	Синдром	Розряд коду	Синдром	Розряд коду	Синдром
1	00 0000 0001	6	00 0010 0000	11	01 1011 1101
2	00 0000 0010	7	00 0011 1111	12	10 0000 0000
3	00 0000 0100	8	00 0100 0110	13	10 1101 1001
4	00 0000 1000	9	00 1000 0000	14	11 0110 1010
5	00 0001 0000	10	01 0000 0000	15	11 1011 0100

Таблиця 3.8 – Синдроми коду для виправлення пакетних помилок довжини $l \leq 3$

Розряд коду	Синдром	Розряд коду	Синдром	Розряд коду	Синдром
1	0000 0001	11	0000 1011	21	0001 0101
2	0000 0010	12	0000 1011	22	0010 0001
3	0000 0100	13	0100 0001	23	0100 1000
4	0000 1000	14	0000 1111	24	1000 0001
5	0001 0000	15	0010 0011	25	0001 1101
6	0010 0000	16	0100 0010	26	0100 0100
7	0000 1001	17	0000 1101	27	1000 0011
8	0001 0010	18	0100 0111	28	0011 0001
9	0010 0100	19	0101 0011	29	0001 0111
10	0100 0000	20	1000 0000	30	1000 0100

Внаслідок складності побудови синдромів для виправлення декількох помилок до побудови синдромів долучають засоби комп'ютерної техніки. Так, Банерджі побудував таблицю кодів для виправлення будь-яких двократних помилок у кодових комбінаціях довжиною до 29 розрядів для кодів до (27, 17). Ці таблиці наведені в літературі, але відрізняються певною складністю для користування.

Надлишкові коди можуть застосовуватися з метою або лише виявлення можливих помилок, або їх виправлення. В усіх випадках бажано досягти максимальної корегувальної здатності. Але, залежно від побудови конкретного коду, його здатність до виправлення тих чи інших помилок може змінюватися в широких межах. Тому виникає питання про те, який з різновидів систематичного коду при заданих n і k має найвищу корегувальну здатність. При деяких значеннях n і k може бути знайдена така вдала побудова коду, при якій ваги всіх дозволених ненульових комбінацій мало відрізняються одна від одної та від половини максимально можливої ваги. При інших значеннях n і k може виявитися, що для деякої малої частини кодових комбінацій з їхнього загального числа 2^k відстань виявляється істотно меншою, ніж для більшості інших. Тому при розгляді характеристик кодів можна виявити, що близькі за надлишковістю і кількістю розрядів коди різко відрізняються за своєю корегувальною здатністю. Крім цього корегувальна здатність одного і того самого коду може значно змінюватися залежно від характеру розподілу помилок у каналах зв'язку.

Оптимальним вважається код, що при заданих значеннях n і k (або надлишковості R) забезпечує найменшу імовірність невизначення помилки. На жаль, загальний аналітичний метод розрахунку оптимальних кодів ще не знайдений. Для певних умов у каналі та для довільних значень n і k загальним способом вибору оптимальних кодів залишається спосіб перебору всіх можливих (n, k)-кодів. У цьому випадку щоразу визначається, яке значення імовірності невизначення помилки $p_н$ є мінімально досяжним.

Література

1. Кодирование информации. Двоичные коды / под ред. Березюка Н.Т. – Харьков: Издательство при Харьковском государственном университете, 1978. – С. 74 – 88.
2. Шварцман В.О., Емельянов Г.А. Теория передачи дискретной информации. – М.: Связь, 1979. – С. 272 – 276.
3. Кузьмин И.В., Ключко В.И., Литвин В.А. Кодирование и декодирование в информационных системах. – К.: Выща школа, 1985. – С. 30 – 33.

3.9 Кодування за алгоритмом Хеммінга

Для кодування за алгоритмом Хеммінга у вигляді початкового беруть двійковий код на всі сполучення з додаванням контрольних символів. Для одного інформаційного символу потрібно 2 контрольних, для двох – 3, для п'яти – 4, для дванадцяти – 5.

Контрольні символи прийнято розташовувати на місцях, номери яких кратні степеню 2, тому для семиелементної комбінації розташування символів кодове слово має вигляд:

$$k_4\ k_3\ k_2\ m_3\ k_1\ m_2\ m_1\,; \tag{3.35}$$

де k - інформаційні символи;

m - перевірні (контрольні) символи.

Контрольні символи формуються додаванням за модулем 2 інформаційних розрядів:

$$\begin{cases} m_1 = k_1 \oplus k_2 \oplus k_4 \\ m_2 = k_1 \oplus k_3 \oplus k_4 \\ m_3 = k_2 \oplus k_3 \oplus k_4 \end{cases}. \tag{3.36}$$

Принцип побудови системи рівнянь ілюструється таблицею 3.9. При її складанні перші три стовпці характеризують значення контрольних розрядів, а четвертий – склад інформаційного слова з контрольними розрядами. У перших трьох стовпцях розписуються комбінації двійкового коду без урахування нульової. Формування рівнянь здійснюється за вертикаллю таким чином, що вибираються інформаційні розряди, у відповідному сто-

Таблиця 3.9 – Перевірна таблиця коду Хеммінга

$m3$	$m2$	$m1$	Символи
0	0	1	$m1$
0	1	0	$m2$
0	1	1	$k1$
1	0	0	$m3$
1	0	1	$k2$
1	1	0	$k3$
1	1	1	$k4$

вищі яких стоять одиниці. Для символу m_1 це: k_1, k_2, k_4, для m_2 – k_1, k_3, k_4, для m_3 – k_2, k_3, k_4. Після цього відповідні значення поєднуються додаванням за модулем 2.

Якщо контрольних розрядів більше або менше за 3, то відповідним чином змінюється кількість стовпців контрольних розрядів у перевірній таблиці.

Зрозуміло, що до системи рівнянь (3.36) входять усі інформаційні розряди, причому кожен з інформаційних розрядів k наявний якнайменше в двох рівняннях з трьох. Тому, розв'язуючи систему рівнянь (3.36), можна однозначно підказати в якому з розрядів сталася помилка.

Нехай під час передавання кодової комбінації 1100110 помилка спотворила третій розряд, тобто прийнято кодову комбінацію 1100010. З системи рівнянь (3.36) можна одержати такі результати перевірки:

$$\begin{cases} m1 \oplus k1 \oplus k2 \oplus k4 = 0 \oplus 0 \oplus 0 \oplus 1 = 1 \\ m2 \oplus k1 \oplus k3 \oplus k4 = 1 \oplus 0 \oplus 1 \oplus 1 = 1 \\ m3 \oplus k2 \oplus k3 \oplus k4 = 0 \oplus 0 \oplus 1 \oplus 1 = 0 \end{cases} \uparrow$$

– Напрямок читання кодової комбінації

За результатами перевірки одержана кодова комбінація 011, тобто помилка знаходиться у третьому розряді. Оскільки найменший розряд (3.35) розташований справа, то відрахунок починається звідси. Замість кодової комбінації 1100010 треба поставити 1100110.

Оскільки зараз найчастіше користуються 8-розрядними кодами (байтовою системою), які доцільно передавати півбайтами і трьома контрольними розрядами, то залишковий розряд можна заповнити перевіркою на парність. Використання засобів обчислювальної техніки дозволяє швидко розв'язувати систему рівнянь (3.36), проводячи кодування та декодування у програмному режимі. Але існують апаратні кодери і декодери, які перетворюють двійковий код на код Хеммінга та навпаки. Можна також

користуватись методикою побудови кодів-супутників, викладеною вище, оскільки використання процесорних схем практично знімає обмеження в обсязі використовуваної пам'яті.

Література

1. Кодирование информации. Двоичные коды / под ред. Березюка Н.Т. – Харьков: Издательство при Харьковском государственном университете, 1978. – С. 94 – 100.
2. Васюра А.С., Кривогубченко С.Г., Кулик А.Я. та ін. Техніка передавання дискретної інформації. – Вінниця: ВДТУ, 1998. – С. 63 – 66.
3. Квєтний Р.Н., Компанець М.М., Кривогубченко С.Г., Кулик А.Я. Основи техніки передавання інформації / Підручник. – Вінниця: Універсум-Вінниця, 2002. – С. 192 – 195.

3.10 Методи ітеративного та каскадного кодування

Ідея побудови ітеративних кодів належить Елайєсу. Ці коди характеризуються наявністю двох або більше систем перевірок для кожної кодової комбінації. Принцип побудови ітеративного коду найпростіше показати на прикладі.

Спочатку інформаційні символи кодової комбінації записуються у вигляді таблиці, що, наприклад, може мати такий вигляд:

10111
00101
11100
01001
11101

Потім до кожного рядка таблиці і до кожного стовпця дописуються перевірні символи відповідно до будь-якого коду, наприклад з перевіркою на парність:

10111	0
00101	0
11100	1
01001	0
11101	0
11011	1

Отримана комбінація є кодовою комбінацією найпростішого двовимірного ітеративного коду, перевірні розряди якого зосереджені в нижньому рядку і правом стовпці. Кожний інформаційний розряд цього коду входить до комбінації двох ітеративних кодів з перевіркою на парність. Передавання одного повідомлення комбінацією ітеративного коду зазвичай відбувається рядками послідовно (від першого до останнього). Наведений код є найпростішим ітеративним кодом з $d = 4$, причому кількість кодових комбінацій ваги $w = 4$ дорівнює $W(4) = k^2 + k^2(k-1)/2 + k(k-1)^2/2$ для квадратної кодової таблиці ($k = l$; k – кількість інформаційних символів у рядку; l – кількість інформаційних символів у стовпці).

Цей код виявляє всі помилки кратністю до трьох і всі помилки непарної кратності. Не виявляються чотирикратні помилки, що розташовуються у вершинах правильного чотирикутника, а також деякі шестикратні, восьмикратні тощо помилки (рис. 3.9). Кількість чотирикратних помилок, що мають показану на рис. 3.9 структуру, дорівнює $C_{n1}^2 \cdot C_{n2}^2$, де n_1 – повна кількість розрядів у рядку, n_2 – повна кількість розрядів у стовпці.

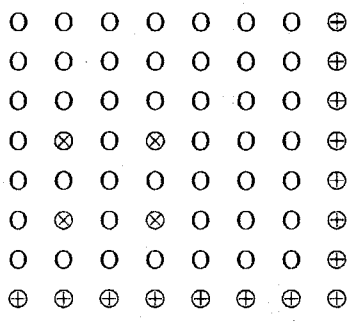
Звідси можна визначити частку помилок кратності 4, що не виявляються, тобто коефіцієнт помилкових переходів $K_n(4) = C_{n1}^2 \cdot C_{n2}^2 / C_{n1 \cdot n2}^4$. Після перетворення формула набуває вигляду

$$K_n(4) = \frac{6 \cdot (n_1 - 1) \cdot (n_2 - 1)}{(n_1 n_2 - 1) \cdot (n_1 n_2 - 2) \cdot (n_1 n_2 - 3)} \approx \frac{6}{(n_1 n_2)^2}$$

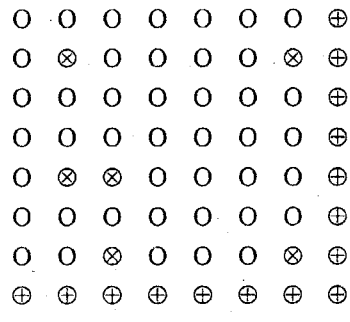
Помилки кратності 6, що не виявляються, розташовані в трьох стовпцях, по двох у кожному. Кількість різних стовпців першого типу дорівнює C_{n1}^2. Другий стовпець може бути вибраний $2(n_1 - 2)$ способами. Третій

стовпець однозначно визначається першими двома. Всі три стовпці можуть бути вибрані C_{n2}^3, способами. Тому $K_n(6) = C_{n1}^2 \cdot 2(n_1 - 2) \cdot C_{n2}^3 / C_{n1 \cdot n2}^6$.

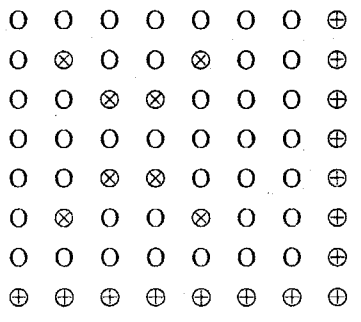
Аналогічно після перетворення $K_n(6) \approx \frac{120}{(n_1 n_2)^3}$. Так само можна визначити частку помилок, що не виявляються, кратності 8 – $K_n(8)$, кратності 10 – $K_n(10)$ тощо.



а)



б)



в)

Рисунок 3.9 – Структури помилок, що не виявляються простим двовимірним ітеративним кодом:
а) – чотирикратні, б) – шестикратні, в) – восьмикратні

Метод виправлення помилок надзвичайно простий: якщо не виконується перевірка для *i*-того рядка та *j*-того стовпця, то символ, що знаходиться на перетині *i*-того рядка та *j*-того стовпця, заміняється на обернений. Можуть бути утворені багатовимірні ітеративні коди, у яких кожний інформаційний розряд входить у комбінації трьох, чотирьох тощо ітеративних кодів. Але такі коди не одержали великого поширення.

Властивості ітеративного коду повністю визначаються параметрами ітерованих кодів. Довжина кодової комбінації n, число інформаційних розрядів k та мінімальна кодова відстань d визначаються через відповідні параметри цих кодів:

$$n = \prod_{i=1}^{S} n_i; \quad k = \prod_{i=1}^{S} k_i; \quad d = \prod_{i=1}^{S} d_i, \tag{3.37}$$

де S – кратність ітерування.

До ітеративних кодів може бути застосований матричний спосіб описання. Для отримання утворювальної матриці ітеративного коду використовується векторний добуток вектора $\mathbf{X} = (x_1, x_2, ..., x_{n1})$ на вектор $\mathbf{Y} = (y_1, y_2, ..., y_{n2})$, який дорівнює $\mathbf{X} \times \mathbf{Y} = (x_1(y_1, \ldots, y_{n2}), x_2(y_1, \ldots, y_{n2}), \ldots, x_{n1}(y_1, \ldots, y_{n2}))$, де $x_i(y_1, \ldots, y_{n2}) = x_i y_1, x_i y_2, ..., x_i y_{n2}$.

Якщо, наприклад, потрібно побудувати утворювальну матрицю ітеративного коду, де як ітеративний використовується код з перевіркою на парність і утворювальною матрицею $\mathbf{G}_1 = \begin{Vmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{Vmatrix}$, то згідно з правилом множення

$$\mathbf{G} = \mathbf{G}_1 \times \mathbf{G}_1 = \begin{Vmatrix} 1 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{Vmatrix} \times \begin{Vmatrix} 1 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{Vmatrix},$$

де $101 \times 101 = 101000101$;

$101 \times 011 = 011000011$;

$011 \times 101 = 000101101$;

$011 \times 011 = 000011011$.

Таким чином утворювальна матриця ітеративного коду

$$\mathbf{G} = \begin{Vmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{Vmatrix},$$

яка породжує код з параметрами $n = 9$, $k = 4$, $d = 4$.

Навіть найпростішому ітеративному коду властиві досить високі здатності виявлення помилок. При дії пакетних помилок виявляється будь-який пакет помилок довжиною $l + 1$ і менше, де l – довжина рядка.

Істотним недоліком ітеративних кодів, що використовують за рядками і стовпцями перевірку на парність, є їх порівняно висока надлишковість, що зазвичай становить 15 – 20% і значно перевищує за інших рівних умов надлишковість циклічних кодів. Але кодування і декодування за допомогою засобів мікропроцесорної техніки таких ітеративних кодів є процедурами набагато простішими, ніж циклічні. Тому найпростіші ітеративні коди, незважаючи на їх високу надлишковість, застосовуються в системах передавання даних, що використовують програмні способи підвищення вірогідності.

Каскадні коди, так само як ітеративні, складаються із двох або декількох кодів, але, на відміну, у них символами коду наступного рівня є слова коду попереднього рівня. Каскадний принцип побудови коду ілюструється схемою рис. 3.10. Як видно з рисунка, система „внутрішній кодер – дискретний канал – внутрішній декодер" створює щодо зовнішніх кодера і декодера мовби розширений дискретний канал, що має словник з 2^N кодових векторів, де N – розрядність внутрішнього коду. Якщо розрядність зовнішнього коду дорівнює n, то розрядність каскадного коду $N_0 = n \cdot N$, і він містить $2^{n \cdot N}$ кодових слів.

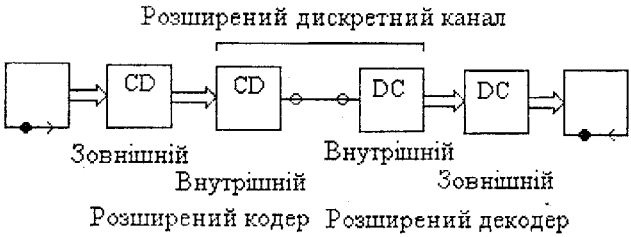


Рис. 3.10 – Структура для побудови каскадного коду

Процедура кодування двійковим каскадним кодом зводиться до того, що:

⇨ інформаційні символи розбиваються на k_2 підблоків по k_1 символів у кожному (рис. 3.11). Кожний підблок з k_1 символів записується як еле-

мент поля $GF(2^{k1})$, в результаті чого отримується вектор з k_2 символів над $GF(2^{k1})$;

- отриманий вектор над $GF(2^{k1})$ розглядається як інформаційний вектор деякого лінійного коду над $GF(2^{k1})$ довжиною n_2 із k_2 інформаційними символами і кодується зазначеним кодом (n_2, k_2), що називається кодом другого рівня. В результаті кодування виходить кодове слово коду другого рівня, тобто деякий вектор довжиною n_2 над $GF(2^{k1})$;
- кожний з n_2 символів коду другого рівня розглядається як двійковий вектор довжини k_2 і кодується двійковим (n_2, k_2)-кодом першого рівня. Результатом є двійкове слово довжиною $n_2 \cdot n_2$, що і є кодовим словом каскадного коду.

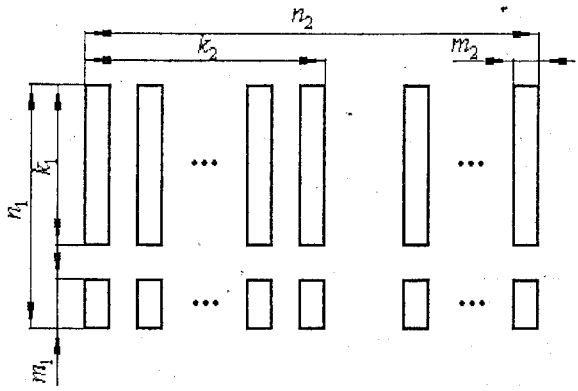


Рис. 3.11 – Принцип побудови каскадного коду

Каскадний код є лінійним, і його кодова відстань d, аналогічно ітеративному коду, не менша, ніж добуток кодових відстаней першого (d_1) і другого (d_2) рівнів: $d_1 \geq d_1 \cdot d_2$. Інші параметри двійкового коду також легко визначаються за параметрами кодів першого і другого рівнів: $n_1 = n_1 \cdot n_2$ та $k_1 = k_1 \cdot k_2$.

Перевагами каскадних кодів, так само як і ітеративних, є відносно велика складність кодувальних і декодувальних пристроїв (пропорційна n у невеликому ступені) і можливість виправлення не лише незалежних і поодиноких помилок, а також багатократних пакетів помилок. Це досягається тим, що як внутрішній використовується код, який виявляє і виправляє поодинокі помилки, а як зовнішній – код, який виявляє і виправляє пакети помилок. Найбільш повно досліджені каскадні коди, у яких як внутрішній використовується код Хеммінга, а як зовнішній – код Ріда-Соломона.

Принцип каскадного кодування аналогічний дії одержувача спотвореної телеграми: якщо наявні окремі помилкові літери в словах (незалежні помилки), те вони можуть бути виявлені та виправлені за допомогою інших літер того самого слова (внутрішнє кодування), а якщо окремі слова спотворені до невпізнанності (пакети помилок), та визначення наявності таких помилок, а тим більше їх виправлення, можливо лише за допомогою інших слів речення або тексту в цілому (зовнішнє кодування). У розглянутій аналогії основу внутрішнього коду становлять надлишковість за рахунок зв'язків між літерами у словах, а зовнішнього коду – за рахунок зв'язків слів у реченні.

Література

1. Кодирование информации. Двоичные коды / под ред. Березюка Н.Т. – Харьков: Издательство при Харьковском государственном университете, 1978. – С. 134 – 138.
2. Шварцман В.О., Емельянов Г.А. Теория передачи дискретной информации. – М.: Связь, 1979. – С. 320 – 323.

3.11 Алгоритми циклічного кодування

Циклічні коди є різновидом систематичних кодів і тому їм властиві всі їх переваги й недоліки. Спочатку вони були створені для спрощення схем кодування та декодування, та ефективність при виявленні й виправленні помилок забезпечила їм широке застосування на практиці. На сьогоднішній день вони є стандартом виявлення і виправлення помилок під час передавання інформації каналами зв'язку.

Циклічні коди більш зручно розглядати, подаючи комбінацію двійкового коду не у вигляді послідовностей нулів і одиниць, а у вигляді полінома деякого степеня:

$$F(x) = b_{n-1}a^{n-1} + b_{n-2}a^{n-2} + \ldots + b_1 a + b_0 , \qquad (3.38)$$

де a – основа системи числення;

b – цифри даної системи числення (у двійковій системі 0 і 1).

Наприклад, двійкова послідовність 01001 може бути записана у вигляді полінома від змінної x: $F(x) = 0 \cdot x^4 + 1 \cdot x^3 + 0 \cdot x^2 + 0 \cdot x^1 + 1 \cdot x^0$. Подання кодових комбінацій у формі (3.38) дозволяє звести дії над комбінаціями до дій над поліномами. При цьому додавання двійкових поліномів зводиться до додавання за модулем два коефіцієнтів при рівних степенях змінної x. Множення здійснюється за звичайним правилом перемножування степеневих функцій, але отримані в цьому випадку коефіцієнти при даному ступені складаються за модулем два. Ділення здійснюється за правилами ділення степеневих функцій, при цьому операції віднімання замінюються операціями додавання за модулем два.

Основна властивість циклічних кодів, яка визначає їхню назву, полягає в тому, що якщо комбінація $a_0\, a_1, \ldots, a_n$ є дозволеною, то комбінація, отримувана з неї шляхом циклічної перестановки розрядів, також належить цьому коду.

Подання комбінацій у формі (3.38) зручно ще й тим, що згадана циклічна перестановка є результатом простого множення даного полінома на x. Дійсно, якщо одна з кодових комбінацій визначається поліномом $V(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1}$, то нова комбінація за рахунок циклічного зсуву буде мати вигляд $xV(x) = a_0x + a_1x^2 + \ldots + a_{n-1}x^n$. Але в останньому члені необхідно замінити x^n на 1 (інакше довжина кодової комбінації перевищить n). Отже, отримана комбінація $V_1(x) = xV(x) = a_{n-1} + a_0x + \ldots + a_{n-2}x^{n-1}$ є циклічним зсувом комбінації $V(x)$.

Ідея побудови циклічних кодів базується на використанні неприводимих поліномів. ***Неприводимим*** називається поліном, що не може бути поданий у вигляді добутку багаточленів нижчих степенів, тобто такий поліном ділиться лише на самого себе або на одиницю і не ділиться ні на який інший. На такий поліном ділиться без залишку двочлен $x^n + 1$. Неприводимі поліноми в теорії циклічних кодів відіграють роль утворювальних поліномів. У табл. 3.10 наведені неприводимі поліноми до 10-ї степеня включно, які позначені $P_i(x^n)$, при розташуванні за ознакою зростання відповідних їм двійкових чисел.

Щоб зрозуміти принцип побудови циклічного коду, множимо комбінацію простого k-розрядного коду $Q(x)$ на одночлен x^m, а потім ділимо на утворювальний поліном $P(x)$, степінь якого дорівнює m. В результаті мно-

ження $Q(x)$ на x^m степінь кожного одночлена, що входить до $Q(x)$, підвищується на m.

Таблиця 3.10 – Неприводимі утворювальні поліноми та їх еквіваленти

Степінь, m	Поліном $P_i(x^n)$	Еквівалент
1	$x+1$	11
2	x^2+x+1	111
3	x^3+x+1	1011
3	x^3+x^2+1	1101
4	x^4+x+1	10011
4	x^4+x^3+1	11001
4	$x^4+x^3+x^2+x+1$	11111
5	x^5+x^2+1	100101
5	x^5+x^3+1	101001
5	$x^5+x^3+x^2+x+1$	101111
5	$x^5+x^4+x^2+x+1$	110111
5	$x^5+x^4+x^3+x+1$	111011
5	$x^5+x^4+x^3+x^2+1$	111101
6	x^6+x+1	1000011
6	$x^6+x^3+x^2+x+1$	1001111
7	x^7+x^3+1	10001001
7	x^7+x^4+x+1	10010011
8	$x^8+x^4+x^3+x^2+1$	100011101
8	x^8+x^2+x+1	100000111
8	$x^8+x^5+x^2+x+1$	100100111
8	$x^8+x^6+x^4+x+1$	101010011
9	x^9+x^4+1	1000010001
9	x^9+x^6+x+1	1001000011
9	$x^9+x^6+x^4+x+1$	1001010011
10	$x^{10}+x^3+1$	10000001001

При діленні добутку $Q(x) \cdot x^m$ на утворювальний поліном результатом буде частка $C(x)$ такого самого степеня, що й $Q(x)$. Результат множення і ділення можна подати у вигляді

$$\frac{Q(x)\cdot x^m}{P(x)} = C(x) + \frac{R(x)}{P(x)}, \qquad (3.39)$$

де $R(x)$ – залишок від ділення $x^m \cdot Q(x)$ на $P(x)$.

Частка $C(x)$ має такий самий степінь, що й кодова комбінація $Q(x)$ простого коду, тому $C(x)$ є кодовою комбінацією цього самого простого k-розрядного коду. Варто відзначити, що степінь залишку не може бути більшим від степеня утворювального полінома, тобто його найвищий степінь може дорівнювати $(m - 1)$. Отже, найбільша кількість розрядів залишку $R(x)$ не перевищує числа m.

Якщо помножити обидві частини рівності (3.39) на $P(x)$ і здійснити певні перестановки, можна одержати

$$F(x) = C(x) \cdot P(x) = Q(x) \cdot x^m + R(x) . \qquad (3.40)$$

У (3.40) знак мінус перед $R(x)$ замінений на знак плюс, тому що віднімання за модулем два еквівалентно додаванню.

Таким чином, кодова комбінація циклічного n-розрядного коду може бути отримана двома способами:

- множенням кодової комбінації $Q(x)$ простого коду на одночлен x^m і додаванням до цього добутку залишку $R(x)$, отриманого в результаті ділення добутку $Q(x) \cdot x^m$ на утворювальний поліном $P(x)$;
- множенням кодової комбінації $C(x)$ простого k-розрядного коду на утворювальний поліном $P(x)$.

Під час побудови циклічних кодів першим способом розташування інформаційних символів у всіх комбінаціях чітко впорядковане – вони займають k старших розрядів комбінації, а інші $(n - k)$ розрядів відводяться під перевірні (контрольні).

При другому способі утворення циклічних кодів інформаційні та контрольні символи в комбінаціях циклічного коду не відділені одні від одних, що ускладнює процес декодування. Тому в основному використовують перший спосіб побудови циклічного коду.

Приклад.

Початковими даними є $k = 4$ та утворювальний поліном третього степеня $P(x) = x^3 + x^2 + 1$. Отже, кодові комбінації циклічного коду будуть мати по сім розрядів. Потрібно записати довільну кодову комбінацію циклічного коду (7,4) першим способом.

Для розв'язання можна взяти довільну чотирирозрядну комбінацію 0111, тобто $Q(x) = x^2 + x + 1$. Добуток буде дорівнювати $Q(x) \cdot x^m = (x^2 + x + 1) \cdot x^3 = x^5 + x^4 + x^3$. Після здійснення ділення:

$$\frac{Q(x) \cdot x^r}{P(x)} = \frac{x^5 + x^4 + x^3}{x^3 + x^2 + 1} = x^2 + 1 + \frac{1}{P(x)}$$

Отже, залишок $R(x) = 1$. Таким чином, у відповідності із сформульованим вище правилом знайдемо комбінацію, що належить циклічному коду (7, 4):

$$F(x) = Q(x) \cdot x^r + R(x) = x^5 + x^4 + x^3 + 1$$

або у двійковій формі $F(1, 0) = 0111\ 001$, де перші чотири розряди – інформаційні, а три останні – контрольні.

Операція утворення циклічного коду може безпосередньо здійснюватися під час записування початкових кодових комбінацій у вигляді двійкових чисел.

Приклад.

Початковими даними є $k = 4$ та утворювальний поліном третього степеня $P(1, 0) = 1101$. Потрібно побудувати циклічний код з простого чотирирозрядного коду другим способом.

За вихідну використаємо просту комбінацію $C(1, 0) = 0011$. Операція множення цієї комбінації на утворювальний поліном $P(1, 0)$ запишеться в такий спосіб

$$\begin{array}{r} 0011 \\ \times\ \ 1101 \\ \hline 0011 \\ 0011 \\ 0011 \\ \hline 0010111 \end{array}$$

Таким чином, просту чотирисимвольну комбінацію $C(1, 0) = 0011$ можна подати семисимвольним циклічним кодом $F(1, 0) = C(1, 0) \cdot P(1, 0) = 0010111$.

Циклічний код, як і будь-який систематичний код, однозначно характеризується підібраними певним чином k початковими кодовими комбінаціями. Вони записуються у вигляді утворювальної матриці, що складається з k рядків та n стовпців.

Для формування рядків утворювальної матриці першим способом беруть не довільні комбінації безнадлишкового коду $Q(x)$, а лише ті з них, які містять одиницю в одному розряді $Q_i(x)$, де $i = 1 \div k$. Саме ці комбінації множаться на x^r і знаходиться остача від ділення $Q_i(x) \cdot x^m / P(x)$, яка дорівнює $R(x)$. Відповідний рядок матриці записується у вигляді $Q(x) \cdot x^m + R(x)$. При цьому вся матриця розбивається на дві підматриці (як це показано вище): одиничну транспоновану та $\mathbf{C_{mk}}$ – підматрицю із числом стовпців m і рядків k, утворену залишками від ділення на $R_i(x)$. Такий спосіб дає можливість отримати одразу утворювальну матрицю в канонічному вигляді. Вона дає можливість отримати перші k комбінацій коду. Інші $2^k - k - 1$ комбінацій формуються додаванням за модулем два рядків утворювальної матриці у всіх можливих сполученнях. Остання комбінація коду є нульовою.

Приклад.

Нехай необхідно утворити циклічний код, що дозволяє виправляти поодинокі помилки в усіх комбінаціях коду на всі сполучення з числом інформаційних символів $k = 4$. Поліном третього степеня має вигляд $P(x) = x^3 + x + 1 \rightarrow 1011$

Залишки від ділення одиниці з нулями на $P(x)$:

```
 10000 | 1011
 1011
 ----
  1100        011
  1011        110
  ----
  1110        111
  1011
  ----
  1010        101
  1011
  ----
     1
```

Утворювальна матриця має вигляд

$$\begin{array}{c} \\ a_1 \\ a_2 \\ a_3 \\ a_4 \end{array} \left\| \begin{array}{ccccccc} k_4 & k_3 & k_2 & k_1 & m_3 & m_2 & m_1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 \end{array} \right\|$$

Це перші чотири комбінації формівного циклічного коду. Інші 11 комбінацій можуть формуватися шляхом додавання за модулем 2 цих комбінацій:

$$a_5 = a_1 \oplus a_2 = 0011101 \qquad a_{11} = a_1 \oplus a_2 \oplus a_3 = 0111010$$
$$a_6 = a_1 \oplus a_3 = 0101100 \qquad a_{12} = a_1 \oplus a_2 \oplus a_4 = 1011000$$
$$a_7 = a_1 \oplus a_4 = 1001110 \qquad a_{13} = a_2 \oplus a_3 \oplus a_4 = 1110100$$
$$a_8 = a_2 \oplus a_3 = 0110001 \qquad a_{14} = a_1 \oplus a_3 \oplus a_4 = 1101001$$
$$a_9 = a_2 \oplus a_4 = 1010011 \qquad a_{15} = a_1 \oplus a_2 \oplus a_3 \oplus a_4 = 1111111$$
$$a_{10} = a_3 \oplus a_4 = 1100010$$

Нульова комбінація також використовується (усі символи – нулі).

При другому способі утворення циклічного коду утворювальна матриця $\mathbf{G}_{nk}$ формується шляхом множення утворювального полінома $P(x)$ степеня m на одночлен x^{k-1} і наступних $k-1$ зсувів отриманої комбінації. Формівні при цьому кодові комбінації мають властивості циклічності, але інформаційні та перевірні символи в них не розділені.

Необхідно зауважити, що під час побудови утворювальної матриці циклічного коду кожний з них можна подати у $k-1$ різних варіантах, які відрізняються один від одного довжиною n, кількістю інформаційних елементів k, а також пропускною здатністю при однакових корегувальних характеристиках. Ці варіанти так званих ***укорочених циклічних кодів*** формуються викреслюванням певної кількості останніх рядків і такої самої кількості стовпців ліворуч в утворювальній матриці $\mathbf{G}_{n,k}$. При цьому кількість контрольних елементів залишається незмінною, а довжина коду і кількість інформаційних елементів зменшуються відповідно на число, що дорівнює кількості викреслених рядків і стовпців.

Так, якщо в утворювальній матриці $\mathbf{G}_{15,11}$ викреслити шість останніх рядків і шість перших лівих стовпців, то можна отримати утворювальну матрицю $\mathbf{G}_{9,5}$ укороченого циклічного коду. Характеристика вкороченого коду залишається такою самою, як і в (15, 11)-коді.

$$\mathbf{G}_{15,11}=\left\|\begin{array}{cccccccccccccc}
0&0&0&0&0&0&0&0&0&0&1&0&0&1&1\\
0&0&0&0&0&0&0&0&0&1&0&0&1&1&0\\
0&0&0&0&0&0&0&0&1&0&0&1&1&0&0\\
0&0&0&0&0&0&0&1&0&0&0&1&0&1&1\\
0&0&0&0&0&0&1&0&0&0&0&0&1&0&1\\
0&0&0&0&0&1&0&0&0&0&0&1&0&1&0\\
0&0&0&0&1&0&0&0&0&0&0&0&1&1&1\\
0&0&0&1&0&0&0&0&0&0&0&1&1&1&0\\
0&0&1&0&0&0&0&0&0&0&0&1&1&1&1\\
0&1&0&0&0&0&0&0&0&0&0&1&1&0&1\\
1&0&0&0&0&0&0&0&0&0&0&1&0&0&1
\end{array}\right\|$$

$$\mathbf{G}^{*}_{9,5}=\left\|\begin{array}{ccccccccc}
0&0&0&0&1&0&0&1&1\\
0&0&0&1&0&0&1&1&0\\
0&0&1&0&0&1&1&0&0\\
0&1&0&0&0&1&0&1&1\\
1&0&0&0&0&0&1&0&1
\end{array}\right\|$$

Якщо необхідно побудувати утворювальну матрицю $\mathbf{G}_{7,4}$. Утворювальний поліном має вигляд x^3+x+1, то перший рядок матриці можна

отримати з виразу $P(x) \cdot x^{k-1} = 1011 \cdot 1000 = 1011000$, наступні $k-1$ рядків – шляхом циклічного зсуву отриманої комбінації. Таким чином формується утворювальна матриця $\mathbf{G}_{7,4}$.

У циклічних кодах, як і в усіх систематичних, процес кодування зводиться до визначення m контрольних розрядів на підставі відомих k інформаційних. Кожний контрольний розряд знаходиться за допомогою перевірного співвідношення, а визначення всіх m перевірних розрядів вимагає m перевірних співвідношень, які записуються одне під одним у вигляді перевірної матриці **H**. У циклічних кодах перевірна матриця **H** може бути знайдена крім вже описаного способу за допомогою так званого контрольного полінома:

$$h(x) = \frac{x^n + 1}{P^{-1}(x)} = b_0 + b_1 x + \ldots + b_k x^k, \qquad (3.41)$$

де $P^{-1}(x)$ – поліном, сполучений з утворювальним поліномом $P(x)$, чи обернений йому.

Оберненими називаються поліноми, які утворюються шляхом підстановки $1/x$ замість x до основного полінома і його множення на одночлен x^i, де i – степінь основного полінома.

У сполучених поліномах члени розташовані у зворотному порядку. Так, поліноми 1101 і 1011 є сполученими. Якщо поліном $h(x)$ представити у вигляді комбінації $b_0, \ldots, b_k$, то перевірну матрицю можна побудувати в такий спосіб. Перший рядок матриці являє собою комбінацію полінома $h(x)$, доповнену $(m-1)$ нулями. Наступні $m-1$ рядків матриці будуються шляхом циклічного зсуву першого рядка. При такій побудові перевірна матриця має вигляд

$$\mathbf{H} = \left\| \begin{array}{cccccccccc} \overbrace{} & & & & & & & & & n \\ b_0 & b_1 & \ldots & b_k & 0 & 0 & 0 & \ldots & 0 & \\ 0 & b_0 & \ldots & b_{k-1} & b_k & 0 & 0 & \ldots & 0 & \\ 0 & 0 & \ldots & b_{k-2} & b_{k-1} & b_k & 0 & \ldots & 0 & \\ \ldots & & & & & & & & & \\ 0 & 0 & & 0 & 0 & \underbrace{b_0} & \underbrace{b_1} & \ldots & \underbrace{b_k} & \\ & & & & & k+1 & & & & \end{array} \right\| \; m$$

Перевірна матриця, побудована за методикою, поданою раніше, зовні може відрізнятися від матриці, побудованої за допомогою перевірного полінома. Але обидві матриці завжди можуть бути зведені до одного вигляду.

Найважливішою задачею побудови циклічних кодів є вибір утворювального полінома, який задовольняє заздалегідь задані умови. Якщо код призначений для виправлення незалежних помилок, такою умовою є забезпечення заданої кодової відстані d. У випадку, коли код призначений для виправлення пакетів помилок, умовою є довжина b пакета помилок, що виправляється або виявляється.

Знаходження порядку полінома починається з вибору інформаційних розрядів k за заданим об'ємом коду $N = 2^k$. Потім визначається найменша довжина кодового слова n, яка забезпечує виявлення або виправлення помилок заданої кратності. Для циклічних кодів ця проблема зводиться до знаходження потрібного полінома $P(x)$. Утворювальний поліном необхідно вибирати, як вже відзначалось раніше, з урахуванням того, що його степінь повинен дорівнювати кількості контрольних символів m. Крім цього, поліном $P(x)$ повинен входити як співмножник у розклад двочлена

$$x^n + 1 = x^{2i-1} + 1 . \tag{3.42}$$

Доведено, що будь-який двочлен типу (3.42) може бути представлений добутком усіх без винятку неприведених поліномів, степені яких є дільниками числа i (від 1 до i включно). Отже, для будь-якого i існує, принаймні, один неприводимий поліном степені i, що входить співмножником у розклад двочлена $x^n + 1$.

Боуз і Чоудхури показали, що для будь-яких цілих додатних чисел i, s існує циклічний код значності

$$n = 2^i - 1 \tag{3.43}$$

із кодовою відстанню $d \geq 2s + 1$. При цьому кількість перевірних символів $m = n - k$ не перевищує величини $i \cdot s$, тобто $m \leq i \cdot s$. Такий код гарантовано виправляє помилки кратності s і менше або виявляє помилки кратності $2s$ і менше. Крім того, код виявляє всі пакети помилок, довжина яких до-

рівнює або менше m. Наведені співвідношення можуть бути використані для вибору утворювального полінома.

Необхідно відзначити, що якщо є помилки різної кратності, то в першу чергу необхідно усунути однократні помилки, імовірність появи яких найбільша.

Оскільки в циклічному коді розпізнавачами помилок є залишки від ділення поліномів помилок на утворювальний поліном $P(x)$, то $P(x)$ повинен забезпечувати необхідну кількість різних залишків при діленні векторів помилок з одиницею у спотвореному розряді (тому що вектор поодинокої помилки має одиницю лише у спотвореному розряді та нулі у всіх інших розрядах). Утворювальними поліномами, як уже згадувалося, вибираються неприводимі, оскільки вони дають найбільшу кількість залишків. При степені полінома $m = n - k$ він може дати $n - k - 1$ ненульових залишків (нульова остача є розпізнавачем безпомилкового передавання).

Таким чином, необхідною умовою виправлення будь-якої поодинокої помилки є виконання нерівності $2^{n-k} - 1 \geq C_n^1 = n$, як вже показано під час розгляду теоретичних засад побудови кодів.

Здатність циклічного коду виявляти помилки визначається не лише степенем утворювального полінома, але і кількістю його членів. Чим більше залишків може бути утворено при діленні полінома повідомлення на утворювальний поліном, тим вищою є корегувальна здатність коду. Найбільше число залишків, яке дорівнює $2^i - 1$ (крім нульового), може забезпечити лише неприводимий поліном степеня i.

Для побудови циклічного (n, k)-коду, що забезпечує виявлення або виправлення помилок заданої кратності, як вже відзначалось, насамперед варто вибрати утворювальний поліном степеня $m = n - k$. Він повинен входити як співмножник у розклад двочлена $x^n + 1$. Однак не кожний поліном степеня m, що входить у розклад даного двочлена, може бути використаний для утворення потрібного (n, k)-коду. При формуванні додаткової матриці $C_{m,k}$ згідно з вибраним поліномом необхідно також враховувати кількість рядків у циклі зміни контрольних розрядів і вагу w кожного рядка (кількість одиниць).

Поняття про обернені поліноми є корисним для вибору утворювальних поліномів під час побудови циклічних кодів. Наприклад, якщо буде встановлено, що поліном $P(x)$ придатний для побудови циклічного коду із

заданими характеристиками, то і обернений йому поліном $P^{-1}(x)$ буде також придатний для побудови циклічного коду з тими самими характеристиками. Ці коди відрізняються лише порядком розташування залишків. Наприклад, матриці залишків для основного полінома $P(x) = x^3 + x + 1 \rightarrow 1011$ і оберненого йому полінома $P^{-1}(x) = x^3 + x^2 + 1 \rightarrow 1101$ мають вигляд

$$\mathbf{C} = \begin{Vmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{Vmatrix}, \qquad \mathbf{C}^{-1} = \begin{Vmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{Vmatrix}$$

Порівнюючи ці матриці, легко помітити, що рядки другої матриці розташовані у зворотному порядку, причому розряди в них також розташовані у зворотному порядку.

Табличні і розрахункові методи знаходження утворювальних поліномів циклічних кодів не завжди дозволяють однозначно вибирати найкращий поліном для певного типу каналу і певного характеру розподілу помилок.

Утворювальний поліном $P(x)$ бере участь у створенні кожної кодової комбінації, тому вона ділиться на утворювальний поліном без залишку. Але без залишку діляться лише ті поліноми (комбінації), які належать даному коду, тобто утворювальний поліном дозволяє вибрати дозволені кодові комбінації з усіх можливих. Якщо ж при діленні прийнятої кодової комбінації циклічного коду на утворювальний поліном буде отриманий залишок, то наявна помилка. Таким чином, залишки від ділення прийнятої комбінації на утворювальний поліном є розпізнавачем помилок циклічних кодів. Але залишки ще не вказують безпосередньо на місце помилки в кодовій комбінації.

У циклічних кодах ідея виправлення помилок ґрунтується на тому, що помилкова комбінація після певної кількості циклічних зсувів „підганяється" під залишок таким чином, щоб сумарно із залишком вона давала б виправлену комбінацію. Залишок при цьому являє собою різницю між спотвореними та правильними символами, а одиниці у залишку розташовують на місцях спотворених розрядів у „підігнаній" циклічними зсувами комбінації. „Підганяють" спотворену комбінацію доти, поки кількість

одиниць у залишку не буде дорівнює кількості помилок у коді. При цьому, природно, кількість одиниць може дорівнювати числу помилок s, що виправляються даним кодом (код виправляє три помилки і у спотвореній комбінації три помилки) або менше (код виправляє три помилки, у прийнятій комбінації – одна помилка).

Таким чином, для виявлення і виправлення помилкового розряду здійснюють такі операції:

1. Прийняту комбінацію ділять на утворювальний поліном;
2. Підраховують кількість одиниць у залишку (вагу залишку w). Якщо $w \le s$, то прийняту комбінацію складають за модулем два з отриманим залишком. Сума дає виправлену комбінацію. Якщо $w > s$, то
3. Роблять циклічний зсув прийнятої комбінації вліво на один розряд. Комбінацію, отриману в результаті циклічного зсуву, ділять на утворювальний поліном $P(x)$. Якщо в результаті повторного ділення $w \le s$, то ділене додають до залишку, після чого
4. Здійснюють циклічний зсув вправо на один розряд комбінації, отриманої в результаті додавання останнього діленого з останнім залишком. Отримана комбінація вже не містить помилок. Якщо після першого циклічного зсуву і наступного ділення залишок виходить таким, що його вага $w > s$, то
5. Повторюють операцію п. 3 доти, поки не буде досягнуто $w \le s$. У цьому випадку комбінацію, отриману в результаті останнього циклічного зсуву, додають до залишку від ділення цієї комбінації на утворювальний поліном, а потім
6. Здійснюють циклічний зсув вправо рівно на стільки розрядів, на скільки зсунена щодо прийнятої комбінація, що додавалась до останнього залишку. В результаті отримується виправлена комбінацію.

Коди Боуза-Чоудхурі-Хоквингема (БЧХ) є різновидом циклічних кодів. Один зі способів знаходження утворювального полінома для кодів БЧХ полягає в тому, що він визначається за заданою кодовою відстанню і довжиною кодової комбінації. Довжина кодової комбінації кодів БЧХ знаходимо з виразу

$$n = 2^i - 1 , \qquad (3.44)$$

де i – будь-яке ціле число.

Таким чином, величина n може дорівнювати 3, 7, 15, 31, 63, 127, 255, 511, 1023 розрядам тощо. Кількість перевірних розрядів коду

$$m = \frac{i \cdot (d-1)}{2}. \tag{3.45}$$

Отже, кількість інформаційних розрядів

$$k \geq 2^i - 1 - \frac{i \cdot (d-1)}{2}. \tag{3.46}$$

Параметри кодів БЧХ (до $n = 255$), обчислюються за формулами (3.44) – (3.46) і зведені до табл. 3.11.

Утворювальний поліном коду Боуза-Чоудхурі-Хоквингема є найменшим спільним кратним (НСК) мінімальних поліномів $i_j(x)$, де $i = 1, 3, 5, ..., (d-2)$ – порядок полінома $P(x) = \text{НСК}((i_1(x) \cdot i_2(x) \cdot \ldots \cdot i_{d-2}(x))$. Обчислені значення мінімальних поліномів для ступеня $i = 2 \div 10$ наведені в табл. 3.12.

Значення $i_j(x)$ подані у таблиці у шістнадцятковій системі числення. Так, поліном 19-го порядку для степеня $i = 10$, записаний у таблиці числом 5FB, визначає двійкову послідовність 101 1111 1011, а в аналітичному вигляді: $x^{10} + x^8 + x^7 + x^6 + x^4 + x^3 + x + 1$.

Для знаходження утворювального полінома коду довжиною $n = 2^{i-1}$ розрядів з кодовою відстанню d необхідно виписати з таблиці всі значення мінімальних поліномів, що відповідають заданому i, до порядку $d - 2$ включно. Якщо даний порядок в таблиці відсутній, необхідно взяти найближчий менший.

Приклад

Нехай необхідно побудувати код довжиною $n = 15$ ($i = 4$) з $d = 7$. Отже, утворювальний поліном $P(x) = i_1(x) + i_3(x) + i_7(x)$.

З табл. 3.12 можна знайти мінімальні поліноми: $i_1(x) = 13$ або $10011 = x^4 + x + 1$; $i_3(x) = 1\text{E}$ або $11111 = x^4 + x^3 + x^2 + x + 1$; $i_5(x) = 7$ або $111 = x^2 + x + 1$.

Таблиця 3.11 – Параметри кодів БЧХ

n	k	r	d	k/n	n	k	r	d	k/n
7	4	3	3	0,57	255	247	8	3	0,97
15	11	4	3	0,73	255	239	16	5	0,94
15	7	8	5	0,47	255	231	24	7	0,91
15	5	10	7	0,33	255	223	32	9	0,87
31	26	5	3	0,84	255	215	40	11	0,84
31	21	10	5	0,68	255	207	48	13	0,81
31	16	15	7	0,52	255	199	56	15	0,78
31	11	20	11	0,35	255	191	64	17	0,75
31	6	25	15	0,19	255	187	68	19	0,73
63	57	6	3	0,9	255	179	76	21	0,70
63	51	12	5	0,81	255	171	84	23	0,67
63	45	18	7	0,72	255	163	92	25	0,64
63	39	24	9	0,62	255	155	100	27	0,61
63	36	27	11	0,57	255	147	108	29	0,58
63	30	33	13	0,48	255	139	116	31	0,55
63	24	39	15	0,37	255	131	124	37	0,51
63	18	45	21	0,29	255	123	132	39	0,48
63	16	47	23	0,25	255	115	140	43	0,45
63	10	53	27	0,16	255	107	148	45	0,42
63	7	56	31	0,11	255	99	156	47	0,39
127	120	7	3	0,95	255	91	164	51	0,38
127	113	14	5	0,89	255	87	168	53	0,34
127	106	21	7	0,84	255	79	176	55	0,31
127	99	28	9	0,78	255	71	184	59	0,28
127	92	35	11	0,72	255	63	192	61	0,25
127	85	42	13	0,67	255	55	200	63	0,22
127	78	49	15	0,61	255	45	210	87	0,18
127	71	56	19	0;56	255	37	218	91	0,15
127	64	63	21	0,50	255	29	226	95	0,11
127	57	70	23	0,45	255	21	234	111	0,08
127	50	77	27	0,39	255	13	242	119	0,05
127	43	84	29	0,34	255	9	246	127	0,04
127	36	91	31	0,28					
127	29	98	43	0,23					
127	22	105	47	0,17					
127	15	112	55	0,12					
127	8	119	63	0,06					

Таблиця 3.12 – Значення мінімальних поліномів

Порядок поліно-ма, *j*	Мінімальні поліноми при значенні степеня *i*								
	2	3	4	5	6	7	8	9	10
1	7	B	13	25	43	89	9D	89	409
3	—	—	1E	3D	57	8F	177	259	80F
5	—	—	7	37	67	9D	1F3	331	50D
7	—	—	—	—	49	F7	169	299	7F9
9	—	—	—	—	D	BF	1BD	313	8AF
11	—	—	—	—	6D	D5	1D7	313	835
13	—	—	—	—	—	83	12B	277	46F
15	—	—	—	—	—	—	1D7	361	5AB
17	—	—	—	—	—	—	13	2DB	74D
19	—	—	—	—	—	CB	165	277	5FB
21	—	—	—	—	7	E5	18B	217	7EB
23	—	—	—	—	—	—	163	3E9	41B
25	—	—	—	—	—	—	109	3E3	523
27	—	—	—	—	—	—	13F	38F	77B
29	—	—	—	—	—	—	—	36B	531
31	—	—	—	—	—	—	—	—	623
33	—	—	—	—	—	—	—	—	3D
35	—	—	—	—	—	—	—	301	613
37	—	—	—	—	—	—	15F	26F	763
39	—	—	—	—	—	—	—	3CD	447
41	—	—	—	—	—	—	—	373	5E5
43	—	—	—	—	—	—	1C3	3CB	519
45	—	—	—	—	—	—	139	27D	631
47	—	—	—	—	—	—	—	—	67F
49	—	—	—	—	—	—	—	—	755
51	—	—	—	—	—	—	1F	3D5	565
53	—	—	—	—	—	—	—	295	58F
55	—	—	—	—	—	—	—	2BD	72B
57	—	—	—	—	—	—	—	—	651

Помноживши отримані мінімальні поліноми, визначимо утворювальний поліном заданого коду БЧХ: $P(x) = 10100110111$. Шляхом побудови утворювальної матриці можна переконатися в тому, що отриманий код дійсно має кодову відстань, рівну семи.

Коди БЧХ мають непарні значення мінімальної кодової відстані *d*. При бажанні кодову відстань можна збільшити на одиницю, застосувавши

утворювальний поліном, який дорівнює добутку утворювального полінома коду БЧХ на двочлен $(x + 1)$.

Так, у розглянутому коді із $d = 7$ мінімальну кодову відстань можна підвищити до восьми, якщо використати утворювальний поліном

$$P(x) = (x + 1) \cdot (x^{10} + x^8 + x^7 + x^6 + x^4 + x^3 + x + 1);$$
$$P(x) = x^{11} + x^{10} + x^9 + x^8 + x^6 + x^4 + x^3 + 1,$$

тобто $P(1, 0) = 111101011001$.

Такий спосіб збільшення мінімальної кодової відстані застосовується до будь-яких систематичних кодів з непарною мінімальною кодовою відстанню. Для цього в циклічних кодах змінюється утворювальний поліном, а в інших систематичних кодах вводиться додаткова перевірка на парність, що охоплює всі інформаційні розряди.

Під час розгляду кодів БЧХ необхідно відзначити такі закономірності. Кількість кодів, що розрізняються за корегувальною здатністю і мають загальну довжину кодової комбінації $n = 2^i - 1$, на дві одиниці менша кількості всіх неприводимих поліномів, на які розкладається двочлен $x^{2-1i} + 1$. Наприклад, можна визначити кількість циклічних кодів для $n = 15$. Оскільки отриманий поліном $x^{15} + 1$ не є найпростішим, то $i = 4$ є старшим степенем неприводимого полінома, на який розкладається двочлен $x^{15} + 1$.

Тепер необхідно виписати всі неприводимі поліноми степені 4, а також неприводимі поліноми тих степенів, показники яких є дільниками числа 4, тобто 1 і 2. Таким чином, степінь двочлена $x^{15} + 1$ складається із сум степенів всіх неприводимих поліномів, кількість яких дорівнює одиниці – для першого степеня, одиниці – для другого степеня і трьом – для четвертого степеня. Виписавши всі ці поліноми, можна знайти розклад двочлена

$$x^{15} + 1 = (x + 1)\cdot(x^2 + x + 1)\cdot(x^4 + x + 1)\cdot(x^4 + x^3 + 1)\cdot(x^4 + x^3 + x^2 + x + 1)$$

Як видно з розкладу, кількість неприводимих поліномів дорівнює п'яти, а отже, кількість циклічних кодів для $n = 15$ дорівнює трьом.

Наступною важливою властивістю коду БЧХ є співвідношення між максимальною кодовою відстанню d і числом i:

$$d_{max} = 2^{i-1} - 1. \qquad (3.47)$$

Для попереднього прикладу при $n = 15$ $(i = 4)$ $d_{max} = 2^{4-1} - 1 = 7$.

Крім цього, варто зауважити, що кількість інформаційних розрядів, яка може бути використана при заданому числі i та максимальній кодовій відстані, визначається як $(i + 1)$. У наведеному прикладі для $d_{max} = 7$ $k = 5$.

За деяких умов циклічні коди Ріда-Соломона (РС) є частковим випадком кодів БЧХ. Коди РС мають величезну корегувальну здатність і дозволяють виправляти декілька пакетів помилок.

Якщо задано корегувальний код з основою $i > 2$, у комбінаціях якого можна виправляти помилки кратності s і кожному символу цього коду поставлена у взаємно однозначну відповідність певна n_1-розрядна двійкова комбінація, то отриманий у такий спосіб двійковий код може виправляти пакети помилок довжиною $b = n \cdot (s - 1) + 1$ і менше. Код із зазначеними властивостями утворюється в тому випадку, коли основа $i = 2^a$, довжина $n = a(2^a - 1)$ і утворювальний поліном

$$P(x) = (x - a_1)\cdot(x - a_2)\cdot \ldots \cdot(x - a_{d-1}), \qquad (3.48)$$

де a – примітивний елемент поля $GF(2^a)$.

Коди зазначеного типу називаються кодами Ріда-Соломона. У (3.48) степінь полінома $P(x)$ дорівнює $d - 1$. В результаті формується код довжини n з $d - 1$ контрольними розрядами і кодовою відстанню d.

Та обставина, що коди РС при будь-якій заданій швидкості мають найбільшу можливу мінімальну відстань Хеммінга, робить їх привабливими з точки зору практичного використання. В той самий час структура цих кодів допускає відносно просту технічну реалізацію, тому практичне застосування цілком можливо у випадках наявності пакетних помилок.

Література

1. Кодирование информации. Двоичные коды / под ред. Березюка Н.Т. – Харьков: Издательство при Харьковском государственном университете, 1978. – С. 164 – 209.
2. Васюра А.С., Кривогубченко С.Г., Кулик А.Я. та ін. Техніка передавання дискретної інформації. – Вінниця.: ВДТУ, 1998. – С. 66 – 71.

3. Квєтний Р.Н., Компанець М.М., Кривогубченко С.Г., Кулик А.Я. Основи техніки передавання інформації / Підручник. – Вінниця: Універсум-Вінниця, 2002. – С. 195 – 200.
4. Шварцман В.О., Емельянов Г.А. Теория передачи дискретной информации. – М.: Связь, 1979. – С. 296 – 318.

3.12 Алгоритми згорткового кодування

На відміну від всіх розглянутих вище кодів, що є блоковими, згорткові коди є неперервними (рекурентними). Їх кодування та декодування здійснюється безупинно, без розділу інформаційної послідовності на блоки. Згорткові коди є прикладом неперервних (рекурентних) кодів. В основу їх побудови покладений принцип формування перевірних розрядів шляхом додавання за модулем 2 кожного інформаційного розряду з деяким набором попередніх розрядів. Приклад найпростішого згорткового кодера наведений на рис. 3.9.

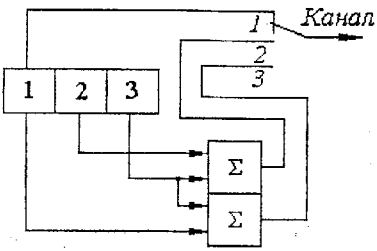


Рисунок 3.9 – Структура згорткового кодера

Вхідна інформаційна послідовність $\mathbf{X} = x_1 x_2, ..., x_n$ надходить у регістр багататактового фільтра ($N = 3$), деякі з комірок якого пов'язані з двома суматорами за модулем 2. На контакт 1 комутатора поданий інформаційний символ, на контакти 2 та 3 – контрольні. Після надходження кожного інформаційного символу комутатор здійснює зчитування трьох символів (інформаційного та двох перевірних) і передає їх до каналу. Оскільки в розглянутому випадку в канал подаються як інформаційний, так і контрольні символи, то вихідна кодова послідовність є систематичною. Разом з тим, вихід з першої комірки на контакт 1 може бути відсутнім або на цей контакт можуть бути подані також виходи інших комірок, внаслідок чого код буде несистематичним. Зчитування вихідних символів комутатором здійснюється після кожного надходження l

інформаційних символів, де $l = 1, 2, 3, ...$, причому зазвичай l є кратним N, тобто $N/l = n$.

Для задання згорткового коду достатньо вказати довжину регістра і які з його комірок пов'язані з кожним з b суматорів за модулем 2. Кількість суматорів у схемі на рис. 3.9 $b = 3$, тому що для спрощення на рисунку не показаний суматор, включений між першою коміркою і контактом 1 комутатора. Зв'язки i-того суматора описуються i-тою породжувальною послідовністю $g_i = g_{i1}, g_{i2}, \ldots, g_{iN}$, де $g_{ij} = 1$, якщо j-та комірка зв'язана з i-тим суматором, інакше $g_{ij} = 0$.

Матриця $\mathbf{G} = \|g_{ij}\|$, $i = 1, 2, ..., b$, $j = 1, 2, ..., N$ називається породжувальною матрицею. Наприклад, для кодера на рис. 3.9 $N = 3$, $b = 3$ і $g_{i1} = 100$, $g_{i2} = 010$, $g_{i3} = 011$, отже, $g_i = 100010011$. Вихідний сигнал i-го суматора після надходження на вхід t-того символу x_t дорівнює:

$$S_i(t) = g_{i1} \cdot x_t \oplus g_{i2} \cdot x_{t-1} \oplus \ldots \oplus g_{iN} \cdot x_{t-N+1}, \qquad (3.49)$$

де $x_t = 0$ при $t \le 0$.

Важливим параметром згорткового коду є ***кодове обмеження*** $\nu = n \cdot b$. Довжина кодового обмеження в теорії згорткових кодів відіграє роль, аналогічну довжині блока в теорії блокових кодів. У випадку $t = 1$, тобто $N = n$, $\nu = N \cdot b$. Кодове обмеження являє собою кількість кодових символів, породжуваних кодером протягом часу між надходженням у нього даного інформаційного символу і виведенням його до каналу. У прикладі $\nu = 3 \cdot 2 = 6$.

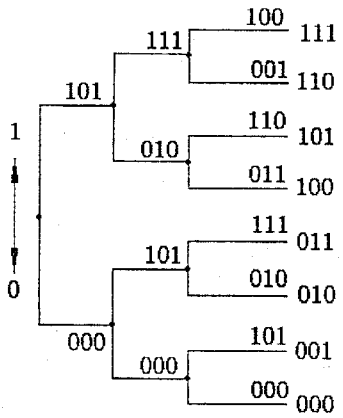


Рисунок 3.10 – Кодове дерево $b = 3$

Зручним апаратом для розгляду кодування та декодування згорткових кодів є кодове дерево. На рис. 3.10 зображений приклад кодового дерева для згорткового кодера (рис. 3.9). Крапками позначені вузли кодового дерева, що відповідають певній інформаційній послідовності на вході кодера. Початковий (крайній ліворуч) вузол відповідає моменту до початку надхо-

дження інформації. Відрізки між двома сусідніми вузлами називаються ***ребрами***. Сукупність декількох послідовних ребер називається ***гілкою***. Для визначення вузла, який відповідає деякій певній інформаційній послідовності, потрібно рухатися з початкового вузла вздовж кодового дерева, роблячи крок униз при надходженні інформаційного символу 0 і крок вверх при надходженні інформаційного символу 1. Уздовж ребер написані кодові символи на виході кодера, генеровані при переході від даного вузла до сусіднього праворуч.

Доцільно розглянути роботу кодера, наведеного як приклад (рис. 3.9), при надходженні на його вхід інформаційної послідовності 101. Нехай до моменту надходження кодової послідовності всі комірки регістра перебували в стані 0. Тоді після запису одиниці до першої комірки на виході кодера буде зчитана кодова комбінація 101 (див. другий рядок табл. 3.12).

Таблиця 3.12 – Таблиця істинності кодера

Крок	Вміст комірки			Вміст суматора			Примітка
	1	2	3	1	2	3	
1	0	0	0	0	0	0	Початковий стан
2	1	0	0	1	0	1	Введення до регістра 001
3	0	1	0	0	1	0	
4	1	0	1	1	1	0	
5	0	1	0	0	1	0	Введення до регістра 000
6	0	0	1	0	1	1	
7	0	0	0	0	0	0	

Потім до першої комірки регістра записується другий символ інформаційної послідовності (нуль), а її перший символ передається до другої комірки, в результаті чого до каналу буде передана кодова комбінація 010. Після записування до першої комірки регістра третього інформаційного символу (одиниці) до каналу буде передана кодова комбінація 110. Після надходження на вхід кодера останнього інформаційного символу подаються N нулів (у розглянутому прикладі $N = 3$), в результаті чого до каналу передаються ще три групи символів: 010, 011, 000, а регістр повертається до початкового стану.

Таким чином, інформаційна послідовність 101, що складається з трьох інформаційних символів ($L = 3$), в результаті згорткового кодування

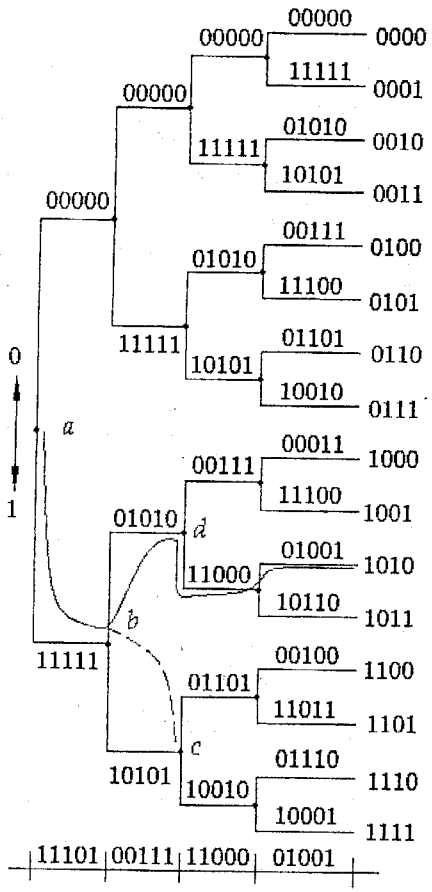


Рисунок 3.11 – Кодове дерево
$N = 4$, $b = 5$

перетворюється в кодову комбінацію 101 010 110 010 011 000, що складається з $(L + N) \cdot b = (3 + 3) \cdot 3 = 18$ символів. Зазвичай інформаційна послідовність складається з великої кількості символів так, що $L \gg N$, тому число символів у вихідній послідовності перевищує їхнє число у вхідний у b разів. Незважаючи на більшу надлишковість, згорткові коди знаходять поширення завдяки своїм корегувальним властивостям.

Процедура декодування згорткових кодів аналогічна процедурі кодування, і її зручно розглядати за допомогою кодового дерева рис. 3.10. Послідовність, що надходить на вхід декодера, аналізується по групах з трьох елементів ($b = 3$). Спочатку b перших елементів подаються на два вхідних дешифратори, перший з яких виділяє комбінацію 101, а другий – комбінацію 000. В залежності від того, яка з комбінацій надійшла в b перших елементів, відкривається шлях до однієї з пар дешифраторів, що виділяють b інших елементів, значення яких визначаються кодовим деревом, і т.д. доти, поки сигнал не з'явиться на одному з $2^N = 8$ виходів декодера. Така процедура декодування отримала назву ***послідовного декодування***.

Описаний процес відбувається саме таким чином, коли в прийнятій послідовності відсутні помилки. Наприклад, під час передавання інформаційної послідовності 101 до дискретного каналу, як було показано вище,

надходить послідовність 101 010 110, що за відсутності помилок відповідно до кодового дерева (рис. 3.10) правильно декодується в 101.

При наявності помилок у дискретному каналі розглянута процедура декодування виявиться неефективною, оскільки окремі групи прийнятої кодової послідовності не будуть збігатися з ребрами кодового дерева. Возенкрафтом запропонована ***імовірнісна процедура декодування***, що полягає у виборі при декодуванні такої кодової комбінації, що відрізняється від прийнятої послідовності в найменшій кількості розрядів. В такому випадку, якщо прийнята послідовність (вірніше, її окрема група з b елементів) не збігається з жодним ребром, що виходить із даного вузла, то декодер крокує спочатку ребром, у якого число символів, що збігаються, більше. Зрозуміло, що при числі помилок у групі з b елементів більшому, ніж $b/2$, такий декодер спочатку дійде до неправильного вузла. Однак малоймовірно, щоб, зробивши таку помилку, декодер знайшов у цьому неправильному вузлі ребро, що добре узгоджується з наступною групою з b прийнятих символів. Розглянемо, наприклад, кодове дерево (рис. 3.11), яке відповідає кодеру та декодеру ($N = 4$, $b = 5$), зображеним на рис. 3.12 та 3.13.

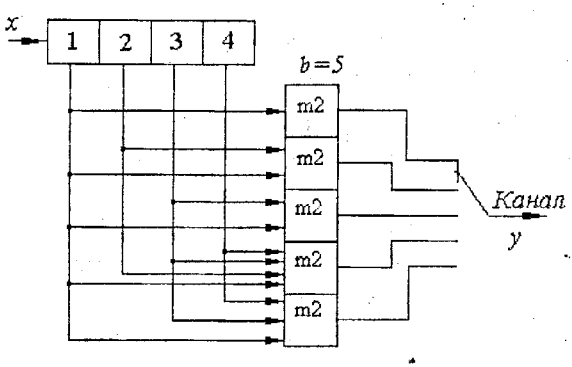


Рисунок 3.12 – Кодер $N = 4$, $b = 5$

При передаванні інформаційної послідовності x = 1010 на виході кодера отримаємо y = 11111 01010 11000 01001. Припустимо, що вектор помилки в каналі **e** = 00010 01101 00000 00000, тоді на вхід декодера надійде послідовність $\hat{x}$=11101 00111 11000 01001. В такому випадку, як показано на рис. 3.11 суцільною лінією, декодер з початкового вузла a крокує спочатку правильним шляхом до вузла b, а з нього – неправильним шляхом (пунктир) до вузла c, тому що 00111 відрізняється від 10101 двома розрядами, а від 01010 – трьома. Але у ребер, що виходять із вузла c, не збігається з 11000 стільки ж розрядів (два або три), скі-

льки й у правильного шляху (у вузол d), що дає підставу декодеру виявити помилковий поворот і повернутися у вузол b для виправлення помилки. Алгоритм Возенкрафта аналогічний послідовності дій водія автомобіля, який, зробивши неправильний поворот на роздоріжжі, швидко виявляє помилку, повертається на розвилку і пробує нову дорогу.

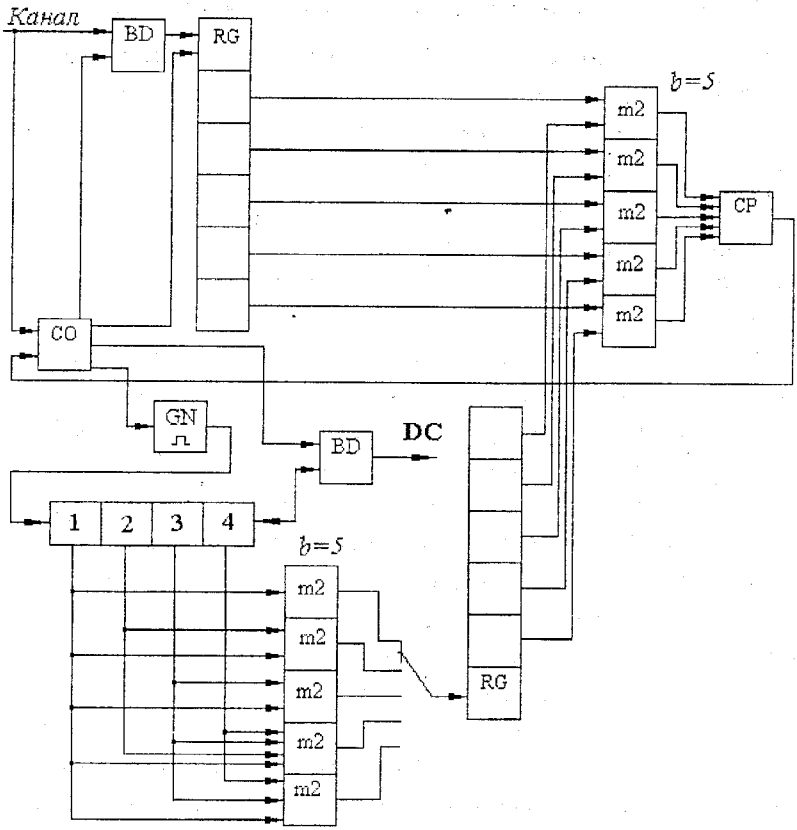


Рисунок 3.13 – Декодер $N = 4$, $b = 5$

Як приклад доцільно розглянути роботу декодера (див. рис. 3.12, 3.13) при надходженні на його вхід послідовності $\hat{x}$, що записується в буфер входу, звідки групами по п'ять елементів пишеться до верхнього регістра. Одночасно до регістру декодера від генератора подається випадкова послідовність нулів та одиниць, до нижнього регістра записується гіпоте-

тична послідовність y^*. Потім здійснюється обчислення хеммінгової відстані між прийнятою та гіпотетичною послідовностями $d(l) = \hat{x} \oplus y^*$. Нехай у перший розряд регістра декодера від генератора записана одиниця, тоді на першому ребрі $d(1) = 11101 \oplus 11111 = 1$.

Оскільки декодер вибирає шлях за принципом $d < b/2$ – шлях правильний, $d > b/2$ – шлях неправильний, то в розглянутому прикладі ($b = 5$, $d = 1$) у вузлі а шлях вибраний правильно. В першому розряді регістра декодера фіксується одиниця. Після цього у верхньому регістрі записується група символів 00111, а до нижнього регістра надходить друга гіпотетична комбінація.

Припустимо, що при цьому до першого розряду регістра декодера від генератора надійшла одиниця, тоді $d(2) = 00111 \oplus 10101 = 2$. Якщо ж до першого розряду регістра декодера був записаний нуль, то $d'(2) = 00111 \oplus 01010 = 3$.

Оскільки $2 < 5/2 < 3$, то декодер у вузлі b приймає неправильне рішення і крокує до вузла с. Для виявлення факту прийняття неправильного рішення декодер протягом руху уздовж кодового дерева обчислює поточне значення $d(l)$ і в кожному вузлі порівнює $d(l)$ з функцією вилучення критерію $k(l)$. Якщо $d(l)$ перевищує $k(l)$, то пробний шлях відкидається як малоймовірний і декодер повертається на найближче недосліджене ребро, для якого $d(l) \le k(l)$, і знову рухається вперед, поки задовольняється ця умова. Для простоти реалізації декодера за $k(l)$ вибирають пряму лінію з коефіцієнтом нахилу $p \cdot b$, що не проходить через нуль при $l = 0$, де $p_0 < p < 0{,}5$, де p_0 – перехідна імовірність каналу.

Назва „рекурентні коди" пов'язана з тим, що початкова формула (3.49) є рекурентною формулою. Як видно, коди такого класу характеризуються складністю алгоритмізації та реалізації. Враховуючи, що сучасні умови передавання суттєво обмежують наявність пакетних помилок, використання згорткових кодів обмежене.

Література

1. Шварцман В.О., Емельянов Г.А. Теория передачи дискретной информации. – М.: Связь, 1979. – С. 323 – 330.

2. Кузьмин И.В., Ключко В.И., Литвин В.А. Кодирование и декодирование в информационных системах. – К.: Выща школа, 1985. – С. 134 – 158.

3.13 Алгоритми кодування з використанням ортогональних функцій

З урахуванням необхідності забезпечення рівності імовірності позитивних і негативних імпульсів, другий варіант відповідає вимогам абсолютно, а перший може задовольнити лише за умови рівності імовірностей нулів та одиниць. Таким чином, використання методів кодування за Хеммінгом, циклічного та БЧХ вимагає додаткового перетворення за алгоритмом AMI або MLT-3, яке, в свою чергу, потребує додаткових програмних та апаратних витрат. Для запобігання цьому під час побудови кодів можна використати природні біполярні ортогональні функції Адамара, Хаара тощо.

Матрицю Адамара можна описати виразом

$$\mathbf{Had} = \mathbf{Had}_{(i-1)(j-1)} \otimes \mathbf{Had}_{(i-1)j} \otimes \mathbf{Had}_{i(j-1)} \otimes \overline{\mathbf{Had}}_{ij}, \qquad (3.50)$$

де символом "⊗" позначається прямий добуток квадратних кліткових матриць. Виходячи з цього можна побудувати матрицю 8 × 8:

$$\mathbf{Had}_8 = \begin{Vmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{Vmatrix}, \qquad (3.51)$$

рядки якої можуть виступати як кодові комбінації. Інші вісім кодових комбінацій можна отримати інвертуванням початкової матриці (3.52).

$$\overline{\mathbf{Had}_8} = \begin{Vmatrix} -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 \\ -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 \\ -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 \\ -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 \end{Vmatrix}. \qquad (3.52)$$

Повна матриця кодування буде мати вигляд (3.53).

$$\mathbf{Had}_8 = \begin{Vmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 \\ -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 \\ -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 \\ -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 \\ -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 \end{Vmatrix}. \qquad (3.53)$$

Принцип кодування полягає в тому, що складається таблиця відповідності між інформаційним напівбайтом та кодовою комбінацією коду Адамара **A**, наприклад, як це подано у табл. 3.13.

Оскільки код не має чіткої відповідності інформаційним розрядам (не є структурованим), то порядок призначення кодових комбінацій для процесу передавання може визначатися довільно.

Таблиця 3.13 – Таблиця кодування для коду Адамара $\mathcal{A}$

k	n	k	n
0000	1 1 1 1 1 1 1 1	1000	–1 –1 –1 –1 –1 –1 –1 –1
0001	1 –1 1 –1 1 –1 1 –1	1001	–1 1 –1 1 –1 1 –1 1
0010	1 1 –1 –1 1 1 –1 –1	1010	–1 –1 1 1 –1 –1 1 1
0011	1 –1 –1 1 1 –1 –1 1	1011	–1 1 1 –1 –1 1 1 –1
0100	1 1 1 1 –1 –1 –1 –1	1100	–1 –1 –1 –1 1 1 1 1
0101	1 –1 1 –1 –1 1 –1 1	1101	–1 1 –1 1 1 –1 1 –1
0110	1 1 –1 –1 –1 –1 1 1	1110	–1 –1 1 1 1 1 –1 –1
0111	1 –1 –1 1 –1 1 1 –1	1111	–1 1 1 –1 1 –1 –1 1

Функції Хаара теж природно трійкові. За допомогою основних функцій Хаара та циклічного зсуву їх розрядів можна побудувати матрицю кодування за умови обмеження кодової відстані $d_{\mathrm{H}_8} \geq 4$ вигляду (3.54). Всього таких кодових комбінацій може бути значно більше шістнадцяти, тому для формування кодових комбінацій можна вибрати будь-які шістнадцять, наприклад, як це подано у табл. 3.14.

Таблиця 3.14 – Таблиця кодування для коду Хаара $\mathcal{H}$

k	n	k	n
0000	1 1 1 1 1 1 1 1	1000	–1 –1 –1 –1 –1 –1 –1 –1
0001	1 1 1 1 0 0 0 0	1001	–1 –1 –1 –1 0 0 0 0
0010	0 0 0 1 1 1 1 1	1010	0 0 0 0 –1 –1 –1 –1
0011	1 1 1 1 –1 –1 –1 –1	1011	–1 –1 –1 –1 1 1 1 1
0100	0 0 1 1 1 1 0 0	1100	0 0 –1 –1 –1 –1 0 0
0101	1 1 0 0 0 0 1 1	1101	–1 –1 0 0 0 0 –1 –1
0110	0 0 1 1 0 0 1 1	1110	0 0 –1 –1 0 0 –1 –1
0111	1 1 0 0 1 1 0 0	1111	–1 –1 0 0 –1 –1 0 0

Отримані коди $\mathcal{A}$ та $\mathcal{H}$ дещо поступаються за параметрами передавання класичним двійковим (7, 4)-кодам, але не вимагають витрат на додаткову реалізацію біполярними сигналами.

$$\mathbf{H}_8 = \begin{Vmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & -1 & -1 & -1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & -1 & -1 & -1 & -1 & 0 & 0 \\ -1 & -1 & 0 & 0 & 0 & 0 & -1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ -1 & -1 & 0 & 0 & -1 & -1 & 0 & 0 \\ 0 & 0 & -1 & -1 & 0 & 0 & -1 & -1 \\ -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ -1 & 0 & -1 & 0 & -1 & 0 & -1 & 0 \\ 0 & -1 & 0 & -1 & 0 & -1 & 0 & -1 \\ -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ & & & \vdots & & & & \end{Vmatrix}. \qquad (3.54)$$

За допомогою функцій Хаара можна також побудувати шістнадцятирозрядний код $\mathcal{H}$ з кодовою відстанню $d_{\mathbf{H}_{16}} = 8$, спроможний виправляти три помилки, який описується матрицею (3.55). Кількість кодових комбінацій, які задовольняють умові кодової відстані, також більша від шістнадцяти, тому можна вибирати будь-які шістнадцять кодових комбінацій.

$$\mathbf{H}_{16} = \left\|\begin{array}{cccccccccccccccc}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
-1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
-1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
-1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\
-1 & -1 & -1 & -1 & 0 & 0 & 0 & 0 & -1 & -1 & -1 & -1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & -1 & -1 & -1 & -1 & 0 & 0 & 0 & 0 & -1 & -1 & -1 & -1 \\
0 & 0 & 0 & 0 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 0 & 0 & 0 & 0 \\
-1 & -1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 & -1 & -1 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
-1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\
 & & & & & & & \vdots & & & & & & & &
\end{array}\right\| \tag{3.55}$$

Коди (4, 1), (11, 3) та (13, 4), у яких $d = 5$, спроможні виправляти дві помилки, але передати всі вісім інформаційних розрядів за допомогою двох восьмирозрядних кодових комбінацій ними неможливо. Формально із запропонованим може конкурувати код БЧХ (15, 5), але він так само вимагає додаткового перетворення на біполярні сигнали, від чого позбавлений код $\mathcal{H}$, який визначається матрицею $\mathbf{H}_{16}$.

Використання класичних (n, k)-кодів з виправленням помилок зазвичай передбачає посимвольне приймання з алгебраїчними методами декодування. Це можна здійснити, оскільки існує чіткий алгоритм кодування, який описується математичними рівняннями. З одного боку, це забезпечує однозначність кодування, а з другого, не використовує можливостей коду щодо захисту інформації за рахунок надлишковості.

Оскільки для побудови кодових комбінацій в даному випадку не визначені алгебраїчні рівняння, то декодування можна здійснювати лише кореляційним методом, який полягає у порівнянні прийнятої кодової комбінації з усіма можливими для даного випадку кодовими словами і виборі того з них, яке знаходиться від прийнятого на мінімальній хемінговій відстані. Якщо вважати, що переданий сигнал належить коду $\mathcal{A}$ або $\mathcal{H}$, то він обов'язково буде входити до складових матриць **H** або **Had**. Прийнятий вектор $\hat{\mathbf{X}} = (x_1, x_2, x_3, ..., x_n)$ необхідно порівняти з векторами матриці, яка є основою прийнятого метода кодування. В результаті з отриманого кореляційного вектора

$$\mathbf{Y} = \hat{\mathbf{X}} \cdot \mathbf{H} = (y_1, y_2, y_3, ..., y_n), \tag{3.56}$$

або

$$\mathbf{Y} = \hat{\mathbf{X}} \cdot \mathbf{Had} = (y_1, y_2, y_3, ..., y_n) \tag{3.57}$$

вибирається компонента y_i, яка має найбільше додатне значення. Якщо $\max_i y_i = y_k$, то прийнятий сигнал можна розглядати як k-тий вектор матриці **H**. Відомо, що для каналу з білим шумом таке декодування оптимальне за критерієм Котельникова. Оскільки ідентифікація прийнятої кодової комбінації нерозривно пов'язана із вилученням шуму з прийнятого сигналу, то докладно цей процес доцільно розглянути пізніше.

Література

1. Кулик А.Я. Адаптивні алгоритми передавання інформації. – Вінниця: УНІВЕРСУМ-Вінниця, 2003. – С. 115 – 126.

3.14 Методи формування канальних кодів

Передавання інформації між двома далекими об'єктами вимагає подання її у вигляді послідовності бітів, характеристики якої залежать від особливостей конкретної системи.

Алгоритм роботи передавача, ретранслятора і приймача визначається вибраним кодом, який передається каналом зв'язку (канальним кодом).

Найбільш простим канальним кодом є уніполярний код ***NRZ*** (non return to zero). Для цього коду нулі подаються відсутністю імпульсів, а одиниці – наявністю імпульсів (рисунок 3.14).

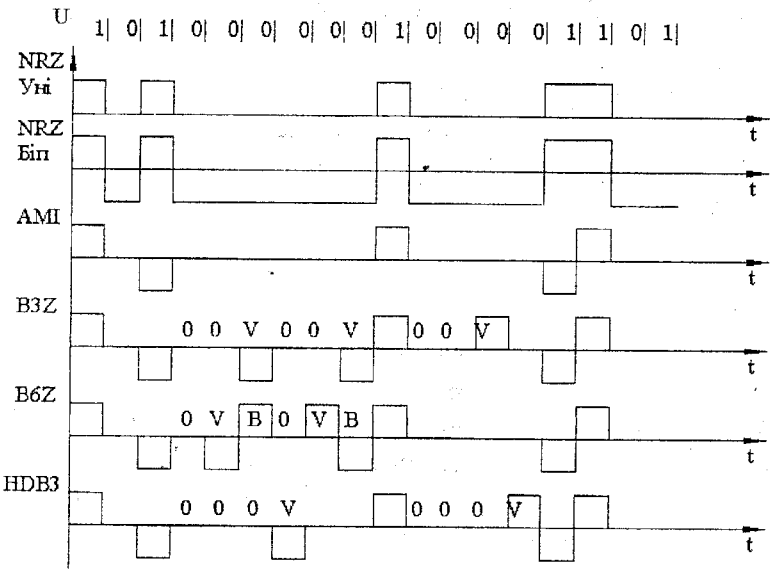


Рисунок 3.14 – Найбільш поширені канальні коди

Але цей код має певні недоліки:

* середня потужність, яка виділяється на навантажувальному резисторі R і дорівнює:

$$P_1 = \frac{U_i^2}{2R}, \tag{3.58}$$

де U_i – амплітуда імпульсу,

удвічі більша, ніж потужність під час біполярного кодування;

* більшість ліній зв'язку з'єднуються з апаратурою за допомогою трансформаторів. Оскільки уніполярні сигнали завжди містять в собі постійну складову і значну частину низькочастотних компонент під час переда-

вання значної кількості одиниць, то таке з'єднання буде реалізувати важко (реактивні елементи на низьких частотах мають великий опір або являють собою "коротке замикання");

* ретранслятори приймача мають змогу надійно відновити синхронізувальний сигнал лише тоді, коли паузи між імпульсами не дуже великі. Поява чергового імпульсу дозволяє коригувати синхросигнал, в той час, як в разі збільшення паузи до 10 000 символів похибка становить плюс-мінус один період, тобто приймач втрачає синхронізацію з передавачем;
* на приймачеві втрачається можливість оперативної реєстрації похибок, тобто зникнення або появи імпульсів.

Біполярний сигнал NRZ має кращі енергетичні показники. Одиниця в ньому подається позитивною напругою, нуль – негативною. Середня потужність сигналу дорівнює :

$$P_2 = \frac{U_i^2}{4R}, \tag{3.59}$$

тобто половині потужності уніполярного сигналу, хоча перепад напруг той самий. Для ліквідації інших трьох недоліків потрібно введення надлишковості, яке робиться одним з двох способів:

- швидкість передавання сигналів лінією дорівнює швидкості передавання інформації, але вводяться додаткові електричні рівні сигналів;
- швидкість передавання сигналів лінією береться більшою ніж швидкість передавання інформації без використання додаткових електричних рівнів сигналів.

Перший спосіб введення надлишковості пов'язаний з утворенням додаткових електричних рівнів. Таким чином формується код ***AMI***. В ньому нулі кодуються відсутністю імпульсів, а одиниці – по черзі позитивними та негативними імпульсами. Постійна складова дорівнює нулю, проблема передавання послідовності одиниць відсутня, а також визначаються помилки, які порушують правильну послідовність знакозмінних сигналів.

Єдина проблема, що залишається, - втрата синхронізації під час передавання послідовності нулів, як і у коді NRZ. Ця проблема вирішується таким чином, що послідовності нулів передавач замінює ланцюгами типових часових діаграм. Такі коди називаються ***BNZS***-кодами. В коді ***B3ZS*** кожні три послідовно розташовані нулі замінюються або комбінацією *B0V*

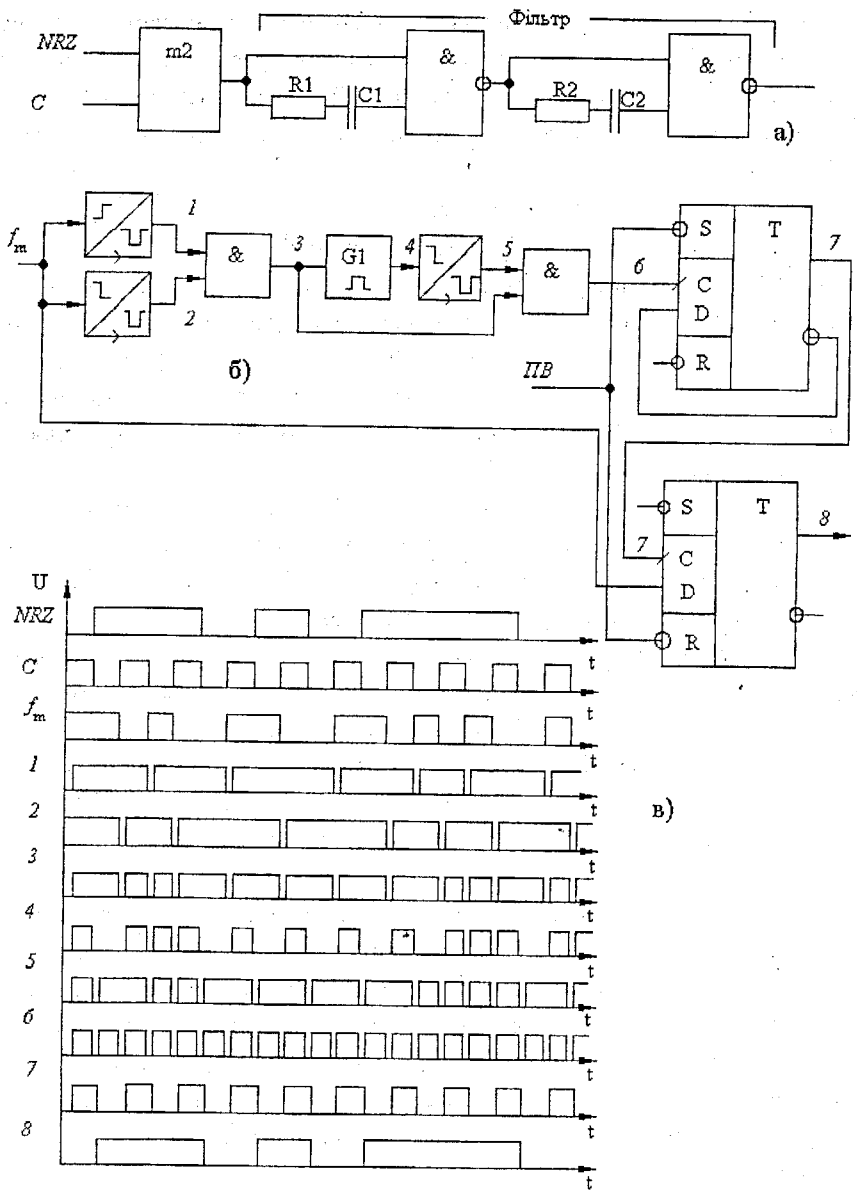
або *00V*. Символ *B* позначає імпульс, який відповідає правилам кодування AMI, символ *V*–імпульс, який порушує правила кодування AMI (збігається за полярністю з попереднім). Вибір комбінації проводиться так, щоб:

- ◊ кількість імпульсів B між двома послідовно розташованими імпульсами *V* була непарною;
- ◊ полярність імпульсів *V* змінювалась.

В коді ***B6ZS*** кожні шість послідовних нулів замінюються комбінацією *0VB0VB*. Ці коди розповсюджені в інформаційних та обчислювальних мережах США та Канади на високих швидкостях передавання. У країнах Західної Європи розповсюджений код ***HDB3***, схожий на BNZS. В ньому кожні чотири послідовних нулі замінюються комбінацією *000V* або *B00V*. Вибір комбінації відбувається таким чином, щоб зберігалося виконання умов, сформульованих для коду B3ZS.

Розповсюджені також коди CMI, PST, 4B3T, які є різновидами коду AMI і утворені для мінімізації вимог до смуги пропускання каналів зв'язку і збільшення завадозахищеності. Для всіх цих кодів розроблені мікросхеми, кожна з яких є шифратором і дешифратором.

Прикладом коду з надлишковістю, введеною згідно з другим способом, є код ***"Манчестер - II"***. Для нього одиниця кодується негативним перепадом сигналу посередині бітового інтервалу, нуль – позитивним перепадом. На границях бітових інтервалів сигнал, якщо це необхідно, змінює значення, готуючись до зображення чергового біта посередині наступного бітового інтервалу. За допомогою коду "Манчестер II" вирішуються всі перераховані проблеми. Оскільки кількість позитивних і негативних імпульсів розрізняється не більше, як на одиницю, постійна складова спектра сигналу дорівнює нулю. Синхронізація приймача або ретранслятора відбувається за кожним імпульсом, тобто за передаванням кожного біта. Спектр сигналу вміщує лише дві складових f_n та $2f_n$, де f_n – частота передавання інформаційних бітів. Наявність лише двох електричних рівнів напруги забезпечує надійне їх розпізнавання. Критерієм помилки може бути затягування сигналу в одному з рівнів на час, більший ніж передавання одного інформаційного біта.



а – шифратор; б – дешифратор; в – часові діаграми

Рисунок 3.15 – Формування коду "Манчестер – II"

Недоліком коду є необхідність підвищення пропускної здатності апаратури. Тому код "Манчестер - II" використовується там, де частотні обмеження не є визначальними.

До каналу зв'язку входять шифратор, дешифратор та дводротова магістраль. Сигнал у коді "Манчестер - II" можна отримати додаванням за модулем 2 сигналів *NRZ* та тактового *C*. Внаслідок цього шифратор коду дуже простий (рисунок 3.15, а). Схема фільтра у шифраторі призначена для вивільнення сформованого сигналу від короткочасних імпульсів, які можуть виникнути за рахунок "перегонів" на входах мікросхем, оскільки інформативним параметром є фронт імпульсу. Дешифратор коду являє собою дещо складнішу схему (рисунок 3.15, б). Часові діаграми пояснюють принцип дії дешифратора. Першим завданням формувача є вилучення з інформативного сигналу синхронізувального. За кожним фронтом інформативного сигналу формується пауза (*3*).

Але при цьому залишаються імпульси подвійної тривалості, які утворюються під час переходу в *NRZ* з "0" до "1" або навпаки. Одновібратор формує імпульси такої самої тривалості, як і імпульси синхросигналу (*4*), за заднім фронтом яких формуються паузи (*5*). Якщо на одновібратор надходить імпульс тривалості синхросигналу, то за його фронтом одновібратор сформує такий самий імпульс і порушення роботи не буде. Сигнали точок *(3)* та (*5*) за допомогою схеми "І" дозволяють сформувати сигнал частотою удвічі більшою за синхросигнал, який можна відновити за допомогою лічильного тригера. Подавши на *D*-тригер сигнал тактової частоти та вхідну комбінацію коду "Манчестер - II", одержують попередню комбінацію у коді NRZ. Таким чином, всі прилади до точки (*7*) призначені лише для формування синхросигналу. Якщо ж його передавати окремою лінією, схема значно спрощується, але на практиці це не використовується.

Переваги коду "Манчестер - II" порівняно з кодом NRZ полягають у тому, що:

- ◊ синхросигнал та інформацію можна передавати одним каналом, в той час як для коду NRZ потрібно два канали або дві лінії;
- ◊ діапазон логічних частот коду NRZ починається з нуля і не перевищує половини тактової частоти, сигнал "Манчестер – II" вміщує лише дві складових $f_c/2$ та f_c. Постійна складова при використанні біполярних сигналів дорівнює нулю. Це означає, що приймач коду "Манчестер - II"

може бути вузькосмуговим і тому більш завадостійким, ніж приймач коду NRZ. Крім цього легко реалізувати трансформаторний зв'язок окремих пристроїв зі спільною дводротовою магістраллю;

◊ значною перевагою коду "Манчестер – II" поряд з телеграфним кодом є бітова синхронізація; крім того затягування фронтів синхросигналу (затримка) на час менший, ніж половина періоду на роботу не впливає.

Недоліком коду "Манчестер – II" є апаратні витрати (шифратор та дешифратор) та подвоєна пропускна здатність.

Найбільш перспективне використання цього коду у волоконно-оптичних лініях за рахунок того, що він дозволяє роботу світловипромінювального елемента з подвійним перевантаженням за потужністю імпульсу тому, що, в середньому, елемент 50% часу вимкнений. Сигнал не залишається в одному стані більше ніж один такт, шпаруватість, в середньому, дорівнює двом.

Література

1. Васюра А.С., Кривогубченко С.Г., Кулик А.Я. та ін. Техніка передавання дискретної інформації. – Вінниця.: ВДТУ, 1998. – С. 75 – 81.

2 Квєтний Р.Н., Компанець М.М., Кривогубченко С.Г., Кулик А.Я. Основи техніки передавання інформації / Підручник. – Вінниця: Універсум-Вінниця, 2002. – С. 203 – 209.

Глосарій

Блокові коди – коди, у яких кожному повідомленню відповідає кодова комбінація (блок з *n* символів), причому блоки кодуються незалежно один від одного.

Вага кодової комбінації (коду) – кількість одиниць у кодовій комбінації.

Довжина коду – кількість розрядів (символів), що складають кодову комбінацію.

Ентропія – середня кількість інформації, що припадає на один символ.

Ентропія повідомлення – середня кількість інформації, що вміщується у повідомленні.

Ємність каналу – гранична швидкість передавання інформації цим каналом.

Інтеграл Лапласа (інтеграл імовірності) – функція, яка визначає імовірність помилки ідентифікації інформативного сигналу.

Інформаційні розряди – розряди кодової комбінації, призначенні для вміщення даних початкового повідомлення.

Інформація – змістовні відомості (дані), що втілюються в повідомленні, попередньо невідомі людині чи машині, яка це повідомлення отримує.

Канал зв'язку – сукупність технічних засобів та тракту для передавання повідомлення на відстань незалежно від інших каналів в лінії зв'язку.

Код – множина символів в деякому алфавіті, поставлена у взаємно однозначну відповідність з початковою множиною символів.

Кодова відстань – мінімальна кількість однойменних розрядів з різними символами.

Кодування – встановлення відповідності між елементом даних і сукупністю символів, яка називається кодовою комбінацією.

Контрольні (перевірні) розряди – розряди кодової комбінації, призначенні для визначення та виправлення помилок.

Крок квантування за рівнем – різниця між сусідніми дискретними значеннями функції.

Лінія зв'язку – сукупність кінцевої апаратури та фізичного середовища, якими здійснюється передавання сигналів від передавача до приймача.

Марківський канал – канал з пам'яттю, для розрахунку та оцінювання якості передавання інформації яким використовується математичний апарат ланцюгів Маркова.

Метрика Хеммінга – відстань $d(\mathbf{X}, \mathbf{Y})$ у просторі $GF(2^n)$, яка визначається кількістю позицій, у яких координати векторів **X** та **Y** не збігаються.

Неперервні коди – коди, у яких процес кодування та декодування має неперервний характер.

Неприводимий поліном – поліном, що не може бути поданий у вигляді добутку багаточленів нижчих степенів.

Обернений поліном – поліном, який утворюються шляхом підстановки $1/x$ замість x до основного полінома і його множення на одночлен x^i, де i – степінь основного полінома.

Об'єм сигналу – максимальна кількість інформації, яка може бути передана каналом за час T за даних умов.

Оптимальність коду – властивість такого коду, який забезпечує найменшу ймовірність невизначення помилки серед всіх кодів тієї ж довжини і надлишковості.

Основа коду – кількість імпульсних ознак, використовуваних у кодових комбінаціях, що відрізняються одна від одної.

Питома ентропія – ентропія на один використовуваний символ алфавіту.

Потужність коду – кількість кодових комбінацій (робочих кодових слів), використовуваних для передавання повідомлень.

Синдром коду – сума за модулем два контрольних розрядів кодової комбінації та контрольних розрядів, обчислених за прийнятими інформаційними символами.

Теорема Котельникова (відрахунків) – якщо функція $x(t)$ не вміщує в собі частот, вищих за f_{max}, то вона повністю визначається своїми миттєвими значеннями у моменти часу, що віддалені один від одного на $1/2f_{max}$.

Типові послідовності – рівноімовірні взаємно незалежні послідовності, які формуються передавачем.

Функція Крампа – інтеграл, який визначає імовірність безпомилкової ідентифікації інформативного сигналу.

Key words and idioms – ключові слова та вирази

Automated control system – система автоматизованого управління.
Binary digit – двійковий символ.
Channel capacity – ємність каналу.
Channel of transfer of the information – канал передавання інформації.
Code combination – кодова комбінація.
Coding – кодування.
Communication line – лінія зв'язку.
Computer system – комп'ютерна система.
Correlation function – кореляційна функція.
Criterion function – критеріальна функція.
Cyclic code – циклічний код.
Data rate – швидкість передавання даних.
Entropy – ентропія.
Error-checking code – код з визначенням помилок.
Error-correcting code – код з виправленням помилок.
Evaluation function – функція оцінки.
Hamming metrics – метрика Хеммінга.
Huffman code – код Хаффмана.
Information – інформація.
Khotelnikov theorem – теорема Котельнікова.
Mathematical model – математична модель.
Number system – система числення.
Probability integral – інтеграл імовірності.
Probability value – імовірність.
Signal base value – база сигналу.
Signal/noise ratio – співвідношення сигнал/шум.
Signal capacity – об'єм сигналу.
Source of the message – джерело повідомлення.
Symmetric channel – симетричний канал.
Threshold function – порогова функція.
Value of conditional probability – значення умовної імовірності.

Післямова

Побудова теорії інформації і кодування пов'язана з роботами В. А. Котельникова та К. Е. Шеннона. На сучасному етапі вчені та інженери продовжують створювати як фундаментальні основи аналізу і синтезу кодів, так і засади для їх використання в комп'ютерних системах і мережах. Розвиваються математичні моделі процесів збирання, оброблювання, зберігання і передавання інформації в дискретних каналах комп'ютерних систем на основі використання ідеальних і реальних моделей, теорій ефективного, завадостійкого та оптимального кодування.

Оптимальне кодування все ширше застосовується в комп'ютерних системах і мережах зв'язку, системах передавання даних в АСУ, радіонавігаційних системах, різноманітних телемеханічних системах вимірювання, контролю та управління.

До основних тенденцій та перспектив розвитку кодерів і декодерів можна віднести: подальше ущільнення і підвищення надійності каналів передавання інформації; застосування широкосмугових методів і пристроїв передачі інформації; широке використання коригувального кодування та декодування сигналів; застосування адаптації для оперативного корегування характеристик каналів; розроблення методів прийняття рішень, оцінки ефективності, якості та оптимальності з урахуванням надійності, швидкодії і витрат; застосування статистичного моделювання процесів передачі повідомлень, з урахуванням функціонально-модульного принципу побудови комп'ютерних систем; пошук нових методів і засобів кодування і декодування інформації на основі турбо-кодів, вейвлет-функцій тощо.

Навчальне видання

Анатолій Ярославович Кулик
Сергій Григорович Кривогубченко

Теорія інформації і кодування

Навчальний посібник

Оригінал-макет підготовлено Куликом А.Я.

Редактор В.О. Дружиніна

Науково-методичний відділ ВНТУ

Свідоцтво Держкомінформу України
серія ДК № 746 від 25.12.2001
21021, м. Вінниця, Хмельницьке шосе, 95, ВНТУ

Підписано до друку 6.08.08 р. Гарнітура Times New Roman
Формат 29,7×42 1/4 Папір офсетний
Друк різографічний Ум. друк. арк. 9.2
Тираж 100 прим.
Зам. № 2008-111

Віддруковано в комп'ютерному інформаційно-видавничому центрі
Вінницького національного технічного університету

Свідоцтво Держкомінформу України
серія ДК № 746 від 25.12.2001
21021, м. Вінниця, Хмельницьке шосе, 95, ВНТУ