ХАРКІВСЬКИЙ ІНСТИТУТ ВПС
ім. І. КОЖЕДУБА

І.М. Бондаренко, А.П. Глушко, О.М. Меньков

КОДИ ТА КОДУВАННЯ

Х А Р К І В
2003

ХАРКІВСЬКИЙ ІНСТИТУТ ВПС
ім. І. КОЖЕДУБА

І.М. Бондаренко, А.П. Глушко, О.М. Меньков

КОДИ ТА КОДУВАННЯ

Навчальний посібник

Х А Р К І В
2003

УДК 621.321

Бондаренко І.М., Глушко А.П., Меньков О.М.

Коди та кодування. Навч. посібник. – Харків. ХІ ВПС, 2003. – 116с.

У посібнику розглянуто питання, які пов′язані з основними принципами побудови, формування та застосування основних видів кодів, що використовуються в системах передачі інформації. Описано основні види кодів та їх характеристики, принципи побудови та особливості функціонування кодеків сигналів.

Ілюстрацій – 49. Таблиць – 11. Бібліографія – 10 найменувань.

Передмова

Зростання обсягів інформації, що передається по каналах зв′язку, кількості та складності радіоелектронних засобів, які при цьому застосовуються, веде до значного ускладнення умов неспотвореної передачі корисних сигналів. Це обумовлено значним зростанням шумів, а також різних можливих небажаних спотворень корисних сигналів в елементах та пристроях, які входять до складу систем зв′язку.

У випадку військових систем зв′язку ці умови ще більш ускладнюються, оскільки треба прийняти до уваги можливість застосування штучних завад, а також вимоги щодо необхідності захисту інформації, що передається, від несанкціонованого втручання чи ознайомлення.

Проблема захисту повідомлень від різного роду завад, спотворень й таке інше зазвичай вирішується за допомогою їх кодування.

Без знання основ кодування неможливе як створення нових сучасних систем передачі інформації, так й експлуатація існуючих та майбутніх телекомунікаційних систем.

Автори сподіваються, що деякі теоретичні знання про способи кодування повідомлень та захисту їх від завад і спотворень, викладені у цьому посібнику, допоможуть користувачам краще зрозуміти принципи побудови основних видів кодів, основи функціонування пристроїв, призначених для кодування та декодування (кодеків).

Посібник призначений для використання як додаткове джерело інформації при вивченні відповідних розділів дисциплін: “Системи радіозв′язку”, “Авіаційні системи радіозв′язку”, “Військова техніка авіаційного радіо- та електрозв′язку”, “Системи передачі інформації по авіаційних каналах радіозв′язку”, “Військова техніка бортових засобів зв′язку”.

Даний підручник може бути характеризований лише як розгорнутий вступ до питань, пов′язаних з кодуванням повідомлень у каналах зв′язку. У випадку необхідності більш повного ознайомлення з питаннями, що у ньому розглядаються, автори пропонують користуватися літературою, список якої наведений наприкінці посібника. Однак при цьому треба враховувати, що цей список теж не є всеосяжним, тому що кодування повідомлень – напрямок науки, який дуже швидко розвивається у даний час.

ВСТУП

Якщо узяти достатньо довге речення та спотворити його шляхом заміни або вилучання чи додавання букв у деяких місцях, то при використанні знань щодо структури окремих слів та речення у цілому, попереднього та наступного тексту, знання предмету, про який їде мова, можна майже у повному обсязі відтворити початкове речення або безпомилково визначити його зміст. Це доводить, що природна мова має велику надмірність.

У техніці також дуже часто використовують однакові дублюючі пристрої на випадок виходу з ладу одного з них. У деяких випадках за допомогою того ж самого пристрою виконуються двічі ті ж самі розрахунки, і якщо результати співпадають, то приймається рішення про безпомилкове виконання розрахунків або працездатність пристроїв, що контролюються. При різниці у розрахунках вони повторюються ще раз, і знайдена помилка усувається або приймається рішення про непрацездатність відповідних пристроїв. Розглянуті випадки є прикладом того, що надмірність може допомогти з′ясувати наявність помилок і підвищити надійність системи.

Наше завдання полягає у тому, щоб досягнути необхідного ступеню надійності за рахунок по можливості мінімальної надмірності, яка спеціально штучно встановлюється. Стосовно різного роду повідомлень це забезпечується за допомогою застосування різного виду кодів та методів кодування.

У даний час основним завданням кодування є підвищення надійності систем зв′язку та обчислювальної техніки за допомогою цілеспрямованого ефективного уведення надмірності у процесі перетворення та подавання інформації. Наявність штучної надмірності веде до зниження кількості повідомлень, які можуть бути передані та оброблені за визначений час, а також передбачає використання у системі додаткових пристроїв для цілеспрямованого уведення надмірності (кодерів), пристроїв для виявлення та виправлення помилок (декодерів) та ряду інших додаткових пристроїв.

На рис.1 показана типова модель системи зв′язку з використанням кодів. Спочатку інформація, що поступає від джерела інформації, перетворюється у послідовність двійкових символів, яка подається до кодеру, де до неї уводиться надмірність. Символи з виходу кодера за допомогою модулятора перетворюються у сигнали, які можуть бути передані по каналу зв′язку. У каналі зв′язку ці сигнали зазвичай спотворюються шумами. На прийомному кінці спотворені сигнали за допомогою демодулятора перетворюються у послідовність двійкових символів, яка містить надмірні символи. За допомогою цієї надмірності декодер виявляє та виправляє помил-

ки. Двійкова послідовність на виході декодеру вже не є надмірною. Якщо вплив шуму на сигнал у каналі не дуже великий, і декодер може виправити усі помилки, що з′явилися, то двійкова послідовність на його виході буде співпадати з двійковою послідовністю, яка була подана на вхід кодера. Одержана на виході декодера послідовність перетворюється у повідомлення за такою формою уявлення, що потрібна одержувачу інформації.

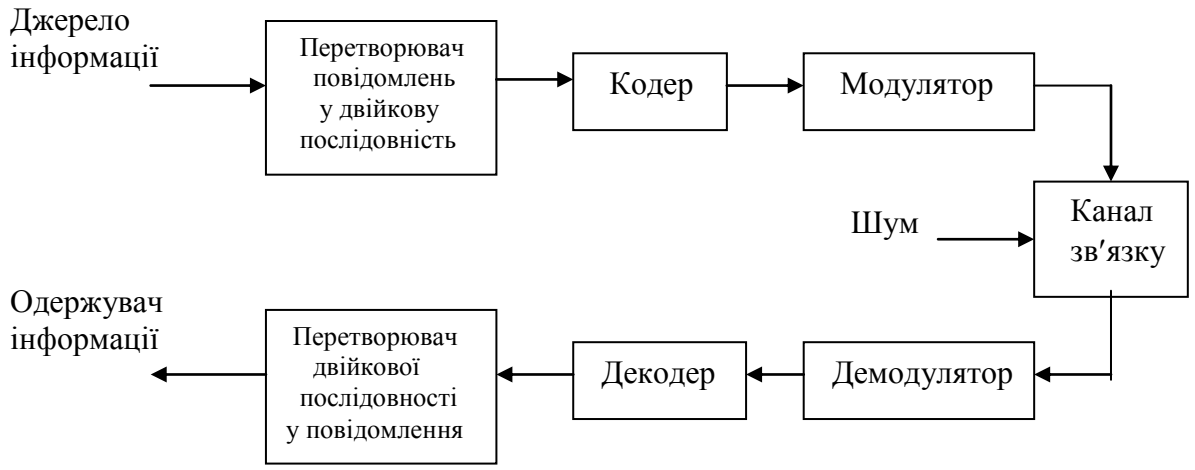


Рис.1

Для кращого розуміння процесу кодування треба знати класифікацію кодів, способи їх подання, їх характеристики, основні принципи і методи оптимального кодування, основні принципи побудови та функціонування кодерів і декодерів.

Усі ці питання будуть розглянуті нижче у наступних розділах цього посібника.

Розділ 1. КОДУВАННЯ. ОСНОВНІ ВИЗНАЧЕННЯ

Кодування – це процес перетворення повідомлення на впорядкований набір символів, елементів, знаків. При кодуванні кожному повідомленню ставиться у відповідність зумовлена кодова комбінація – набір символів (елементів, знаків) з деякої скінченної кількості їх, яка називається алфавітом.

Множина кодових комбінацій, побудованих за одним правилом кодування, називається кодом. Залежно від алфавіту, який застосовується для побудови кодових комбінацій, коди поділяються на двійкові, алфавіт яких складається з двох символів (0 і 1), та недвійкові (багатопозиційні, q-коди), алфавіт яких містить більше двох символів.

Розрізняють дві групи кодів: безнадмірні (некоректувальні, первинні, прості) та надмірні (завадостійкі). Перші не дають змоги виявити та виправити неспотворені елементи в своїх комбінаціях, другі – забезпечують можливість виявлення або виявлення та виправлення елементів кодових комбінацій, спотворених унаслідок дії завад.

У надмірних кодах комбінації можуть мати інформаційні та перевірні елементи. Обидві групи кодів поділяються на рівномірні та нерівномірні, тобто коди зі сталою та змінною кількістю розрядів.

Надмірні коди також бувають неперервними (рекурентними) і блоковими. В неперервних кодах процес кодування та декодування має неперервний характер, у блокових – кожному повідомленню відповідає кодова комбінація (блок) зі скінченої кількості елементів. Блоки кодуються та декодуються окремо.

Блокові коди, в свою чергу, можуть бути подільними та неподільними. До перших належать коди, що будуються доповненням інформаційних елементів перевірними; до других – коди, в яких немає чітко зумовлених інформаційних і перевірних елементів.

Подільні блокові коди бувають систематичними та несистематичними. Систематичним подільним блоковим кодом називається такий код, у комбінаціях якого перші k позицій (розрядів) зайнято інформаційними елементами, а решту r = n – k позицій (n – загальна кількість позицій у кодовій комбінації) – перевірними. До несистематичних подільних блокових кодів належать коди, в яких інформаційними елементами не зайнято всі k перших позицій.

Різновидом подільних систематичних блокових кодів є також циклічні коди.

При виборі кодів для передачі інформації керуються вимогами до вірогідності інформації, що передається, та швидкості передачі, які визначаються такими характеристиками кодів:

– кількістю k інформаційних елементів;

– кількістю r перевірних елементів (для коректувальних кодів);

– довжиною (розрядністю) n – кількістю елементів (символів), які входять до складу кодової комбінації (n = k + r);

– основою (алфавітом) q;

– потужністю $N_д$ – кількістю дозволених кодових комбінацій, що використовуються для передачі повідомлень;

– повною кількістю N кодових комбінацій, тобто кількістю всіх можливих комбінацій, яка дорівнює q^n (для двійкових кодів $N = 2^n$);

– надмірністю

$$R_{над} = 1 - \frac{\log_q N_д}{\log_q N} \text{ (для неподільних кодів)}$$

або

$$R_{над} = 1 - k/n = r/n \text{ (для подільних кодів при } N = 2^k \text{ і } N = 2^n);$$

– відносною швидкістю R, яка характеризує ступінь використання у надмірному коді інформаційних можливостей його потужності, причому

$$R = \frac{\log_q N_д}{\log_q N} \qquad \text{або} \qquad R = \frac{k}{n} = 1 - R_{над};$$

– вагою w кодової комбінації (для двійкового коду визначається кількістю одиниць у ній);

– мінімальною кодовою відстанню $d_{min} = \min d_{ij}$, тобто мінімальною відстанню між парами кодових комбінацій

$$d_{ij} = \sum_{l=1}^{n} \left| a_{li} - a_{lj} \right|,$$

де a_{li}, a_{lj} – елементи, що знаходяться в l-му місці в i- та j-й комбінаціях. Це означає, що d_{ij} визначається кількістю однойменних розрядів з різними значеннями;

– імовірністю $P_{нвп}$ невиявленої помилки, тобто імовірністю такої події, за якої прийнята кодова комбінація відрізняється від переданої, а властивості коду не дають змоги визначити факт наявності помилки;

– імовірністю $P_{вп}$ виявленої помилки, тобто імовірністю, за якої прийнята кодова комбінація відрізняється від переданої і завдяки властивостям коду встановлюється факт наявності помилки в кодовій комбінації;

– імовірністю $P_{впп}$ виправленої помилки, тобто імовірністю такої події, за якої прийнята кодова комбінація відрізняється від переданої і завдяки властивостям коду виправляється помилка в кодовій комбінації;

– імовірністю $P_п$ виникнення помилки, тобто імовірністю такої події, за якої прийнята кодова комбінація відрізняється від переданої ($P_п = P_{нвп} – P_{вп}$ – для кодів, які виявляють помилки, та $P_п = P_{нвп} + P_{вп} + P_{нвпп}$ – для кодів, які виправляють помилки, де $P_{нвпп}$ – імовірність невиправленої виявленої помилки);

– кратністю v помилки, що визначається кратністю $v_в$ виявлених та $v_{вп}$ виправлених помилок;

– ефективністю

$$r_{еф} = \frac{N_д}{N} \frac{P_n}{P_n - \sum_{i=1}^{v} P_i} ,$$

де P_i – імовірність виявленої або виправленої помилки залежно від властивостей коду.

Ступінь захисту інформації від помилок відповідним способом кодування залежить головним чином від мінімальної кодової відстані d_{min} даного коду.

Розрізняють три види кодової відстані: Хеммінга, Лі та матричну. Перша знайшла найбільше поширення. Кодова відстань Хеммінга нероздільно пов′язана з поняттям ваги w кодової комбінації – кількістю її елементів, які не дорівнюють нулю.

Кодова відстань Хеммінга d між двома комбінаціями однієї довжини n визначається як кількість однойменних розрядів (позицій), які мають неоднакові елементи. Так, для двійкових кодів, оскільки в двійковій арифметиці додавання однакових елементів дає 0, а неоднакових – 1, відстань Хеммінга між двома кодовими комбінаціями можна визначити порозрядним додаванням їх за модулем 2 та подальшим підрахунком кількості ненульових елементів, тобто визначенням ваги w такої суми.

Загальна кількість кодових комбінацій завдовжки n дорівнює 2^n, а кількість тих з них, які віддалені від заданої на відстань d, - кількість сполучень з n по d:

$$C_n^d = n!/[d!(n-d)!] .$$

Щоб визначити кодову комбінацію, яка віддалена від заданої на відстань d, до цієї комбінації можна додати будь-яку комбінацію вагою w = d (з d одиницями та n – d нулями). Додавання – порозрядне за модулем 2.

Для виявлення всіх помилок кратністю $v_в$ кодова відстань має становити $d \geq v_в + 1$, а для виправлення помилок кратністю $v_{вп}$ повинна виконуватись умова $d \geq 2v_{вп} + 1$. Щоб виправити та виявити всі помилки, має виконуватися умова $d \geq v_{вп} + v_в + 1$.

Через те, що загалом кожний елемент (розряд) комбінації недвійкового (багатопозиційного) коду може мати на відміну від двійкового й понад однієї позиції ($m \geq 1$) з алфавіту q, кодова відстань при цьому визначається виразом

$$d = \sum_{i=1}^{m} d_i ,$$

де m – кількість позицій у кожному розряді (поодиноковому часовому інтервалі, що відповідає тривалості одного елемента) кодової комбінації.

У метриці Хеммінга кодова відстань, як і для двійкового коду, визначається кількістю однойменних розрядів з різними позиціями (символами):

$$d_i(x_k, x_l) = \begin{cases} 0, x_k = x_l; \\ 1, x_k \neq x_l. \end{cases}$$

У метриці Лі

$$d_i(x_k, x_l) = \min\{|x_k - x_l|, q - |x_k - x_l|\} \equiv \min\{d_{j\,\mathrm{mod}}, q - d_{j\,\mathrm{mod}}\},$$

де $d_{j\,\mathrm{mod}} = |x_k - x_l|$.

У модульної метриці $d_i(x_k, x_l) = |x_k - x_l|$, тобто слід виконувати віднімання за модулем q.

Відзначимо, що коли значення кодової відстані для двійкового коду в різних метриках збігаються, для недвійкового коду при q = 3 значення d в метриках Хеммінга та Лі також збігаються. При q > 3 значення d у різних метриках різняться.

При конкретній реалізації недвійкового коду з використанням позицій тих або інших ознак сигналу кодова відстань визначається відповідною метрикою.

У теорії інформації, кодування, передачі даних і системах обміну інформацією найпоширенішими є двійкова, вісімкова та шіснадцяткова системи числення. Проте це ні в якому разі не означає, що на практиці не користуються іншими системами числення. Узагалі ціле число N у будь-якій системі числення можна записати у вигляді ряду

$$N = \sum_{i=0}^{n-1} \alpha_i q^i ,$$

де α_i – розрядні коефіцієнти, значення яких змінюються від 0 до q – 1; q – основа (алфавіт) системи числення; *i* – номер розряду; n – кількість їх.

Назва системи числення походить від основи (алфавіту) q: q = 2 – двійкова, q = 3 – трійкова, q = 8 – вісімкова система числення тощо.

Для запису чисел, наприклад, у дев′ятковій системі, використовують 10 цифр (0, 1, 2, 3, 4, 5, 6, 7, 8, 9); у двійковій – дві (0 і 1); у трійковій – три (0, 1, 2); у вісімковій – вісім (0, 1, 2, 3, 4, 5, 6, 7); в шістнадцятковій – 16 знаків, з них – 10 цифр (0…9) і шість літер (A, B, C, D, E, F).

Для запису десяткового числа у будь-якій системі числення треба поділити його на основу вибраної системи. Після першого ділення дістанемо цілу частку й остачу. Продовживши ділення цілої частки, матимемо нову цілу частку та остачу. Ділення цілих часток продовжуємо доти, доки частка не стане меншою від основи q системи числення. Ця остання частка й буде старшим розрядом числа у вибраній системі числення. Інші розряди відповідатимуть остачам від ділення. Молодший розряд – це остача від першого ділення.

Методика побудови багатьох кодів основана на використанні властивостей послідовності двійкових чисел, тому в подальшому будемо переважно розглядати коди і операції кодування та декодування стосовно послідовностей двійкових чисел.

Розглянемо деякі операції над елементами двійкових кодів (q = 2).

Правила додавання за модулем 2 визначаються такими операціями:

$$0 \oplus 0 = 0; \quad 1 \oplus 1 = 0; \quad 0 \oplus 1 = 1; \quad 1 \oplus 0 = 1.$$

Наприклад, при додаванні за модулем 2 двійкових послідовностей чисел 0111000 і 10010 матимемо 0101010.

Операція віднімання за модулем 2 нічим не відрізняється від операції додавання.

Множення та ділення двійкових чисел за модулем 2 виконують за допомогою операції додавання за модулем 2.

Дуже зручно операції додавання, віднімання, множення та ділення за модулем 2 виконувати з двійковими числами, записаними у вигляді поліномів. Так, двійкові комбінації 110010 і 100001 можна записати поліномами

$$V_1(x) = x^5 + x^4 + x; \qquad V_2(x) = x^5 + 1.$$

Тоді при додаванні $V_1(x) \oplus V_2(x)$ за модулем 2 дасть

$$V_1(x) \oplus V_2(x) = x^5 + x^4 + x + x^5 + 1 = x^4 + x + 1 \rightarrow 010011.$$

Результатом множення буде

$$V_1(x) \cdot V_2(x) = (x^5 + x^4 + x)(x^5 + 1) = x^{10} + x^9 + x^6 + x^5 + x^4 + x \rightarrow 11001110010.$$

Після ділення цих поліномів дістанемо

$$V_1(x):V_2(x) = (x^5 + x^4 + x):(x^5 + 1) = 1 + \frac{x^4 + x + 1}{x^5 + 1}\ .$$

Код кожного виду має свій найраціональніший спосіб подання, що випливає з його властивостей. Проте відомо також кілька загальних способів подання кодів, які є досить універсальними і можуть застосовуватися для опису широкого класу кодів. До цих способів належать подання кодів у вигляді: 1) таблиць кодових комбінацій; 2) кодового дерева; 3) геометричної моделі; 4) матриці.

Перший спосіб полягає в поданні коду у вигляді таблиці всіх його комбінацій. Наприклад, п′ятиелементний двійковий блоковий код зі сталою вагою, в кожній комбінації якого містяться три одиниці, задається так:

Номер кодової комбінації	**Комбінація двійкового блокового коду з вагою 3**
1	00111
2	01011
3	01101
4	01110
5	10011
6	10101
7	10110
8	11001
9	11010
10	11100

Цей спосіб застосовується для подання будь-яких блокових кодів, але не може бути використаний для неперервних кодів.

Другий спосіб подання кодів полягає в зображенні комбінації коду у вигляді кодового дерева, коли комбінації розміщуються в його вузлах. Під кодовим деревом розумітимемо графічний образ, який складається з точок і ліній, що розходяться від них і також закінчуються точками. Останні називатимемо вузлами, а лінії, які їх з′єднують, – ребрами. Перший вузол, від якого починається розходження ребер, називається коренем дерева, а кількість ребер, які треба пройти від кореня до будь-якого вузла – рівнем, або порядком, цього вузла.

Максимальна кількість вузлів, які зустрічаються під час руху вздовж кодового дерева в напрямку від кореня до вершини, визначає висоту h кодового дерева. Вона дорівнює максимальній довжині комбінації коду, побудованого за допомогою цього дерева.

Вузли кодового дерева розташовуються на різних рівнях. Кожний рівень дерева рівномірного коду може мати q^i вузлів, де q – основа коду, i – номер рівня (i = 1,2,…n, тут n – довжина коду). Для рівномірного двійково-

го простого коду кількість вузлів на останньому рівні n дорівнює кількості N комбінацій коду, тобто $2^n = N$.

Вузли, що не з′єднуються з наступними рівнями, називаються кінцевими; вони відповідають комбінаціям коду.

Основою коду обмежується максимальна кількість ребер, яка може виходити з кожного вузла дерева, а максимальною довжиною кодової комбінації – максимальна кількість рівнів кодового дерева. Кожному вузлу приписується значення розрядів комбінацій, що відповідає напрямкам руху вздовж ребер від кореня дерева до вузла. Ребра, що йдуть від кореня до вузлів першого рівня, визначають значення першого зліва розряду кодової комбінації, а ті, що з′єднують вузли першого та другого рівнів. – значення другого зліва розряду і т. п. На рис.1.1 показано приклади кодових дерев: рівномірних двоелементного двійкового (рис.1.1,а), двоелементного трійкового (рис.1.1,б), триелементного двійкового (рис.1.1,в) та нерівномірного двійкового (рис.1.1,г). Цей спосіб застосовується для зображення як блокових, так і неперервних кодів.

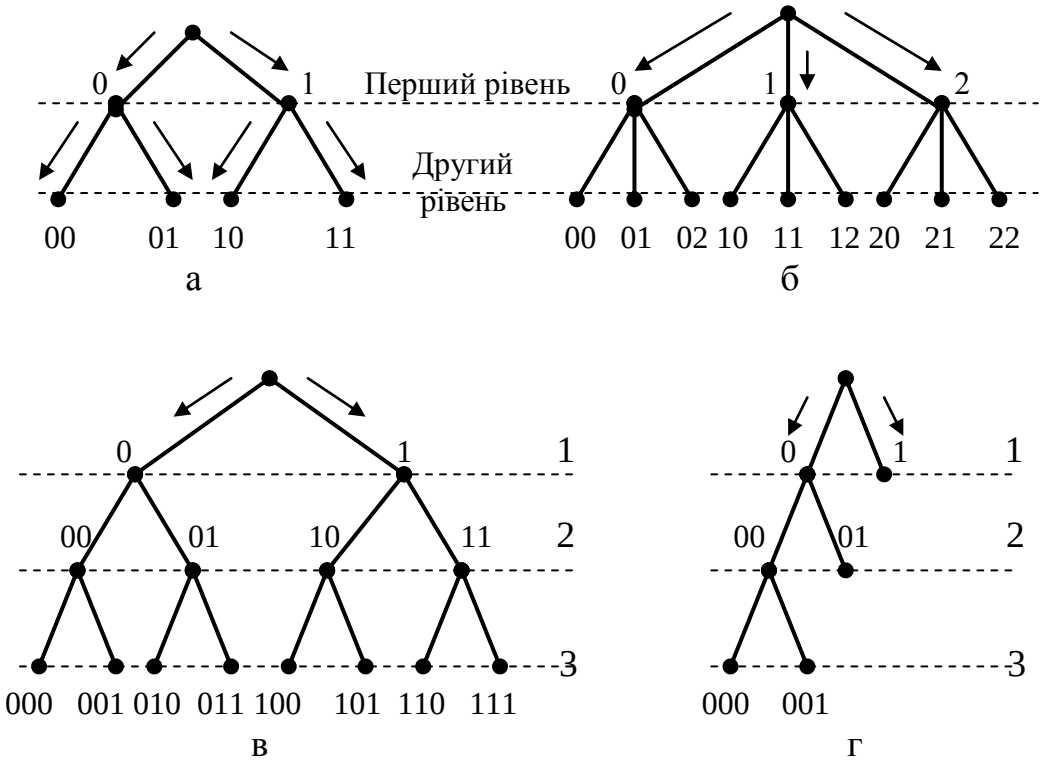


Рис. 1.1

Третій спосіб подання кодів полягає в зображенні комбінацій коду точками дискретного n-вимірного векторного простору. Так, кожну комбінацію рівномірного блокового коду (з основою q і довжиною n) $V = (V_n, V_{n-1},\ldots, V_2, V_1)$ можна розглядати як вектор або точку деякого n-вимірного

векторного простору з координатами V_n, V_{n-1},…, V_2, V_1. Якщо значення q скінчене, а будь-яка координата вектора є цілим додатним числом від 0 до q – 1, то зазначений код можна розглядати як дискретний n-вимірний простір, що складається з $N = q^n$ точок, які відповідають кінцям усіх можливих векторів.

Цей n-вимірний простір дістав назву кодового. Кількість просторових вимірювань кодового простору з будь-якою основою дорівнює довжині n коду, а кількість градацій по кожній з осей (напрямків вимірювання) визначається основою коду і становить q – 1.

Якщо для дискретного n-вимірного простору, що розглядається, увести поняття кодової відстані d між точками V_i та V_j, то матимемо

$$d(V_i, V_j) = \sum_{k=1}^{n} (V_{ki} - V_{kj}). \qquad (1.1)$$

Цілком природно, що для простору з відстанню (1.1), як і для будь-якого іншого кодового простору, $d(V_i, V_j) = d(V_j, V_i)$.

Одним з основних параметрів коду з довільною основою q, що визначають його завадостійкість, є мінімальна кодова відстань d_{min}. На відміну від кодової відстані d, що визначає кількість станів, які мають пройти якісні ознаки кодової комбінації, щоб опинитися в стані, який відповідає порівнюваній кодовій комбінації, мінімальна кодова відстань характеризує не дві окремо взяті комбінації, а код у цілому, і визначається мінімальною кількістю якісних ознак, за якими відрізняються одна від одної будь-яка пара комбінацій цього коду.

Для визначення кодової відстані між комбінаціями коду з основою q треба виконати їх порозрядне віднімання за модулем q. Кодова відстань дорівнює вазі комбінації, що складається з різниці значень комбінацій, між якими визначається ця відстань.

З′єднавши кожну точку простору, що розглядається, прямими лініями з усіма точками, віддаленими на відстань $d(V_i, V_j) = 1$, дістанемо геометричну фігуру сіткової структури. Цю фігуру називають геометричною моделлю n-елементного q-коду.

Точки дискретного простору, які містить ця геометрична фігура, називаються її вершинами, а лінії, що їх з′єднують, - ребрами.

Моделлю будь-якого двозначного набору якісних ознак (двоелементного коду) є фігура двовимірного простору – квадрат або фігура, що складається з квадратів; моделлю будь-якого тризначного набору якісних ознак (триелементного коду) – фігура тривимірного простору – куб або фігура, що складається з кубів. Для n-елементного коду n-вимірний куб повинен мати 2n вершин, $n \cdot 2^{n-1}$ ребер, $n(n-1) \cdot 2^{n-3}$ граней, а найвіддаленіша

від певної його вершини точка має знаходитися на відстані n ребер. Відстань між будь-якими його вершинами, тобто між двома кодовими комбінаціями, згідно (1.1) можна визначити як кількість розрядів, якими вони різняться. Відстань між комбінаціями 010 і 100 дорівнює двом, оскільки вони різняться елементами в двох розрядах – першому та другому.

Зручність геометричної моделі зображення будь-якого коду полягає в тому, що кожна її вершина відповідає одній комбінації коду, а відстань між комбінаціями V_i та V_j згідно (1.1) дорівнює кількості ребер, які треба пройти найкоротшим шляхом з вершини V_i до вершини V_j.

Недоліком геометричної моделі є те, що при довжині коду $n > 3$ зобразити її у звичайному тривимірному просторі неможливо. Тому вона застосовується лише для рівномірних блокових кодів з метою наочного зображення та полегшення аналізу їхніх властивостей.

Четвертий спосіб подання кодів у вигляді матриці з 2^n рядками та n стовпцями можливий тільки для рівномірних n-елементних двійкових блокових кодів. Якщо матрицею подається сукупність ненульових комбінацій коду, то кількість рядків дорівнюватиме $2^n - 1$.

З урахуванням того, що матриця n-елементного коду складається з $2^n - 1$ комбінацій, записаних у вигляді рядків, особливість такого запису полягає в тому, що додавання за модулем 2 будь-якої кількості рядків цієї матриці приводить до появи дозволеної комбінації коду, в тому числі й нульової. Якщо останню відкинути, то дістанемо нову матрицю коду, але вже з меншою кількістю рядків. Повторивши аналогічну операцію додавання рядків матриці за модулем 2, можна знову дістати нульову комбінацію коду. Ця операція повторюється доти, доки не буде здобута матриця з лінійно незалежними рядками, додавання яких за модулем 2 вже не приведе до утворення нульової комбінації коду.

Квадратна матриця, діагональ якої складається з одиниць, а решта її елементів – нулі, називається одиничною. Якщо рядки такої n-елементної матриці додавати за модулем 2, то підбором відповідної комбінації їх можна дістати всі комбінації n-елементного коду. Тому такі матриці ще називаються визначальними.

Якщо напрямок головної діагоналі матриці проходить справа наліво, то матриця називається транспонованою.

Загалом визначальна матриця n-елементного коду має n рядків і n стовпців.

Розглянутий приклад утворення визначальної матриці й здобута одинична матриця можуть бути використані тільки для побудови всіх комбінацій двійкового простого колу з мінімальною кодовою відстанню $d_{min}=1$.

Матричний спосіб може бути застосований також для побудови коректувальних кодів з $d_{min} > 1$, здатних виявляти та виправляти помилки. Проте при цьому твірна (породжувальна) матриця складається з двох підматриць – уже відомої одиничної (інформаційної) та додаткової (перевірної).

За допомогою одиничної підматриці E_k утворюють інформаційну частину кодової комбінації коректувального коду, яка складається з k інформаційних елементів і визначає розмір підматриці (k×k), що відповідає розмірам визначальної квадратної матриці двійкового простого коду, оскільки кількість $N_д$ комбінацій коректувального коду дорівнює кількості N комбінацій початкового двійкового простого коду, які треба закодувати цим коректувальним кодом.

За допомогою додаткової перевірної підматриці $C_{r,k}$, правило побудови якої буде описано далі при розгляді коректувальних кодів, утворюють перевірну частину комбінації коректувального коду, що складається з r перевірних елементів. Тому додаткова перевірна підматриця має розмір r×k.

Таким чином, загальний розмір твірної матриці коректувальних кодів дорівнює n×k, оскільки n = k + r.

Надмірність повідомлень і кодів. Від надмірності повідомлень і кодів, якими вони передаються, залежить максимальна кількість інформації, що може бути передана по каналу за одиницю часу. Якщо повідомлення передаються алфавітом q, то максимальну кількість інформації на один елемент (символ, знак) повідомлення H = logq можна дістати лише в разі його рівноймовірних й незалежних елементів. Реальні коди, які використовуються для кодування повідомлень, майже ніколи не задовольняють цю умову, тому що інформаційне навантаження кожного елемента їх, як правило, менше від того, яке вони могли б забезпечувати. Це свідчить про те, що повідомлення мають інформаційну надмірність.

Розрізняють два види надмірностей: природну та штучну. Першою описується надмірність первинних алфавітів, а другою – вторинних. Природна надмірність поділяється на семантичну та статистичну.

Семантична надмірність випливає з того, що будь-яку думку, яка міститься в повідомленні, можна висловити коротше. Взагалі вважають, що коли повідомлення можна скоротити без втрат його змісту, а потім поновити останній, воно має семантичну надмірність.

Є багато способів усунення семантичної надмірності: заміною деяких типових повідомлень, які зустрічаються досить часто, умовними позначеннями; уведенням таблиць, куди заносяться характерні елементи повідомлення; застосуванням скорочень тощо. Але всі ці перетворення стосуються первинного алфавіту.

Систематична семантична надмірність спричинена нерівномірним розподілом якісних ознак первинного алфавіту та взаємозалежністю їх. Це можна побачити на прикладі англійського алфавіту, що містить 26 літер. Максимальне значення ентропії англійського алфавіту $H_{max} = \log_2 q = \log_2 26 = 4{,}7$ біт. Проте у зв′язку з тим, що ймовірність появи літер англійського алфавіту не однакова, ентропія англійської мови значно менше, ніж 4,7 біт, і без урахування взаємозалежності між словами становить приблизно 2,35 біт.

Якщо ж урахувати дійсну частоту появи літер у текстах, різних сполученнях і слів у різних повідомленнях, то інформацію, що передається, можна значно скоротити, стиснути. Коефіцієнт ущільнення інформації визначається виразом $К_{ущ} = H/H_{max}$, а надмірність – виразом

$$R_{над} = 1 - К_{ущ} = 1 - H/H_{max}. \qquad (1.2)$$

Із (1.2) випливає, що для зменшення надмірності повідомлення необхідно збільшити ентропію первинного алфавіту.

Для англійської мови $R_{над} = 1 - 2{,}35/4{,}7 = 1 - 0{,}5 = 0{,}5$, тобто можна відновити зміст англійських текстів, складених з 50 % алфавіту.

До видів статистичної надмірності алфавітів належать такі поняття, як надмірність $R_{над.зв}$, зумовлена статистичним зв′язком між елементами повідомлення, та надмірність $R_{над.р}$, спричинена нерівноймовірним розподілом елементів у повідомленні.

Повна статистична надмірність алфавіту визначається виразом $R_{над} = R_{над.зв} + R_{над.р} - R_{над.зв} \cdot R_{над.р}$. При незначних $R_{над.зв}$ і $R_{над.р}$ цей вираз набуває вигляду $R_{над} = R_{над.зв} + R_{над.р}$.

Для усунення статистичної надмірності алфавітів використовують оптимальні нерівномірні коди; при цьому статистична надмірність первинного алфавіту значно зменшується завдяки більш раціональній побудові повідомлень у вторинному алфавіті.

Вираз

$$n \geq \frac{H}{\log q} = \frac{\log N}{\log q} \qquad (1.3)$$

можна застосувати для визначення довжини кодів з рівноймовірними та взаємонезалежними елементами. Для двійкового коду (q = 2) цей вираз дійсний тільки тоді, коли ймовірність появи 0 та 1 однакова. Проте в рівномірних кодах, як правило, нулі зустрічаються частіше, ніж одиниці. Тому надмірність, закладену в природу коду, повністю усунути не можна. Надмірність від нерівноймовірності появи елемента зменшується зі збільшенням довжини кодового блоку.

На відміну від природної надмірності, яка характерна для первинних

алфавітів і присутня в повідомленні ще до того, як воно перетворюється на код, штучна надмірність уводиться до нього у вигляді r додаткових елементів спеціально для підвищення його завадостійкості. Таким чином, з n розрядів коду, з яких k несуть інформаційне навантаження, r = n – k розрядів уводяться як коректувальні. Ця величина характеризує абсолютну коректувальну надмірність, а величина $R_{над.r} = (n – k)/n = 1 – k/n = r/n$ – відносну коректувальну надмірність коду.

Основна теорема кодування. Повідомлення при передачі по каналах кодуються для того, щоб зменшити вплив завад у каналі та забезпечити надійний зв′язок між відправником й одержувачем повідомлень.

Імовірність неправильної передачі повідомлення по каналу може бути дуже малою, якщо воно передається за допомогою досить великої кількості повторень одного й того самого вхідного сигналу. Проте це пропорційно збільшує час, який відводиться на передачу; при цьому швидкість передачі (тобто кількість інформації, що передається за одиницю часу) прямує до нуля.

Теореми кодування для каналів допомагають зрозуміти, що існують нетривіальні способи кодування, які дають змогу здійснити передачу повідомлень зі скільки завгодно високою вірогідністю та відносно високою швидкістю. Ці теореми не вказують конкретних шляхів побудови пристроїв кодування та декодування, але показують, що вплив завад може бути зведений до мінімуму завдяки вибраному способу кодування та його реалізації.

Теорема кодування для каналу із завадами (яку ще називають основною теоремою Шеннона для дискретного каналу із завадами) доводить, що його пропускна здатність визначає верхню межу швидкості безпомилкової передачі інформації по каналу. Формулюється вона так: існує такий спосіб кодування для дискретного каналу із завадами, при якому можна забезпечити безпомилкову передачу інформації від джерела, якщо продуктивність останнього менша від пропускної здатності каналу, тобто

$$V_{дж}H(A) < V_k[\log_2 k – H(B/B′)] = C_k, \qquad (1.4)$$

де $V_{дж}$ – кількість повідомлень, вироблених джерелом А за одиницю часу; H(A) – ентропія джерела; V_k – кількість символів коду, що подаються на вхід каналу за одиницю часу; $[\log_2 k – H(B/B′)]$ – максимальна кількість інформації, яка переноситься одним символом коду; H(B/B′) – надійність каналу, що визначається дією завад; В – алфавіт обсягом k символів на вході каналу; B′ - алфавіт символів, які з′являються на виході каналу.

У теорії інформації обчисленням середньої імовірності помилки декодування доведено, що серед множини способів кодування є принаймні один, який дає змогу порівняти будь-яку прийняту кодову комбінацію з

алфавіту B′ з однією з комбінацій алфавіту B, використаних при кодуванні, що є умовою вірогідного декодування, причому середня ймовірність помилки декодування із збільшенням довжини коду прямує до нуля.

Теорема Шеннона не є конструктивною, оскільки вона не встановлює певний спосіб кодування для каналу із завадами, який забезпечує безпомилкову передачу інформації зі швидкістю, як завгодно близькою до пропускної здатності каналу, а лише доводить наявність такого способу на рівні його існування. Однак вона дає змогу зробити важливий висновок: вірогідність передачі інформації по дискретному каналу із завадами тим вища, чим більша довжина кодової комбінації та менша продуктивність джерела A відносно пропускної здатності каналу.

Таким чином, стає можливою заміна ефективності використання каналу вірогідністю передачі інформації, що широко застосовується у реальних каналах і системах передачі даних.

Для однозначного декодування прийнятих повідомлень, а також для передачі великих обсягів інформації з якомога мінімальними матеріальними та часовими витратами, коди мають задовольняти деякі вимоги.

Оптимальне кодування. Знайти код, який був би оптимальним з усіх точок зору, практично неможливо. Тому код може бути оптимальним тільки за певних умов (з точок зору швидкості передачі інформації, здатності виправляти помилки тощо).

У теорії інформації існує кілька методик побудови оптимальних з точки зору швидкості передачі інформації безнадмірних кодів.

До оптимальних безнадмірних кодів (з точки зору довжини їх, тобто швидкості передачі інформації) належать нерівномірні коди, які передають повідомлення комбінаціями мінімальної середньої довжини. Це зовсім не означає, що вони дійсно є абсолютно безнадмірними, оскільки такими вважаються коди, які задовольняють умову рівності обсягу та кількості інформації. Ці коди все ж таки мають потенційну надмірність через заборонені кодові комбінації, до яких належать комбінації, що доповнюють вершини неповного кодового дерева, яке відповідає оптимальному нерівномірному коду (ОНК), до повного утворення рівномірного коду.

Оптимальним кодуванням називається процедура перетворення символів первинного алфавіту q_1 на кодові комбінації вторинного алфавіту q_2, при якій середня довжина повідомлення у вторинному алфавіті мінімальна.

Таким чином, основним завданням оптимального кодування є досягнення рівності між кількістю інформації I, що виробляється джерелом повідомлень, та обсягом інформації Q на вході приймача повідомлень. Якщо $I = QI_{сер} = H$, то збільшення швидкості передачі інформації завдяки поліпшенню процедури кодування стає неможливим.

Для дискретних ансамблів повідомлень {X, p(x)} із середньою довжиною кодових комбінацій $\overline{n(x)} = H(X)/\log q$ можна запропонувати дві універсальні методики побудови ОНК.

Перша універсальна методика побудови ОНК грунтується на методиці Шеннона – Фано і передбачає цю побудову в кодовому алфавіті з кількістю якісних значень q. Згідно з цією методикою виконують такі процедури:

1) множину з N повідомлень, які кодуються, розташовують у порядку спадання імовірності;

2) впорядковані за ймовірностями повідомлення розбивають, по можливості, на q рівноймовірних груп;

3) кожній з груп завжди в одній і тій самій послідовності присвоюють символи алфавіту q (всім повідомленням першої групи – першу якісну ознаку цього алфавіту, всім повідомленням другої групи – другу якісну ознаку тощо);

4) створені групи розбивають, по можливості, на рівноймовірні підгрупи, кількість яких дорівнює або менша, ніж q (якщо після розбивання в групі остається одне повідомлення, то подальший поділ стає неможливим);

5) кожній з утворених підгруп присвоюють якісні ознаки з алфавіту q за процедурою п.3;

6) розбивання та присвоєння ознак алфавіту q повторюють доти, доки після чергового поділу в утворених підгрупах залишиться не більш як одне повідомлення.

Для побудови ОНК за викладеною методикою слід урахувати також відхилення від рівноймовірних значень, що утворюються при поділі на підгрупи. Вони враховуються згідно з правилами заліку остач ділення та середнього відхилення:

1) для того, щоб повідомлення первинного джерела можна було поділити по можливості на якомога рівноймовірні підгрупи при побудові ОНК з алфавітом q, остача попереднього ділення додається за абсолютним значенням сумарної ймовірності чергового ділення [остачею ділення називається різниця між квантом ділення та реальним значенням сумарної ймовірності в групі (підгрупі), де квант ділення дорівнює 1/q];

2) середнє відхилення має бути меншим або дорівнювати значенню ймовірності першого символу чергового ділення. Якщо середнє відхилення не дорівнює нулю, то середнє значення сумарної ймовірності в групі (підгрупі) при черговому діленні підраховується з додаванням значення середнього відхилення (середнім відхиленням називається абсолютне значення суми остач ділень на проміжних етапах побудови коду).

Друга універсальна методика побудови ОНК грунтується на методиці Хаффмена. Вона, як і методика Шеннона – Фано, передбачає побудову ОНК у кодовому алфавіті з кількістю якісних значень q. Згідно з цією методикою виконують такі процедури:

1) множину з N повідомлень, що кодуються, розташовують у порядку спадання ймовірностей;

2) останні N_0 повідомлень ($2 \le N \le q$) об′єднують у нове повідомлення з імовірністю, що дорівнює сумі ймовірностей об′єднуваних повідомлень;

3) утворену множину ($N - N_0 + 1$) повідомлень розташовують у порядку спадання ймовірностей;

4) об′єднують останні q повідомлень і впорядковують множину повідомлень у порядку спадання ймовірностей. Так діють доти, доки ймовірність чергового об′єднаного повідомлення не дорівнюватиме одиниці;

5) будують кодове дерево, починаючи з кореня, і гілкам цього дерева присвоюють якісні ознаки кодового алфавіту q.

Кодові комбінації ОНК – це послідовність якісних ознак, які зустрічаються на шляху від кореня до вершини кодового дерева.

Обидві універсальні методики мають неоднозначність, але перша з них дає змогу точніше будувати ОНК. До недоліків другої універсальної методики побудови ОНК слід віднести громіздкість (особливо зі збільшенням кількості повідомлень N та алфавіту q коду), що пояснюється необхідністю побудови кодового дерева.

Переваги другої універсальної методики побудови ОНК з $q > 2$ при $N < q^n$ будуть вагоміші при більш ретельному виборі кількості найменш імовірних повідомлень, що об′єднуються на першому етапі ($2 \le N_0 \le q$). На всіх наступних етапах ця кількість має дорівнювати q.

Розділ 2. ПЕРВИННІ КОДИ

Для кодування повідомлень, які надходять від джерела інформації, на першому етапі (первинне оброблення повідомлень) використовуються первинні коди, які мають мінімальну кодову відстань $d_{min} = 1$ і не можуть застосовуватися для виявлення та виправлення помилок.

Для кодування повідомлень при підготовці та уведенні даних у системи передачі та оброблення інформації застосовуються, як правило, первинні коди, до яких належать n-розрядні коди з основою (алфавітом) q, в яких використовуються всі q^n кодових комбінацій з потужністю $q^n \geq N_д > q^{n-1}$.

Розрізняють нерівномірні та рівномірні первинні коди. З перших найвідомішими є оптимальні двійкові коди Шеннона – Фано та Хаффмена, а також двійковий код Морзе.

До рівномірних двійкових кодів, які широко застосовуються на практиці, належать рекомендовані МККТТ (Міжнародний консультативний комітет з телеграфії та телефонії – тепер Міжнародний союз електрозв′язку) та Міжнародною організацією із стандартизації (ISO) коди: п′ятирозрядний двійковий, міжнародний стандартний телеграфний код №2 (МТК-2), міжнародний семирозрядний стандартний двійковий код №5 для передачі даних. Свого часу були розроблені і широко використовувались двійкові коди міжмашинного обміну інформацією КОІ-$7Н_0$, КОІ-$7С_1$, КОІ-8, код ДКОІ для внутрішнього обміну інформацією та код КПК-12 для подання даних на перфокартах.

Крім перелічених вище кодів, до первинних належать також коди, що мають специфічне використання. Це рівномірні рефлексні коди, що застосовуються в техніці аналого-цифрового перетворення і телевимірюванні, та двійково-десяткові коди, що поширені в системах відображення інформації або використовуються як проміжні при введенні в ЕОМ даних, поданих у десятковому коді.

2.1. Нерівномірні двійкові первинні коди

Крім двійкових ОНК Шеннона – Фано та Хаффмена, що згадувались у попередньому розділі, до цього часу широко застосовується нерівномірний (неповний) код Морзе, комбінації якого передаються елементами різної тривалості (крапки та тире). Цей код в основному використовується для передачі телеграфних повідомлень при радіозв′язку з морськими та повітряними судами, геологорозвідувальними та пошуковими партіями, полярними станціями та у військовому зв′язку.

Код Морзе було розроблено з урахуванням статистичних особливостей англійської мови (частоти появи окремих літер у тексті), яка у даний час є мовою міжнародного спілкування. При переході до національного алфавіту необхідно збільшувати кількість кодових комбінацій, щоб можна було передавати літери, які не мають аналогів у латинському алфавіті. До переваг коду Морзе (табл. 2.1) слід зарахувати його простоту, легкість запам′ятовування, можливість візуального приймання та приймання на слух, до недоліків – необхідність декодування тексту перед врученням споживачеві, а також надмірність. Крім того, цей код не враховує статистичних особливостей національної мови.

Таблиця 2.1

№	Літери алфавітів		Набір елементів	№	Цифри, знаки	Набір елементів
	укр/рос.	лат.				
1	А	A	·–	32	1	·–––––
2	Б	B	–···	33	2	··–––
3	В	W	·––	34	3	···––
4	Г	G	––·	35	4	····–
5	Д	D	–··	36	5	·····
6	Е	E	·	37	6	–····
7	Ж	V	···–	38	7	––···
8	З	Z	––··	39	8	–––··
9	І/И	I	··	40	9	––––·
10	Й	J	·–––	41	0	–––––
11	К	K	–·–	42	Крапка	·····
12	Л	L	·–··	43	Крапка з комою	–·–··
13	М	M	––	44	Кома	·–·–·–
14	Н	N	–·	45	Лапки	·–··–·
15	О	O	–––	46	Двокрапка	–––···
16	П	P	·––·	47	?	··––··
17	Р	R	·–·	48	!	––·–·–
18	С	S	···	49	Апостроф	·––––·
19	Т	T	–	50	Тире	–····–
20	У	U	··–	51	Дужки	–·––·–
21	Ф	F	··–·	52	Підкреслення	··––·–
22	Х	H	····	53	№	–··–·
23	Ц	C	–·–·	54	Чекати	·–···
24	Ч		–––·	55	Зрозумів	–––·–·
25	Ш		––––	56	Дробова риска	–··–·
26	Щ	Q	––·–	57	Знак поділу	–···–
27	Ь/Ъ	X	–··–	58	Перебій	········
28	И/Ы		–·––	59	Початок передачі	–·–·–·
29	Ю		··––			
30	Я		·–·–			
31	Є/Э	E	··–··			

Код Морзе широко застосовується при слуховому телеграфному(ТЛГ) зв′язку. Комбінації коду складені з двох таких елементів, що легко розпізнаються при прослуховуванні: крапки (коротки імпульси) та тире (у три рази довші імпульси). Нерівномірність коду Морзе ускладнює автоматичну обробку сигналів, але при слуховому прийомі полегшує розпізнавання букв.

Швидкість передавання знаків при слуховому ТЛГ зв′язку залежить від підготовки оператора та складає приблизно 100 знаків на хвилину. Передавання сигналів коду Морзе може здійснюватись радистом за допомогою спецключа, але при такому способі передавання супротивник має можливість слідкувати за переміщенням радіостанції, фіксуючи особливості щодо роботи радиста. Щоб це виключити, спрямовуються до стандартизації сигналів. З цією метою застосовують так звані датчики коду Морзе (ДКМ). Це електронний прилад, що пов′язаний з клавіатурою друкуючої машинки. Радист з допомогою клавіатури набирає текст, а ДКМ формує стандартні комбінації коду Морзе, що відповідають клавішам, які натискаються. Не дивлячись на слабку автоматизацію процесу зв′язку та малу швидкість передавання повідомлень, слуховий телеграф продовжує застосовуватися до сьогодення завдяки високій завадостійкості вуха людини (квазіоптимального приймача сигналу на фоні завади).

У число-імпульсному коді, який ще має назву одинично-десяткового, кожний розряд десяткового числа записується у вигляді відповідної кількості одиниц. Для можливості приймання їх приймачем окремі розряди кодових комбінацій відокремлюються інтервалами. Код не є рівномірним, хоча може бути перетворений на рівномірний дописуванням у кожній комбінації зліва нулів для заповнення загальної кількості їх елементів до 10. Так, запис десяткового числа 45 має вигляд 1111, 11111 (у варіанті рівномірного число-імпульсного коду це число записується так: 0000001111, 0000011111).

2.2. **Рівномірні двійкові первинні коди**

Рівномірні двійкові первинні коди широко застосовуються для передачі телеграфних повідомлень і даних, а різняться вони кількістю елементів, з яких складаються кодові комбінації, та комбінаціями цих елементів.

У цих кодах, які ще називаються простими, всі повідомлення нумеруються порядковою послідовністю у двійковій системі числення, що утворює їхній двійковий код. Кількість комбінацій двійкового коду $N = 2^n$,

тобто для запису у двійковому коді N повідомлень треба мати n розрядів: $n = \log_2 N$, де n – ціле число.

У числових двійкових кодах використовуються всі можливі комбінації ($N_д = N$); тому ці коди є безнадмірними та завадонезахищеними, а мінімальна кодова відстань у них $d_{min} = 1$.

Для використання в телеграфних апаратах МККТТ рекомендується міжнародний телеграфний код №2 (табл. 2.2).

Таблиця 2.2

№	Регістр			Комбінація				
	лат.	укр./рос.	цифр.	1	2	3	4	5
1	A	А	–	1	1	0	0	0
2	B	Б	?	1	0	0	1	1
3	C	Ц	:	0	0	1	1	1
4	D	Д	Хто там?	1	0	0	1	0
5	E	Е	3	1	0	0	0	0
6	F	Ф	Є/Э	1	0	1	1	0
7	G	Г	Ш	0	1	0	1	1
8	H	Х	Щ	0	0	1	0	1
9	I	І/И	8	0	1	1	0	0
10	J	Й	Ю	1	1	0	1	0
11	K	К	(	1	1	1	1	0
12	L	Л	)	0	1	0	0	1
13	M	М	.	0	0	1	1	1
14	N	Н	,	0	0	1	1	0
15	O	О	9	0	0	0	0	0
16	P	П	0	0	1	1	0	1
17	Q	Я	1	1	1	1	0	1
18	R	Р	4	0	1	0	1	0
19	S	С	Апостроф	1	0	1	0	0
20	T	Т	5	0	0	0	0	1
21	U	У	7	1	1	1	0	0
22	V	Ж	=	0	1	1	1	1
23	W	В	2	1	1	0	0	1
24	X	Ь	/	1	0	1	1	1
25	Y	И/Ы	6	1	0	1	0	1
26	Z	З	+	1	0	0	0	1
27	Повернення каретки			0	0	0	1	0
28	Переведення рядка			0	1	0	0	0
29	Латинський регістр			1	1	1	1	1
30	Цифровий регістр			1	1	0	1	1
31	Пробіл			0	0	1	0	0
32	Національний регістр			0	0	0	0	0

У цьому п′ятиелементному коді з 32 комбінацій 29 застосовуються для передачі літер, цифр, розділових і службових знаків у трьох регістрах (латинському, національному, цифровому), для яких призначено решту кодових комбінацій.

При передачі даних, крім літер, цифрових, арифметичних і службових знаків міжнародного телеграфного коду № 2, необхідно передавати також не тільки малі, а й великі літери, додаткові розділові, службові та керуючі знаки. Розроблений для цієї мети міжнародний семирозрядний стандартний код № 5 (табл. 2.3), який рекомендовано для передачі та оброблення інформації, побудовано так, щоб будь-який знак цієї кодової таблиці можна було відобразити семиелементною послідовністю, яка містить три старші розряди, що відповідають стовпцю $a_7a_6a_5$, і чотири молодші розряди, які відповідають рядку $a_4a_3a_2a_1$ (наприклад, літері В відповідає кодова послідовність 1000010). При цьому у разі необхідності простим виключенням старших розрядів можна дістати підмножини комбінацій меншої розрядності.

Таблиця 2.3

								0	0	0	0	1	1	1	1
								0	0	1	1	0	0	1	1
								0	1	0	1	0	1	0	1
a_7	a_6	a_5	a_4	a_3	a_2	a_1	№	0	1	2	3	4	5	6	7
			0	0	0	0	0	**NUL**	**(TC_7) DLE**	Space	0	@	P	\·	p
			0	0	0	1	1	**(TC_1) SOH**	**DC_1**	!	1	A	Q	a	q
			0	0	1	0	2	**(TC_2) STX**	**DC_2**	“	2	B	R	b	r
			0	0	1	1	3	**(TC_3) ETX**	**DC_3**	#	3	C	S	c	s
			0	1	0	0	4	**(TC_4) EOT**	**DC_4**	$	4	D	T	d	t
			0	1	0	1	5	**(TC_5) ENQ**	**(TC_8) NACK**	%	5	E	U	e	u
			0	1	1	0	6	**(TC_6) ACK**	**(TC_9) SYNC**	&	6	F	V	f	v
			0	1	1	1	7	**BEL**	**(TC_{10}) ETB**	·/	7	G	W	g	w
			1	0	0	0	8	**(FE_0) BS**	**CAN**	(	8	H	X	h	x
			1	0	0	1	9	**(FE_1) HT**	**EM**	)	9	I	Y	i	y
			1	0	1	0	10	**(FE_2) LF**	**SUB**	*	:	J	Z	j	z
			1	0	1	1	11	**(FE_3) VT**	**ESC**	+	;	K	[	k	
			1	1	0	0	12	**(FE_4) FF**	**(IS_4) FS**	,	<	L		l	
			1	1	0	1	13	**(FE_5) CR**	**(IS_3) GS**	–	=	M	]	m	
			1	1	1	0	14	**SO**	**(IS_2) RS**	.	>	N	^	n	
			1	1	1	1	15	**SI**	**(IS_1) US**	/	?	O	-	o	**DEL**

Цей код у США використовується під назвою коду ASCII (або USASCII) як засіб взаємодії з ЕОМ. Він дає змогу перетворювати машинні дані, записані у двійковому коді, на звичайні знаки (числа, літери), які можна роздрукувати та вивести на термінал. Оскільки восьмибітові коди застосовуються в ЕОМ значно частіше, ніж семибітові, в коді ASCII-8 восьмий (крайній лівий) біт використовується як біт парності (1 – якщо праві сім бітів складають непарне число одиниць і 0 – при парному їх числі для перевірки правильності передачі даних. При виявленні помилки користувачеві видається повідомлення Parity Error – помилка парності).

Міжнародний стандартний код № 5 логічно може бути поділений на чотири зони. До першої зони (колонки 0, 1) належать функціональні символи, за винятком символу DEL (витирання, перебій), для якого відведено останнє місце (комбінація 1111111). Основна частина функціональних символів поділяється на чотири групи:

– перша – для керування передачею інформації по каналах зв′язку ($ТС_1 \ldots ТС_{10}$);

– друга – для керування друком ($FE_0 \ldots FE_5$);

– третя – для керування кінцевими пристроями ($DC_1 \ldots DC_4$);

– четверта – для роздільників інформації ($IS_1 \ldots IS_4$).

Символи першої групи мають два призначення: використовуються для обрамлення повідомлення у формат, який легко розпізнається, або у послідовність, яка може оброблятися споживачем; застосовуються для керування передачею даних у мережі.

Як відомо, текст – це інформаційний зміст повідомлення. Якщо воно досить тривале, то його, як правило, розбивають на кілька блоків, які передають один за одним по лінії зв′язку. Залежно від системи, що використовується для передачі, перед блоками може бути заголовок, який повинен мати адресну та керуючу інформацію, що супроводжує текст повідомлення. Заголовок може містити відомості про пріоритет повідомлення, дату та час його відправлення, ідентифікатор лінії зв′язку, по якій передається повідомлення, відомості про ступінь секретності тощо. Отже, в заголовку подаються відомості про те, як повідомлення має оброблятися на шляху від джерела до одержувача.

Рішення про використання заголовка повідомлення, а також його зміст приймається на основі характеристик конкретної системи передачі даних і програмного забезпечення. Якщо повідомлення містить, наприклад, чотири блоки тексту, то перший його блок передається із заголовком, у якому подаються необхідні характеристики повідомлення, а всі наступні блоки передаються без заголовка.

Розглянемо призначення окремих символів зв′язку більш докладно.

Перша група. Символ $ТС_1$ (початок заголовка) використовується як перший символ заголовка інформаційного повідомлення і повідомляє одержувача, що інформація, яка подається після нього, має інтерпретуватися (тлумачитися) як заголовок повідомлення.

Аналогічно символ $ТС_2$ (початок тексту) розміщується на початку тексту і застосовується для позначення кінця заголовка, а також показує, що інформація, яка подається після нього, є текстом повідомлення.

Символ $ТС_3$ (кінець тексту) передається в кінці тексту й означає, що повідомлення було передано повністю.

Символ $ТС_4$ (кінець передачі) використовується для зазначення кінця передачі одного або кількох текстів.

Символ $ТС_5$ (хто там?) застосовується для запиту відповіді віддаленої станції, причому відповідь може містити ідентифікатор і статус станції.

Символ $ТС_6$ (підтвердження) передається приймачем як підтвердження прийому запиту передавача.

Символ $ТС_7$ (перший авторегістр) використовується для розширення функцій керування передачею даних; при цьому він змінює значення обмеженої кількості символів, які передаються безпосередньо за ним. До цих символів можуть належати тільки графічні символи та символи зв′язку.

Символ $ТС_8$ (негативна квитанція) передається приймачем як негативна відповідь передавачу.

Символ $ТС_9$ (синхронізація) застосовується у синхронних системах передачі за відсутності інформаційних символів для встановлення та підтримки синхронізації кінцевого устаткування.

Символ $ТС_{10}$ (кінець блоку) використовується для зазначення кінця блоку тоді, коли дані, що передаються, розбиваються на блоки.

У деяких системах при передачі багатоблокового повідомлення символ $ТС_3$ (кінець тексту) має бути в кінці кожного блоку для того, щоб одержувач міг скласти з блоків повне повідомлення.

Друга група. До цієї групи належать символи керування друком, які використовуються при розміщенні інформації на друкованому аркуші або на екрані пристрою візуального зображення з метою полегшення сприйняття даних. Перший символ FE_0 (повернення на крок) відповідає поверненню на крок і дає змогу повернути головку пристрою друку на один крок назад. Для пристроїв візуального зображення цей символ означає переведення покажчика на одну позицію ліворуч.

Символ FE_1 (горизонтальна табуляція) дає змогу перемістити головку друку в задане положення у горизонтальному напрямку; символ FE_2 (переведення рядка) – у те саме положення в наступному рядку; символ FE_3 (вертикальна табуляція) – в те саме положення через кілька рядків у межах однієї сторінки; символ FE_4 (переведення формату) – в те саме положення на зумовленому рядку на іншій сторінці; символ FE_5 (повернення каретки) – в початкове положення рядка.

Третя група. До цієї групи належать символи керування пристроями, що встановлюють фізичні функції на термінал. Так, символ DC_1 призначений для приєднання до терміналу касетного накопичувача; символ DC_2 – для вимикання цього накопичувача; символ DC_3 – для виведення інформації з пристрою візуального відображення на допоміжний пристрій друку, а символ DC_4 – для блокування пристрою візуального зображення, щоб оператор не зміг вивести з нього дані.

Четверта група. Ця група символів має чотири роздільники інформації, призначені для логічного розмежовування інформації з метою полегшення її оброблення на ЕОМ. Так, символ IS_1 використовується для розмежовування найменшого обсягу інформації і називається роздільником одиниць; символ IS_2 – для розмежовування підгруп інформації, які можуть містити кілька одиниць; символ IS_3 – для розмежовування підгруп інформації, які можуть складатися з кількох підгруп, а символ IS_4 – для розмежовування файлів, які можуть містити кілька груп інформації.

Решту зон табл. 2.3 зайнято графічними знаками. Її другу зону (колонки 2, 3) виділено для спеціальних математичних знаків, а також знаків пунктуації і цифр. У двох останніх зонах цієї таблиці розміщуються великі й малі латинські літери відповідно до вимог лексико-графічної впорядкованості (положення цифр, знаків пунктуації та пробілу також вибрано з урахуванням цих вимог). Тут знаходяться й усі резервні позиції.

Знак «Пробіл» («Space») не друкується, але належить до числа графічних і застосовується для поділу слів і переміщення позиції друку на один крок уперед. Цифри кодуються звичайним двійковим кодом. Побудова чотирирозрядних комбінацій для них виконується відкиданням трьох старших розрядів.

Є два методи декодування знаків у міжнародному стандартному коді № 5. По-перше, можна застосувати їх двійкове подання (наприклад, послідовність 1010100 відповідає знаку Т). Інший метод полягає у використанні номерів рядків і стовпців для однозначного визначення конкретного знака (наприклад, запис 5/04 відповідатиме тому самому знаку Т, який знаходиться у п′ятому стовпці та четвертому рядку).

Відсутність у розглядуваному коді знаків, які відповідали б національному алфавіту (в тому разі, коли він відрізняється від латинського), не дає змоги широко використовувати його у країнах з нелатинськими алфавітами, у тому числі й у нашій країні. Тому на основі коду № 5 було розроблено код, в якому враховано особливості національного алфавіту. У цей код уведено національний регістр (укр/рос) шляхом додавання ще восьми стовпців, з яких стовпці 8…11 відповідають стовпцям 0…3 коду № 5, а стовпці 12…15 призначені для розміщення великих та малих літер національного алфавіту. Стовпцям 0…7 присвоюється додаткова ознака 0, а стовпцям 8…15 – ознака 1. Таким чином код, в який уведено національний регістр, перетворюється у висьмирозрядний порівняно з семирозрядним кодом № 5. Зручність використання такого коду в системах передачі даних полягає в простоті його перетворення на восьмирозрядний код з перевіркою на парність, що дає змогу підвищити завадостійкість передачі інформації по каналах із завадами.

За принципами побудови коди КОІ-7$Н_0$, КОІ-7$С_1$, КОІ-8, ДКОІ і КПК-12, які згадувались вище, схожі з міжнародним кодом № 5.

Рефлексні коди. Особливість побудови рефлексних кодів полягає в тому, що сусідні кодові комбінації на відміну від двійкових простих кодів різняться цифрою тільки в одному розряді, тобто кодова відстань між ними дорівнює одиниці.

Іншою особливістю цих кодів є те, що зміна елементів у кожному розряді при переході від комбінації до комбінації відбувається в два рази рідше, ніж у простому коді, завдяки чому значно спрощується кодер. Крім того, при додаванні двох сусідніх комбінацій рефлексного коду за модулем 2 кількість одиниць дорівнюватиме кількості розрядів мінус 3, тобто одиниці, що використовується для перевірки правильності прийнятої кодової комбінації.

Свою назву рефлексні коди дістали через наявність осей симетрії, відносно яких виразно проглядається ідентичність елементів у деяких розрядах.

Можна утворити велику кількість двійкових рефлексних кодів, у яких дві сусідні комбінації відрізняються тільки одним символом (табл. 2.4).

Найбільшого поширення з рефлексних кодів дістав код Грея (табл. 2.5), який, на відміну від інших, простіший при перетворенні його на двійковий простий код. Обернене перетворення двійкового простого коду на код Грея виконується за алгоритмом: $y_i = x_i \oplus x_{i+1}$, де y_i – значення і-го розряду коду Грея; x_i, x_{i+1} – відповідні значення розрядів двійкового числа (i = 1, 2,…, n, починаючи зліва).

Таблиця 2.4

Десяткове число	Варіанти рефлексних кодів				
	перший	другий	третій	четвертий	п′ятий
0	000	000	000	000	000
1	010	100	100	001	001
2	011	101	110	011	101
3	001	001	010	010	100
4	101	011	011	110	110
5	111	111	111	111	111
6	110	110	101	101	011
7	100	010	001	100	010

Таким чином, для утворення комбінації коду Грея практично досить зсунути двійкову комбінацію простого коду на один розряд праворуч, порозрядно додати її за модулем 2 до початкової кодової комбінації без перенесення між розрядами і відкинути молодший розряд здобутої суми.

Таблиця 2.5

Десяткове число	Двійковий простий код	Код Грея	Десяткове число	Двійковий простий код	Код Грея
0	0000	0000	8	1000	1100
1	0001	0001	9	1001	1101
2	0010	0011	10	1010	1111
3	0011	0010	11	1011	1110
4	0100	0110	12	1100	1010
5	0101	0111	13	1101	1011
6	0110	0101	14	1110	1001
7	0111	0100	15	1111	1000

Декодування (обернене перетворення) коду Грея можна виконати двома способами:

– перший спосіб

$$\begin{cases} x_n = y_n; \\ x_i = x_{i+1} \oplus y_i, \end{cases}$$

де x_n і y_n – відповідно значення старшого розряду двійкового простого коду та коду Грея ($i = n-1, n-2, \ldots, 1$, починаючи зліва);

– другий спосіб

$$x_j = \sum_{j=1}^{n} y_j,$$

де y_j – значення розрядів коду Грея, а сума береться за всіма розрядами цього коду від i- до n-го (старшого, крайнього зліва).

Іншими словами, щоб перейти від коду Грея до двійкового простого коду, треба:

– залишити цифру старшого розряду без зміни;

– кожну наступну цифру інвертувати стільки разів, скільки одиниць є перед нею в коді Грея, або виконати послідовне порозрядне підсумовування за модулем 2 першого (старшого) та другого розрядів комбінації цього коду (1⊕2), після чого послідовно додати 1⊕2⊕3, 1⊕2⊕3⊕4 і т. д.

До характерних особливостей коду Грея належить те, що, по-перше, кожна наступна комбінація завжди відрізняється від попередньої тільки в одній позиції (одному розряді); по-друге, зміна значень елементів у кожному розряді при переході від комбінації до комбінації відбувається в два рази швидше, ніж у двійковому простому коді, що дає змогу при тій самій швидкості кодера досягати вищої точності кодування порівняно з двійковим простим кодом; по-третє, при додаванні двох сусідніх комбінацій за модулем 2 кількість одиниць дорівнюватиме кількості розрядів мінус 3, що використовується для перевірки наявності помилки у прийнятій кодовій комбінації; по-четверте, в цьому коді можна виділити кілька осей симетрії, відносно яких спостерігається ідентичність елементів у деяких розрядах. Так, має місце симетрія деяких розрядів відносно осей, проведених між числами 1 і 2, 3 та 4, 5 і 6, 7 та 8, 9 і 10, 11 та 12 (див. табл. 2.5).

Код Грея широко застосовується для аналого-цифрового перетворення різних неперервних повідомлень. Він дає змогу зменшити кількість помилок від завад, які виникають при передачі інформації по каналах зв′язку.

До недоліків цього коду належить «невагомість» кодової комбінації, коли вага одиниці в ній не визначається номером розряду, на місці якого вона знаходиться, а переведення кодової комбінації з двійкової системи числення в десяткову не визначатиме порядковий номер комбінацій в коді Грея. Такі коди важко декодувати, тому перед декодуванням їх, як правило, перетворюють на двійковий простий код, після чого й обробляють останній.

2.3. **Аналогово-цифрове та цифро-аналогове перетворення**

Перетворення неперервних повідомлень у кодований двійковий сигнал та зворотне перетворення є в даний час основою цифрового зв′язку.

Основний алгоритм представлення аналогового сигналу у цифровому вигляді полягає у послідовному здійсненні трьох етапів перетворення: дискретизація у часі, квантування за рівнями, кодування. Цей алгоритм одержав назву імпульсно-кодової модуляції (ІКМ).

Перше перетворення (дискретизація) полягає в тому, що неперервний процес замінюється послідовністю неперервнозначних величин, що надходять через однакові інтервали часу, які називають *інтервалом дискретизації*.

Можуть застосовуватися різні процедури дискретизації. Серед них найбільш поширена лінійна дискретизація, при якій

$$c_k = \int_{-\infty}^{\infty} f_k(t)c(t)dt.$$

У цій формулі величини c_k називаються вибірковими значеннями процесу c(t), а функція $f_k(t)$ – ваговою функцією вибору.

У задачах дискретизації більш частіше розглядається випадок точкового вибору, при якому вагова функція вибору являє собою дельта-функцію. Така процедура дискретизації просто реалізується за допомогою ключових схем.

Другою, менш поширеною процедурою дискретизації є дискретизація з інтегруванням (із прямокутною функцією вибору).

Визначаючи процедуру дискретизації, потрібно установити функцію вибору $f_k(t)$ і інтервал дискретизації за часом Т. При цьому треба виходити з критерію мінімума середнього квадрата помилки передачі повідомлення.

Теореми відліків. Однією з перших теорем, що відносяться до області дискретизації безперервних повідомлень, є теорема відліків. Уперше деякі положення теореми відліків були висловлені без доказу в 1928 р. у статті відомого вченого США Н. Найквиста. У 1933 р. академік В.А. Котельников у статті «Про пропускну здатність ефіру і дроту в електрозв'язку» привів доказ теореми відліків. Зараз під теоремою відліків розуміють кілька теорем, що формулюються нижче.

Пряма теорема відліків (перша теорема Котельникова). Детермінована функція часу c(t), спектр якої (перетворення Фур'є) неперервний і обмежений смугою кругових частот (-Δ,Δ) й дорівнює нулю за межами смуги, може бути представлений у виді ряду

$$c(t) = \sum_{-\infty}^{\infty} c\left(\frac{n\pi}{\Delta}\right) \frac{\sin\left[\Delta\left(t - \frac{n\pi}{\Delta}\right)\right]}{\Delta\left(t - \frac{n\pi}{\Delta}\right)}. \qquad (2.1)$$

Друга теорема Котельникова. Детермінована функція часу, спектр якої неперервний і обмежений смугою частот (-Δ,Δ), може бути безпомилково передана за допомогою послідовності Δ/π відліків в одиницю часу.

Зворотна теорема відліків. Спектр функції c(t), що існує в інтервалі (–T/2, T/2) і дорівнює нулю за межами цього інтервалу, може бути представлений у вигляді

$$Z(\omega)=\sum_{n=-\infty}^{\infty} Z\left(\frac{2\pi n}{T}\right)\frac{\sin\left(\frac{\omega T}{2}-n\pi\right)}{\frac{\omega T}{2}-n\pi}.$$

Приведені теореми доводяться для детермінованих функцій часу. Можна вважати, що така детермінована функція часу являє собою одну з безлічі функцій, що утворюють даний випадковий процес. Якщо спектральна щільність випадкового процесу обмежена в смузі частот, то представляючи кожну реалізацію цього процесу за формулою (2.1), будемо допускати деяку помилку, квадрат якої, усереднений за нескінченною безліччю реалізацій, прагне до нуля. У цьому випадку кажуть, що випадковий процес з обмеженою спектральною щільністю сходиться до процесу, для якого справедливе представлення (2.1) у середньоквадратичному змісті. Це дає підставу використовувати перші з двох теорем для випадкових процесів із обмеженою спектральною щільністю. Хоча і не виключається, що в нескінченній безлічі реалізацій, які утворюють даний випадковий процес, знайдуться реалізації, для яких представлення (2.1) буде несправедливим.

Для зв'язку найбільш важливими є перша і друга теореми. Друга теорема дозволяє визначити крок дискретизації за часом T чи частоту дискретизації f = 1/T. Наприклад, якщо вважати, що мовний процес характеризується спектром, обмеженим вищою частотою 3,4 кГц, то за другою теоремою частоту дискретизації варто вибирати рівною 6,8 кГц. Практично спектр мови не є ідеально обмеженим, тому вибирається більша частота дискретизації, яка дорівнює 8 кГц.

Перша теорема і формула (2.1) показують, як треба відновлювати неперервне повідомлення на прийомному боці системи зв'язку після прийому відліків $c(t_i)$. Для цього відліки процесу $c(t_i)$, що є його координатами, повинні множитися на координатні функції

$$f_i(t)=\frac{\sin\left[\Delta\left(t-\frac{n\pi}{\Delta}\right)\right]}{\Delta\left(t-\frac{n\pi}{\Delta}\right)}.$$

Ця операція називається *процедурою згладжування*.

Теоретично реалізувати процедуру згладжування (2.1) можна різними способами (наприклад, з використанням ЕОМ чи в аналоговому варіанті за допомогою ідеального лінійного фільтра з прямокутною частотною характеристикою). Однак на практиці процедуру згладжування можна реалізувати лише приблизно.

Таким чином на першому етапі з безперервного сигналу формується послідовність відліків (див. рис. 2.1).

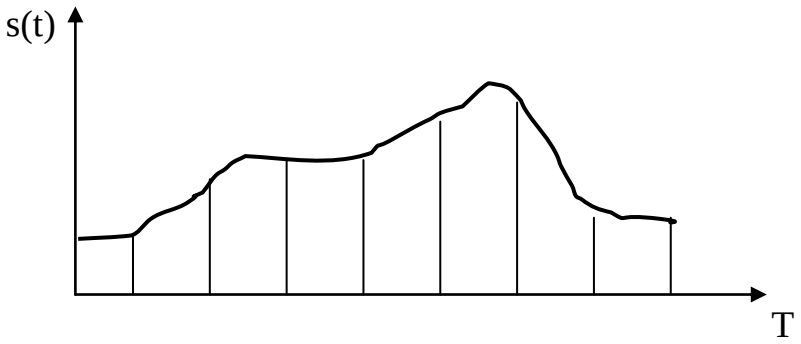


Рис. 2.1

Послідовність відліків може формуватись з використанням рівних чи нерівних інтервалів часу. Тому розрізняють рівномірну та нерівномірну дискретизації. Поширенішою на практиці є рівномірна дискретизація завдяки найбільш простій технічний реалізації, тому що частота дискретизації в цьому випадку постійна.

Вимоги щодо частоти дискретизації визначаються теоремою Котельникова – $T_д = 1/2F_{max}$.

Для відновлення сигналу з його дискретизованого вигляду може використовуватись фільтр низьких частот (ФНЧ) із частотою зрізу, яка визначається такою умовою:

$$F_{max} \leq f_ф \leq f_д - F_{max} .$$

Для відтворення сигналу за допомогою реального ФНЧ частота дискретизації повинна задовольняти умови

$$f_д = 2 R F_{max} ,$$

де $R = 1,1 – 1,5$ – постійний коефіцієнт.

Другим етапом ІКМ-перетворення є квантування одержаних відліків.

Квантування являє собою перетворення сигналу, при якому діапазон можливих значень параметрів сигналу поділяється на кінцеве число зон, кожна з яких представляється одним фіксованим значенням параметра цього сигналу. Коротше, квантуванням називається перетворення безперервних випадкових величин у дискретні.

У системі зв'язку квантування за рівнями і кодування здійснюється, як правило, в одному пристрої, який називається кодером. На виході системи зв'язку декодування кодових комбінацій і утворення дискретних випадкових величин виробляється в декодері. Відповідні один одному кодер і декодер разом утворюють кодек.

Розглянемо процеси, що протікають при квантуванні, більш докладно. Припустимо, що перешкоди в каналі зв'язку не діють. Амплітудна характеристика квантувача має вигляд, показаний на рис. 2.2. По горизонтальній осі відкладені значення вхідних безперервних величин, а по вертикальній осі – вихідних дискретних. Видно, що характеристика має східчастий характер і є нелінійною.

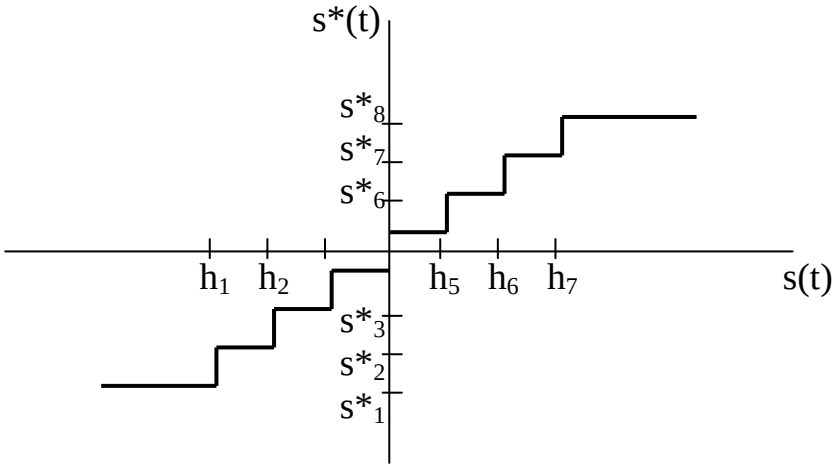


Рис. 2.2

При цьому безперервний інтервал значень відліків замінюють кінцевою множиною дозволених для передавання рівнів квантування. Рівні квантування поділяють весь діапазон зміни амплітуд відліків на кінцеве число інтервалів, що мають назву кроків квантування. Кожному рівню квантування відповідає відповідна зона значень амплітуд відліків. Кордони між цими зонами називаються порогами квантування.

Як бачимо з рисунка, будь-яке значення амплітуди вхідного сигналу в межах між двома сусідніми порогами буде представлене одним і тим же рівнем квантування. Тому процес квантування завжди супроводжується

помилками, які звуться шумом квантування. ІКМ з рівномірним квантуванням називають лінійним. Вплив шуму квантування можна суттєво зменшити, якщо використовувати нерівномірне квантування. При цьому більші рівні сигналів квантуються більшим кроком, а менші – меншим. Рівномірне квантування здійснюється простіше, але при нерівномірному квантуванні, коли кроки обирати узгоджено із характеристиками повідомлення, можна одержати більш високу точність передачі. Технічна процедура нерівномірного квантування складна. Тому використовується спосіб, що одержав назву квантування з компандуванням. Компандерна система являє собою комплекс з двох нелінійних перетворювачів із взаємно зворотними характеристиками.

Компресор стискає динамічний діапазон вхідного сигналу, а потім використовує стандартний лінійний ІКМ-кодер.

Третім етапом ІКМ-перетворення є кодування квантованих значень набором двійкових символів.

Найпростіше це здійснюється шляхом запису номера рівня квантування у вигляді двійкового числа. При кількості двійкових розрядів на відлік, який становить 8, прикладом запису номера рівня квантування може бути – 00111001.

Відомо декілька типів цифрових систем зв'язку, призначених для передачі аналогових повідомлень. До одного з них, найбільш поширеного, відносяться системи зв'язку з імпульсно-кодовою модуляцією (ІКМ). Для них характерно те, що дискретизації і квантуванню підлягає безпосередньо саме повідомлення. До іншого типу відносяться системи зв'язку з диференціальною імпульсно-кодовою модуляцією (ДІКМ), у яких дискретизації і квантуванню підлягає різниця між повідомленням та його передбаченими значеннями, отриманими із використанням попередніх цифрових сигналів.

Системи зв′язку з імпульсно-кодовою модуляцією (ІКМ). Повідомлення можуть являти собою безперервні величини чи безперервнозначні процеси. Безперервними величинами можуть бути такі повідомлення, як координати цілі, заданий курс, задана висота польоту та інше. Вони передаються одноразово і в цьому випадку немає можливості сформувати передбачене значення повідомлення із попередніх сигналів, тому що такі сигнали відсутні. Тому при передачі безперервних величин систему із ДІКМ використати неможливо, а треба застосовувати тільки систему зв′язку з ІКМ. Коли ж повідомлення являє собою безперервнозначний випадковий процес, наприклад, мовний сигнал, тоді для його передачі може бути використана як система зв′язку з ІКМ, так і з ДІКМ.

Схема системи зв′язку з ІКМ зображена на рис. 2.3.

Система включає в себе відправника повідомлення, дискретизатор, кодер, цифровий канал зв′язку, декодер та пристрій згладжування, з виходу якого оцінка повідомлення передається одержувачу. При передачі випадкової величини замість згладжування здійснюється запам′ятовування прийнятого повідомлення, а при передачі безперервнозначного процесу на виході системи зв′язку здійснюється згладжування оцінки повідомлення для послаблення помилок, пов′язаних з дискретизацією та квантуванням. На практиці такі процедури, як дискретизація, квантування і кодування, робляться сумісно в одному пристрої, який називається аналого-цифровим перетворювачем (АЦП). Зворотна процедура здійснюється за допомогою перетворювача, який називається цифро-аналоговим (ЦАП).

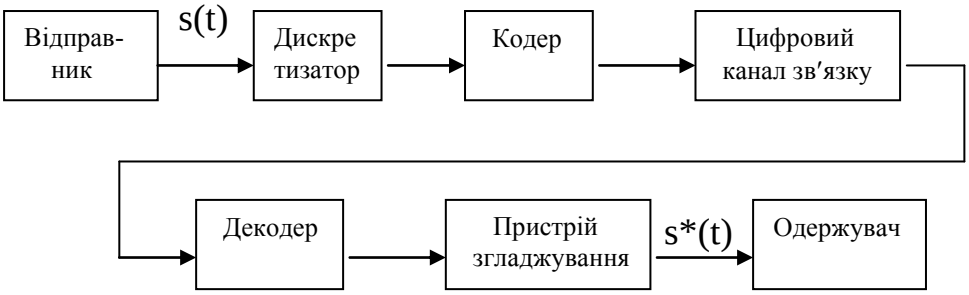


Рис. 2.3

Тоді система зв′язку з ІКМ виглядає, як показано на рис. 2.4.

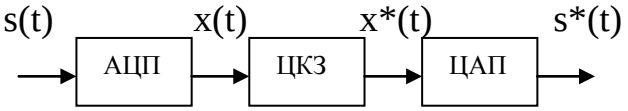


Рис. 2.4

Операції дискретизації та квантування здійснюються в АЦП. На виході АЦП формується дискретна послідовність x(t). На виході цифрового каналу зв′язку (ЦКЗ) за допомогою ЦАП робиться декодування прийнятих кодових комбінацій. Процес дискретизації, квантування та кодування показаний на рис. 2.5.

При квантуванні за рівнями інтервал можливих значень s(t) поділяється на N зон рівнями квантування h_1, h_2,…h_{N-1}. Коли часовий відлік сигналу попадає у деяку зону квантування, то в АЦП формується номер цієї зони, який передається у ЦКЗ у вигляді послідовного двійкового коду. Наприклад, запис сигналу для повідомлення, зображеного на рис. 2.5, буде у двійковому коді виглядати так: 01101000101001110111110101101101101. На виході після декодування в ЦАП цього дискретного сигналу виявляється напруга s*(t), пропорційна номеру рівня. Точність встановлення по-

відомлення за його квантованими відліками можна оцінити помилкою ε=s(t)-s*(t). Абсолютна величина помилок не перевищує половини кроку квантування: $|\varepsilon| < \Delta/2$, де $\Delta = h_i - h_{i-1}$. Послідовність ε часто називають "шумом квантування". Із ростом числа рівнів квантування потужність шумів квантування зменшується.

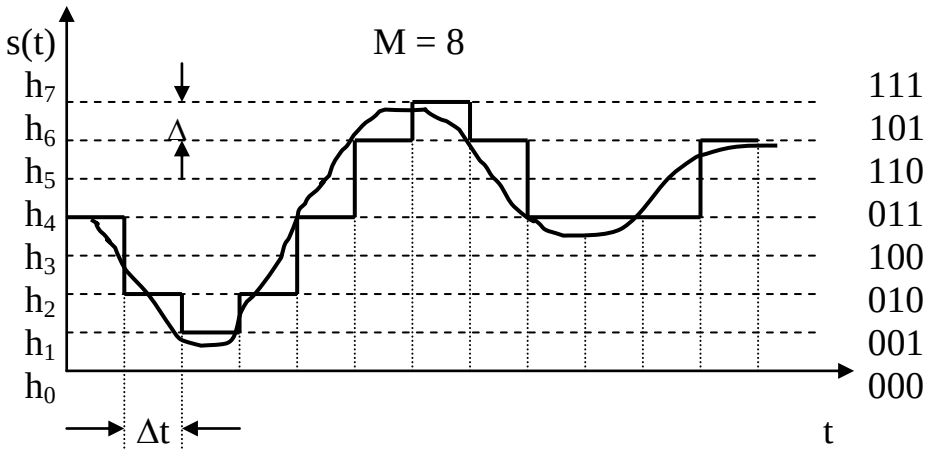


Рис. 2.5

При ІКМ квантовані рівні безперервного повідомлення у разі використання двійкового коду передаються комбінаціями імпульсів, кожний з яких може мати одне з m = 2 значень (1 або 0). При цьому:

$$n = \log_2 M, \qquad (2.2)$$

де M – загальне число рівнів в ансамблі квантованого повідомлення.

Системи зв′язку з диференціальною імпульсно-кодовою модуляцією (ДІКМ). Аналіз ІКМ показує, що відлік вхідного сигналу кодується незалежно від сусідніх. Це означає, що така система не враховує статистичну надмірність мовних сигналів, і для створення кожного відліку використовується надмірна кількість біт. Дані обставини призводять до високих потрібних швидкостей передавання у цифровій формі. Наприклад, для передачі мовного сигналу з доброю якістю потрібна швидкість $V_{мс} = f_д \cdot n$ = 8 кГц·8 біт = 64 кбіт/с. Один зі шляхів зменшення швидкості передачі – це усунення статистичної надмірності.

Найпростіше надмірність можна усунути, якщо на кожному такті піддавати кодуванню не саме значення відліку, а тільки його зміну відносно попереднього значення. Згідно цієї ідеї має місце врахування статистичних характеристик сигналу на якомусь попередньому часовому інтервалі та використання їх для передбачення значень наступних відліків.

Наявність надмірності у сигналі гарантує отримання достатньо точного передбачення. Помилка передбачення визначається як різниця між істинним та передбаченим значенням відліку і має у цьому випадку невеликий динамічний діапазон та допускає використання меншої, ніж при ІКМ, кількості рівнів квантування. Практична реалізація таких процесів виконується шляхом відрахування передбаченого значення із величини, що квантується. Засіб, що реалізує випадок, коли передбачене значення сигналу формується із попереднього цифрового, отримав назву диференційної ІКМ (ДІКМ).

Структурна схема ДІКМ наведена на рис. 2.6. Принцип дії ДІКМ пояснюється за допомогою рис. 2.7.

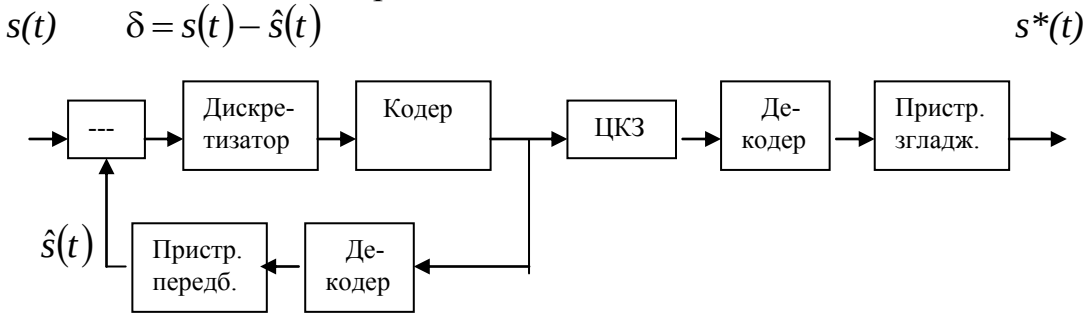


Рис. 2.6

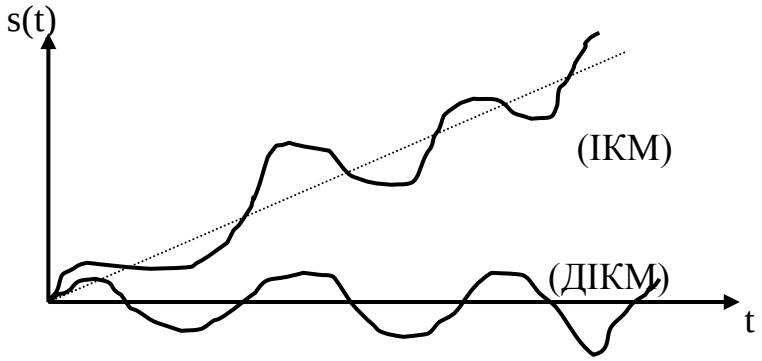


Рис. 2.7

У кодері квантувач АЦП охоплено зворотним зв’язком, що дозволяє уникнути накопичення помилок квантування при декодуванні. Блок передбачення на основі аналізу попередніх відліків оцінює (пророкує) значення поточних відліків. Треба відмітити, що пристрій згладжування є еквівалентним фільтру, який згладжує сигнал у приймальній частині системи зв′язку.

Позитивна дія кола зворотного зв′язку є в усуненні надмірності, яка є в повідомленні й апріорно відома. В результаті значно зменшується ди-

намічний діапазон квантованого сигналу, що дозволяє зменшити смугу пропускання ЦКЗ.

Аналіз роботи ДІКМ-кодерів показує, що усунення статистичної надмірності мовних сигналів дозволяє при однаковій з ІКМ із стандартним сигналом якості використовувати в два рази менше рівнів квантування, що дозволяє знизити швидкість їх передавання до ~ 32 кбіт/с.

Системи зв′язку з дельта –модуляцією (ДМ). ДМ може розглядатись, як частковий випадок ДІКМ, при якому помилка передбачення квантується тільки на два рівні. Таке обмеження призводить до дуже простої технічної реалізації кодеку ДМ. Структурна схема кодера та декодера ДМ в найбільш загальному вигляді зображена на рис. 2.8.

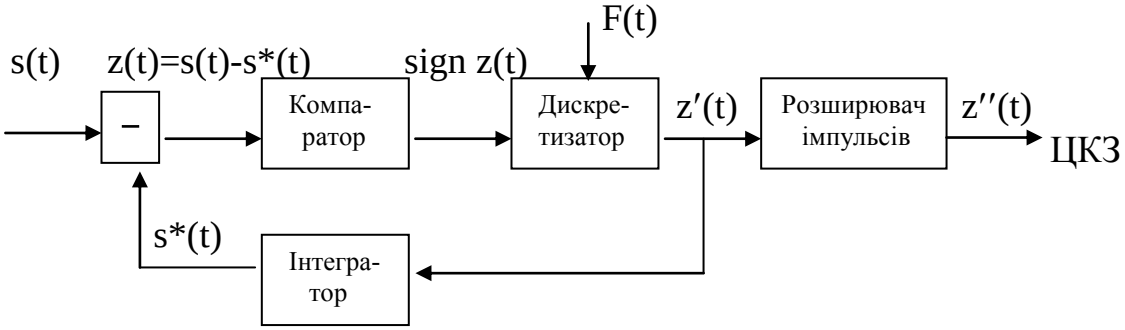


Рис. 2.8

До складу пристрою ДМ входять: пристрій, що віднімає, на виході якого формується сигнал z(t) – помилка передбачення; компаратор на два рівні; часовий дискретизатор, на виході якого формуються короткі імпульси з частотою F; інтегратор, на виході якого формується передбачене значення повідомлення.

Часова діаграма, що пояснює роботу кодера , зображена на рис. 2.9.

У залежності від знаку різниці z(t)=s(t)-s*(t) на виході дискретизатора виникає плюсовий чи від′ємний короткий імпульс фіксованої амплітуди. Вихідні імпульси дискретизатора подаються у коло зворотного зв′язку на вхід інтегратора, на виході якого формується східчаста напруга s*(t). Плюсовий імпульс відповідає плюсовому ступеню на виході інтегратора, від′ємний - від′ємному ступеню. В імпульсному розширювачі короткі імпульси розширюються на весь період тактового інтервалу. Двійковий сигнал поступає в ЦКЗ.

Ще одна функціональна схема формування дельта-модуляції наведена на рис. 2.10.

Як видно з рисунків, на передавання значення помилки передбачення використовується тільки один розряд (біт). Тому швидкість передавання в такій системі співпадає зі значенням частоти дискретизації.

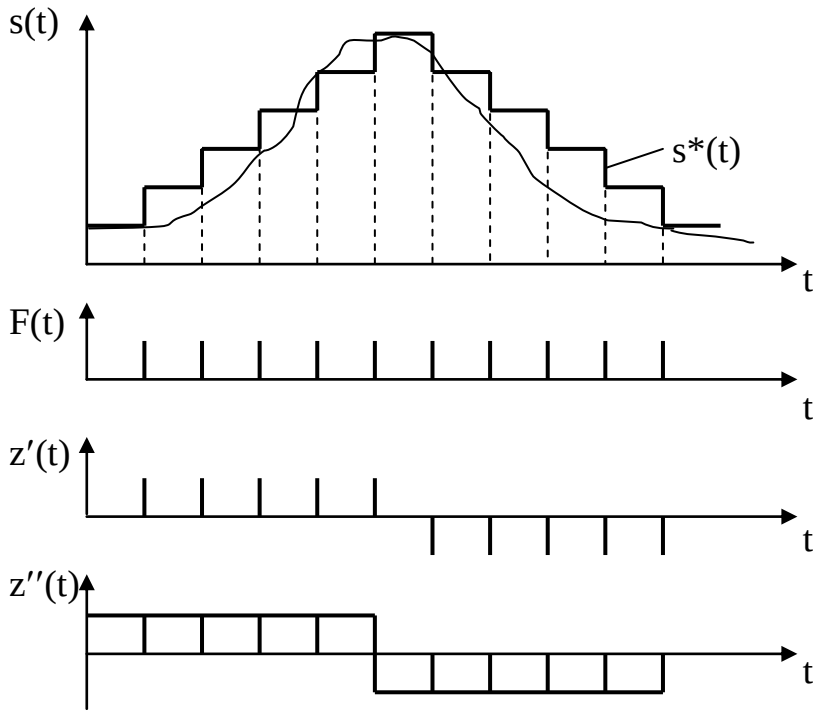


Рис. 2.9

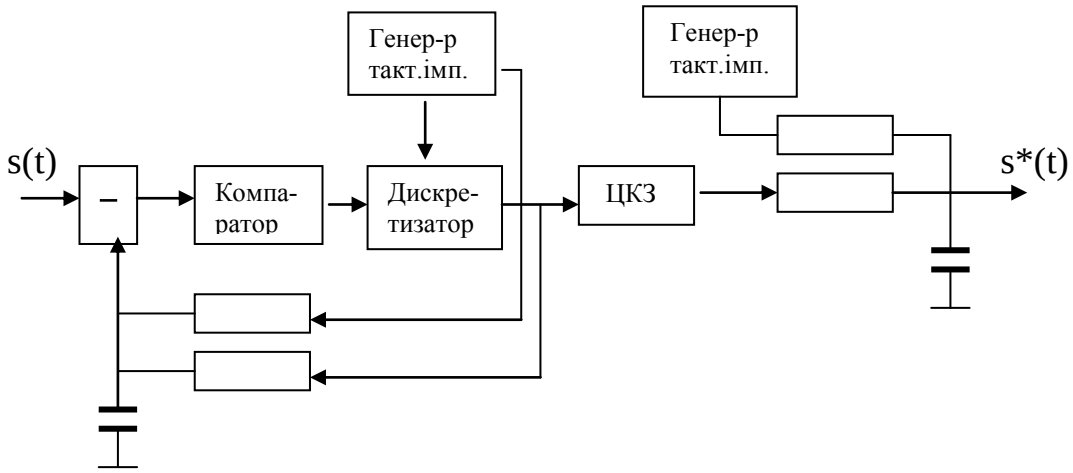


Рис. 2.10

Система (рис. 2.10) містить пристрій віднімання з повідомлення його передбаченого значення, компаратор, в якому здійснюється квантування на два рівні помилки передбачення z, дискретизатор, за допомогою якого здійснюється дискретизація повідомлення тактовими імпульсами. Одержані двійкові імпульси поступають до цифрового каналу зв′язку і кола зворотного зв′язку (ЗЗ) кодера. Формування аналогового процесу з двій-

кових імпульсів (цифро-аналогове перетворення) на приймальному боці і в колі зворотного зв′язку (ЗЗ) кодера здійснюється за допомогою однакових інтегруючих RC ланцюжків. На практиці у якості квантуючого елемента замість компаратора можуть застосовуватись також інші пристрої, які відносяться до групи “електронних реле”. У тому числі тригер Шміта, підсилювач-обмежувач, очікуючий мультивібратор і т. п. Сумісно з двійковими імпульсами прямої послідовності на інтегруючі ланцюжки подаються періодичні імпульси тактового генератора половинної амплітуди і протилежної полярності. При підсумовуванні цих сигналів в інтегруючих ланцюжках створюється ефект дії одної двополярної послідовності. Пристрій віднімання із повідомлення його передбачених значень практично не використовується. Замість віднімання здійснюється складання двох процесів різної полярності.

В ланцюгу ЗЗ формується апроксимуюча напруга, що являє собою ступінчату криву. Сусідні значення цієї напруги обов’язково відрізняються один від одного однією тією ж самою величиною, що дорівнює кроку квантування. Декодер в системі з ДМ являє собою послідовно з’єднані інтегратор та ФНЧ.

Приймальна частка системи зв′язку (дельта-демодулятор) містить пристрій формування коротких імпульсів (аналогічно часовому дискретизатору) та інтегратор (див. рис. 2.11).

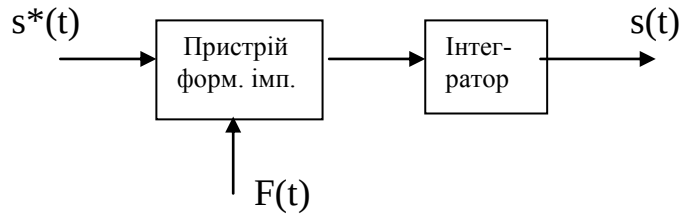


Рис. 2.11

У системах зв'язку з ДІКМ без перешкод зі зменшенням кроку дискретизації за часом (і відповідному збільшенні швидкості передачі сигналу) середній квадрат помилки передачі повідомлення безмежно зменшується. При дії перешкод у каналі зв'язку цей висновок може бути несправедливий. Зазвичай виникає така ситуація. Задаються потужність передавача і спектральна густина шуму. Тоді зі збільшенням швидкості передачі сигналів зменшується їхня енергія і, отже, зменшується відношення сигнал/шум. Це призводить до збільшення імовірності помилкового прийому біта, що збільшує середній квадрат помилки передачі повідомлення. З іншого боку, зменшення кроку дискретизації зменшує помилку дискретизації. У результаті дії цих двох суперечливих факторів в зазначених умовах

існує оптимальний крок дискретизації за часом, який можна розрахувати з урахуванням залежності ймовірності помилкового прийому бітів від відношення сигнал/шум для виду маніпуляції, що використовувався.

При оцінці цифрових систем зв'язку треба виходити з умови їхнього застосування. Припустимо, що передається траєкторна інформація, яка зчитується з екрана радіолокаційної станції. Радіолокаційне зображення обновлюється після кожного оберту антени, тобто через 5-10 с. У даному випадку період обертання антени визначає інтервал дискретизації повідомлення, і зменшення помилки передачі можна забезпечити, тільки збільшуючи число рівнів квантування. При великому числі рівнів квантування можуть працювати тільки системи зв'язку з ІКМ чи ДІКМ. При порівнянні цих систем ураховують, що система з ІКМ легше з′єднується з ЕОМ, чим система з ДІКМ, хоча остання має більш високу точність передачі повідомлення. В даний час для передачі траєкторної інформації застосовуються системи з ІКМ, а застосування систем з ДІКМ залишається відкритим.

При цифровій передачі мовних повідомлень обмежень на частоту дискретизації немає. Можна компенсувати зменшення числа рівнів квантування збільшенням частоти дискретизації. Тому для телефонного зв'язку застосовуються системи зв'язку з ДМ зі швидкістю передачі мовного сигналу 16 кбіт/с. Перевага дельта-модуляції перед ІКМ чи ДІКМ полягає в тому, що спрощується синхронізація. При ДМ передача ведеться одноімпульсними сигналами, і тому потрібна тільки тактова поелементна синхронізація. При ІКМ і ДІКМ сигнали являють собою комбінації імпульсів, і тому в системі зв'язку повинна здійснюватися як поелементна (тактова), так і групова (циклова) синхронізація.

Для передачі факсимільних і телевізійних повідомлень також може використовуватися дельта-модуляція. Дослідження показали, що в таких системах частота дискретизації повинна вибиратися приблизно у 10-15 разів більшою за вищу частоту спектра повідомлення. Дельта-модуляція має один суттєвий недолік: система погано відпрацьовує різкі стрибки повідомлення, які відбуваються у час, менший за період дискретизації. Тому в тих випадках, коли доцільно зберегти чіткі контури зображення, для передачі використовують ДІКМ.

2.4. **Недвійкові первинні коди**

Основа (алфавіт) недвійкових кодів завжди більша від двох, тобто $q \geq 3$; тому для побудови їх використовують методи теорії комбінаторики:

перестановки P_q з q елементів, розміщення A_q^m і сполучення C_q^m з q по m елементів.

Для кодів, які грунтуються на перестановках символів алфавіту, довжина кодової комбінації $n = q$ = const. Загальна кількість перестановок визначається виразом

$$N = P_q = \prod_{i=1}^{n} i = 1 \cdot 2 \cdot 3 \ldots n = n! = q!. \qquad (2.3)$$

Так, для коду з алфавітом $q = 3$ (*a, b, c*) всього буде шість перестановок: *abc, acb, bac, bca, cab, cba*, тобто $N = 6$ (2.3). Збільшення алфавіту коду приводить до зростання кількості перестановок, а, отже, й кількості кодових комбінацій N.

Відмітною особливістю такого коду є відсутність однакових символів в одній кодовій комбінації; тому їх можна віднести до кодів з виявленням однократних і деяких багатократних помилок. Дійсно, перехід будь-якого символу в комбінації призводить до появи в ній кількох однакових символів, що автоматично виявиться на приймальному боці і спричинить захисну відмову в прийманні комбінації.

Для кодів, які грунтуються на розміщеннях символів алфавіту, загальна кількість комбінацій визначається виразом

$$N = A_q^m = q(q-1)(q-2)\ldots(q-m+1) = q!/(q-m)!, \qquad (2.4)$$

де m – кількість символів алфавіту q, які містить кодова комбінація. Завжди $q > m$, а довжина кодової комбінації $n = m$.

Так, для коду з алфавітом $q = 3$ (*a, b, c*) і $n = m = 2$ загальна кількість кодових комбінацій $N = 6$ (2.4). Це комбінації *ab, ac, ba, ca, bc, cb.*

Ці коди, на відміну від кодів на перестановки, дають змогу виявляти тільки деякі однократні помилки, коли під дією завад виникає перетворення, що зумовлює подвоєння символів у комбінації. Решта перетворень символів у кодовій комбінації утворять іншу дозволену комбінацію. Тому така помилка не буде виявлена на приймальному боці.

Для кодів, які грунтуються не певному числі сполучень символів алфавіту, загальна кількість комбінацій визначається виразом

$$N = C_q^m = q!/[(q-m)!m!]. \qquad (2.5)$$

При цьому $q > m$, а довжина кодової комбінації $n = m$. Від кодів на розміщення ці коди відрізняються відсутністю комбінацій, які різняться тільки порядком розташування символів, тобто до таких кодів належать кодові комбінації, що різняться самими символами q.

Так, для коду с алфавітом $q = 3$ (*a, b, c*) та $n = m = 2$ загальна кількість кодових комбінацій N = 3 (2.5). Це комбінації *ab, ac, bc*. До комбіна-

ції коду не можуть належати сполучення *ba, ca, cb*, оскільки в них використані ті самі сполучення символів, що й в дозволених комбінаціях.

У таких кодах, як і у кодах, що грунтуються на розміщеннях, в одній комбінації не може бути двох однакових символів. Ці комбінації легко виявляються на приймальному боці.

Коди, які грунтуються на всіх сполученнях символів алфавіту. В одній комбінації можуть містится будь-які, в тому числі й однакові, символи. При цьому загальна кількість комбінацій визначається виразом

$$N = q^n. \qquad (2.6)$$

Для таких кодів можна відзначити збільшення кількості комбінацій порівняно з кодами на розміщення. Це пояснюється тим, що $q^n > A_q^m$.

Так, при $q = 3$ та $n = m = 2$ кількість кодових комбінацій N = 9 (2.6). Це комбінації *aa, ab, ac, bb, ba, bc, cc, ca, cb*. Збільшення кількості комбінацій досягається завдяки використанню таких комбінацій, як *aa, bb, cc.*

Змінно-якісний код можна дістати з коду на всі сполучення символів, якщо накласти на нього деякі обмеження. Так, у комбінації змінно-якісного коду однакові символи не повинні знаходитися поруч. Загальна кількість комбінацій такого коду визначається виразом

$$N = q(q-1)^{n-1}. \qquad (2.7)$$

Наприклад, при $q = 3$ та $n = 3$ можна утворити N = 12 (2.7) кодових комбінацій: *aba, aca, abc, acb, bab, bcb, bac, bca, cac, cbc, cab,cba*.

До переваг змінно-якісного коду слід віднести можливість розрізнення кодових комбінацій і виявлення в них помилок, тому що в комбінаціях цього коду два однакових символи не повинні знаходитися поруч.

Розділ 3. **ЗАВАДОСТІЙКЕ КОДУВАННЯ**

Кодування, при якому використовуються первинні коди, що не виявляють і не виправляють помилок, вже є до деякого ступеня завадостійким. Це обумовлено тим, що коли здійснюється перетворення дискретнозначного або неперервного повідомлення у код, кількість різних елементів (символів), за допомогою яких передається повідомлення, значно скорочується (у двійковому коді, наприклад, до двох). Скорочення різних символів веде до поліпшення умов встановлення їх на прийомному боці системи зв′язку.

Кожний з кодових символів модулює відповідний параметр сигналуносія, вид якого залежить від середовища передачі. На прийомному боці виконується встановлення переданих кодових символів на основі жорстких або м′яких рішень.

При жорстких рішеннях оцінки переданих кодових символів формуються шляхом прийняття кінцевих рішень відносно їх значень. Якість оцінки при цьому характеризується умовними ймовірностями помилки при демодуляції кодових символів. Наприклад, при когерентній демодуляції сигналів з двійковою фазовою модуляцією, на які впливає адитивний білий гаусівський шум, жорсткі рішення формуються шляхом порівняння вихідного сигналу інтегратора зі скидом в знаковому компараторі з нульовим порогом. Умовні ймовірності помилки залежать тільки від відношення енергії сигналів E до однобічної спектральної щільності шуму N_0.

При м′яких рішеннях формуються не тільки оцінки переданих кодових символів, а й додаткові показники надійності зроблених оцінок. У розглянутому прикладі м′які рішення можна формувати порівнянням вихідного сигналу інтегратора зі скидом у багатопороговому компараторі з декількома порогами, тобто багатобітовим квантуванням. При трибітовому квантуванні значення двох молодших бітів можна розглядати як показники надійності зроблених оцінок.

Після встановлення виду символу можна підкорегувати форму сигналу, за допомогою якого він передається, і таким чином компенсувати якусь частину дії завад. Однак, це не вирішує проблему безпомилкової передачі повідомлень при умовах дії сильних завад, великої кількості завад, різних викривлень та перекручувань.

Тому у даний час активно застосовуються і розвиваються методи підвищення завадостійкості систем передачі цифрової інформації за рахунок використання статистичної різниці між детермінованими сигналами і завадами (завадостійке кодування).

Розгляду цього питання присвячений даний розділ посібника.

3.1. **Основні відомості про завадостійке кодування**

Принципова можливість використання статистичної різниці між сигналами і завадами щодо підвищення завадостійкості системи зв′язку була доведена Шенноном у його теоремі для каналу з завадами: якщо швидкість передачі інформації менша за пропускну здатність каналу, то існують методи кодування, що дозволяють отримати яку завгодно малу ймовірність помилки символу (див. розділ 1).

Ця теорема не дає конкретних способів такого кодування, а лише стверджує, що такі коди повинні існувати, й, зрозуміло, що вони повинні бути надмірними.

Процес уведення надмірності до первинного цифрового сигналу називається завадостійким кодуванням, надмірні коди – завадостійкими, тому що їх застосування дозволяє на приймальному боці виявляти та виправляти помилки, які з′являються при передачі сигналів по каналу зв′язку з завадами.

У системах передачі цифрової інформації з використанням завадостійкого кодування найбільш широко застосовуються двійкові коди і m-кові коди, у яких $m = 2^a$, де a – ціле додатне число. Основна перевага цих кодів полягає у тому, що основна логічна операція (додавання за модулем 2), яка використовується під час їх опису, легко реалізується за допомогою елементів цифрової техніки.

Під час опису завадостійких кодів є зручним наведення зображення їх кодових комбінацій у вигляді векторів n-мірного простору

$$X = x_1\vec{a}_1 + x_2\vec{a}_2 + \ldots + x_i\vec{a}_i + \ldots + x_n\vec{a}_n,$$

де $\vec{a}_i$ ($i = 1,\ldots,n$) – система ортогональних одиничних векторів, які створюють базис n- мірного простору; x_i – координати кінця вектора у цьому просторі, зображені символами m-кового коду.

Далі замість термінів «вектор» і «кодова комбінація» будемо використовувати термін «кодове слово», маючи на увазі кодову комбінацію, яка наведена у векторному вигляді і записується наступним чином

$$X_j = x_{j1}x_{j2}\ldots x_{ji}\ldots x_{jn}, \qquad (3.1)$$

де j – номер кодового слова, що відповідає дискретному повідомленню; i – номер координати вектора даної кодової комбінації.

Число ненульових символів у кодовому слові називається його вагою. Для ваги кодового слова уведемо наступний запис: $w(X)$. Наприклад, якщо X = 10110, то $w(X) = 3$.

З урахуванням викладеного зробимо уточнення узагальненої структурної схеми стосовно до передачі інформації завадостійкими кодами.

Модель системи передачі цифрових сигналів завадостійкими кодами наведена на рис. 3.1.

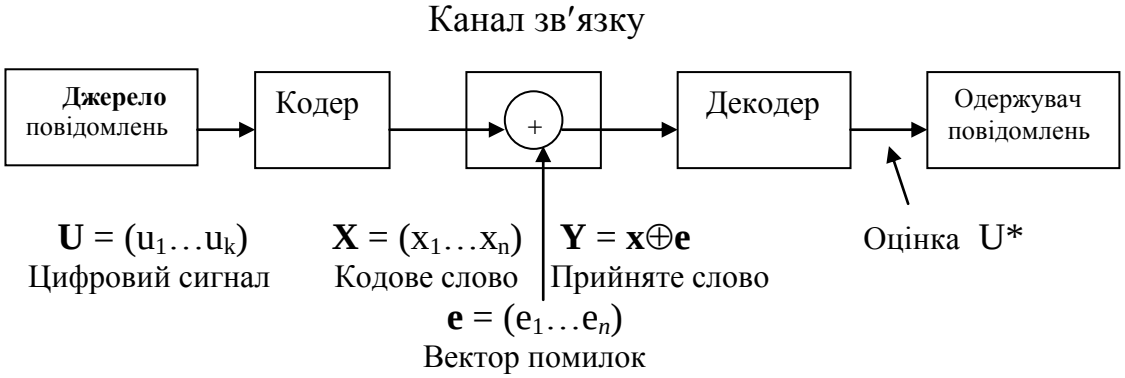


Рис. 3.1

Від джерела повідомлень на вхід кодера поступає k-елементний первинний цифровий сигнал, поданий кодовим словом $\mathbf{U} = u_1 \ldots u_k$. За рахунок уведення надмірності на виході кодера створюється n-елементний цифровий сигнал, поданий кодовим словом **X**, який поступає на вхід каналу (передавальний пристрій, лінія зв′язку і приймальний пристрій). Завади у каналі зв′язку викривлюють кодове слово **X**, додаючи до нього вектор помилок **e**, тобто

$$\mathbf{Y} = \mathbf{X} \oplus \mathbf{e}. \qquad (3.2)$$

У результаті на вхід декодера поступає цифровий сигнал, поданий кодовим словом **Y.** У декодері під час аналізу **Y** повинно бути прийнято рішення, яке **X** було передано, тобто визначити найбільш імовірний щодо прийнятого **Y** вектор помилок **e***. Після визначення e* декодер видає оцінку прийнятого слова

$$\mathbf{X}^* = \mathbf{Y} \oplus \mathbf{e}^* \qquad (3.3)$$

і на основі (3.3) – оцінку кодового слова **U***, тобто прийнятого дискретного повідомлення. Символи **e***, **X***, **U*** означають, що обраний вектор помилок і оцінка кодових слів (дискретного повідомлення) можуть бути помилковими.

У даний час відома велика кількість кодів, за допомогою яких можна теоретично виявляти та виправляти помилки довільної кратності. При цьому велике значення для практики має завдання побудови ефективного декодера, що реалізує можливості завадостійкого коду. Існують два підходи до рішення завдання декодування: імовірнісний та алгебраїчний. Імовірнісний підхід дозволяє побудувати оптимальні схеми декодера, але він потребує використання великих кодових слів. При цьому кількість операцій, які виконуються декодером, є показовою функцією довжини коду, що веде до великих втрат обладнання та часу. Крім того, необхідно враховувати можливість внесення декодером додаткових помилок внаслідок влас-

них збоїв та відказів. Тому зрозуміло, що на практиці більший ефект може бути отриманий при використанні неоптимального алгоритму декодування, який має до того ж просту схемну реалізацію. Ця ідея лежить в основі алгебраїчного підходу до рішення завдання декодування. На цьому напрямку була розвинута теорія лінійних кодів, відповідно якої можна зробити декодер технічно простим і доступним для використання в багатьох каналах зв′язку. Однак досягається це за рахунок заміни оптимальної процедури декодування на неоптимальну, при якій можуть виявлятися та виправлятися помилки, що належать до деякої фіксованої множини. Далі будуть розглядатися тільки алгебраїчні завадостійкі коди, класифікація яких за деякими ознаками наведена на рис. 3.2.

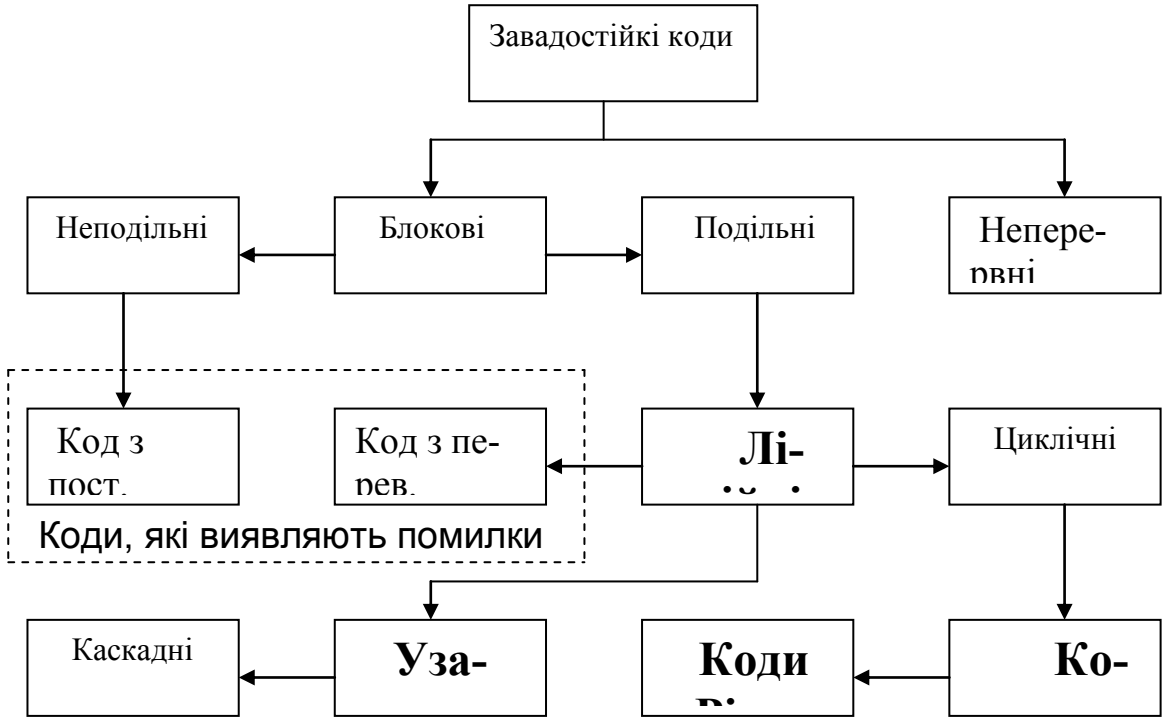


Рис. 3.2

За способами декодування коди, що розглядаються, розділяються на дві підгрупи: блокові та неперервні (згорточні). Блокові коди можна декодувати лише після того, як в декодер поступить усе кодове слово. Неперервні коди допускають декодування у процесі надходження в декодер кодового слова. Блокові коди можуть бути подільні та неподільні. До подільних відносяться такі коди, в яких позиції для інформаційних і перевірочних символів у кодовому слові чітко розмежовані. У неподільних кодах такого розмежовування немає. Якщо у блокових подільних кодах перевірочні символи є лінійними комбінаціями інформаційних, то такі коди називають

систематичними. Підкласами лінійних кодів є циклічні коди, з яких найбільш детально пророблені коди Боуза – Чоудхурі – Хоквінгема (БЧХ). Коди Ріда – Соломона (РС) є окремим випадком m-кових кодів БЧХ. До лінійних кодів відносяться також каскадні коди, які є об′єднанням деяких з них (наприклад, кодів БЧХ і кодів Ріда – Соломона). Лінійні систематичні коди при m = 2 називаються груповими. Деякі з кодів, що згадуються вище і наведені в схемі класифікації (рис. 3.2), далі будуть розглянуті більш детально.

Найбільш характерною ситуацією використання кодування є передача дискретних повідомлень в реальному часі при обмеженій потужності передавача. Це означає, що n-символьне кодове слово може бути передано за час, який дорівнює часу видачі k символів джерелом повідомлення. Якщо ця умова не виконується, то кодування не має сенсу, оскільки послідовність символів повідомлення, які передаються, може бути зчитана з меншою швидкістю. У результаті характеристики завадостійкості можуть бути поліпшені лише за рахунок збільшення енергії символів, що передаються. Нехай потужність передавача дорівнює P, а тривалість повідомлення, яке містить k символів, дорівнює T_w. Тоді енергія сигналу на слово повідомлення дорівнює PT_w.

У випадку блокового надмірного кодування енергія розподіляється на n символів, тому енергія на один кодовий символ – PT_w/n. Оскільки n>k, то при кодуванні енергія на символ зменшується. Це веде до того, що в системі з надмірним кодуванням імовірність помилки на символ буде вищою, ніж в системі без кодування. Якщо код має велику здатність до коригування, то завдяки наявності надмірних символів ці втрати ніби компенсуються і забезпечується додатковий виграш, який прийнято називати енергетичним виграшем кодування (ЕВК). ЕВК є кількісною мірою ефективності кодування. Його значення оцінюють, звіряючи енергетичні втрати на передавання одного біту при фіксованій імовірності помилкового прийому символу чи біту повідомлення в системах з кодуванням і без кодування.

3.2. **Вірогідність передачі кодованих повідомлень**

Вірогідністю передачі кодованих повідомлень оцінюється відповідність між кодовими комбінаціями, прийнятими на приймальному боці, та комбінаціями, переданими до каналу зв′язку.

У свою чергу, оцінка вірогідності обміну інформацією визначається ймовірністю спотворень повідомлень, тобто прийняттям $P_п$ помилкового повідомлення при відомій імовірності P_e спотворення елемента повідом-

лення, що передається. Таким чином, вірогідність передачі є похідною характеристикою, яка залежить як від коректувальної здатності коду, так і від типу каналу (лінії) зв′язку та умов передачі по ньому елементів кодової комбінації.

Для двійкових кодів дія завад на елемент кодової комбінації може призвести до різних наслідків у несиметричних і симетричних каналах. Так, у несиметричних каналах імовірності переходу під впливом завад 0 в 1 (P_{01}) та 1 в 0 (P_{10}) не будуть однаковими, а в симетричних вони збігаються. Проте для спрощення розрахунків при оцінюванні вірогідності повідомлень, що передаються, вважатимемо двійковий канал симетричним, тобто $P_{01} = P_{10} = P_e$.

Крім того, розрізняють канали з незалежними помилками, коли виникнення однієї помилки не залежить від появи іншої (канал без пам′яті), та канали з пакетним розподілом помилок, в яких є залежність імовірності спотворення наступного елемента, що передається, від спотворення попереднього (канал має пам′ять).

Розглянемо оцінку вірогідності при передачі кодованих повідомлень по цих двійкових симетричних каналах.

У разі передачі повідомлень по каналах із незалежними помилками ймовірність відсутності спотворень двійкового елемента повідомлення позначимо як $(1 - P_e)$. Тоді для двійкової послідовності завдовжки n елементів імовірність правильно прийнятої послідовності

$$P_{пр} = (1 - P_e)^n, \tag{3.4}$$

а ймовірність помилки в прийнятій послідовності

$$P_п = 1 - (1 - P_e)^n. \tag{3.5}$$

Останній вираз можна подати так:

$$P_{П} = C_n^1 P_e + C_n^2 P_e^2 + C_n^3 P_e^3 + \ldots + C_n^v P_e^v, \tag{3.6}$$

де $C_n^v = \dfrac{n!}{v!(n-v)!}$, а v = 1, 2, 3,… - кратність помилки.

Через те, що $P_e << 1$, ймовірність помилки в n-елементній кодовій послідовності можна записати як $P_п \approx nP_e$.

Як відомо, коректувальні коди дають змогу виявляти або виправляти (залежно від кодової відстані) ту чи іншу кількість помилок. Тому для оцінювання ефективності кодів необхідно знати ймовірність виникнення в кодовій комбінації помилок будь-якої кратності.

При незалежних помилках імовірність появи v-кратних помилок визначається за формулою Бернуллі

$$P_{П}(v) = C_n^v P_e^v (1 - P_e)^{n-v}. \tag{3.7}$$

Для кодів з $d_{min} > 1$, що використовуються з метою виявлення всіх помилок кратністю $v_в = d_{min} - 1$ і меншою, ймовірність помилкової (неправильної) комбінації на виході декодера легко знайти, врахувавши, що при передачі комбінації можуть бути такі чотири ситуації:

– комбінація, яка приходить з каналу, прийнята без помилок (правильно) з імовірністю $P_{пр}$;

– комбінація містить не більше $v_в$ спотворених елементів, що виявляються кодом (імовірність такої події $P_{в.п}$);

– комбінація містить $v > v_в$ помилок, але вони розташовані так, що виявляються кодом (імовірність такої події $P'_{в.п}$);

– комбінація містить $v > v_в$ помилок, які кодом не виявляються, з імовірністю $P_{нв.п}$.

Оскільки сума ймовірностей всіх перелічених подій дорівнює 1, а ймовірність $P'_{в.п} \approx 0$,

$$P_п = P_{в.п} + P_{нв.п}. \tag{3.8}$$

З урахуванням того, що спотворені комбінації, які виявляються декодером, не видають споживачеві інформації, ймовірність здобуття ним помилкових комбінацій оцінюватиметься тільки ймовірністю невиявленої помилки $P_{нв.п}$, яку можна записати у вигляді

$$P_{НВ.П} = \sum_{v=d_{\min}}^{n} W(w) P_e^v (1-P_e)^{n-v}, \tag{3.9}$$

де *W(w)* – вагова характеристика коду (кількість його комбінацій вагою w, тобто кількість варіантів помилок, які не виявляються цим кодом); d_{min} – мінімальна кодова відстань.

Значення *W(w)* визначається за спеціальними методиками для різних кодів. Так доведено, що коли двійковий (n, k)-код має кодову відстань d, то

$$W(w) = \begin{cases} = 0, v \le d; \\ \le \dfrac{C_n^{v-t}}{C_n^t}, v \ge d, \end{cases} \tag{3.10}$$

де $t = (d - 1)/2$.

З урахуванням (3.10) маємо

$$P_{НВ.П} \le \frac{1}{(1-P_e)^t C_{n+t}^t} \left[1 - \sum_{v=0}^{2t} C_{n+t}^t P_e^t (1-P_e)^{n+t-v} - \sum_{v=n+1}^{n+t} C_{n+t}^v P_e^v (1-P_e)^{n+t-v} \right]. \tag{3.11}$$

Права частина (3.11) при $0 < P_e < 0{,}5$ обмежена зверху значенням $P_e=0{,}5$; тому в будь-якому каналі з незалежними помилками $P_{нв.п} \le 2^t / C^t_{n+t}$.

Цю оцінку можна застосувати для коротких кодів з невеликою надмірністю. Для кодів з великою надмірністю бажано користуватися виразом

$$P_{нв.п} \le 2^k (d/n)^d (1 - d/n)^{n-d},$$

де k – кількість інформаційних елементів; d – мінімальна кодова відстань; n – довжина коду.

На практиці поширенішою є формула для приблизного оцінювання ймовірності виникнення невиявленої помилки

$$P_{НВ.П} \approx \frac{1}{2^r} \sum_{v=d}^{n} C_n^v P_e^v (1 - P_e)^{n-v}, \qquad (3.12)$$

де r – кількість перевірних елементів коду; v – кратність помилки; d – мінімальна кодова відстань.

Для кодів з d > 2, що використовуються для виправлення всіх помилок кратністю $v_{вп} = [(d - 1)/2]$, де […] означає цілу частину й менше, ймовірність $P_п$ виникнення помилкової комбінації на виході декодера можна знайти, врахувавши, що після проходження кодової комбінації по каналу можливими є такі чотири ситуації:

– комбінація прийнята без помилок (правильно) з імовірністю $P_{пр}$;

– комбінація містить не більше $v_{вп}$ спотворених елементів, які виявляються кодом з імовірністю $P_{вп.п}$;

– комбінація містить $v > v_{вп}$ помилок, розташованих так, що вони виправляються кодом з імовірністю $P'_{вп.п}$;

– комбінація містить $v > v_{вп}$ помилок, які не виправляються кодом (імовірність такої події $P_{н.нв.п}$).

Оскільки ймовірність $P'_{вп.п} \approx 0$, маємо

$$P_п = P_{вп.п} + P_{н.нв.п}, \qquad (3.13)$$

звідки $P_{н.нв.п} = P_п - P_{вп.п}$.

При незалежних помилках імовірність виправлення помилок кратністю до v кодами, що виправляють помилки, визначається виразом

$$P_{ВП.П} = \sum_{i=1}^{v} C_n^i P_e^i (1 - P_e)^{n-i}. \qquad (3.14)$$

З урахуванням виразів (3.5) та (3.14) дістаємо

$$P_{Н.ВП.П} = 1 - (1 - P_e)^n - \sum_{i=1}^{v} C_n^i P_e^i (1 - P_e)^{n-i}. \qquad (3.15)$$

На основі здобутих значень $P_п$ можна визначити коректувальний код, оптимальний для даного каналу.

Двійковий коректувальний код завдовжки n з N комбінаціями називається оптимальним для двійкового симетричного каналу, якщо ймовірність $P_п$ виникнення помилкової комбінації на виході декодера не переви-

щує такої самої ймовірності для будь-якого іншого двійкового коду тієї самої довжини n із тією самою кількістю комбінацій N.

У разі передачі повідомлень по каналах з пакетним розподілом помилок визначення ймовірності їх за формулами (3.6) – (3.15) дають значення, які набагато відрізняються від реальних. Це пояснюється тим, що в цих каналах на проходження сигналів (а це в основному радіоканали) сильно впливають сезонні та добові зміни метеорологічних умов, промислові завади, інтенсивність яких змінюється протягом доби та тижня, тощо. Все це призводить до виникнення в каналах пакетів (пачок) помилок. Визначити імовірність їх за таких умов досить складно, оскільки необхідно провести дослідження реальних характеристик каналів.

Формула, що дає приблизне значення ймовірності помилок при пакетному розділі їх і передачі двійкової послідовності n елементів, має вигляд

$$P_{П} \approx \frac{P_e}{\bar{l}} \sum_{b=1}^{b_{\max}} \left(1+\frac{n-1}{b}\right) \frac{bP_b}{\sum\limits_{b=1}^{b_{\max}} bP_b}, \qquad (3.16)$$

де P_e – імовірність спотворення двійкового елемента; $\bar{l}$ - щільність помилок у пакеті, яка визначається відношенням кількості помилок у ньому до довжини пакета b; P_b – умовна ймовірність виникнення пакета помилок завдовжки b.

Для кодів, що виявляють пакети помилок, імовірності помилок можна знайти за формулами:

$$P_{В.П} \approx \frac{P_e}{\bar{l}} \left\{ \sum_{b=1}^{b_{\max}} \left(1+\frac{n-1}{b}\right) \frac{bP_b}{\sum\limits_{b=1}^{b_{\max}} bP_b} - \frac{1}{2^r} \sum_{b=l_k+1}^{b_{\max}} \left[1+\frac{n-(2l_k+1)}{b}\right] \frac{bP_b}{\sum\limits_{b=1}^{b_{\max}} bP_b} \right\}; \qquad (3.17)$$

$$P_{НВ.П} \approx \frac{1}{2^r} \frac{P_e}{\bar{l}} \sum_{b=l_k+1}^{b_{\max}} \left[1+\frac{n-(2l_k+1)}{b}\right] \frac{bP_b}{\sum\limits_{b=1}^{b_{\max}} bP_b}, \qquad (3.18)$$

де $\bar{l}_k$ – довжина пакета помилок, яка виявляється.

Значення усіх величин, які входять у ці формули, дістають експериментально, визначаючи характер розподілу помилок, або беруть із літератури для каналів аналогічного типу.

Можливий опис реальних каналів за допомогою двох параметрів: імовірності P_e спотворення двійкового елемента та показника α групуван-

ня помилок. При цьому наближені формули для визначення ймовірності невиявлених помилок мають такий вигляд:

– для кодів, що виявляють помилки,

$$P_{НВ.П} \approx \frac{P_e}{2^r}\left(\frac{n}{d}\right)^{1-\alpha};$$

– для кодів, що виправляють помилки,

$$P_{НВ.П} \approx \left(\frac{n}{v+1}\right)^{1-\alpha} P_e;$$

– для кодів, що виявляють і виправляють помилки,

$$P_{НВ.П} \approx \frac{\sum_{i=0}^{v} C_n^i}{2^r}\left(\frac{n}{d-v}\right)^{1-\alpha} P_e,$$

де d – мінімальна кодова відстань; v – кратність помилки, що виправляється; r – кількість перевірних елементів.

Ці формули дають непогані результати при $v < 0{,}3n$, де n – кількість елементів кодової комбінації.

3.3. **Основні типи блокових кодів**

Між параметрами n, k і t блокового коду (n – кількість елементів в кодовій комбінації, k – кількість інформаційних елементів, $t = (d_{min} - 1)/2$ – кратність помилок, d_{min} – мінімальна кодова відстань Хеммінга) існує визначене співвідношення, яке встановлюється так називаною межею Хеммінга

$$2^{n-k} \geq \sum_{i=0}^{t}\binom{n}{i}. \qquad (3.19)$$

$\binom{n}{i} = \frac{n!}{i!(n-i)!}$ - кількість можливих конфігурацій з *n* символів, які містять *i* помилок.

Коди, для яких умова (3.19) виконується суворо, мають назву досконалі. Прикладом досконалого коду є код Хеммінга, який виправляє поодинокі помилки, а також код Голея. Інші коди можуть виправляти деякі конфігурації помилок, кратність яких перевищує t. Для цих кодів (3.19) можна трактувати, як корисну, верхню межу.

В таблиці 3.1 приведені приклади блокових кодів, які виправляють помилки кратності t, та їх параметри.

Блокові коди можна використовувати й для виявлення помилок кратності u. В цьому випадку мінімальна відстань Хеммінга між словами коду повинна бути $d_{min} = u + 1$.

Якщо блоковий код призначений для виправлення та виявлення помилок кратності t і u відповідно, то мінімальна кодова відстань повинна задовольняти умові $d_{min} \geq t + u + 1$.

Таблиця 3.1

Кратність помилок, що виправляються, і мінімальна відстань	n	k	Код	Кодова швидкість ($R_k = k/n$)
$t = 1, d_{min} = 3$	3	1	(3, 1)	0,33
	4	1	(4, 1)	0,25
	5	2	(5, 2)	0,4
	6	3	(6, 3)	0,5
	7	4	(7, 4)	0,57
	15	11	(15, 11)	0,73
	31	26	(31, 26)	0,838
$t = 2, d_{min} = 5$	10	4	(10, 4)	0,4
	15	8	(15, 8)	0,533
$t = 3, d_{min} = 7$	10	2	(10, 2)	0,2
	15	5	(15, 5)	0,33
	23	12	(23, 12)	0,52

Лінійні блокові коди. У лінійному блоковому коді *l*-й символ кодового слова $\mathbf{B} = (b_1, b_2, \ldots, b_l, \ldots, b_n)$ є лінійною комбінацією k інформаційних символів. У матричному вигляді

$$\mathbf{B} = \mathbf{A} \cdot \mathbf{G}, \qquad (3.20)$$

де **G** – породжувальна (твірна) матриця коду, яка містить k рядків і n стовпців

$$\mathbf{G} = \begin{bmatrix} g_{11} & g_{12} & \cdots & g_{1k} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2k} & \cdots & g_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ g_{k1} & g_{k2} & \cdots & g_{kk} & \cdots & g_{kn} \end{bmatrix}. \qquad (3.21)$$

Таким чином, процедура конструювання коду зводиться до визначення елементів g_{il} породжувальної матриці. Оскільки для систематичного коду перші k символів кодового слова **B** є інформаційними символами слова **A**, тобто $b = a$, $g_{il} = 1$, якщо $i = l$, $g_{il} = 0$, якщо $i \neq l$, то породжувальна (твірна) матриця коду має вигляд

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & \dots & 0 & \dots & g_{1,k+1} & \dots & g_{1,n} \\ 0 & 1 & \dots & 0 & \dots & g_{2,k+1} & \dots & g_{2,n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & \dots & g_{k,k+1} & \dots & g_{k,n} \end{bmatrix}, \quad (3.22)$$

або

$$\mathbf{G} = [\mathbf{I}:\mathbf{P}], \quad (3.23)$$

де **I** – одинична матриця k×k; **P** відповідає останнім (n – k) стовпцям породжувальної матриці.

З породжувальною матрицею лінійного коду пов′язана перевірочна матриця **H**:

$$\mathbf{H} = \begin{bmatrix} P \\ \dots \\ I_{n-k} \end{bmatrix} = \begin{bmatrix} g_{1,k+1} & g_{1,k+2} & \dots & g_{1,n} \\ \dots & \dots & \dots & \dots \\ g_{k,k+1} & g_{k,k+2} & \dots & g_{k,n} \\ 1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{bmatrix}. \quad (3.24)$$

Декодування лінійного коду здійснюється множенням вихідної послідовності **Z** демодулятора на перевірочну матрицю **H**, в результаті якого формується слово, що називається синдром **S**:

$$\mathbf{S} = \mathbf{Z}\cdot\mathbf{H}.$$

Для двійкових кодів вихідна послідовність **Z** може бути подана як сума за модулем 2 кодового слова **B**, що передається, і вектора помилок E. Тому синдром може бути уявлений як

$$\mathbf{S} = (\mathbf{B} \oplus \mathbf{E})\mathbf{H} = \mathbf{BH} \oplus \mathbf{EH} = \mathbf{S}^{(1)} \oplus \mathbf{S}^{(2)}. \quad (3.25)$$

Згідно (3.23) j-й елемент $\mathbf{S}^{(1)}$ може бути записаний у вигляді

$$S_j^{(1)} = \sum_{i=1}^{k} b_i g_{i,k+j} \oplus b_{k+j}. \quad (3.26)$$

Для систематичних кодів $b_i = a_i$, $i \le k$, тому

$$S_j^{(1)} = \sum_{i=1}^{k} a_i g_{i,k+j} \oplus b_{k+j}, \qquad j = 1,2,\dots,n-k. \quad (3.27)$$

З рівняння (3.23) слідує, що

$$\sum_{i=1}^{k} a_i g_{i,k+j} = b_{k+j}. \qquad (3.28)$$

Відповідно,

$$S_j^{(1)} = b_{k+j} \oplus b_{k+j} = 0, \qquad j = 1,2,..n-k. \qquad (3.29)$$

Оскільки всі $(n - k)$ елементів $S^{(1)}$ дорівнюють нулю, то

$$\mathbf{S}^{(1)} = [\mathbf{0}], \qquad (3.30)$$

і синдром визначається співвідношенням

$$\mathbf{S} = \mathbf{E}\cdot\mathbf{H}. \qquad (3.31)$$

Таким чином, синдром, який складається з одних нулів, означає, що прийнята послідовність належить до множини кодових слів лінійного коду. Тобто, при прийомі не трапилось жодної помилки, або конфігурація помилок була такою, що трансформувала передане кодове слово в інше кодове слово. Якщо мінімальна кодова відстань коду дорівнює d_{min}, то повинно трапитись d_{min} помилок при трансформуванні одного кодового слова в інше.

Зміст процесу декодування є у визначенні для кожного синдрому вектора помилок мінімальної ваги, що задовольняє рівнянню $\mathbf{S} = \mathbf{E}\cdot\mathbf{H}$. Визначений вектор помилок підсумовується за модулем 2 з прийнятою послідовністю Z. У результаті формується найбільш вірогідне слово.

3.3.1. **Коди, що виявляють помилки**

Особливість кодів, що виявляють помилки, полягає в тому, що кодові комбінації, які входять до складу цих кодів, різняться кодовою відстанню, не меншою, ніж $d_{min} = 2$.

Такі коди умовно можна поділити на дві групи: коди, в яких використовуються всі комбінації, але до кожної з них за обумовленим правилом додаються r перевірних елементів; коди, утворені зменшенням кількості дозволених комбінацій.

До першої групи кодів, що виявляють помилки, належать коди з перевіркою на парність і непарність; код із простим повторенням; інверсний та кореляційний коди; до другої – коди зі сталою вагою. Код з кількістю одиниць у комбінації, кратною трьом, може належати до першої або другої групи кодів залежно від методики його побудови.

Код із перевіркою на парність. Це найпоширеніший код, який застосовується для виявлення поодиноких помилок і всіх помилок непарної кратності. Код містить (n – 1) інформаційних й один перевірний елементи, належить до систематичних кодів і позначається як (n, n – 1)-код.

Перевірний елемент коду визначається сумою за модулем 2 всіх інформаційних елементів:

$$b_1 = \sum_{i=1}^{n-1} 0 a_i ,$$

тобто він утворюється доповненням комбінації k-елементного первинного коду одним елементом таким чином, щоб кількість одиниць у новому n-розрядному (n = k + 1) коді була парною. Кодова відстань $d_{min} = 2$.

Для виявлення помилки на приймальному боці перевіряють на парність усю прийняту кодову комбінацію, визначаючи кодовий синдром

$$S^{(1)} = \sum 0 a_i' \oplus b_1' ,$$

де a'_i, b'_1 – прийняті на приймальному боці відповідно інформаційні та перевірні елементи.

Вважається, що при $S^{(1)} = 0$ помилки в комбінації немає, а при $S^{(1)} = 1$ помилка є. Надмірність коду визначається виразом: $R_{над} = 1 - k/(k + 1) = 1/(k + 1)$.

Код із перевіркою на непарність. Цей код відрізняється від попереднього тим, що кожна його комбінація має непарну кількість одиниць, тобто додатковий перевірний елемент формують, виходячи з кількості одиниць у початковій кодовій комбінації; при парній кількості перевірний елемент дорівнює одиниці, а при непарній – нулю.

Для виявлення помилки в кодовій комбінації на приймальному боці її перевіряють на непарність. Код є подільним завдовжки n – 1 інформаційних й один перевірний елементи; він може так само виявляти помилки та має надмірність, як і коди із перевіркою на парність.

Код із простим повторенням. Код із простим повторенням (без інверсії) є подільним лінійним кодом. Він містить k інформаційних і r = k перевірних елементів. У цьому коді r перевірних елементів є простим повторенням k інформаційних елементів первинної кодової комбінації: $b_i = a_i$, де $i = 1,\ldots,k$.

У блоковому коді виду (n, 1) значення інформаційного символу повторюється (n – 1) разів, тобто (n – 1) перевірочних символів є повторенням інформаційного. Кодова швидкість дорівнює 1/n і при достатньо великих n буде вкрай низькою. Мінімальна відстань коду дорівнює n, відповідно при великих n коди повторень мають велику здібність до виправлення помилок. Оскільки мінімальна відстань дорівнює n, то кратність виправлення помилок у кодовому слові буде складати t = (n – 1)/2.

Через те, що код має відстань $d_{min} = 2$, він може використовуватися для виявлення поодиноких помилок. Ця процедура зводиться до порівнян-

ня однойменних інформаційних і перевірних елементів у прийнятій кодовій комбінації. Незбіг їх свідчить про наявність помилок у ній. Код дає змогу виявити не тільки однократні помилки, а й деякі помилки більшої кратності, за винятком «дзеркальних», коли в інформаційній та перевірній послідовностях кодової комбінації внаслідок дії завад спотворюються елементи, що знаходяться на однакових за номером розрядах.

Надмірність коду визначається виразом: $R_{над} = 1 - k/(2k) = 1/2$.

Інверсний код. Інверсний код (із повторенням та інверсією) є подільним лінійним кодом, який має k інформаційних і стільки ж перевірних елементів. Його відмінність від попереднього коду полягає в тому, що значення перевірних елементів у ньому залежать від значення суми за модулем 2 всіх інформаційних елементів. За умови $\sum_{i=1}^{k} \mathrm{O} a_i = 0$ (де $\sum \mathrm{O}$ – знак суми за модулем 2), тобто при парній кількості одиниць у початковій кодовій комбінації перевірні елементи просто повторюють інформаційні ($b_i = a_i$, де $i = 1,\ldots,k$), а за умови $\sum_{i=1}^{k} \mathrm{O} a_i = 1$, тобто при непарній кількості значених одиниць перевірні елементи повторюють інформаційні в інвертованому вигляді (в оберненому коді): $b_i = a_i \oplus 1$, де $i = 1,\ldots,k$.

Для виявлення помилок на приймальному боці у послідовності, що складається з 2k елементів, спочатку підсумовують одиниці, які знаходяться в перших k елементах. Якщо їх кількість парна, то решту k елементів приймають у позитиві. Обидві зареєстровані частини комбінацій поелементно порівнюють (перший елемент із першим, другий – з другим і т.д.). За наявності хоча б одного незбігу вся послідовність елементів бракується.

Якщо кількість одиниць серед перших k елементів непарна, то решту k елементів приймають у негативі (інвертують), після чого поелементно порівнюють їх. Наявність незбігу призводить до відбраковування всіх 2k елементів. Така побудова коду дає змогу виявляти майже всі випадки спотворення його елементів, крім двократних «дзеркальних» помилок.

Надмірність коду визначається виразом: $R_{над} = 1 - k/(2k) = 1/2$.

Кореляційний код. У цьому коді кожний розряд двійкового початкового коду записується у вигляді двох елементів: 0 – як 01, а 1 – як 10. Так, початковій кодовій комбінації 010011 відповідатиме комбінація 011001011010 кореляційного коду. В технічній літературі такий двійковий запис дуже часто називається Манчестер-кодом.

Приймальний пристрій у кожному такті, що складається з двох сусідніх елементів кореляційного коду, має зафіксувати перехід $0 \rightarrow 1$ або $1 \rightarrow$

0. У разі прийняття двох нулів або одиниць приймальний пристрій фіксує наявність помилки.

Кореляційний код дає змогу виявляти помилки будь-якої кратності, але не здатний виявити двократні «дзеркальні» помилки, коли сусідні елементи одного такту під впливом завад змінюються на протилежні за значенням.

Надмірність коду визначається виразом: $R_{над} = 1 - k/(2k) = 1/2$.

До переваг кореляційного коду, крім відсутності постійної складової в напрузі кодового сигналу при передачі кодової комбінації по каналу зв′язку, можна віднести також можливість самосинхронізації генератора приймача, оскільки прийняття кожного біта супроводжується фронтом сигналу, що приймається, в центрі біта.

Код зі сталою вагою. Код зі сталою вагою, тобто з незмінною кількістю одиниць і нулів у комбінаціях, часто називається кодом на одне сполучення. Загальна кількість комбінацій цього коду визначається виразом

$$N = C_n^m = \frac{n!}{m!(n-m)!},$$

де m – кількість одиниць у кодовій комбінації завдовжки n.

Такий код утворюється з двійкового простого коду відбором комбінацій, що мають однакову кількість одиниць m. Приймальний пристрій, підраховуючи кількість одиниць у прийнятій кодовій комбінації, виявляє помилки, якщо їх кількість відрізнятиметься від m.

Код зі сталою вагою має мінімальну кодову відстань $d_{min} = 2$. Він виявляє всі помилки непарної кратності, а також усі помилки парної кратності, що призводять до порушення умови m = const.

Надмірність коду визначається виразом: $R_{над} = 1 - \left(\log_2 C_n^m\right)/n$.

Порівняно з кодом із простим повторенням цей код при меншій його надмірності дає змогу виявляти помилки тієї самої кратності.

Код із кількістю одиниць у комбінації, кратною трьом. Цей код можна утворити або додаванням до кожної комбінації початкового коду r = 2 перевірних елементів, або зменшенням кількості дозволених комбінацій початкового коду з накладанням додаткової угоди: кількість одиниць у кожній комбінації має бути кратною трьом.

У першому випадку до початкової кодової комбінації додаються два перевірних розряди, які мають такі значення, що сума одиниць у кодовій комбінації стає кратною трьом. Так, якщо початкова кодова комбінація має дві або п′ять одиниць, то для здобуття ваги w = 3 або 6 кодової комбінації треба доповнити її двома перевірними елементами 10. Якщо ж у початковій комбінації є одна або чотири одиниці, то вона доповнюється двома пе-

ревірними елементами 11. Так, комбінація 01010 початкового коду закодована кодом із кількістю одиниць, кратною трьом, матиме вигляд 0101010, а 10000 – 1000011, 0110 → 011010, 101100 → 10110000, 110110 → 11011011, 0111011 → 011101110 тощо.

У другому випадку з усіх комбінацій початкового коду вибирають тільки ті, що мають вагу w = 3 та 6. Решту комбінацій використовувати не можна.

Код дає змогу виявити всі поодинокі помилки та деякі помилки більшої кратності, що призводять до порушення умови w = 3 або 6, де w – кількість одиниць у кодовій комбінації. Здатність коду виявляти помилкові комбінації майже така сама, як і коду зі сталою вагою.

Надмірність коду з доповненням до необхідної кількості одиниць визначається виразом $R_{над} = 1 – 2/(k + 2)$, а коду, що утворюється відбором із загальної кількості комбінацій з відповідною кількістю одиниць (3 або 6), - виразом:

$$R_{над} = 1 - \frac{\log_2\left(C_n^3 + C_n^6\right)}{n}.$$

Недвійкові коди, що виявляють помилки. Розрізняють два принципи побудови надмірних недвійкових (q-кодів, багатопозиційних) кодів, що виявляють помилки: уведенням додаткових перевірних елементів, які утворюються після виконання лінійних операцій над елементами кодової комбінації; збільшенням надмірності завдяки зменшенню кількості дозволених і зростанню кількості недозволених кодових комбінацій. В обох випадках досягається збільшення кодової відстані до значення, що дає змогу виявити ту чи іншу кількість помилок у комбінації.

Як відомо, мінімальна кодова відстань для кодів, які виявляють помилки, визначається виразом $d_{min} \geq v_в + 1$, де $v_в$ – кратність помилки, що виявляється.

Із недвійкових кодів з додатковими перевірними елементами, що виявляють помилки, найпростіше реалізуються коди з перевіркою на парність за модулем 2 та код із простим повторенням, а із недвійкових кодів, утворених збільшенням кількості дозволених кодових комбінацій, найбільшого поширення дістали незвідні змінно-позиційні коди (НЗ-коди) з елементами однієї та різної ваг.

Код з перевіркою за модулем q. Цей код будується аналогічно двійковому коду з перевіркою на парність за модулем 2. Відмінність у побудові полягає у доповненні комбінацій первинного q-коду перевірним розрядом до значення основи (алфавіту) коду, тобто якщо кодова комбінація є множиною k елементів $\{a_1a_2...a_k\}$, де $a_1, a_2,\ldots,a_k$ – інформаційні елементи

комбінації, що набувають значень від 0 до (q – 1), то перевірний розряд визначається сумою цих елементів за модулем q: $b_1 = (a_1 \oplus a_2 \oplus \ldots \oplus a_k) \mathrm{mod} q$.

Цей вираз є алгоритмом побудови недвійкового коду з перевіркою за модулем q.

Якщо кожний розряд кодової комбінації має m позицій, тобто є множиною позицій (знаків алфавіту q), то перевірний розряд також повинен мати m позицій. Значення позицій перевірного розряду в цьому разі визначається сумою відповідних номерів позицій всіх розрядів кодової комбінації за модулем q.

Цей код має незначну надмірність $R_{над} = 1/(k + 1)$ і дає змогу виявляти наявність помилок у розрядах кодової комбінації при невідповідності значення перевірного розряду сумі k інформаційних розрядів за модулем q.

Код із повторенням. В основу побудови цього коду за аналогією з двійковим покладено повторення початкової кодової комбінації. Відмінність q-коду від аналогічного двійкового полягає в тому, що повторення кодової комбінації першого може виконуватися паралельно в часі уведенням додаткової позиції надмірності. Так, при використанні багаточастотного коду подвоєння кількості частотних позицій забезпечує паралельну передачу комбінації цього коду.

При цьому з′являються додаткові переваги над двійковим кодом: передача інформаційної та перевірної частин комбінації багаточастотного коду виконується з рознесенням за частотою, що підвищує завадостійкість коду при селективних завмираннях, характерних для деяких типів безпроводових ліній зв′язку; при використанні кількох ознак сигналу передача інформаційної та перевірної частин кодової комбінації може виконуватися позиціями різних ознак (наприклад, інформаційна частина може передаватися частотними позиціями, а перевірна – фазовими, що застосовується для підвищення або вірогідності, або швидкості передачі інформації).

Надмірність коду з повторенням можна оцінити надмірністю позицій ознак сигналу. При цьому надмірність $R_{над} = 0{,}5$. Однак часова надмірність, яка згадувалася вище, може не підвищуватися.

Алгоритм побудови коду із повторенням має вигляд

$$a_i \Leftrightarrow b_i, \qquad i \in [1, k], \tag{3.32}$$

де a_i, b_i – множини позицій, призначені для передачі i-х інформаційного та перевірного елементів кодової комбінації відповідно; k – кількість інформаційних елементів.

Розглядуваний код згідно з алгоритмом (3.32) дає змогу виявити всі помилки, за винятком помилок у парних множинах позицій, призначених

для передачі інформаційної та перевірної частин коду, що несуть одну й ту саму інформацію.

Незвідні змінно-позиційні коди. Головна перевага цих кодів полягає у малій кількості елементів і відповідно часових позицій (інтервалів) у комбінації. що має виграш у швидкості передачі порівняно з двійковими кодами.

З класу змінно-позиційних кодів найбільшого поширення дістали НЗ-коди, при використанні яких відпадає необхідність у жорсткій синхронізації приймальної апаратури, що, цілком природно, підвищує надійність цих кодів. Розглянемо методику побудови їх.

Під незвідним змінно-позиційним кодом будемо розуміти код, який задовольняє такі умови:

– кожна кодова комбінація складається з однакової кількості елементів, які передаються послідовно;

– кожний елемент комбінації містить m позицій (знаків) з q;

– сусідні елементи кодової комбінації різняться хоча б однією позицією;

– останній елемент комбінації збігається з її першим елементом, тобто перші та основні елементи кодової комбінації мають різні багатопозиційні сполучення, що не збігаються.

Виконання останньої умови забезпечує незвідність коду, що дає змогу виконувати передачу елементів без пауз і в деяких випадках відмовитися від синхронізації, а також спрощує послідовність виконання операцій при декодуванні.

Послідовність побудови НЗ-коду загалом така:

– береться множина m з q позицій сигналу;

– визначається кількість сполучень позицій за заданою кількістю позицій у кожному сполученні;

– вся кількість сполучень позицій розбивається на n груп, де n – кількість елементів кодової комбінації;

– утворюються кодові комбінації з n елементів, для кожного з яких беруться сполучення позицій із закріпленої за елементом групи.

За методом побудови кодових комбінацій багатопозиційні НЗ-коди можна поділити на два класи: без поділу алфавіту коду на групи; з поділом алфавіту коду на групи. Останній клас, у свою чергу, поділяють на два підкласи, що містять: НЗ-код, кожний елемент якого має m позицій з різних груп; НЗ-код, кожний елемент якого містить m позицій з однієї групи.

Під НЗ-кодом з елементами однієї ваги розуміється код, елементи якого складаються з однакової кількості позицій m.

Незвідний змінно-позиційний код з елементами різної ваги на відміну від НЗ-коду з елементами однієї ваги має властивість поелементної синхронізації завдяки тому, що його елементи містять різну кількість позицій. Це дає змогу утворювати значно більшу кількість кодових комбінацій.

У зв′язку з тим, що елементи кодових комбінацій всіх без винятку НЗ-кодів мають обумовлену вагу, такі коди можуть виявляти будь-які помилки, що призводять до зміни ваги елементів (зменшення або збільшення кількості позицій елемента) кодової комбінації, забезпечуючи її числовий захист.

Надмірність НЗ-кодів визначається виразом

$$R_{над} = 1 - \frac{\log_2 N_Д}{\log_2 N_{\max}},$$

де N_{max} і $N_Д$ – відповідно максимально можлива та дозволена до використання в коді кількість комбінацій.

3.3.2. **Коди, що виправляють помилки**

Коди, що виправляють помилки (або коректувальні коди), повинні мати мінімальну кодову відстань $d_{min} \geq 3$. Її зростання досягається збільшенням кількості n розрядів коду або зменшенням кількості $N_Д$ дозволених кодових комбінацій, які використовуються для передачі повідомлень, тобто підвищення надмірності коду.

Найбільшого поширення серед двійкових коректувальних кодів дістали систематичні та несистематичні блокові коди (вони, у свою чергу, поділяються на лінійні та нелінійні), а також рекурентні коди. З недвійкових кодів для захисту інформації від помилок застосовуються узагальнений код Хеммінга, ланцюговий та ітеративний коди.

Лінійні систематичні групові (блокові) коди. Лінійним систематичним груповим двійковим (n, k)-кодом називається код, у якого перевірні елементи b_j (де $j = 1,\ldots,r$) знаходяться як суми за модулем 2 обумовлених інформаційних елементів a_i (де $i = 1,\ldots,k$).

Таким чином, у лінійному коді перевірні елементи визначаються як

$$\begin{aligned} b_1 &= \sum_{i=1}^{k} \alpha_{ji} a_i; \\ &\ldots\ldots\ldots\ldots \\ b_r &= \sum_{i=1}^{k} \alpha_{ri} a_i, \end{aligned} \qquad (3.33)$$

де α_{ji} – коефіцієнти, значення яких дорівнюють 0 або 1.

Як випливає з (3.33), закон побудови лінійного коду визначається вибором *kr* коефіцієнтів α_{ji}.

Одна з властивостей лінійних кодів полягає в тому, що сума за модулем 2 будь-яких двох дозволених кодових комбінацій також є дозволеною комбінацією цього коду.

Така властивість дає можливість побудувати всі дозволені комбінації лінійного коду, маючи тільки обмежену кількість їх. При цьому побудова лінійного коду виконується на основі твірної (породжувальної) матриці. Ця матриця будується так, щоб:

– кількість початкових кодових комбінацій дорівнювала k, тобто кількості інформаційних елементів первинного коду;

– всі початкові кодові комбінації були різними;

– нульова комбінація не входила до складу початкових;

– всі початкові комбінації були лінійно незалежними;

– кількість одиниць в кожній початковій комбінації була не меншою, ніж d_{min};

– кодова відстань між будь-якими парами початкових комбінацій також була не меншою, ніж d_{min}.

Підібрані за цим правилом початкові комбінації записуються у вигляді твірної матриці $G_{(n,k)}$, яка містить k рядків і n стовпців:

$$G_{(n,k)} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1k} & b_{11} & b_{12} & \dots & b_{1r} \\ a_{21} & a_{22} & \dots & a_{2k} & b_{21} & b_{22} & \dots & b_{2r} \\ . & . & . & . & . & . & . & . \\ a_{k1} & a_{k2} & \dots & a_{kk} & b_{k1} & b_{k2} & \dots & b_{kr} \end{bmatrix}. \qquad (3.34)$$

Матрицю (3.34) можна подати також у вигляді двох підматриць: інформаційної E_k та перевірної $C_{(r,\ k)}$. Першу зручно записати в канонічній формі як одиничну підматрицю, що має k стовпців і стільки ж рядків:

$$E_k = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ . & . & . & . & . \\ 0 & 0 & 0 & \dots & 1 \end{bmatrix}.$$

Перевірна підматриця $C_{(r,\ k)}$ будується підбором r-розрядних комбінацій з кількістю одиниць в рядку не меншою від ($d_{min} - 1$). При цьому не-

обхідно враховувати, що сума за модулем 2 будь-яких розрядів повинна мати більше, як ($d_{min} - 2$) одиниць.

Ураховуючи викладене, можна дати таке визначення: лінійним систематичним груповим двійковим (n, k)-кодом називається код, у якого всі його ($2^k - 1$) ненульові комбінації можуть бути утворені як суми за модулем 2 рядків деякої матриці $G_{(n, k)}$ розміром $k \times n$, яка називається твірною матрицею коду.

Розрізняють два основних методи виправлення помилок у систематичному груповому коді: за допомогою кодового синдрому та за допомогою кодів-супутників.

Перевірка кодової комбінації, що приймається при використанні кодового синдрому, виконується зіставленням її перевірних розрядів з перевірними розрядами, які обчислюються на основі прийнятих інформаційних.

За відсутності помилки комбінація синдрому складається з одних нулів. Присутність хоча б одного ненульового елемента в комбінації синдрому вказує на спотворення елемента у прийнятій кодовій комбінації.

Між комбінацією синдрому та помилковою комбінацією, що спричинила створення синдрому, немає взаємної однозначної відповідності, тому за кожним синдромом закріплюється така комбінація помилок, що виправляється, виникнення якої в каналі є найімовірнішим.

Побудова синдромів для виправлення подвійних, потрійних і помилок більшої кратності складна. Тому метод виправлення помилок за допомогою кодового синдрому використовується головним чином для виправлення поодиноких помилок, імовірність виникнення яких значно більша, ніж помилок більшої кратності.

Метод виправлення помилок з використанням кодів-супутників передбачає побудову кодової таблиці з кодами-супутниками за таким правилом (табл. 3.2): в першому її рядку розташовують усі кодові комбінації V_i, для яких необхідно знайти коди-супутники; у другому рядку записують вектори, утворені підсумовуванням за модулем 2 кодових комбінацій V_i з вектором помилки e_1, вага якого $w = 1$, а одиниця знаходиться в першому розряді; третій рядок є результатом підсумовування за модулем 2 кодових комбінацій V_i з вектором e_2, вага якого $w = 1$, а одиниця розміщується у другому розряді, і т.д. Так діють доти, доки не будуть підсумовані з кодовими комбінаціями V_i всі вектори e_i вагою $w = 1$ з одиницями в кожному з n розрядів, потім підсумовують за модулем 2 вектори e_i вагою $w = 2$ з послідовним перекриванням усіх можливих розрядів (вага векторів e_i визначає кількість помилок, що виправляються, а розрядність цих векторів відповідає розрядності кодової комбінації).

Таким чином, для кожної кодової комбінації V_i лінійного систематичного коду дістають свою групу кодів-супутників, розташованих у відповідному стовпці (див. табл. 3.2), які зберігаються в пам′яті ЕОМ. У разі приймання комбінації, що збігається з одним із кодів-супутників, спотворена комбінація розшифровується як початкова робоча комбінація, до якої належить цей код-супутник.

Недоліком розглянутого методу є велика ємність пам′яті ЕОМ і значні затрати часу на перебір комбінацій кодів-супутників.

Таблиця 3.2

e_i	V_i				
	V_1	V_2	V_3	…	$V_{(2^k-1)}$
e_1	$e_1 \oplus V_1$	$e_1 \oplus V_2$	$e_1 \oplus V_3$	…	$e_1 \oplus V_{(2^k-1)}$
e_2	$e_2 \oplus V_1$	$e_2 \oplus V_2$	$e_2 \oplus V_3$	…	$e_2 \oplus V_{(2^k-1)}$
–	–	–	–	–	–
–	–	–	–	–	–
$e_{(2^n-1)}$	$e_{(2^n-1)} \oplus V_1$	$e_{(2^n-1)} \oplus V_2$	$e_{(2^n-1)} \oplus V_3$	…	$e_{(2^n-1)} \oplus V_{(2^k-1)}$

Коди Хеммінга. Це одні з найпоширеніших систематичних кодів, які виправляють помилки. До кодів Хеммінга належать коди з мінімальною кодовою відстанню $d_{min} = 3$, що виправляють всі поодинокі помилки.

Формування r перевірних елементів у комбінації цих кодів виконують за k інформаційними елементами. Таким чином, довжина кодової комбінації $n = k + r$. Перевірними елементами є лінійні комбінації інформаційних елементів з ваговими коефіцієнтами 1 та 0.

Послідовність одиниць і нулів у кодовій комбінації називається ще кодовим вектором. Кодам Хеммінга притаманні властивості лінійних кодів: сума (різниця) векторів лінійного коду дає вектор, який належить цьому коду; лінійні коди утворюють алгебричну групу відносно операції додавання за модулем 2; мінімальна кодова відстань між векторами групового коду дорівнює мінімальній вазі ненульових кодових векторів.

При передачі кодового вектора може бути спотворений будь-який елемент, кількість таких ситуацій $C_n^1 = n$. До цього слід додати ще одну ситуацію, коли помилка не виникає. Таким чином, загальна кількість 2^r комбінацій перевірних елементів має перевищувати кількість можливих помилкових ситуацій в коді з урахуванням відсутності помилок для правильного розрізнення їх і визначення місць помилки:

$$2^r \geq n + 1. \qquad (3.35)$$

Оскільки $2^n = 2^{k+r} = 2^k \cdot 2^r$, можна записати

$$2^n \geq (n + 1) \cdot 2^k, \qquad (3.36)$$

де 2^n – повна кількість комбінацій коду.

Мінімальне співвідношення коректувальних та інформаційних розрядів, нижче якого код не може зберігати задані коректувальні властивості, визначається виразом $2^r - 1 = n$.

Для розрахунку основних параметрів кодів Хеммінга можна задати кількість перевірних елементів r; тоді з останнього виразу визначається n, а кількість інформаційних елементів k =n – r. Співвідношення між r, n і k для кодів Хеммінга наведено в табл. 3.3.

Таблиця 3.3

k	1	1	2	3	4	4	5	6	7	8	9	10	11	11
r	2	3	3	3	3	4	4	4	4	4	4	4	4	5
n	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Код Хеммінга з кодовою відстанню $d_{min} = 4$ називається розширеним. Він забезпечує виправлення всіх однократних і виявлення всіх дво- та трикратних помилок. Для цього уводиться додатковий перевірний розряд b_0, який дописується до перевірної матриці Хеммінга з кодовою відстанню $d_{min} = 3$, завдяки чому остання збільшується до 4.

Циклічні коди. Ці коди широко застосовуються для захисту інформації від помилок. Подання комбінацій в них виконують за допомогою поліномів формальної змінної *x*, що дає змогу звести дії над кодовими комбінаціями до дій над поліномами, які самі фізичного змісту не мають.

Лінійні систематичні (n, k)-коди, в яких циклічний зсув a_{n-2}, a_{n-3}, a_{n-4}, …, a_2, a_1, a_0, a_{n-1} дозволеної комбінації a_{n-1}, a_{n-2}, a_{n-3},…, a_1, a_0 також є дозволеною комбінацією, що належить цьому коду, називаються циклічними. Така циклічна перестановка елементів виникає після множення полінома на *x*. Якщо $V(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1x + a_0$, то $xV(x) = a_{n-1}x^n + a_{n-2}x^{n-1} + \ldots + a_1x^2 + a_0x$. Щоб степінь полінома не перевищував $n - 1$, член $a_{n-1}x^n$ замінюється одиницею. Тому $xV(x) = F(x) = a_{n-2}x^{n-1} + \ldots + a_1x^2 + a_0x + a_{n-1}$.

Особливу роль у теорії циклічних кодів відіграють твірні поліноми. Помічено, що комбінації лінійного коду мають властивість циклічності, коли як твірні використовуються поліноми, що є дільниками двочлена x^n+1. Кожний такий двочлен може бути розкладений на кілька незвідних поліномів, тобто таких, які можуть бути подані у вигляді добутку поліномів нижчих степенів (вони діляться самі на себе або на одиницю).

Як твірні поліноми різних циклічних кодів можуть бути застосовані всі незвідні поліноми та добутки їх, тому що вони також є дільниками двочлена x^n+1.

Можна дати ще одне визначення двійкового циклічного коду – це лінійний двійковий систематичний (n, k)-код, всі 2^k комбінацій якого подано

поліномами степеня $x - 1$ і менше, що діляться на деякий поліном $P(x)$ степеня $r = n - k$, який є дільником двочлена x^n+1. Деякі твірні поліноми наведено в табл. 3.4.

Таблиця 3.4

r	Твірний поліном $P(x)$	Двійковий запис полінома
1	$x + 1$	11
2	$x^2 + x + 1$	111
3	$x^3 + x + 1$	1011
4	$x^3 + x^2 + 1$	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
6	$x^6 + x^5 + x^4 + 1$	1110001
8	$x^8 + x^7 + x^6 + x^5 + x^2 + x + 1$	111100111
9	$x^9 + x^5 + x^3 + 1$	1000101001
15	$x^{15} + x^{14} + x^{13} + x^{12} + x^4 + x^3 + x^2 + x + 1$	1111000000011111
16	$x^{16} + x^{12} + x^5 + 1$	10001000000100001

Розрізняють алгебричні та матричні методи побудови циклічного коду. Побудова дозволеної кодової комбінації (алгоритм кодування) перших зводиться ось до чого:

– подати інформаційну частину з k елементів у вигляді полінома $Q(x)$ степеня $k - 1$;

– помножити $Q(x)$ на x^r (що еквівалентно зсуву k-розрядної кодової комбінації на r розрядів);

– поділити поліном $x^rQ(x)$ на вибраний твірний поліном $P(x)$, степінь якого дорівнює r, і визначити остачу від ділення $R(x)$, тобто

$$\frac{x^rQ(x)}{P(x)} = C(x) \oplus \frac{R(x)}{P(x)}, \qquad (3.37)$$

де $C(x)$ – частка від ділення, яка має той самий степінь, що й поліном $Q(x)$; $R(x)$ – остача від ділення, яка має степінь, не більший від $r - 1$ [менший, ніж степінь дільника $P(x)$].

Зазначимо, що r розрядів остачі є r перевірними елементами кодової комбінації, причому

$$x^r Q(x) = C(x)P(x) \oplus R(x), \tag{3.38}$$

або

$$F(x) = C(x)P(x) = x^r Q(x) \oplus R(x), \tag{3.39}$$

де $F(x)$ – комбінація циклічного коду.

З виразу (3.39) випливають два рівноцінних алгебричних методи побудови комбінацій циклічного коду:

$$F_1(x) = x^r Q(x) \oplus R(x); \tag{3.40}$$

$$F_2(x) = C(x)P(x). \tag{3.41}$$

Ще один метод можна дістати, замінивши в (3.41) частку від ділення $C(x)$ на поліном $Q(x)$ кодової комбінації r-елементного двійкового простого коду, що подається для кодування циклічним кодом. Ця заміна цілком слушна, оскільки поліноми $C(x)$ і $Q(x)$ мають однаковий найбільший степінь (однакову кількість розрядів). Отже,

$$F_3(x) = Q(x)P(x). \tag{3.42}$$

У комбінаціях циклічних кодів, побудованих за першим і другим методами [див. вирази (3.40) і (3.41)], розташування інформаційних і перевірних елементів підпорядковується такому правилу: k старших розрядів комбінації є інформаційними, решта n – k = r розрядів – перевірними.

При використанні третього методу побудови циклічних кодів (3.42) дістають комбінації неподільного циклічного коду, в яких інформаційні та перевірні елементи не відокремлені один від одного, що ускладнює процес декодування. Тому на практиці найпоширенішими є перші два алгебричні методи побудови циклічного коду.

Очевидно, що комбінація F(x) має ділитися на поліном P(x) без остачі. На цьому й грунтується перевірка комбінації на наявність помилок при її прийманні. Якщо прийнята комбінація F(x) ділиться на поліном P(x) без остачі, то вона визнається безпомилковою. Якщо ж остача не нульова, то помилка є.

Оскільки поліном остачі має степінь, менший від r, кількість різних ненульових остач може досягати $2^r - 1$. Для коду, що виправляє одну помилку ($d_{min} = 3$), кількість таких остач дорівнює довжині n кодової комбінації ($2^r - 1 \geq n$) або перевищує її. Номер розряду комбінації, в якій виникла помилка, однозначно пов′язаний з виглядом остачі.

Для виправлення помилки виконують умову, за якої кількість різних нульових остач дорівнюватиме кількості елементів (при кратності виправлення $v_{вп} = 1$) або кількості комбінацій з n по $v_{вп}$, де $v_{вп}$ – кількість помилок, яка виправляється кодом. Це значить, що, наприклад, при n = 15 і $v_{вп}=2$ треба мати $C_{15}^2 = 105$ ненульових остач для однозначного виправлен-

ня двох будь-яких помилок у коді завдовжки n. Для цього необхідно вибрати поліном $P(x)$ степеня r = 7 і побудувати код завдовжки n = 15 при r = 7 перевірних елементів (при цьому k = 8).

Коди Боуза-Чоудхурі-Боквінгема. Ці коди є різновидом циклічних кодів з кодовою відстанню $d_{min} \geq 5$. Вони дають змогу виявляти та виправляти будь-яку кількість помилок. При кодуванні задаються кількістю помилок, яку слід виправити, або мінімальною кодовою відстанню та загальною кількістю n елементів у кодовій комбінації. Кількість інформаційних k і перевірних r елементів визначають при побудові коду БЧХ. Розглянемо деякі правила цієї побудови.

Довжину n комбінації кодів БЧХ можна визначити так:

$$n = 2^h - 1 \text{ або } n = (2^h - 1)/g, \qquad (3.43)$$

де h > 0 – ціле число; g – непарне додатне число, при діленні на яке n стає цілим непарним числом. Таким чином, довжина n може мати тільки непарну кількість.

Керуючись (3.43), установлюємо, що n може дорівнювати 3, 7, 15, 31, 63, 127, 255, 511, 1023 розрядам і т.д.

Кількість перевірних елементів коду визначається виразом

$$r \leq \frac{h(d-1)}{2} = [\log_2(n+1)]\frac{d-1}{2}, \qquad (3.44)$$

а кількість інформаційних елементів – виразом

$$k \geq \left(2^h - 1\right) - \frac{h(d-1)}{2} \quad \text{або} \quad k = n - r. \qquad (3.45)$$

Кодова відстань d пов′язана з кількістю виправляємих помилок $v_{вп}$ виразом – $d > 2v_{вп} - 1$.

Твірний поліном коду БЧХ є найменшим спільним кратним (НСК) мінімальних поліномів $M_i(x)$,де $i = 1, 3, 5, \ldots, d_{min} - 2$ – порядок полінома $P(x) = \text{НСК}\,[M_1(x)M_2(x)\ldots M_{d-2}(x)]$. Отже, кількість L мінімальних поліномів визначається кількістю помилок $v_{вп}$, які виправляються кодом: $L = v_{вп}$.

Найбільше значення степеня x мінімального полінома є найменшим цілим числом, при якому $2^l - 1$ ділиться на n або ng без остачі, тобто $n=2^l-1$ або $ng = 2^l - 1$. Звідси випливає, що l = h.

Степінь b твірного полінома залежить від НСК і не перевищує добуток $lv_{вп}$ або lL тому, що $L = v_{вп}$. Так, для коду БЧХ завдовжки $n = 15$, що виправляє $v_{вп} = 2$ помилки, кількість мінімальних поліномів L = 2, а найбільший степінь мінімального полінома l залежить від довжини n коду ($n= 2^l - 1$), тобто $l = 4$. При цьому твірний поліном $P^b(x)$, де $b = lL = 4 \cdot 2 = 8$, визначається виразом $P^8(x) = \text{НСК}[M_1^4(x)M_3^4(x)]$, який після підстановки зна-

чень $M(x)$ набуває вигляду: $P^8(x) = (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1) = x^8 + x^7 + x^6 + x^4 + 1 \rightarrow 111010001$.

Найбільший степінь твірного полінома $P(x)$ визначає кількість перевірних елементів у комбінації ($r = 8$), а кількість інформаційних елементів $k = n - r = 15 - 8 = 7$. Маємо (15, 7)-код БЧХ з $v_{вп} = 2$.

В таблиці 3.5 приведені співвідношення між параметрами деяких кодів БЧХ. Можна відмітити, що при $v_{вп} = 1$ параметри n і k відповідають параметрам коду Хеммінга. Тобто, код Хеммінга теж є кодом БЧХ, який виправляє одиночні помилки.

Таблиця 3.5

n	k	$v_{вп}$	n	k	$v_{вп}$	n	k	$v_{вп}$	n	k	$v_{вп}$
7	4	1	127	120	1	255	247	1	255	99	23
15	11	1	127	113	2	255	239	2	255	91	25
15	7	2	127	106	3	255	231	3	255	87	26
31	26	1	127	99	4	255	223	4	255	79	27
31	21	2	127	92	5	255	215	5	255	71	29
31	16	3	127	85	6	255	207	6	255	63	30
31	11	5	127	78	8	255	199	7	255	55	31
63	57	1	127	71	9	255	191	8	255	47	42
63	51	2	127	64	10	255	187	9	255	45	43
63	45	3	127	57	11	255	179	10	255	37	45
63	39	4	127	50	13	255	171	11	255	29	47
63	36	5	127	8	31	255	163	12			
63	10	13				255	115	21			
63	7	15				255	107	22			

Кількість помилок, які можуть виправляти коди БЧХ, не обмежена, але зі збільшенням кратності помилки значно зростає складність пристроїв декодування, що призводить до зменшення швидкості передачі інформації.

Код Голея. Цей код є досконалим і дозволяє виправляти помилки високої кратності ($v_{вп} > 1$). Код Голея (23, 12) є циклічним і виправляє всі конфігурації помилок, кратність яких не перевищує трьох. З кодом Голея (23, 12) пов′язаний код (24, 12), який створюється додаванням до кодових слів коду (23, 12) додаткового перевірочного символу. Коди (23, 12) і (24, 12) мають мінімальні кодові відстані 7 та 8 відповідно. Тому код (24, 12), крім виправлення помилок кратністю 3, забезпечує також виявлення помилок кратністю 4 при незначній зміні кодової швидкості. Код (24, 12) відноситься до найбільш поширених кодів.

Код Файра. Коди БЧХ розраховані на виправлення кількох помилок, які не обов′язково знаходяться поруч; тому вони потребують значної кількості перевірних елементів. Двійковий код Файра призначений для виправлення поодиноких пачок помилок, для чого він потребує значно меншої кількості перевірних елементів порівняно з кодами БЧХ.

Під пачкою (пакетом) помилок розуміють не тільки групу помилок, розташованих поруч, а й групу або кілька спотворених і неспотворених елементів, які знаходяться між двома спотвореними елементами. В останньому випадку до пачки помилок, крім двох крайніх спотворених елементів пачки, належать ще спотворені та неспотворені елементи, розташовані між ними, тобто в середині пачки.

Твірний поліном коду Файра визначається виразом

$$P_{\Phi}(x) = P(x)(x^{c} + 1), \qquad (3.46)$$

де $P(x)$ – незвідний поліном степеня, що належить h; с – просте число, яке не повинно ділитися на h без остачі.

Поліном $P(x)$ має деякий степінь h, якщо h – найменше додатне число таке, що двочлен $x^{h} + 1$ ділиться на $P(x)$ без остачі. Для будь-якого l існує принаймні один незвідний поліном $P(x)$ степеня l, який належить числу

$$h = 2^{l} - 1. \qquad (3.47)$$

Незвідний поліном $P(x)$ вибирається з табл. 3.4 так, щоб виконувалась умова (3.46), причому $l \geq b$, де $b = v_{вп}$ – довжина пачки помилок. Так, якщо $P(x) = x^3 + x^2 + 1$ ($l = 3$), то $h = 2^{l} - 1 = 7$, а число c може мати значення, які не діляться на 7, тобто 15, 16, 17, 18, 19, 20, 22 тощо.

Довжина коду Файра визначається виразом

$$n = \text{НСК}(c, h), \qquad (3.48)$$

тобто є НСК чисел c та h, тому що тільки в цьому разі двочлен $x^{n} + 1$ буде ділитися на поліном $P_{\Phi}(x)$ без остачі.

Кількість перевірних елементів цього коду визначається так:

$$r = c + 1, \qquad (3.49)$$

а інформаційних – так

$$k = n - c - 1. \qquad (3.50)$$

Код Файра виправляє будь-яку поодиноку пачку помилок завдовжки b або менше й одночасно виявляє будь-яку пачку помилок завдовжки $B \geq b$ або менше, якщо $c \geq b + B - 1$ і $l \geq b$.

Якщо користуватися цим кодом тільки для виявлення помилок, то можна виявити будь-яку комбінацію з двох пачок помилок, довжина найменшої з яких не перевищує l, а сума довжин обох пачок менша, ніж $c + 1$. Можна також виявити будь-яку поодиноку пачку помилок з довжиною, не більшою від $r = c + 1$, де r – кількість перевірних елементів.

Все це зумовлює використання коду Файра при передачі інформації по каналах з великою ймовірністю виникнення пачок помилок.

Код з багатократним повторенням. Код з багатократним повторенням (без інверсії) є подільним лінійним кодом. Він містить k інформаційних і $n_R k$ перевірних елементів, де $n_R \geq 2$ – кількість повторень початкової кодової комбінації. В цьому коді кожні k перевірних елементів є просто повторюваними інформаційними елементами

$$b_j = b_{j+2k} = b_{j+3k} = \ldots = b_{j+(n_R-1)k} = a_j, \qquad j = 1, \ldots, k.$$

Через те, що код має кодову відстань $d_{\min} = n_R + 1$, він може використовуватися для виявлення та виправлення помилок. Процедура виявлення помилок у прийнятій кодовій комбінації полягає в порівнянні однойменних інформаційних і перевірних елементів. Незбіг їх свідчить про наявність помилок у прийнятій комбінації.

При виправленні помилок у кодовій комбінації застосовується мажоритарний принцип виправлення для кожного інформаційного елемента, тобто «голосування за більшістю», коли за істинне значення приймається те, яке найчастіше зустрічається в цьому інформаційному та відповідних перевірних елементах. Код дає змогу виправити помилки кратністю від 1 до $(d_{\min} - 1)/2$ та деякі помилки більш високої кратності залежно від кількості повторень їх.

Надмірність коду визначається виразом: $R_{над} = n_R/(n_R + 1)$.

Ітеративні коди. Ці коди характеризуються двома або більшою кількістю перевірок усередині кодової комбінації, а властивості цих кодів повністю визначаються параметрами їх.

Так, довжина n кодової комбінації, кількість інформаційних параметрів k та мінімальна відстань $d_{\min}$ визначаються виразами

$$n = \prod_{i=1}^{S} n_i; \qquad k = \prod_{i=1}^{S} k_i; \qquad d_{\min} = \prod_{i=1}^{S} d_{\min i},$$

де n_i, k_i, $d_{\min\, i}$ – параметри ітерованих кодів; S – кратність ітерування; П - знак множення.

На практиці широко застосовуються двовимірні лінійні ітеративні коди з кодуванням за рядками та стовпцями з однією перевіркою на парність. Дозволяється використовувати коди з кількістю перевірних елементів 8, 9 і 16. Для коду з $r = 8$ застосовується блок інформаційних елементів розміром 3×4 (з $k_1 = 3$ рядками та $k_2 = 4$ стовпцями). При цьому кількість інформаційних елементів $k = k_1 k_2 = 3 \cdot 4 = 12$, а перевірних $r = 8$; $n = 20$. Для коду з $r = 9$ беруть $k = k_1 k_2 = 4 \cdot 4 = 16$, $n = 25$; для коду з $r = 16$ або $k = k_1 k_2 = 8 \cdot 7 = 56$, $n = 72$, або $k = k_1 k_2 = 7 \cdot 8 = 56$, $n = 72$.

Ці коди мають мінімальну кодову відстань $d_{min} = 2 \cdot 2 = 4$ і дають змогу виявити помилки будь-якої кратності, за винятком деяких чотири-, шести- та восьмикратних помилок, якщо вони розміщуються на вершинах прямокутників або попарно в певному порядку. У режимі виправлення та виявлення помилок код виправляє будь-які поодинокі помилки і виявляє всі подвійні та деякі помилки більшої кратності.

При виявленні помилок на приймальному боці виконується перевірка на парність кожних рядка та стовпця. Невиконання умови парності в якомусь стовпці свідчить про наявність спотворених елементів у прийнятій кодовій комбінації.

При виправленні та виявленні помилок на приймальному боці визначаються рядки і стовпці, для яких не виконується умова парності. Спотворений інформаційний елемент знаходиться на місці перетину рядка та стовпця, для яких не виконується перевірка на парність.

Надмірність двовимірних ітеративних кодів становить: $R_{над} = 1 - k/n = r/n = 8/20 = 2/5$ при $r = 8$; $R_{над} = 9/25$ при $r = 9$; $R_{над} = 16/72 = 2/9$ при r=16.

При побудові ітеративних кодів для кодування елементів по рядках і стовпцях можна використовувати не тільки код із перевіркою на парність (або непарність), а й інші коди (наприклад, Хеммінга). При цьому мінімальна кодова відстань d_{min} збільшується, а значить, зростає й здатність коду виправляти помилки.

Суттєвим недоліком ітеративних кодів є порівняно висока надмірність їх, яка значно перевищує надмірність циклічних кодів, здатних виявляти та виправляти ту саму кількість помилок за інших однакових умов. Однак їх використання в системах передачі даних зумовлює більш просте порівняно з циклічними кодами кодування та декодування за допомогою ЕОМ.

Ітеративні коди знайшли широке застосування для виявлення та виправлення помилок, які виникають при запису, зберіганні та зчитуванні інформації на магнітних носіях.

Недвійкові коди, що виправляють помилки. Двійкові блокові коди призначені в основному для виправлення незалежних помилок. Відповідні їм q-коди також виправляють помилки аналогічного походження. Проте слід урахувати, що один елемент q-коду несе $\log_2 q$ (при m = 1) або $\log_2 C_q^m$ (при $m \geq 2$) бітів інформації залежно від методу побудови конкретного коду.

Зазначена особливість q-коду дає підставу стверджувати, що навіть недвійковий блоковий код дає змогу виправляти умовний пакет помилок із $\log_2 q$ або $\log_2 C_q^m$ бітів інформації, який, якщо б він виник у аналогічному

двійковому коді, не міг бути ним виправлений. Це є однією з переваг використання недвійкових кодів, що виправляють помилки.

Прикладами деяких недвійкових кодів, що виправляють помилки, є: код із багатократним повторенням; узагальнений код Хеммінга; коди БЧХ; коди Ріда-Соломона.

Код із багатократним повторенням. Даний метод кодування застосовується при передачі інформації по каналах з високим рівнем завад для істотного підвищення вірогідності, коли немає можливості для цієї мети використати зворотний канал.

При використанні q-коду можна увести аналог n_R-кратного повторення, збільшивши кількість позицій та ознак сигналу (алфавіт коду). У разі передачі інформації по радіоканалах, де, крім селективних завмирань, діють також завмирання сигналу в часі, аналог багатократного повторення можна увести за кілька часових позицій (інтервалів).

Узагальнений код Хеммінга. Серед q-кодів найпростішими кодами, які мають алгебричну структуру й забезпечують нескладні процедури кодування та декодування, є лінійні блокові коди, що виправляють одну помилку. У класі двійкових кодів існує аналог їх – код Хеммінга. Хоча між цими кодами є суттєві відмінності, такий q-код часто називають узагальненим кодом Хеммінга, маючи на увазі узагальнення коду на недвійковий алфавіт $q > 2$.

Коди БЧХ. Недвійкові коди БЧХ є різновидом циклічних кодів. Як і двійкові, недвійкові коди БЧХ будуються за допомогою твірних поліномів $P(x)$, які визначаються за даною мінімальною кодовою відстанню d_{min} і довжиною n кодової комбінації.

Коди Ріда-Соломона. Ці коди використовуються для передачі інформації по каналах з високою інтенсивністю завад, коли виникають помилки кратності два й більше, пачки помилок, а також сполучення пачок і однократних помилок. Коди Ріда-Соломона (коди РС) відносяться до класу недвійкових кодів БЧХ. У кодері повідомлення, що складається з k q-значних символів, обраних з алфавіту, який містить $q = 2^m$ символів, перетворюється в кодове слово РС-коду із n двійкових символів. Вхідні та вихідні символи при цьому можуть бути подані за допомогою m-розрядних двійкових слів. Таким чином, вхідне повідомлення можна розглядати як km-розрядне слово, а вихідне кодове слово – як nm-розрядне двійкове слово. Довжина коду РС дорівнює $n = q - 1$. Якщо виправляюча здібність коду дорівнює t помилковим символам, то має місце умова $n - k = 2t$. Коди РС існують при $1 \le k \le n - 2$, а їх розширення має довжини блоку: $n = q$ та $n = q + 1$. Найпростіше коди РС реалізуються для алфавіту, де m = 2, 4, 8,… .

Каскадні коди. Збільшення мінімальної кодової відстані $d_{\min}$ і, як наслідок, здатності коду виправляти помилки можна досягти, якщо застосувати кілька ступенів кодування (каскадний принцип кодування). Такі коди дістали назву каскадних.

На практиці поширеними є каскадні коди, що складаються з двох кодів (два ступені кодування), які називаються внутрішнім і зовнішнім. При цьому зовнішній код використовується для кодування повідомлень, що надходять від джерела у вигляді первинного коду, а внутрішній – для кодування комбінацій зовнішнього коду перед передачею їх у канал зв′язку. На рис. 3.3 показано спрощену схему системи передачі з каскадним принципом кодування повідомлень.

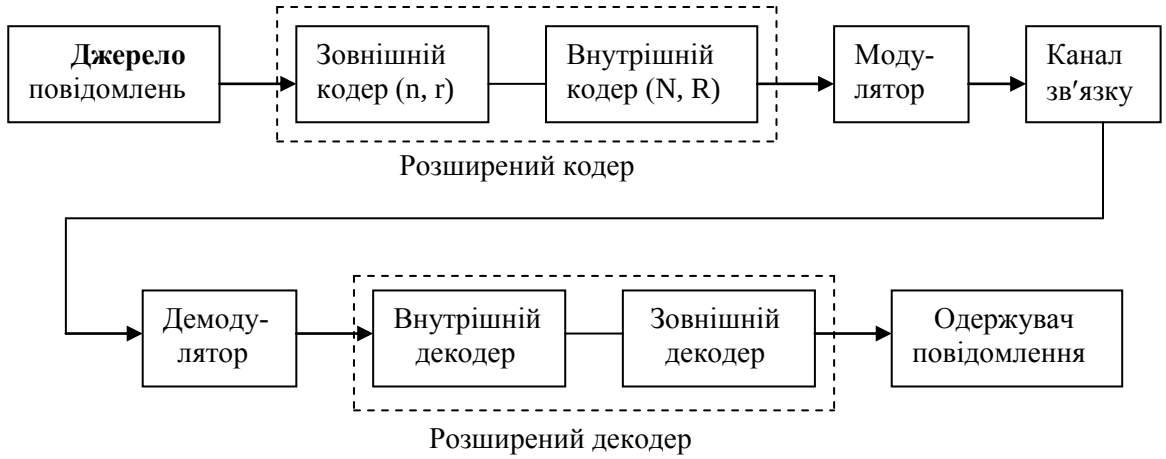


Рис. 3.3

Як зовнішні коди звичайно використовуються коди Ріда-Соломона або коди БЧХ. Вибір внутрішнього коду залежить від характеристик каналу зв′язку та інтенсивності виникнення помилок. Це може бути код БЧХ, код Хеммінга чи інший код. Взагалі задачею внутрішнього коду є забезпечення прийнятої ймовірності помилки, а зовнішнього – зниження результуючої ймовірності неправильного декодування до заданого значення.

При кодуванні зовнішнім кодом як інформаційні елементи комбінацій первинного коду приймаються всі елементи комбінації первинного коду, що надходять від джерела повідомлень, а при кодуванні внутрішнім кодом – усі елементи (інформаційні та перевірні) комбінації зовнішнього коду. Декодування виконується у зворотному порядку – спочатку декодується комбінація внутрішнього коду, а потім – зовнішнього.

Для завдання кожного символу зовнішнього коду використовуються k біт від джерела повідомлень, причому $2^{k_1} = M$, де M – основа зовнішнього коду. Наприклад, якщо в якості зовнішнього використати 32-ковий код РС, то його символами будуть комбінації по 5 біт кожна. У процесі коду-

вання k_2 символів зовнішнього коду перетворюються в n_2 символів. На цьому процес зовнішнього кодування закінчується і починає працювати внутрішній кодер. Кожний символ зовнішнього коду, що являє собою послідовність з k_1 бітів, розглядається вже як k_1-розрядне інформаційне слово внутрішнього двійкового коду. Тобто, внутрішній кодер буде працювати n_2 раз (за кількістю символів в слові зовнішнього коду), формуючи кожного разу n_1- бітові слова, які й передаються в канал зв′язку.

Описані операції можна пояснити за допомогою схеми формування блока каскадного блоку (рис. 3.4) ($\Rightarrow$ – кодування зовнішнім кодом РС; $\rightarrow$ - кодування внутрішнім двійковим кодом БЧХ). Для прикладу використані (15, 5) неподільний код БЧХ і (7, 4) неподільний 32-ковий код РС.

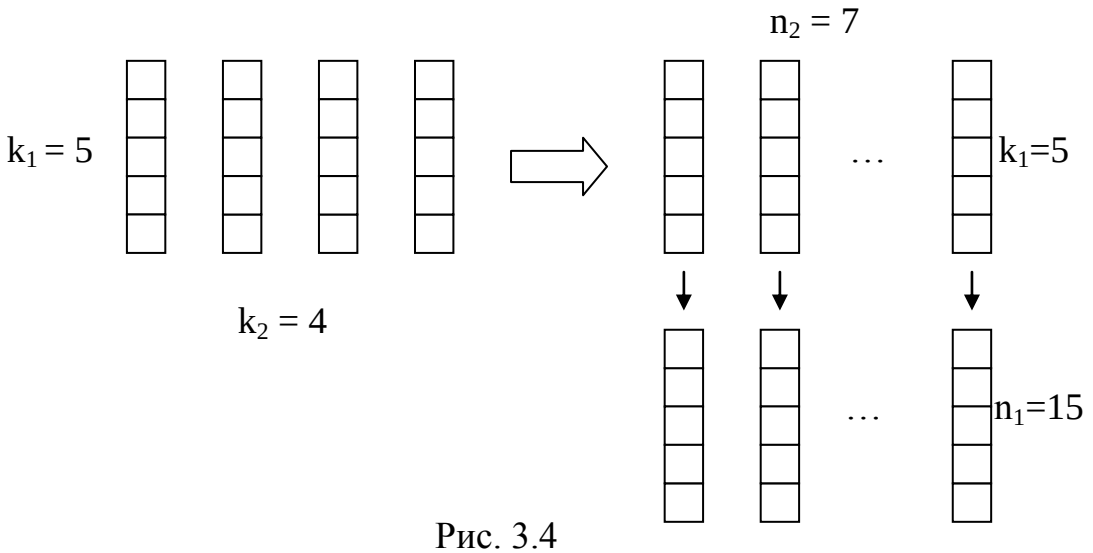


Рис. 3.4

Символи коду БЧХ – біти, а коду РС – 5-бітові послідовності. Для наведеного прикладу інформаційний блок із $k_1 \times k_2 = 4 \times 5 = 20$ біт перетворений в блок каскадного коду із $n_1 \times n_2 = 15 \times 7 = 105$ біт.

Таким чином, параметри каскадного коду можна визначити такими даними: довжина блоку $n = n_1 \times n_2$; кількість інформаційних бітів $k = k_1 \times k_2$; кількість перевірочних бітів $r = n - k$.

Загалом, тобто при S ступенях (каскадах) кодування, мінімальна кодова відстань каскадного коду визначається кодовими відстанями кодів, які використовуються для його побудови: $d_{\min} = \prod_{i=1}^{S} d_{\min i}$.

Застосування каскадного кодування значно спрощує технічну реалізацію кодеків. Крім того, у схемах каскадного кодування можна ефективно використати корисну властивість кодів РС встановлювати повне кодове

слово з n символів за допомогою k символів, що приймаються. Для цього внутрішній декодер при виявленні у прийнятому слові помилки визначає цей символ зовнішнього коду стертим. Зовнішній декодер повинний виконувати виправлення стирань, кількість яких може сягати s = d – 1, де d – кодова відстань зовнішнього коду.

Якщо шляхом деякого ускладнення декодеру додати йому можливість виправляти як помилки, так і стирання, то можна забезпечити виправлення будь-якої конфігурації із t помилок і s стирань, коли виконується умова d = 2t + s + 1.

Швидкість і надмірність каскадного коду також залежать від кодів, що використовуються при його побудові.

Каскадні коди знайшли широке застосування для передачі повідомлень по радіоканалах із великим рівнем завад, зокрема в супутникових лініях зв′язку.

3.4. **Неперервні (згорточні) коди**

Неперервними (рекурентними) називаються коди, що подаються неперервною послідовністю кодових елементів без поділу на окремі комбінації.

Неперервні коди відрізняються від блокових кодів структурою. У блоковому коді *n* символів коду, які формуються за допомогою кодера у будь-який визначений час, залежать тільки від *k* інформаційних символів, що поступили на його вхід протягом того ж самого відрізку часу. У рекурентному коді блок з *n* символів, які формуються у кодері у будь-який обраний відрізок часу, залежить не тільки від *k* інформаційних символів, що поступили на його вхід протягом цього ж відрізку часу, але і від інформаційних символів, що поступили протягом (К – 1) попередніх інтервалів. Параметр К має назву довжини кодового обмеження.

Рекурентні коди дають суттєвий ефект при захисті інформації, яка передається по каналах, де можливе виникнення помилок великої кратності та пачок помилок. Найпростіше ці коди реалізуються при надмірності $R_{над} = 1 - a/l = 0{,}5$, де *a* – кількість інформаційних елементів; *l* – довжина ділянки послідовності елементів, що передаються.

Від блокових рекурентні коди відрізняються тим, що дають змогу кодувати інформаційну послідовність неперервно, не поділяючи її на блоки фіксованої довжини *n* з *k* інформаційними та *r* перевірними елементами. Такі коди ще називаються ланцюговими. В них при передачі кожний перевірний елемент формується додаванням за модулем 2 двох інформаційних елементів, відстань між якими дорівнює кроку додавання $t_{кр} = k - i$:

$$a_i \oplus a_k = b_{i,k}; \qquad a_{i+1} \oplus a_{k+1} = b_{i+1,k+1};$$

$$a_k \oplus a_{k+t_{кр}} = b_{k,k+t_{кр}}; \quad a_{k+1} \oplus a_{k+1+t_{кр}} = b_{k+1,k+1+t_{кр}}; \quad \ldots .$$

Кількість перевірних елементів, сформованих за час Т, дорівнює кількості інформаційних елементів, які надійшли за той самий час. Ці елементи передаються через один (*a, b, a, b, a, b*,…). На приймальному боці вони розділяються й реєструються незалежно.

Із прийнятої послідовності інформаційних елементів формуються контрольні елементи b_i'' за тим самим алгоритмом, що й елементи b_i при кодуванні. При цьому кожний контрольний елемент b_i'' порівнюється із прийнятим перевірним елементом b_i'. Якщо спотворень не було, то $b_i' = b_i''$ (перевірний елемент збігається із відповідним контрольним). Наявність двох незбігів контрольних і перевірних елементів, зсунутих один відносно одного на $t_{кр}$ елементів, свідчить про спотворення інформаційного елемента, спільного для обох перевірних елементів, і його значення необхідно змінити на протилежне.

При спотворенні тільки перевірного елемента й правильному прийманні інформаційних елементів a_i' та a_k' буде тільки один незбіг контрольних і перевірних елементів, що вказує на помилкове приймання перевірного елемента, і ніяких виправлень роботи не потрібно. З принципу виправлення помилок у ланцюговому коді випливає, що правильне виправлення помилок можливе тільки у тому разі, коли два елемента з трьох, охоплені перевіркою, прийняті правильно.

Кодер двійкового ланцюгового коду містить *k*К-розрядний регістр і *n* суматорів за модулем 2. Узагальнена структурна схема кодера ланцюгового коду наведена не рис. 3.5.

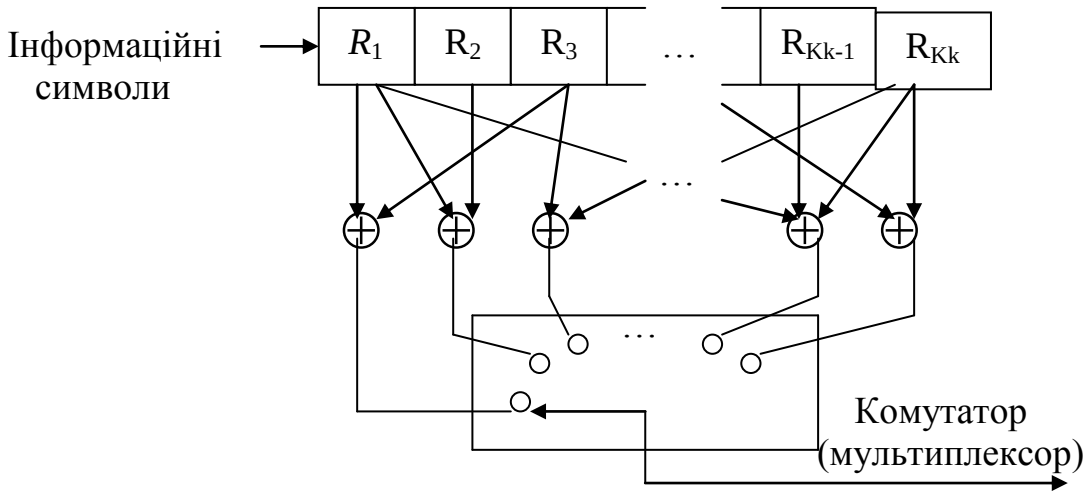


Рис. 3.5

Інформаційні символи поступають на вхід регістру, а символи коду формуються на виході комутатора. Комутатор послідовно протягом відрізку часу, який дорівнює тривалості інформаційного символу, з′єднує виходи суматорів за модулем 2 з виходом кодера.

Коректувальна здатність ланцюгового коду залежить від кроку додавання $t_{кр}$. Якщо кожний перевірний елемент перед передачею в канал затримати на час $T_з$ і пачки помилок, розташовані поруч, розділити захисним інтервалом А, який не містить спотворених елементів ($A = 6t_{кр} + 1$; $T_з = 3(t_{кр} + 1)\tau_e$, де τ_e – тривалість одного елемента), то ланцюговий код може виправити пачку помилок завдовжки $2t_{кр}$. Зміною довжини кроку $t_{кр}$ коректувальну здатність коду можна узгоджувати з характеристиками каналу зв′язку, зменшуючи чи збільшуючи допустиму частість помилок.

3.5. **Методи перестановок**

Зміна за визначеним правилом початкового слідування символів у деякій кодовій послідовності називається процедурою перестановок (рос. – перемежения; англ. – interleaving). Ще зустрічається такий вираз, як скремблірування (тобто, пристрій, який виконує перестановку за визначеним законом, – скремблер, той, що виконує зворотну перестановку, – дескремблер).

Методи перестановок звичайно використовуються для руйнування пакетів помилок великої довжини, які формуються, наприклад, при завмираннях сигналу, що приймається, і, як наслідок, зменшують степінь групування помилок в послідовності символів, що поступають на вхід канального декодера. При перестановці кодове слово, яке передається, формується із символів різних кодових слів. Тому при зворотній операції пакет помилок трансформується у послідовність незалежних помилок, для виправлення яких можна використати менш потужний код. Із збільшенням глибини перестановок можна очікувати поліпшення характеристик завадостійкості, оскільки при цьому послаблюється кореляція помилок. Однак при цьому зростає затримка повідомлення, яка пов′язана з виконанням процедур перестановки. Тому, зазвичай, треба приймати компромісне рішення між поліпшенням характеристик завадостійкості і можливою затримкою повідомлення.

Розглянемо деякі ефективні методи перестановок.

Блокова перестановка. При блоковій перестановці кодові слова довжиною n символів записуються у вигляді таблиці шириною W і глибиною D символів (див. рис. 3.6).

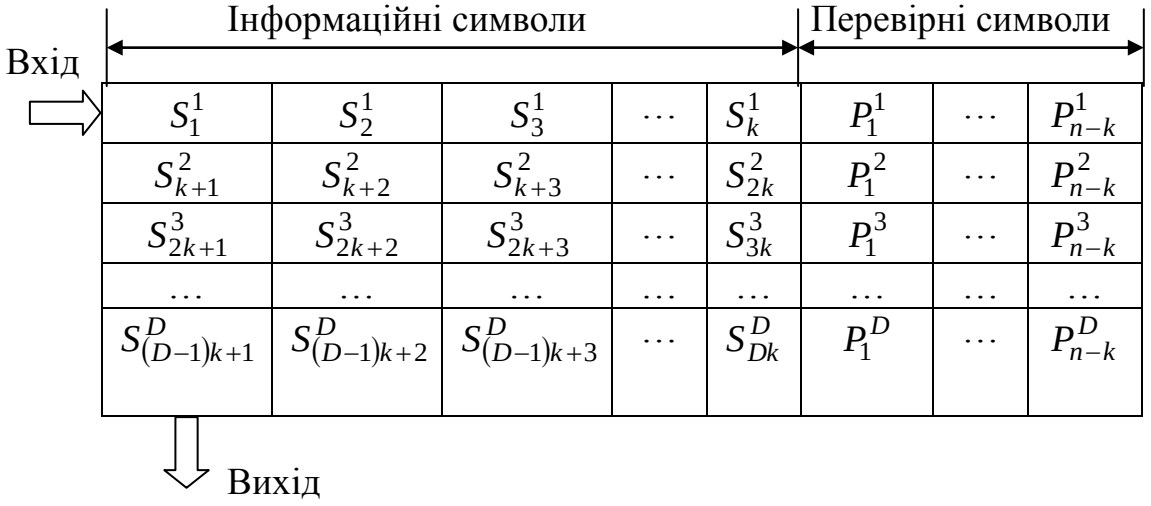


Рис. 3.6

Допустимо, що $W = n$. Тоді рядки таблиці подають кодові слова, які містять k інформаційних символів і $(n - k)$ перевірних символів. Після заповнення таблиці здійснюється послідовне зчитування символів за стовпцями та їх передача по каналу зв′язку. У приймачі виконується зворотна процедура – послідовний запис символів по стовпцях до повного заповнення таблиці. Потім виконується зчитування символів за рядками таблиці та їх декодування. Такий скремблер дозволяє зруйнувати пакет помилок довжиною $l < D$, в результаті чого у кожному кодовому слові буде не більше одної помилки. Однак періодична послідовність поодиноких помилок, що розташовані одна від одної на відстані D символів, призведе до повного ураження помилками якогось одного слова. Затримка при виконанні процедур скремблірування-дескремблірування дорівнює $2WD$ символів. Об′єм пам′яти і скремблера й дескремблера складає WD символів.

Можлива також інша послідовність перестановки, при якій інформаційні символи записуються не по рядках, а по стовпцях. Причому перевірні символи формуються із k інформаційних, які рознесені в початковій послідовності один від одного на D символів. Зчитування символів також здійснюється за стовпцями. Перевагою цього методу є передача інформаційних символів у природному порядку слідування і відсутність затримки в скремблері. Загальна затримка складає WD символів і обумовлена виконанням процедури дескремблірування. Параметри D і W обираються з урахуванням того, що ймовірні значення довжин пакетів помилок були менше D. Однак цей тип скремблера не є стійким по відношенню до періодичної послідовності поодиноких помилок, що рознесені на D символів. В цій ситуації усі символи в рядку будуть помилковими, і канальний декодер переповниться.

Міжблокова перестановка. При міжблоковій перестановці за вхідний блок приймається блок із NB символів, і кожний блок із N символів розподіляється між наступними B вихідними блоками. Нехай x та y подають вхідний та вихідний символи скремблера. Тоді правило відображення m-го символу i-го вхідного блоку в $(j + Bt)$-й символ $(i + j)$-го вихідного блоку можна визначити так:

$$y(i + j, j + Bt) = x(i, m)$$

для усіх i і при $j = m \bmod B$, $t = m \bmod N$.

Приклад міжблокової перестановки при $B = 3$ і $N = 2$ наведений на рис. 3.7. Символи i-го, $(i + 1)$-го і $(i + 2)$-го вхідних кодових блоків визначені відповідно a, b, c. Згідно приведеному правилу відображення

$$y(i + j, j + 3t) = x(i, m)$$

для усіх i і при $j = m \bmod 3$, $t = m \bmod 2$.

При $m = 0$ маємо $y(i, 0) = x(i, 0)$; $m = 1 – y(i + 1, 4) = x(i, 1)$; $m = 2 – y(i + 2, 2) = x(i, 2)$ і т.п.

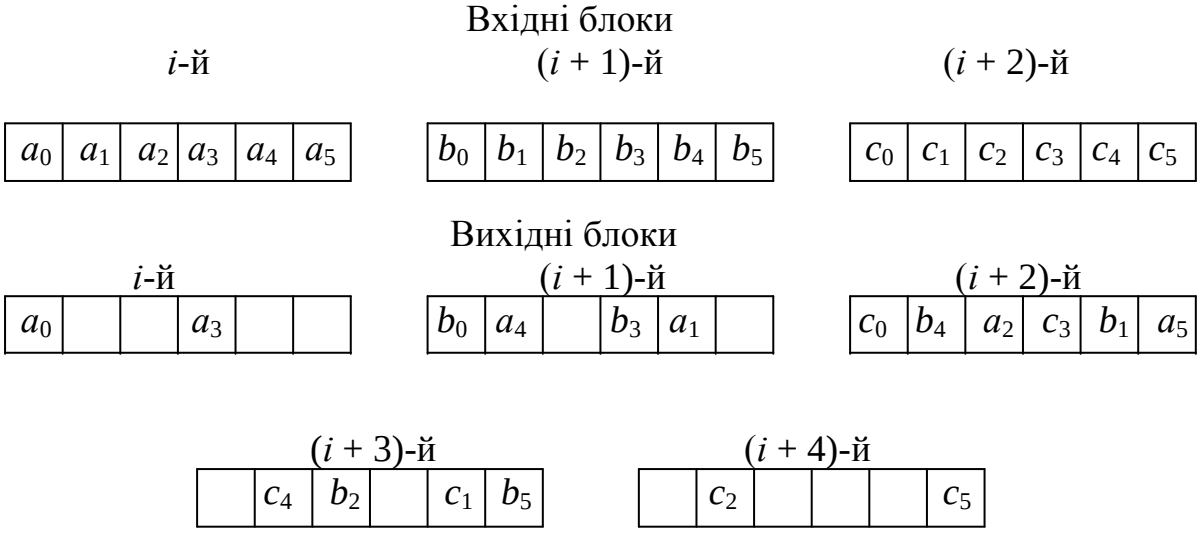


Рис. 3.7

Відмітимо, що символи, які послідовно слідують з i-го вхідного блоку відображаються у символах B вихідних блоків з нерегулярним зміщенням позицій $(j + Bt)$ у кожному блоці. Таке нерегулярне зміщення дозволяє зменшити вплив періодичної завади, що діє в каналі зв′язку. Для однозначного відображення символів необхідно, щоб B і N не мали загального дільника. Це обмежує свободу вибору довжини блока із BN символів. Недоліки такого методу перестановки є в тому, що вихідні сигнали розподіляються в межах B блоків, і загальна затримка складає B^2N символів (BN сим-

волів у зв′язку з необхідністю запам′ятовування $(B-1)BN$ вхідних блоків для виконання процедури розподілення символів).

Згорточна перестановка. Структурна схема згорточного скремблера-дескремблера наведена на рис. 3.8.

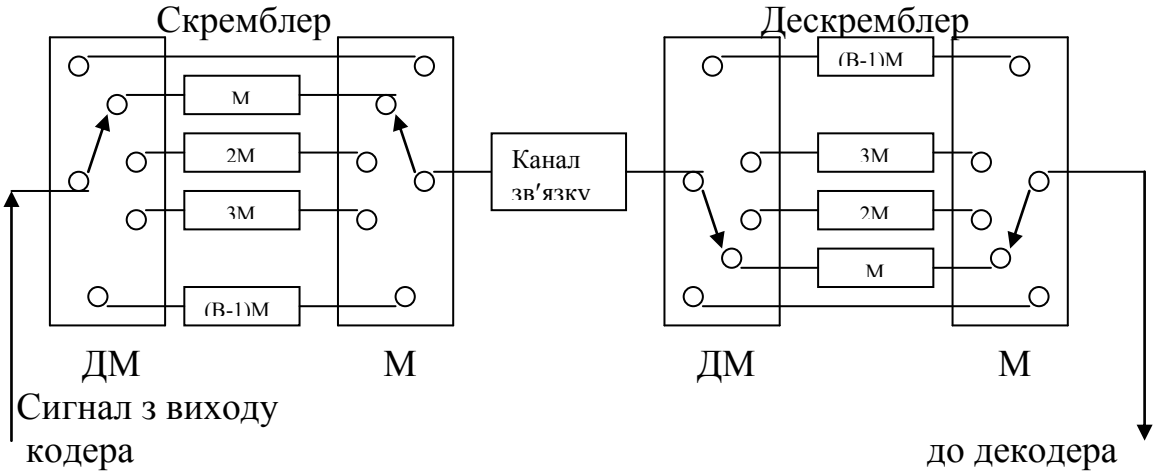


Рис. 3.8

Передбачається, що мультиплексори (М) і демультиплексори (ДМ) передавача і приймача синхронізовані. Демультиплексор здійснює послідовне підключення виходу кодера до різних рядків пам′яти скремблера. Мультиплексор відповідно підключає вхід декодера до різних рядків пам′яти дескремблера. Кожен з рядків пам′яти є регістром зсуву, кількість елементів затримки якого показано відповідним числом, що вписане у прямокутник. Перший елемент кодованої послідовності записується до верхнього рядка і одразу передається по каналу зв′язку. Записується він також у перший рядок пам′яти дескремблера, що забезпечує затримку на (В – 1)М символів. Другий елемент кодованої послідовності записується у другий рядок пам′яти скремблера, що забезпечує затримку на М символів. Таким чином, сусідні символи кодованої послідовності розносяться на М символів. При прийомі другий символ додатково затримується на (В – 2)М символів, так що загальна затримка символів складає (В – 1)М символів. Всі символи кодової послідовності після перестановки і зворотного перетворення мають однакову затримку, тому порядок слідування символів на виході кодера і вході декодера зберігається однаковим.

Розділ 4. ОСНОВНІ ПРИНЦИПИ ПОБУДОВИ КОДЕКІВ ЗАВАДОСТІЙКИХ КОДІВ

Кодування і декодування можуть бути реалізовані за допомогою спеціалізованих пристроїв, які, в свою чергу, будуються застосуванням різних сполучень на основі регістрів зсуву, суматорів за модулем 2 і елементів множення. Як правило, ця апаратура будується з використанням звичайних (стандартних) інтегральних і великих інтегральних схем і виконує відносно нескладні операції кодування і декодування.

Якщо операції кодування і декодування та коди, що застосовуються при цьому, значно ускладнюються, тоді для виконання залучають програмні методи. У цьому випадку необхідні операції здійснюються за допомогою універсальних ЕОМ, міні-ЕОМ або спеціалізованих процесорів. При обміні даними між ЕОМ для кодування і декодування може бути залучена частина обчислювальної потужності і пам′яти ЕОМ.

У цьому розділі посібника будуть в основному розглядатися стандартні схеми, які використовуються при апаратній реалізації кодування і декодування групових, циклічних та неперервних кодів.

Кодеки групових кодів. На рис. 4.1 наведена спрощена структурна схема кодера для (n, k) кода. Пристрій складається із n-розрядного регістра зсуву і r суматорів за модулем 2. Регістр містить дві частини: інформаційну (k-комірок) і перевірочну (r-комірок). Кожний суматор використовується для формування перевірочного символу, який має визначену позицію. Підключення інформаційних комірок регістру до відповідних суматорів виконується за правилами побудови даного коректувального коду.

Цифрова інформація у вигляді кодової комбінації первинного коду записується одночасно (паралельно) в k інформаційних комірок регістру. Одночасно з тим по всіх r двійкових суматорах здійснюється формування перевірочних символів, які записуються в r перевірочних комірках регістру. Наступним етапом є виведення отриманої кодової комбінації з регістру. Це забезпечується подачею тактових імпульсів (імпульсів зсуву) від генератора тактових імпульсів (ГТІ). Після n тактових імпульсів кодова комбінація буде виведена з регістру, і ГТІ відключається від регістру для подальшої підготовки останнього до запису й формування наступної кодової комбінації. Кодова комбінація з виходу регістра поступає на модулятор передавальної частини системи зв′язку.

Формування коректувальних кодів за допомогою регістрів зсуву розповсюджено дуже широко. Цей метод простий в реалізації, дозволяє створювати високонадійні схеми і забезпечує можливість зміни параметрів

коду у процесі роботи. Дійсно, якщо змінити частоту тактових імпульсів, то зміниться тривалість кожного символу і відповідно енергія кодової комбінації та швидкість передачі. Якщо при цьому узгоджено (за командою) змінити відповідні параметри в прийомному пристрої, то можна отримати адаптивну (у деякому розумінні) систему зв′язку.

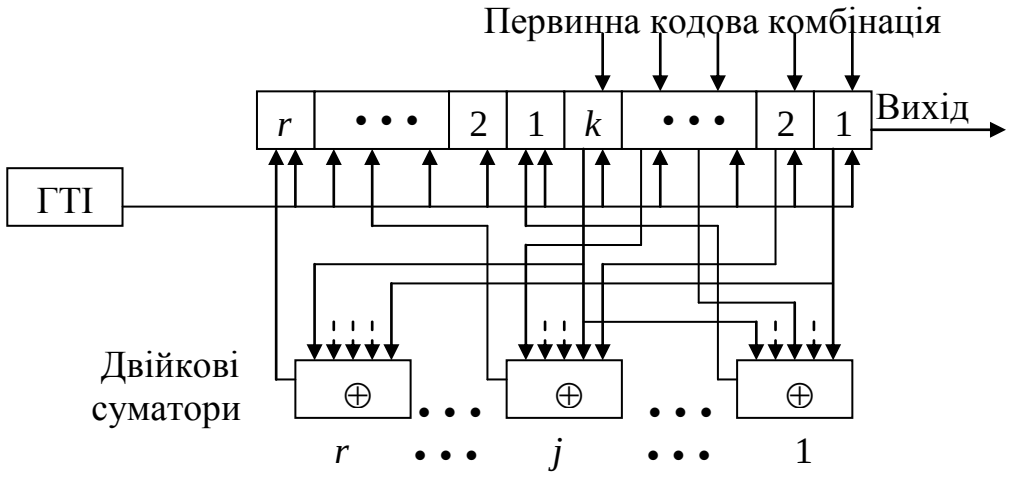


Рис. 4.1

Розглянемо принцип роботи декодуючого пристрою, спрощена структурна схема якого наведена на рис. 4.2. Пристрій складається з n тригерних комірок, r суматорів за модулем 2 і аналізатора помилок.

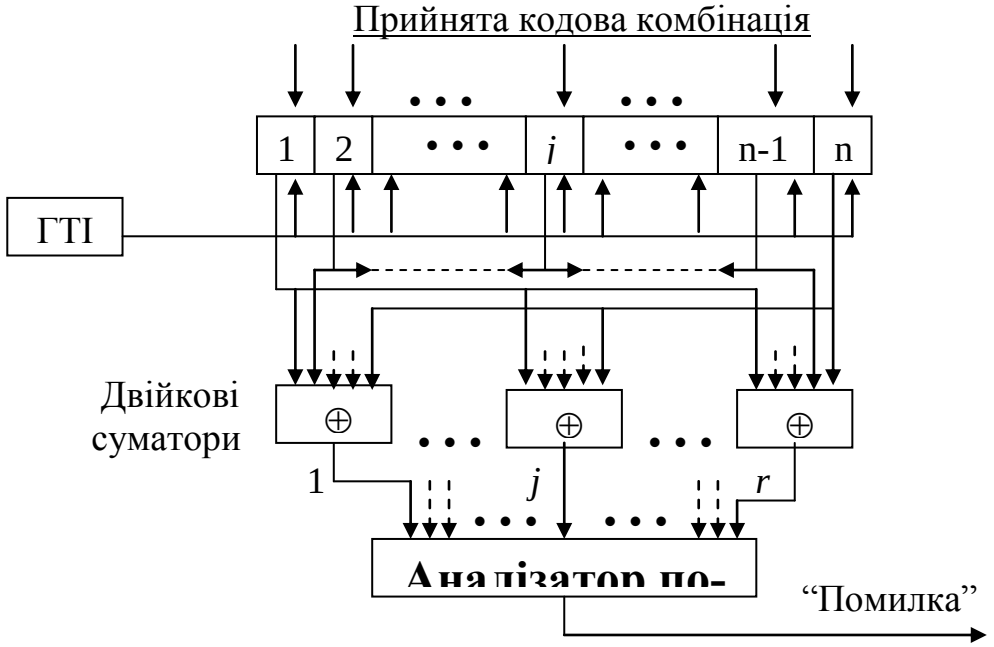


Рис. 4.2

Послідовність символів прийнятої кодової комбінації (частка цих символів може бути прийнята з помилками внаслідок дії завад) записується в n комірок регістру, і за допомогою суматорів проводиться перевірка на парність для r підмножин інформаційних і перевірочних символів, які при кодуванні формуються за визначеними для даного коду правилами. Якщо у прийнятій кодовій комбінації помилок немає, то на виході всіх суматорів формуються символи, що відповідають нулю. Якщо помилкові символи є, то на виході деяких суматорів будуть символи, що відповідають одиниці, оскільки умова перевірки на парність в цих суматорах не виконується. Аналізатор помилок у цьому випадку видає сигнал: «помилка».

Розглянемо структурні схеми кодера і, відповідно, декодера конкретного групового коду (7, 4).

Структурна схема кодера наведена на рис. 4.3.

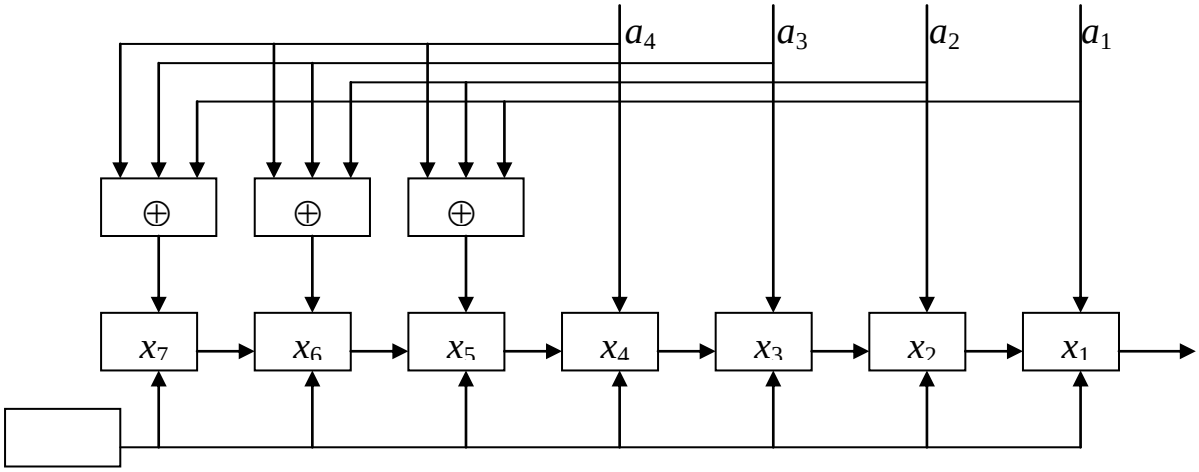


Рис. 4.3

Основу кодера складає семиелементний зсувний регістр і три суматори за модулем 2 на три входи кожний. Як елементи регістра, що виконують затримку символів на один такт, можна використати синхронні тригери з настановними входами.

Кодове слово у вигляді паралельного коду безпосередньо записується в перші чотири елементи регістру ($x_1 = a_1$, $x_2 = a_2$, $x_3 = a_3$, $x_4 = a_4$). Перевірочні символи формуються за правилом $x_5 = a_1 \oplus a_2 \oplus a_4$; $x_6 = a_2 \oplus a_3 \oplus a_4$; $x_7 = a_1 \oplus a_3 \oplus a_4$. Після заповнення всіх елементів регістру його зміст завдяки дії зсувних імпульсів поступає в канал у вигляді семиелементного послідовного коду.

При збільшенні надмірності коду і ускладненні пристрою перевірки та аналізу помилок декодуючий пристрій зможе не тільки виявляти помилки при прийомі окремих символів, а також виправляти деякі з них. Це при-

зведе до значного ускладнення схеми декодера порівняно зі схемою, яка наведена на рис. 4.2. Декодер повинен містити додаткові пристрої для запам′ятовування виправляємої кодової комбінації, логічні пристрої для виправлення символів на тих позиціях кодової комбінації, де вони були прийняті помилково, і т.п.

Розглянемо, як приклад, принцип виправлення помилок в процесі декодування (7, 4)-кода (див. рис. 4.4).

Прийняте кодове слово **Y** після заповнення прийомного регістру (на рис. не показаний) переписується паралельним кодом у семибітний запам′ятовуючий пристрій (ЗП). Елементами пам′яті ЗП можуть бути, наприклад, асинхронні тригери. Схема визначення синдрому містить три суматори за модулем 2 на чотири входи кожний. На виході кожного суматора формуються елементи вектора **S**. Зіставлення кожному з синдромів одного з векторів помилок здійснюється за допомогою дешифратора. Дешифратор має три входи і $2^3 = 8$ виходів, на кожному з яких формується одиничний символ у відповідності з таблицею 4.1.

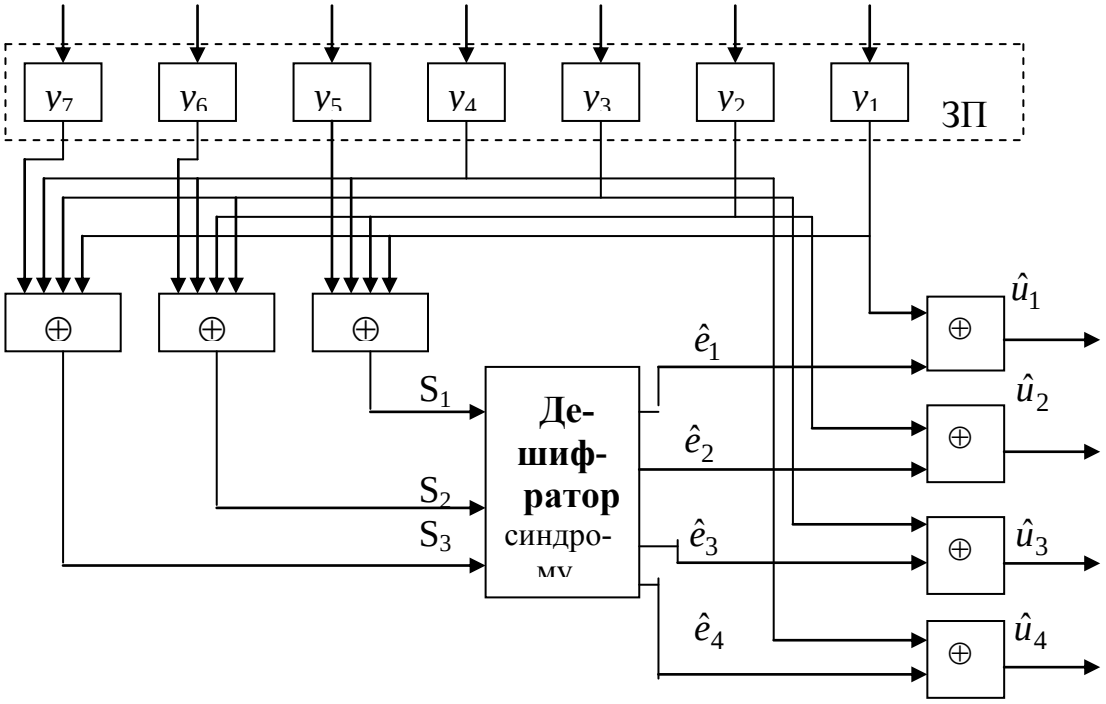


Рис. 4.4

Подільний код дозволяє отримати оцінку $\hat{U}$, якщо скористатися скороченими векторами $\mathbf{e_y} = e_1e_2e_3e_4$ і $\mathbf{Y_y} = y_1y_2y_3y_4$, які визначають тільки помилки у інформаційній частині кодового слова $\hat{U} = \mathbf{Y_y} \oplus \mathbf{e^*_y}$.

У зв′язку з цим з восьми виходів дешифратора використовуються тільки чотири, тобто дешифратор формує один із скорочених векторів по-

милок: $e_{1y} = 1000$, $e_{2y} = 0100$, $e_{3y} = 0010$, $e_{4y} = 0001$. Схема, яка реалізує оцінку $\hat{U}$, складається з чотирьох двовхідних суматорів за модулем 2 (за кількістю компонент скороченого вектору помилок). До одного входу кожного з суматорів подається інформаційний символ кодового слова $\mathbf{Y_y} = y_1y_2y_3y_4$, до другого – відповідний символ вектору $\mathbf{e^*_y}$. У результаті на виходах суматорів формується оцінка $\hat{U}$ у вигляді паралельного чотирьохелементного коду.

Таблиця 4.1

Вектор помилок	Синдром
$e_0 = 0\,0\,0\,0\,0\,0\,0$	$S_0 = 0\,0\,0$
$e_1 = 1\,0\,0\,0\,0\,0\,0$	$S_1 = 1\,0\,1$
$e_2 = 0\,1\,0\,0\,0\,0\,0$	$S_2 = 1\,1\,0$
$e_3 = 0\,0\,1\,0\,0\,0\,0$	$S_3 = 0\,1\,1$
$e_4 = 0\,0\,0\,1\,0\,0\,0$	$S_4 = 1\,1\,1$
$e_5 = 0\,0\,0\,0\,1\,0\,0$	$S_5 = 1\,0\,0$
$e_6 = 0\,0\,0\,0\,0\,1\,0$	$S_6 = 0\,1\,0$
$e_7 = 0\,0\,0\,0\,0\,0\,1$	$S_7 = 0\,0\,1$

Наприклад, треба передати $U_7 = 0111$, якому відповідає кодове слово $X_7 = 0111010$. Припустимо, що під впливом завад в каналі спотворений другий символ у X_7, тобто прийняте кодове слово $Y = 0011010$. Елементи синдрому при цьому дорівнюють: $S_1 = 0 \oplus 0 \oplus 1 \oplus 0 = 1$; $S_2 = 0 \oplus 1 \oplus 1 \oplus 1 = 1$; $S_3 = 0 \oplus 1 \oplus 1 \oplus 0 = 0$. Відповідно табл. 4.1 дешифратор сформує скорочений вектор $e_{2y} = 0100$, тобто на другому виході дешифратора буде одиничний символ, на інших – нульові. В результаті на виході другого суматора за модулем 2, що формує оцінку компоненти u_2, символ зміниться на протилежний. Отримана оцінка $\hat{U} = 0111$ співпадає з переданим повідомленням, тобто $\hat{U} = U_7$ (правильний прийом).

Припустимо тепер, що у переданому слові X_7 спотворились два символи, наприклад, перший і останній, тобто прийнято $Y = 1111011$. Тоді отримаємо: $S_1 = 1$; $S_2 = 0$; $S_3 = 0$. Відповідно табл. 4.1 скорочений вектор помилок буде дорівнювати нулю, оскільки одиничний символ повинен бути на п′ятому виході дешифратора, який не використовується. В результаті отримаємо оцінку $\hat{U} = 1111$, що не співпадає з переданим повідомленням (помилковий прийом).

Численні дослідження довели, що для кодів з великою коректувальною спроможністю (які, відповідно, являють собою послідовності з великою кількістю символів n), кількість операцій при оптимальному декоду-

ванні зростає експоненціально зі збільшенням числа надмірних символів. Ці обставини значно ускладнюють технічну реалізацію декодерів. Тому в останні роки велика увага приділяється питанням розробки таких методів декодування, для яких залежність числа потрібних операцій від довжини кодової послідовності є не експоненціальною, а степеневою або лінійною функцією. У даний час розроблені два підходи до вирішення задачі спрощення процедури декодування: імовірнісний і алгебричний.

При імовірнісному чи послідовному декодуванні уся сукупність можливих кодових комбінацій (включаючи дозволені і недозволені) ділиться на дві групи: високоймовірні й малоймовірні. Якщо прийнята комбінація ближче до високоймовірної групи, вона декодується одразу без перевірки. Якщо ж прийнята комбінація ближче до малоймовірних комбінацій, то при декодуванні виконується перевірка і виправлення помилок. Таким чином, сильно спотворені комбінації виправляються, а слабко спотворені декодуються без виправлення. Таке декодування значно поступається у завадостійкості оптимальному, однак воно значно простіше у реалізації.

При алгебричному декодуванні виправляється тільки визначена частина помилок, тобто коректувальні можливості коду використовуються частково. Це означає, що застосовується неоптимальний алгоритм декодування, який дозволяє більш просту схемну реалізацію. З точки зору спрощення операції декодування особливо зручні циклічні і безперервні (рекурентні) коди.

Кодеки циклічних кодів. Алгебричний опис циклічних кодів базується на такому понятті лінійної алгебри, як кільце.

Кільце – це адитивна група, в якій уведена операція множення елементів, і для цієї операції виконується закон замкнутості.

Далі під елементами кільця будемо розуміти множину $N = 2^n$ *n*-елементних комбінацій, поданих у вигляді многочленів деякої змінної *x*. Показники степеню *x* відповідають номерам елементів комбінації, а коефіцієнти приймають значення 1 або 0 відповідно зі значенням символів на даній позиції. Найбільший степінь *x* у доданку з ненульовим коефіцієнтом зветься степенем многочлена. Кодова *n*-елементна комбінація, подана у вигляді многочлена змінної *x*, є кодове слово. Наприклад, кодова комбінація 10011 подається кодовим словом $1\cdot x^0 + 0\cdot x^1 + 0\cdot x^2 + 1\cdot x^3 + 1\cdot x^4 = 1 + x^3 + x^4$ у вигляді многочлена четвертого степеня.

Для виконання умови замкнутості кільця операція множення многочленів у ньому задається так:

– многочлени перемножуються за звичайними правилами зі зведенням подібних членів за модулем 2;

– якщо вищий степінь добутку не перевищує $n - 1$, то результатом множення є отриманий добуток;

– якщо вищий степінь добутку перевищує або дорівнює n, то многочлен добутку ділиться на біном $1 + x^n$, і результатом множення приймається остача від ділення.

Степінь остачі при цьому не буде перевищувати $n - 1$, і, відповідно, цей многочлен буде належати кільцю.

Уведена операція множення многочленів кільця зветься узяттям остачі або приведенням за модулем $1 + x^n$.

Розглянемо показану на рис. 4.5 схему множення фіксованого многочлена $b(x) = 1 + x^2 + x^3 + x^5 + x^7$ на вхідний многочлен $a(x) = a_0 + a_1x + \ldots + a_mx^m$.

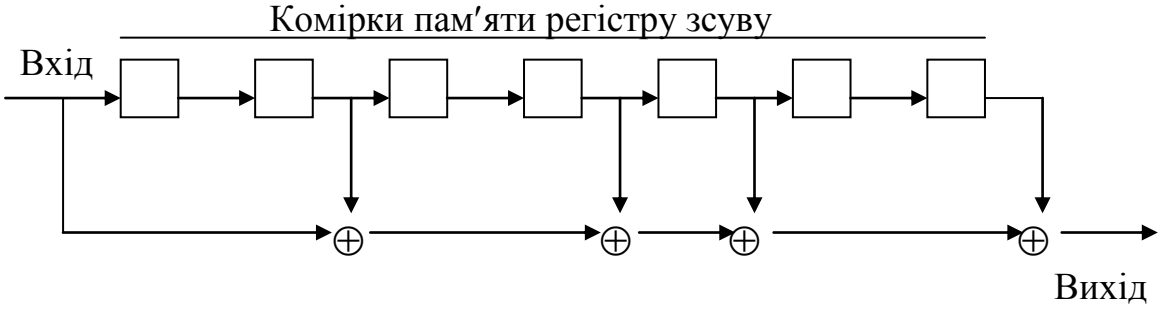


Рис. 4.5

На початку всі комірки пам′яти регістру зсуву містять нульові символи. Приймемо, що на вхід регістру зсуву першими подаються члени з більшими степенями. Член a_mx^m без змін подається на вихід. Також без змін подається на вихід схеми $a_{m-1}x^{m-1}$. Після того, як на вхід регістру зсуву поступить $a_{m-2}x^{m-2}$, за допомогою крайнього лівого суматору він додається до a_mx^m, що поступив раніше, і їх сума $a_{m-2}x^{m-2}\cdot x^7 + a_mx^m\cdot x^5 = (a_{m-2} + a_m)\cdot x^{m+5}$ поступає на вихід схеми. Так само обчислюються наступні члени добутку.

У загальному випадку множення вхідного многочлена $a(x) = a_0 + a_1x + \ldots + a_mx^m$ на фіксований многочлен $b(x) = b_0 + b_1x + \ldots + b_nx^n$ можна виконати аналогічно (див. рис. 4.6).

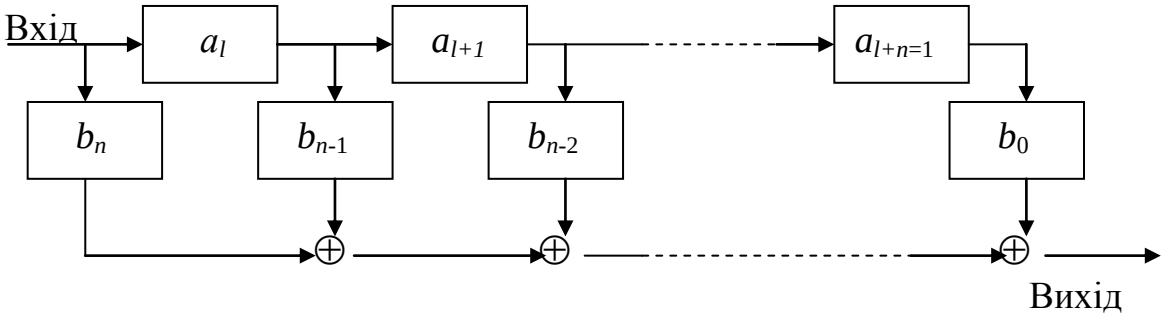


Рис. 4.6

Існує ще один тип схем, які призначені для отримання вказаного вище добутку. На рис. 4.7 приведена схема множення многочлена $a(x)$ на фіксований многочлен $b(x) = 1 + x^2 + x^3 + x^5 + x^7$, а на рис. 4.8 – для загального випадку множення $a(x)$ на $b(x)$.

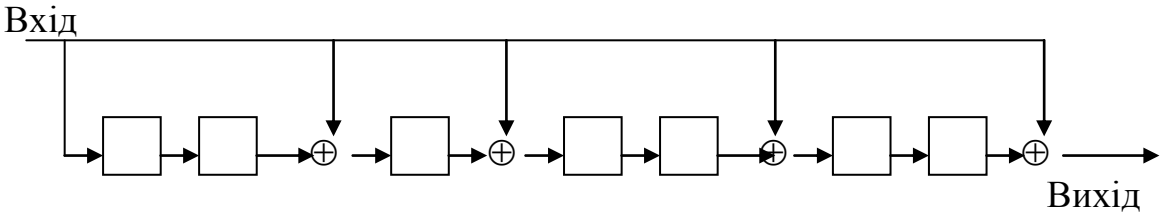


Рис. 4.7

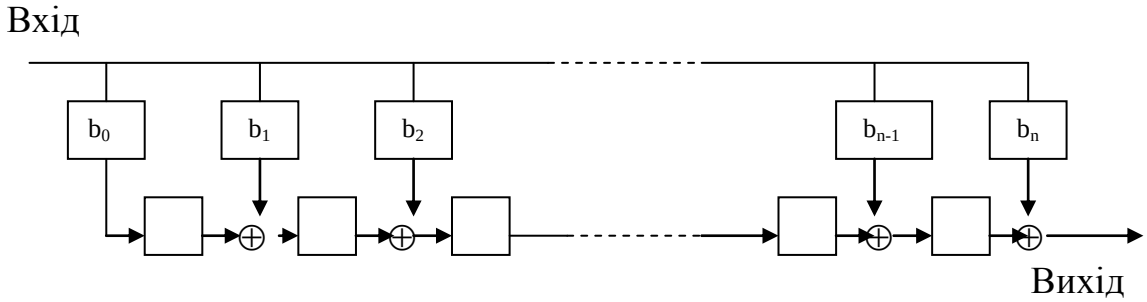


Рис. 4.8

На перший погляд схеми (рис. 4.5, 4.6, 4.7, 4.8) не дуже різняться одна від одної, оскільки містять ту ж саму кількість розрядів регістру зсуву і суматорів за модулем 2. Однак у схемі рис. 4.8 суматори за модулем 2 розміщуються між розрядами регістру зсуву, а в схемі рис. 4.6 суматори розташовані окремо від регістру зсуву. Така побудова схеми множення (рис. 4.6) більш зручна при використанні інтегральних схем.

Основою побудови циклічних кодуючих і декодуючих пристроїв є також схеми ділення. Приклад схеми ділення многочлена $a(x)$ на многочлен $b(x) = 1 + x^2 + x^3 + x^5 + x^7$ приведений на рис. 4.9, а для загального випадку – на рис. 4.10.

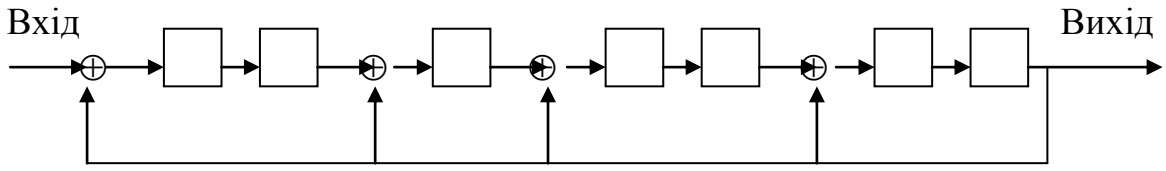


Рис. 4.9

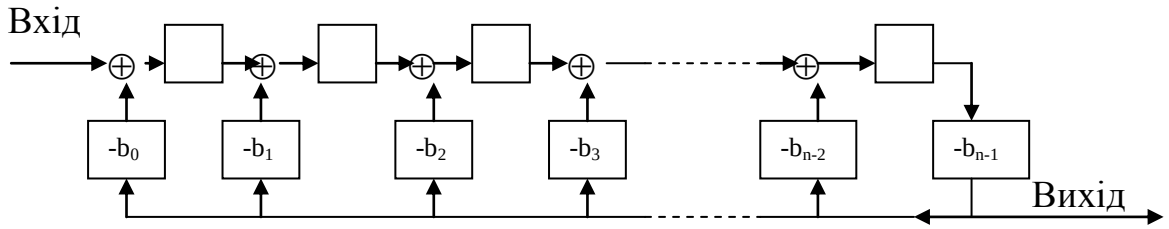


Рис. 4.10

При діленні $a(x)$ на $b(x)$ за допомогою схеми, що приведена на рис. 4.9, спочатку в регістр зсуву послідовно уводяться коефіцієнти вхідного многочлена при x^{10}, …, x^4. При приході до входу регістра коефіцієнта при x^3 коефіцієнт при x^{10} на вході поступає на вихід схеми як коефіцієнт при x^3 остачі. Одночасно коефіцієнт при x^{10} з виходу регістру подається на входи трьох суматорів за модулем 2, які встановлені на виходах 3, 4 і 5-й зліва комірок пам′яти регістру зсуву, і додає їх до вихідних символів цих комірок. При наступному зсуві коефіцієнт 0 при x^9 вхідного многочлена виводиться як 0 при x^2 остачі. При наступному зсуві символ 0, який отриманий в результаті додавання коефіцієнта 1 при x^8 вхідного многочлена з коефіцієнтом 1 при x^{10}, що поступає по колу зворотного зв′язку, виводиться як коефіцієнт 0 при x^1 остачі. Після уведення всіх символів вхідного многочлена в регістрі залишиться остача $x + x^2 + x^3 + x^4 + 0 + x^6$.

Всі кодові слова циклічного коду діляться на породжувальний (твірний) многочлен коду $b(x)$. Якщо циклічний код є, до того ж систематичним, то у кожному кодовому слові можна виділити інформаційні і перевірні (надмірні) символи. Тому при використанні циклічних кодів спочатку по каналу зв′язку передаються інформаційні символи й одночасно ці символи уводяться в схему ділення многочленів, принцип роботи якої був описаний вище. Після того, як усі інформаційні символи уведені в регістр зсуву, в останньому виявляється остача від ділення інформаційного многочлену на твірний многочлен. Якщо цю остачу передати по каналу зв′язку після інформаційних символів, то повна передана послідовність буде ділитися на $b(x)$, тобто буде кодовим словом.

Циклічні коди дозволяють побудувати достатньо прості схеми кодерів на основі використання регістрів зсуву зі зворотними зв′язками через суматори за модулем 2. З алгоритмів кодування/декодування циклічних кодів слідує, що ці операції засновані на використанні операції ділення многочлену на многочлен. Як відомо (див. вище), процес ділення у цьому випадку являє собою додавання за модулем 2 коефіцієнтів подільника з коефіцієнтами при старших степенях діленого, а потім з коефіцієнтами при

старших степенях остач до тих пір поки степінь остачі не стане меншим за степінь діленого. Ці операції реалізуються на базі регістрів зсуву із зворотними зв′язками. Регістри зсуву являють собою послідовне з′єднання елементів пам′яти (для двійкового коду – тригери). Елементи пам′яти регістру ще називають його комірками, або розрядами. Для здійснення ділення многочлену $a(x)$ на многочлен $b(x)$ будується спеціальний регістр зсуву зі зворотними зв′язками, який відповідає подільнику, тобто многочлену $b(x)$. Розглянемо правила побудови регістрів зсуву зі зворотними зв′язками:

– кількість комірок регістру повинно дорівнювати степеню многочлена подільника $b(x)$;

– кількість суматорів за модулем 2 у колі зворотного зв′язку обирають на одиницю меншою числа ненульових членів многочлена $b(x)$ (сума коефіцієнтів при старших розрядах діленого й подільника завжди дорівнює нулю);

– входи комірок регістру помічають x^i, $i = 0, 1, 2, \ldots, \deg b(x)$;

– суматори за модулем 2 встановлюються на входах тих комірок, для яких в формулі многочлена $b(x)$ коефіцієнти при відповідних степенях дорівнюють одиниці;

– вихід останньої комірки з′єднується з одним із входів суматорів;

– виходи попередніх комірок з′єднуються із входами наступних через суматори або без них (в залежності від їх наявності).

Розглянемо це на прикладі циклічного (7, 4)-коду на основі п′ятирозрядного регістру зсуву (див. рис. 4.11).

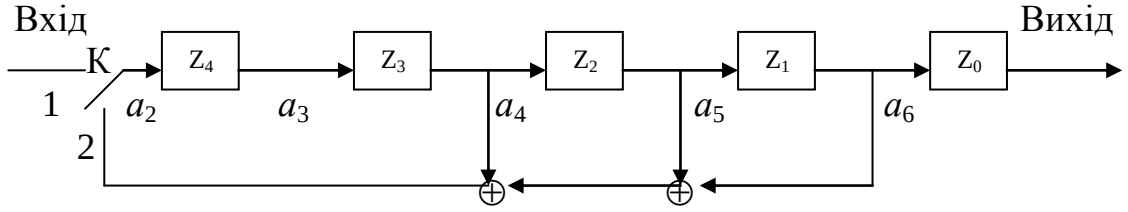


Рис. 4.11

У вихідному стані ключ К находиться в положенні 1. Протягом перших чотирьох тактів інформаційні символи заповнюють комірки регістру Z_1, Z_2, Z_3, Z_4 (Z_0 - буферна комірка). Після цього ключ переводиться у положення 2, і на вході Z_4 сформується перевірний символ, який відповідає коефіцієнту a_2 (перевірними для даного кодеру прийняті перевірні символи, що відповідають коефіцієнтам a_0, a_1, a_2). На п′ятому такті відбувається видача першого інформаційного символу (коефіцієнт a_6) до каналу

і одночасний зсув символів зі входів на виходи всіх комірок регістру. В результаті на виходах комірок Z_1, Z_2, Z_3 значення символів будуть визначатися коефіцієнтами a_5, a_4, a_3 відповідно, і на вході Z_4 сформується другий перевірочний символ a_1. На шостому такті на виходах Z_1, Z_2, Z_3 будуть коефіцієнти a_4, a_3, a_2, і на вході Z_4 сформується третій перевірочний символ a_0. Одночасно другий інформаційний символ видається до каналу. На цьому процес формування перевірочних символів закінчується, ключ К переводиться у положення 1. Протягом наступних чотирьох тактів зміст регістру видається до каналу й одночасно відбувається заповнення комірок новою інформаційною послідовністю.

Декодування циклічних кодів можна проводити різними методами. Основними з них є: синдромне декодування; декодування, засноване на обчисленні остачі від ділення прийнятої кодової комбінації на твірний поліном коду; мажоритарне декодування.

При будь-якому методі декодування до складу декодера уводиться буферний n-елементний регістр для збереження прийнятої комбінації на час проведення операції виявлення помилок.

Метод синдромного декодування не відрізняється від методу, який застосовується для групових (n, k)-кодів.

Декодування за методом обчислення остачі від ділення засноване на тому, що будь-яке кодове слово при діленні на твірний поліном дає нульову остачу. Якщо прийняте кодове слово внаслідок завад трансформувалося у заборонене, то остача від ділення буде відрізнятися від нуля. Причому для всіх дозволених кодових слів помилка на одній і тій же позиції дає однакову остачу, за видом якої помилку можна виправити.

Мажоритарний метод декодування заснований на використанні системи контрольних перевірок для одного або декількох символів кодового слова циклічного коду. Результат кожної перевірки поступає на входи мажоритарного елемента, в якому приймається рішення про значення прийнятого символу a_i «за більшістю». При цьому сформована система контрольних перевірок може бути застосована для декодування всіх символів кодового слова. Це слідує з того, що контрольним співвідношенням задовольняють всі дозволені кодові слова, в тому числі й отримані з прийнятого дозволеного циклічним зсувом. Тому для декодування символу a_{i+k} за допомогою системи перевірок, яка сформована для a_i, достатньо виконати k-кратний зсув і використати той же мажоритарний елемент.

Загальна можлива схема декодера циклічного коду приведена на рис. 4.12. Прийняте кодове слово у цьому декодері одночасно уводиться в буферний регістр і схему ділення поліномів, яка зображена під ним. Після уведення прийнятого слова в схему ділення в регістрі зсуву залишиться ос-

тача від ділення прийнятого слова на твірний поліном коду; у залежності від того, дорівнює остача нулю або ні, приймається рішення щодо відсутності або наявності помилок у ньому.

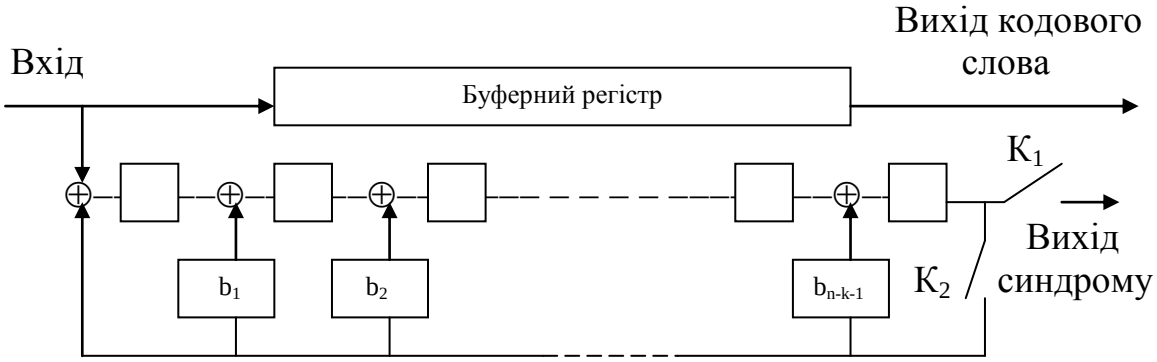


Рис. 4.12

Ключ $К_1$ замикається на час проходження інформаційних символів, ключ $К_2$ – на час проходження перевірних елементів.

Кодеки неперервних (рекурентних або згорточних) кодів. Схеми підключення суматорів за модулем 2, значення кількості інформаційних елементів k, довжини кодової комбінації n і довжини кодового обмеження К повністю описують неперервний код. Наприклад, код, який формується за допомогою кодеру, що зображений на рис. 4.13, має твірні вектори $g_1 = 111$ та $g_2 = 101$ і твірні поліноми $g_1(x) = x^2 + x + 1$ та $g_2(x) = x^2 + 1$.

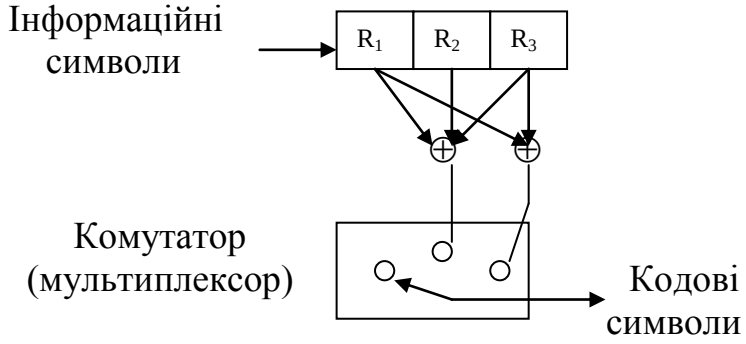


Рис. 4.13

Рекурентний код може бути завданий імпульсною характеристикою, що визначається послідовністю символів коду на виході кодера при подачі на його вхід єдиного символу 1. Легко перевірити, що імпульсна характеристика даного коду дорівнює 111011 (див. рис. 4.13). Оскільки операція додавання за модулем 2 є лінійною, вихідна послідовність кодеру може розглядатися як результат згортання вхідної послідовності з імпульсною

характеристикою кодера. Це й обумовило виникнення назви коду і методу кодування – згорточні.

Поведінку кодеру можна повністю описати за допомогою діаграми станів, що зображена на рис. 4.14. Якщо кодер має стан *a* і на його вхід поступає 1, то на виході буде формуватися комбінація 11 і кодер перейде до стану *b*, який відповідає $R_3 = 0$ і $R_2 = 1$. Аналогічно, при наявності на вході символу 0 кодер збереже стан *a*, а на виході буде комбінація 00.

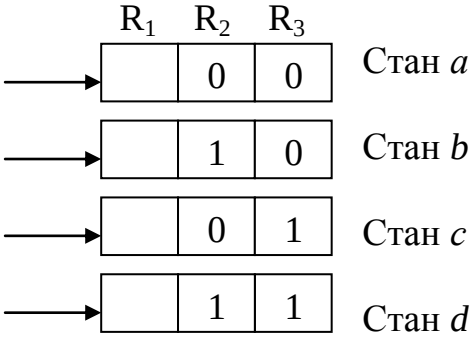


Рис. 4.14

Прямий перехід зі стану *a* до стану *c* або *d* неможливий. Прямий перехід з будь-якого стану можливий тільки до одного з двох станів.

Іншим корисним способом опису є ґратчаста діаграма, що зображена на рис. 4.15.

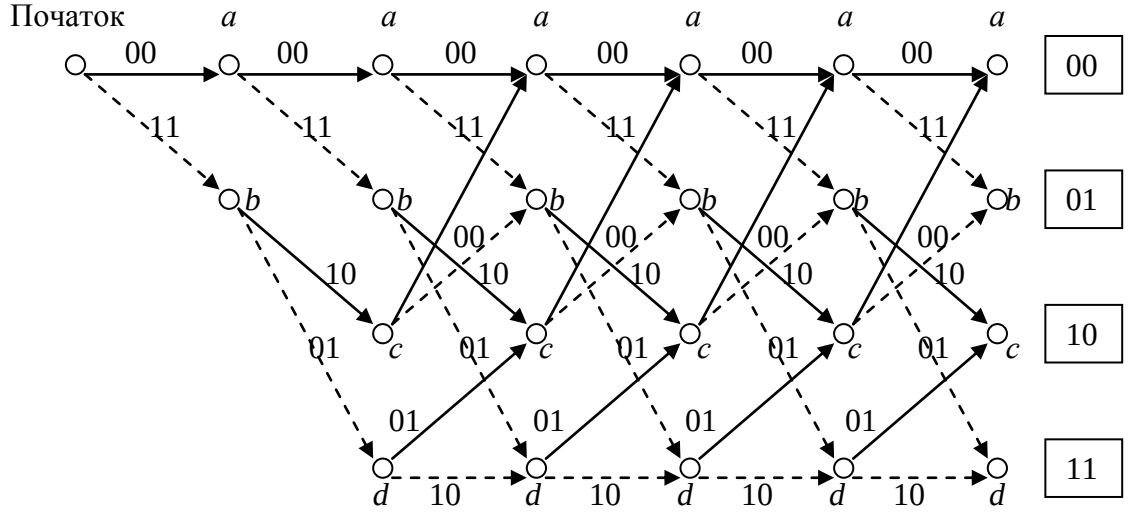


Рис. 4.15

Діаграма бере початок зі стану *a* і на ній відображаються усі можливі переходи при надходженні на вхід чергового символу. Суцільним лініям відповідають переходи при надходженні символу 1, пунктирним – символу 0. При надходженні на вхід двох символів кодер переходить до одного з чотирьох станів: *a, b, c* або *d*. Гратчаста діаграма повторюється і тому може бути легко побудована за допомогою діаграми станів.

Алгоритм декодування Вітербі. Серед різних алгоритмів декодування рекурентних кодів алгоритм максимальної правдоподібності Вітербі (АВ) отримав найбільше поширення в системах зв′язку, де необхідно забезпечити економію енергетичного ресурсу.

При декодуванні за критерієм максимальної правдоподібності із множини можливих кодових слів обирається те, що ближче розташоване до прийнятого кодового слова у просторі кодових слів. Оскільки маємо 2^K кодових слів, то при реалізації АВ треба забезпечити запам′ятовування всіх кодових слів та їх порівняння з прийнятим кодовим словом. Із зростанням К складність обчислювань і, відповідно, декодеру, зростає.

Вітербі запропонував спрощену процедуру обчислення при реалізації алгоритму максимальної правдоподібності. Він помітив, що кожний із чотирьох вузлів має тільки двох попередників, тобто кожного з цих вузлів можна дістатися, минаючи тільки два вузли (див. рис. 4.15), і тільки один шлях, що відповідає послідовності, яка найбільш близька до прийнятої послідовності (шлях з мінімальною відстанню), треба зберігати для кожного вузла. На прикладі гратчастої діаграми завдання є у тому, щоб для деякої прийнятої послідовності знайти на неї шлях, який відповідав би вихідній послідовності, яка максимально співпадає з прийнятою послідовністю.

При реалізації АВ об′єм пам′яти та складність обчислювань пропорційні 2^K, і тому його зручно використовувати при довжині кодового обмеження $K < 10$. При більших довжинах кодового обмеження, які необхідні для досягнення низьких значень вірогідності помилки, зазвичай використовується алгоритм послідовного декодування.

Алгоритм послідовного декодування. При послідовному декодуванні, алгоритм якого був запропонований Возенкрафтом, складність декодеру зростає лінійно із зростанням довжини кодового обмеження. Для опису особливостей алгоритму розглянемо кодер з $K = 4$ і $n = 3$, зображений на рис. 4.16. Кожний вхідний інформаційний символ породжує три кодових символи і впливає на чотири групи з трьох символів. При декодуванні треба розглядати тільки три (або n) символів одночасно, щоб прийняти проміжне рішення, яке передбачає можливість його зміни при виникненні труднощів у майбутньому.

Декодер, що реалізує алгоритм послідовного декодування, можна порівняти з водієм, який приймає невірні рішення на розвилці шляху, однак швидко виявляє свої помилки (за допомогою шляхових покажчиків), вертається назад і рухається по новому шляху.

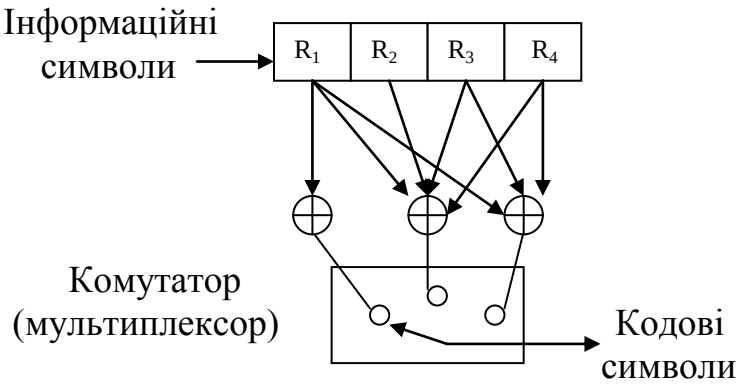


Рис. 4.16

Стосовно алгоритму, що розглядається, це означає наступне. З початкового вузлу n_1 для перших трьох прийнятих символів є два шляхи довжиною три символи. Вибирається той шлях, який відповідає послідовності, що має найменшу відстань Хеммінга від перших трьох прийнятих символів. В результаті вибирається найбільш імовірний вузол. З цього вузла також виходять два шляхи, довжина яких дорівнює трьом символам. Для другої групи з трьох прийнятих символів також вибирається шлях, що відповідає послідовності з мінімальною відстанню Хеммінга, і здійснюється перехід до четвертого вузла. Якщо має місце велика кількість помилок у визначених групах з n прийнятих символів, то був обраний помилковий шлях, при русі по якому будуть мати місце труднощі узгодження прийнятої послідовності символів із послідовностями, що відповідають хибному вузлу. Це є основою для прийняття рішення про помилку при виборі шляху.

Основним є питання про вибір критерію за яким приймається рішення про вибір хибного шляху. Залежність математичного очікування кількості помилок n_{E} від кількості символів d, що декодуються, є пряма ($\bar{n}_E = P_{\text{b}}d$) із нахилом, який визначається імовірністю помилки P_{b}, приведена на рис. 4.17. Там же показано правдиве значення кількості помилок, відповідне обраному шляху. Якщо кількість помилок лежить у визначених межах, встановлених межовим рівнем, то декодування продовжується. В іншому випадку здійснюється перехід назад до ближнього вузла і робляться спроби розшукати інший шлях. Якщо кількість помилок продовжує зростати,

то повернення здійснюється до наступного за порядком вузла, і так до тих пір, доки кількість помилок не буде у допустимих межах.

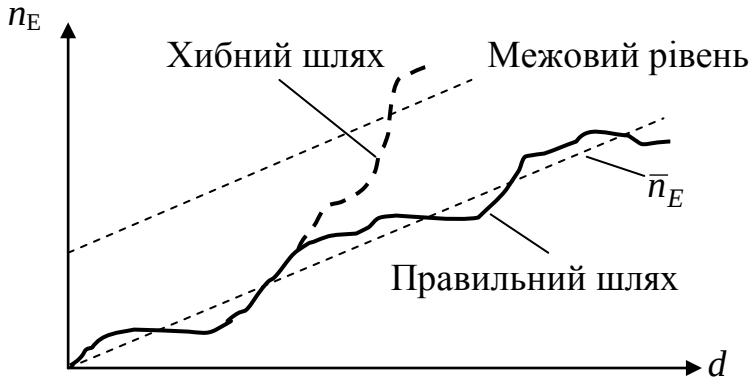


Рис. 4.17

Якщо значення межового рівня обрати близьким до математичного очікування кількості помилок, це скоротить середній обсяг обчислювань. З іншого боку, якщо значення межового рівню встановити занадто «жорстким» (тобто дуже близьким до математичного очікування кількості помилок), то при декодуванні будуть відкидатися всі можливі шляхи у деяких дуже нечастих випадках, коли за рахунок впливу шуму може трапитися надзвичайно велика кількість помилок. Це явище може бути враховане шляхом вибору «жорсткого» межового рівня на початку процесу декодування, і якщо при декодуванні будуть відкидатися всі шляхи, то межовий рівень поступово збільшується, доки не буде розшуканий один з можливих шляхів.

При послідовному декодуванні ймовірність помилки зі збільшенням К зменшується за експоненціальним законом, а його складність – за лінійним. При цьому середня кількість хибних шляхів, які аналізуються, на один символ, що декодується, залишається обмеженим, якщо величина $\eta = 1/n$ буде меншою межової обчислювальної швидкості η_0.

Алгоритм послідовного декодування має такі недоліки:

– кількість хибних ділянок і, відповідно, обчислювальна складність є випадковою величиною, яка залежить від рівня завад у каналі зв′язку;

– для зниження необхідного об'єму пам′яти швидкість декодування повинна у 10…20 разів перевищувати швидкість надходження вхідних даних, що обмежує максимальну швидкість передачі повідомлень;

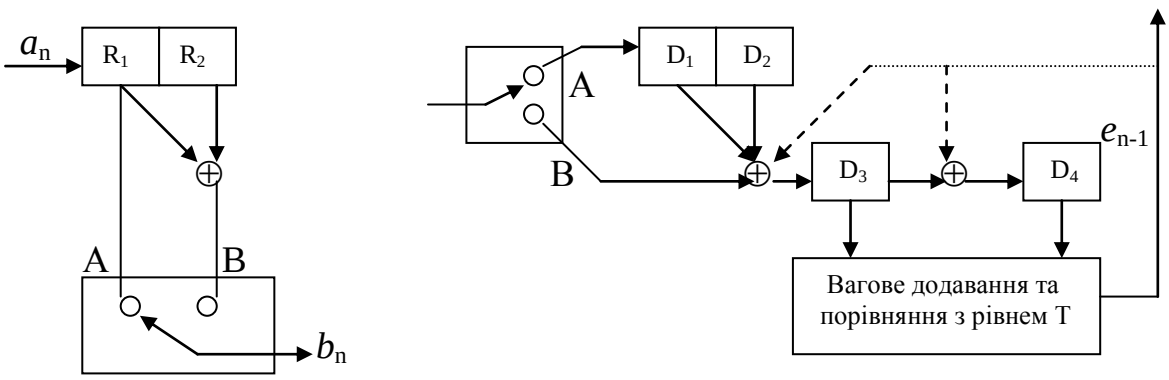
– середня кількість хибних ділянок шляху, що аналізуються, епізодично може бути надзвичайно великою і призведе до переповнення

пам′яти, а це може привести до появи порівняно довгих вихідних послідовностей, які містять велику кількість помилок.

Характеристики завадостійкості рекурентних кодів при використанні цих алгоритмів в основному можуть бути отримані тільки методами математичного моделювання.

До найбільш простих алгоритмів декодування рекурентних кодів відносяться алгоритм декодування із зворотним зв′язком та алгоритм межового (мажоритарного) декодування. Однак характеристики цих алгоритмів значно поступаються тим двом, що були розглянуті вище.

Межове декодування. Розглянемо приклад, що ілюструє можливості межового декодування. Структурна схема кодера зображена на рис. 4.18,а. Нехай зміст розрядів регістру є $R_1 = a_n$ і $R_2 = a_{n-1}$, а вихідна послідовність (b_n, $b_n \oplus b_{n-1}$). Структурна схема межового декодера зображена на рис. 4.18,б.



а б

Рис. 4.18

Послідовність символів на вході кодеру

$$(b_n \oplus e_n^1, b_n \oplus b_{n-1} \oplus e_n^2),$$

де e_n^1, e_n^2 - послідовність символів вектору помилок, які виникають у каналі зв′язку при передачі першого і другого символів відповідно. Ключ в положенні А при декодуванні першого символу і в положенні В при декодуванні другого символу відповідно.

$$D_1 = b_n \oplus e_n^1,$$

$$D_2 = b_{n-1} \oplus e_{n-1}^1,$$

$$D_3 = b_n \oplus b_{n-1} \oplus e_n^2 \oplus D_1 \oplus D_2 = e_n^1 \oplus e_{n-1}^1 \oplus e_n^2,$$

$$D_4 = e_{n-1}^1 \oplus e_{n-2}^1 \oplus e_{n-1}^2.$$

При відповідних значеннях відношення сигнал/шум в D_3 і D_4 міститься достатньо інформації для надійного рішення.

Якщо D_3 і D_4 дорівнюють 1, то маємо дві можливості. По-перше, символ e_{n-1}^1 дорівнює 1, по-друге $e_{n-1}^1 = 0$, тоді e_n^1 або e_{n-1}^2 дорівнюють 1 і e_{n-2}^1 або e_{n-1}^2 дорівнюють 1. Для малих імовірностей помилки в каналі ймовірність того, що e_{n-1}^1 дорівнює 1, приблизно є p_1. В іншій ситуації потрібно, щоб у послідовності $e_n^1, e_n^2, e_{n-1}^1, e_{n-1}^2$ мали місце дві помилки. Імовірність цієї події p_1^2. Таким чином, якщо і D_1 і D_2 дорівнюють 1, то з великою ймовірністю e_{n-1}^1 дорівнює 1. Оцінити це можна за допомогою схеми з рівнем, встановивши його значення 0,5. Якщо рівень перевищується, то з великою імовірністю визначається помилка у попередньому інформаційному символі (код систематичний).

Імовірність появи помилки при декодуванні визначається імовірністю того, що в послідовності $e_n^1, e_n^2, e_{n-1}^1, e_{n-1}^2 e_{n-2}^1$ більше одної помилки. Імовірність цієї події

$$P_E = \sum_{i=1}^{5} \binom{5}{i} \cdot p_1^i (1 - p_1)^{5-i}.$$

Для малих значень p_1 – $P_E = 10 p_1^2$.

При малих значеннях p_1 зниження імовірності помилки стає відчутним.

Розділ 5. СИГНАЛИ ЗІ ШТУЧНИМ РОЗШИРЕННЯМ СПЕКТРУ

Системи зв'язку із широкосмуговими сигналами (ШСС) з притаманими їм можливостями за ослабленням дії завад знаходять все більше поширення в системах радіозв'язку. Наприклад, вони використовуються в системах зв'язку короткохвильового діапазону для боротьби з багатопроменевістю, у системах мобільного зв'язку з багатостанційним доступом і кодовим або часовим розподілом каналів, у системах супутникового зв'язку і т.п.

Під широкосмуговою розуміють таку систему передачі інформації, в якій сигнал займає смугу частот, що суттєво перевищує мінімально необхідну для передачі цієї інформації.

Розширення спектра сигналу повинно здійснюватись незалежно від повідомлення, що передається за допомогою того чи іншого способу модуляції або кодування , котрий повинен бути відомим на стороні прийому.

Таке штучне розширення спектра можна зробити порізному.

Спектр аналогового повідомлення може бути значно розширено при застосуванні ЧМ з великим індексом модуляції.

$$\Delta f_{\text{ЧМ}} = 2m_{\text{ЧМ}} \cdot F_{\lambda}$$

Однак таке розширення спектра пов′язане безпосередньо з повідомленням, що передається, тому ЧМ сигнал не підходить під визначення “широкосмугового”.

Широкосмуговість сигналу визначається не абсолютним значенням його смуги частот, а ступенем розширення спектра (частотною надмірністю). Наприклад, телевізійні сигнали займають смугу частот у декілька мегагерц. Однак вони не відносяться до класу широкосмугових, бо ширина спектра ТВ сигналу приблизно дорівнює ширині спектра повідомлення (відеосигналу).У той же час, якщо якась система зв'язку буде використовувати смугу у декілька мегагерц для передачі мовного сигналу, то вона буде широкосмуговою.

Уведене визначення широкосмугового сигналу відноситься як до аналогових, так і до цифрових повідомлень. У подальшому розгляд властивостей широкосмугових систем зв'язку будемо вести відносно цифрових систем передачі.

Технологія розширення спектру сигнала полягає у навмисному збільшенні у передавачі смуги частот, яку займає сигнал-носій повідомлення, до величин, що значно перевищують необхідні для передачі з потрібною швидкістю і рівнем спотворень, і зворотному її зменшенні до початкового значення у приймачі системи зв′язку. Внаслідок виконання операції розширення спектру відбувається зменшення рівня спектральної щільності

сигналу, який передається. що утрудняє виявлення факту роботи системи зв′язку і перехоплення повідомлень, які передаються.

Завдяки низькому рівню спектральної щільності сигналів з розширеним спектром таки системи зв′язку можуть використовувати зайняті ділянки радіочастотних діапазонів, не створюючи завад іншим системам зв′язку.

При зворотній операції стискання спектру відбувається встановлення початкового спектру сигналу-носія повідомлення і розширення спектрів сигналів природних і штучних завад. Оскільки в інформаційну смугу попадає частина енергії сигналів завад, розподіленої в широкій смузі частот, то в результаті забезпечується збільшення відношення сигнал/завада (визначається відношенням смуг частот до і після стискання).

Методи модуляції з розширенням спектру сигнала можна класифікувати у відповідності з тим, за яким параметром радіосигналу (амплітуді, фазі, частоті чи часовому положенню – затримці) здійснюється модуляція сигналом, що розширює спектр.

Оскільки для забезпечення високого коефіцієнта корисної дії (к.к.д.) вихідних каскадів передавача амплітуду бажано зберегти постійною, то на даний час найбільше розповсюдження отримали методи розширення спектру, основані на зміні їх фази, частоти і часового положення (затримки) у відповідності з визначеним законом. Серед цих методів можна виділити наступні базові:

– безпосередня модуляція носійної частоти псевдовипадковою послідовністю (ПВП), інакше кажучи, псевдовипадкова частотна або фазова маніпуляція; в результаті формується сигнал, що називають сигнал з прямим розширенням спектру;

– програмне перестроювання робочої частоти (ППРЧ), яке призводить до формування сигналу зі стрибкоподібною зміною носійної частоти;

– програмне перестроювання часового положення імпульсних сигналів або псевдовипадкова часо-імпульсна модуляція (ПЧІМ); при цьому отримуються імпульси зі стрибкоподібною зміною часового положення;

– частотна модуляція за лінійним законом (ЛЧМ); у цьому випадку миттєва частота радіосигналу протягом інтервалу часу, який дорівнює тривалості сигналу, або зростає, або зменшується за лінійним законом, що веде до формування ЛЧМ сигналів з різними законами зміни частоти.

Властивості і характеристики ШСС. Важливою характеристикою ШСС є база сигналу. Під базою сигналу розуміють відношення ширини спектра сигналу Δf_c до ширини спектра повідомлення ΔF

$$B = \Delta f_c / \Delta F.$$

База ШСС кількісно характеризує частотну надмірність, що уводиться в сигнал. У вузькосмугових системах із звичайними видами модуляції база сигналу близька до одиниці (рис. 5.1). ШСС, як правило, мають базу набагато більшу за одиницю. Наприклад, якщо для розширення спектра використовують внутрішньосистемне кодування з фазовою маніпуляцією (посилка довжиною T розбивається на L елементів, що відрізняються початковими фазами, зміна яких відбувається за якимось законом), то база такого сигналу буде дорівнювати L.

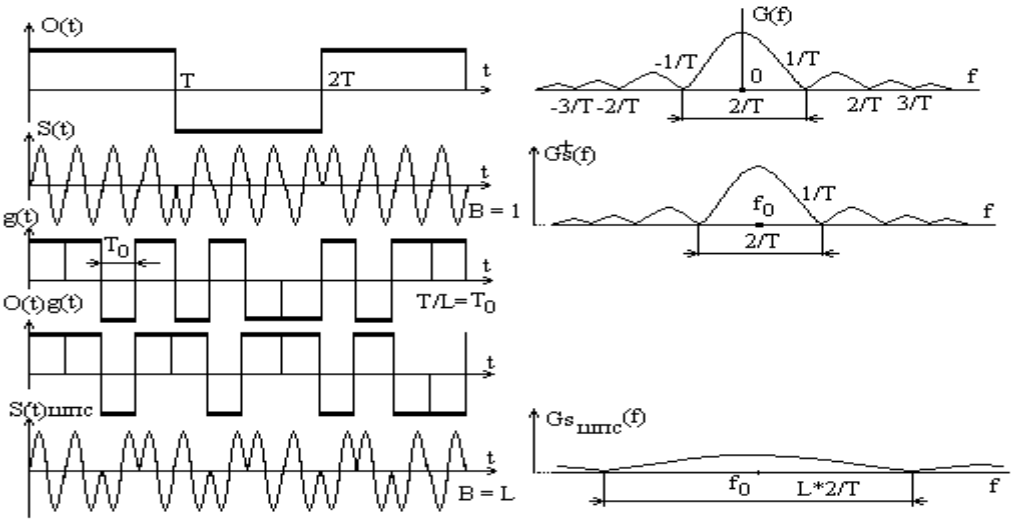


Рис.1

Рис. 5.1

ШСС мають такі гарні властивості:

– висока завадостійкість в умовах організованих завад;

– скритність передачі (мала вірогідність виявлення і перехоплення повідомлень);

– можливість зв'язку декількох абонентів у загальній смузі частот (багатостанційний доступ на основі кодового розподілу каналів);

– висока точність оцінки часу приходу сигналу (боротьба з багатопроменевістю, можливість часової синхронізації, точний вимір дальності до кореспондента);

Підвищена завадостійкість ШСС при дії завад є їх найважливішою властивістю.

Згадаємо, що завадостійкість прийому сигналів на фоні широкосмугової завади ($\Delta f_{\text{п}} > \Delta f_{\text{с}}$) типу білого гаусовського шуму (БГШ) з спектральною щільністю потужності (СЩП) $N_0/2$ визначається тільки величиною

$Q = 2E / N_0$, де $E = P_C \cdot T$ – енергія сигналу, P_C – потужність сигналу і не залежить від виду сигналу.

Тому при заданій СЩП завади завадозахищеність оптимального приймача ШСС до широкосмугових завад дорівнює завадозахищеності оптимального прийому вузькосмугових сигналів за цих умов .

З іншого боку, для передавача завад противника , як правило, існують обмеження не на СЩП завад, а на потужність $P_з$ передавача завад. При цьому ширина спектра завади підтримується меншою або рівною ширині спектра сигналу ($\Delta f_з \le \Delta f_с$) . В умовах $P_з$ = const, ($\Delta f_з > \Delta f_с$), використання ШСС забезпечує значне підвищення відношення сигнал/шум Q відносно вузькосмугових сигналів.

Дійсно, нехай $\Delta f_з = \Delta f_с = B \cdot \Delta F$. При цьому відношення сигнал/шум на виході кореляційного приймача (або узгодженого фільтра) дорівнює:

$Q = 2E/N_0 = (2P_cT)$: $(P_з/\Delta f_с) = (\Delta F = 2/T, T = 2/\Delta F) = 4B \cdot P_с/P_з$.

Це співвідношення показує, що відношення сигнал/шум при оптимальному прийомі ШСС збільшується пропорційно базі сигналу. При дії вузькосмугової завади ($\Delta f_з << \Delta f_с$) остання може бути виключеною за допомогою режекторного фільтра. При цьому потужність корисного сигналу на виході фільтра зменшується не набагато (рис. 5.2).

Суть скритності передачі ШСС пов′язана зі зменшенням СЩП сигналу внаслідок збільшення його бази. Дійсно, при рівності потужностей вузькосмугового і широкосмугового сигналів, СЩП ШСС з великою базою може бути значно менше СЩП шуму на вході розвідувального приймального пристрою. Тому при невідомій структурі ШСС вірогідність його виявлення мала. Крім цього, ефект зменшення СЩП у В разів при ШСС у ряді випадків дозволяє забезпечити ЕМС радіосистем (рис. 5.3).

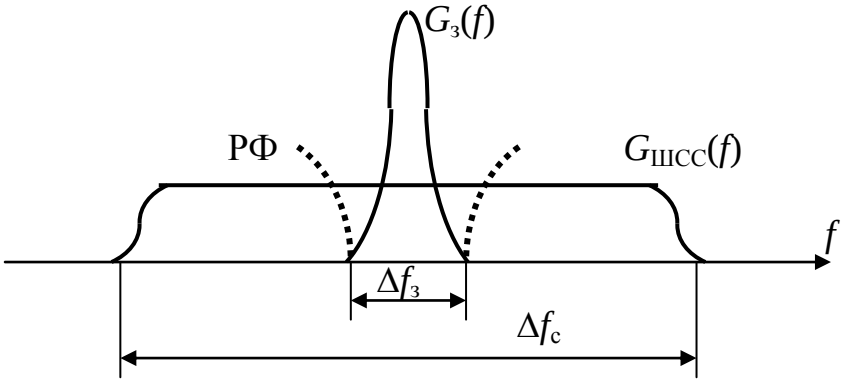


Рис. 5.2

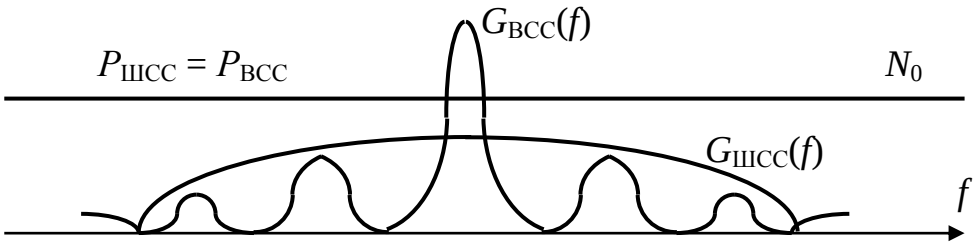


Рис. 5.3

Багатостанційний доступ різних абонентів у загальній смузі частот може бути забезпечений при кодовому розподілі каналів на основі використання ШСС. При кодовому розподілі окремі абоненти мають різну форму ШСС (розширення спектра частот відбувається на основі способів модуляції або кодування, різних для кожного каналу). Сигнали різних абонентів вибирають такими, щоб вони були приблизно ортогональні:

$$\int S_i(t) \cdot S_j(t) \cdot dt \approx 0.$$

Ця умова забезпечується при великих базах вибором спеціальних кодових послідовностей для кожного з каналів. Зазначимо, що кодовий розподіл каналів не дозволяє досягти збільшення числа каналів у порівнянні з методами частотного або часового розподілу, однак при кодовому розподілі підвищується завадостійкість і скритність системи радіозв'язку.

Висока точність оцінки часу приходу сигналу (розрізнювальна спроможність) забезпечується тим, що при оптимальній обробці ШСС узгодженим фільтром на його виході формується відгук, пропорційний кореляційній функції сигналу. Оскільки ШСС має кореляційну функцію з вузьким піком, ширина якого зворотно пропорційна базі ШСС (або ширині спектра сигналу Δf_c), то при прийомі ШСС досягається висока розрізнювальна спроможність сигналів за часом (див. рис. 5.4).

У багатопроменевих каналах вузька функція кореляції ШСС дозволяє в точці прийому розділити сигнали окремих променів і тим самим позбавитись інтерференції сигналів, що приймаються.

Різновиди псевдовипадкових та поріднених їм послідовностей. У загальному випадку до ПВП, що використовуються для розширення спектру сигналів, повинні задовольняти наступним вимогам:

– великий об′єм ансамблю послідовностей, які формуються за допомогою єдиного алгоритму;

– «добрі» авто- та взаємокореляційні властивості послідовностей, що входять до складу ансамблю;

– максимальний період для завданої довжини регістру зсуву, який формує послідовність;

– непередбачуваність структури послідовності за її неспотвореним сегментом обмеженої довжини.

У відповідності з алгоритмами формування різні ПВП можна класифікувати на лінійні, нелінійні, комбіновані і каскадні.

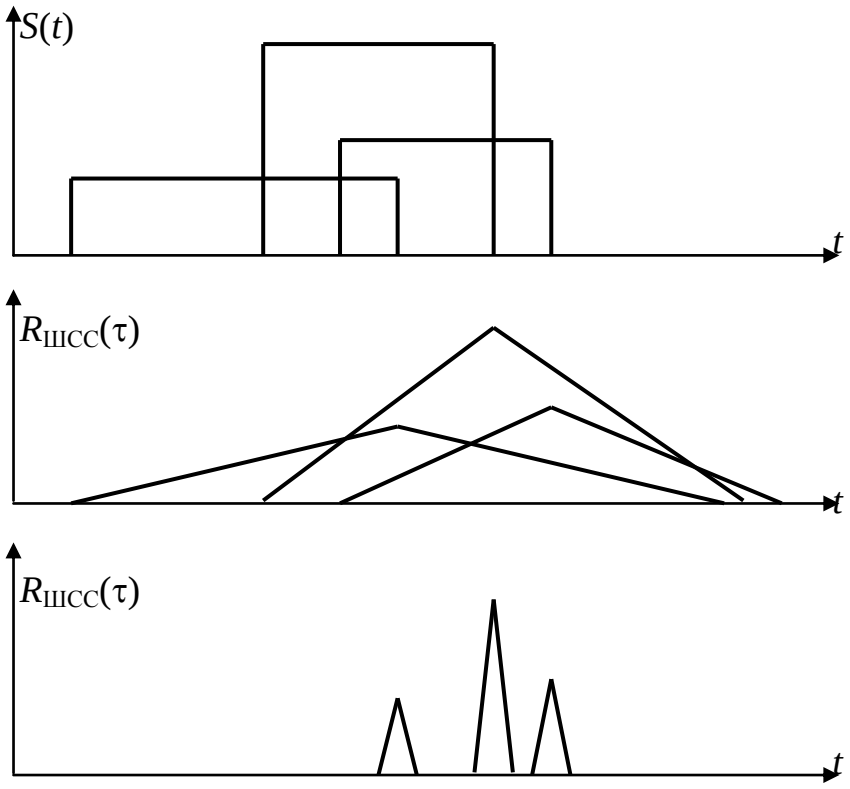


Рис. 5.4

Закон формування лінійних ПВП визначається лінійним рекурентним співвідношенням

$$a_j = \sum_{i=1}^{n} c_i a_{j-i} = a_j c_1 + a_{j-1} c_2 + \ldots + a_{j-n} c_n,$$

де множення та додавання здійснюються за модулем 2, а коефіцієнти c_i приймають значення 0 або 1 і визначаються характеристичним многочленом

$$f(D) = D^n + c_{n-1} D^{n-1} + \ldots + c_1 D + 1.$$

Структурна схема генератора лінійної ПВП у вигляді регістру зсуву із лінійним зворотним зв′язком через суматори за модулем 2 зображена на рис. 5.5.

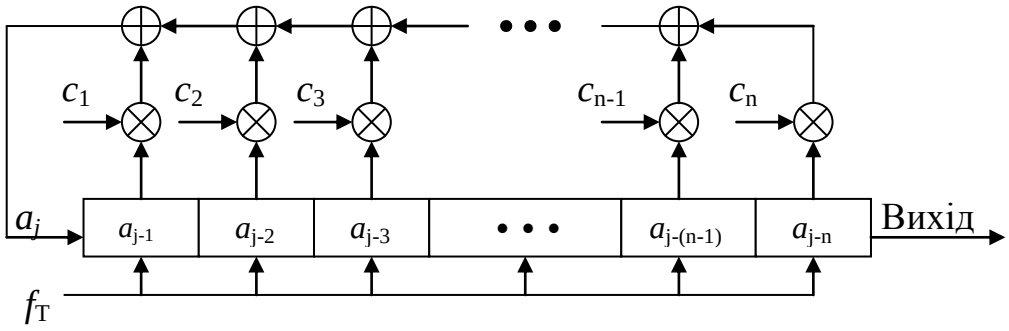


Рис. 5.5

Для формування нелінійних ПВП маються наступні можливості:

– використання зовнішньої нелінійної логічної функції для комбінування елементів ПВП з періодом $L = 2^n - 1$, яка отримана за допомогою регістру зсуву із лінійним зворотним зв′язком;

– використання регістрів зсуву з нелінійною логічною функцією у колі зворотного зв′язку (внутрішня логічна функція), яка дозволяє отримати ПВП з періодом $L = 2^n$.

Комбіновані послідовності є результатом об′єднання за визначеним правилом двох або більше лінійних ПВП.

Іншими варіантами формування комбінованих послідовностей є часове мультіплексування та мажоритарне додавання лінійних ПВП з різними періодами.

Особливості формування каскадних ПВП є у використанні декількох ступенів отримання лінійних ПВП таким чином, що вихідна послідовність попереднього ступеня управляє тактуванням наступного ступеня.

Методи формування та обробки ШСС. Формування ШСС тривалістю T і смугою частот Δf_c у більшості випадків засноване на його складенні з L елементарних сигналів зі смугою частот Δf_k і тривалістю Δt_k. Величини Δf_k і Δt_k для будь-якого k-го елементарного сигналу (k = 1,…,N) задовольняють умовам

$$1/T \le \Delta f_k \le \Delta f_c\,, \qquad 1/\Delta f_c \le \Delta t_k \le T.$$

Закон, за яким розміщуються величини Δf_k і Δt_k у обмеженій значеннями 0 – T, 0 – Δf_c частотно-часовій зоні, називається частотно-часовою матрицею ШСС.

Всі основні види сигналів можна відобразити за допомогою трьох частотно-часових матриць (рис. 5.6). Відповідно з цим розрізняють: паралельні (рис. 5.6,а), послідовні (рис. 5.6,б) і послідовно-паралельні (рис. 5.6,в) ШСС.

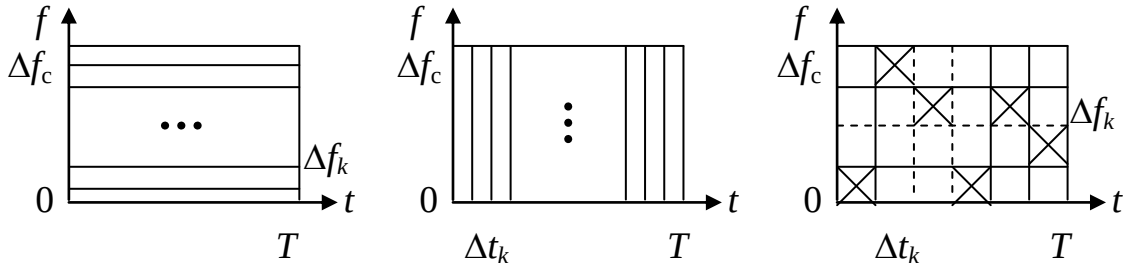
Тривалості і смуги сигналів для будь-яких k ≠ j задовольняють умовам:

– паралельні – $\Delta t_k = \Delta t_j = T,\ 1/T \le \Delta f_k = \Delta f_j < \Delta f_c$;

– послідовні – $1/\Delta f_c \le \Delta t_k = \Delta t_j < T,\ \Delta f_k = \Delta f_j = \Delta f_c$;

– послідовно-паралельні – $1/\Delta f_c \le \Delta t_k = \Delta t_j < T,\ 1/T \le \Delta f_k = \Delta f_j < \Delta f_c$.

В останньому випадку частотно-часова матриця може бути різною, наприклад такою, як показано на рис. 5.6,в штрихами.



а б в

Рис. 5.6

Широке застосування в системах радіозв'язку знайшли ШСС з двійковою фазовою маніпуляцією (ФМ – ШСС).

$$S_{\text{фм шсс}} = A\cdot\sin[\omega_0 t + \pi/2\cdot\Theta(t)\cdot g(t)].$$

Тут $\Theta(t)$ – дискретний інформаційний параметр сигналу, можлива зміна значень якого (-1, 1) відбувається в моменти часу $k\cdot T$, k = 0,1,2, …; $g(t)$ – псевдовипадкова послідовність (ПВП), що розширює базу сигналу.

Часові діаграми у схемі формування ШСС з фазовою маніпуляцією розглянуто на рис. 5.7.

База ФМ-ШПС сигналу дорівнює кількості елементів ПВП на довжині інформаційного такту – $B = L$.

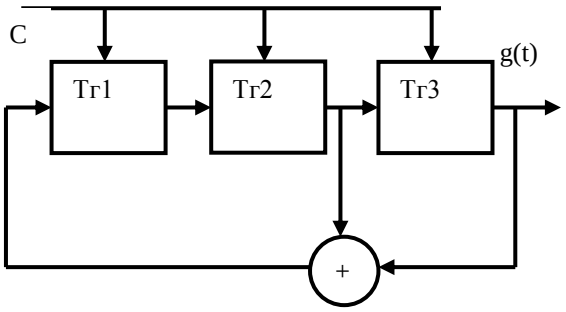
Спектральні і кореляційні характеристики ФМ-ШСС суттєво залежать від виду ПСП. На практиці широке використання зазнали кодові послідовності Хаффмена (m-послідовності максимальної довжини).

М-послідовністю називається періодична послідовність символів d_1, d_2,…, d_j, яка задовольняє рекурентному правилу:

$$a_0 d_j = \sum_{i=1}^{n} a_i d_{j-i} = a_1 d_{j-1} \oplus a_2 d_{j-2} \oplus \ldots \oplus a_n d_{j-n}. \qquad (5.1)$$

Параметр n визначає кількість комірок регістру зсуву, за допомогою якого за правилом (5.1) формується сама послідовність. Такий регістр із визначеною структурою зворотного зв′язку створює неповторну комбінацію з максимальною довжиною $L = 2^n - 1$.

Простота технічної реалізації генератора ПВП на основі М- послідовностей є однією з суттєвих причин використання цих сигналів у системах радіозв'язку.



Такт	1	2	3	4	5	6	7	8	9	10
Тг1	1	1	0	1	0	1	1	1	0	1
Тг2	1	1	0	0	1	0	1	1	1	1
Тг3	1	1	1	0	0	1	0	1	1	1

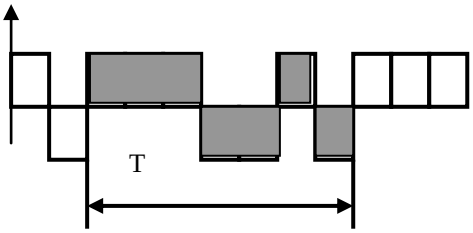


Рис. 5.7

Більш суттєве розширення спектра сигналу можна досягти при використанні сигналів з дискретною частотною маніпуляцією (ДЧМ). ДЧМ сигнали утворюються в результаті стрибкоподібної зміни значення частоти несучої за законом ПВП при постійній амплітуді і крокові квантування за часом і частотою. Такі сигнали часто називають сигналами з програмною перебудовою частоти (ППЧ). Сигнали з ППЧ можуть змінювати частоту декілька разів за біт інформації (швидка ППЧ), або один раз за час передачі декількох біт (повільна ППЧ).

Функціональні схеми формування ШСС наведені на рис. 5.8.

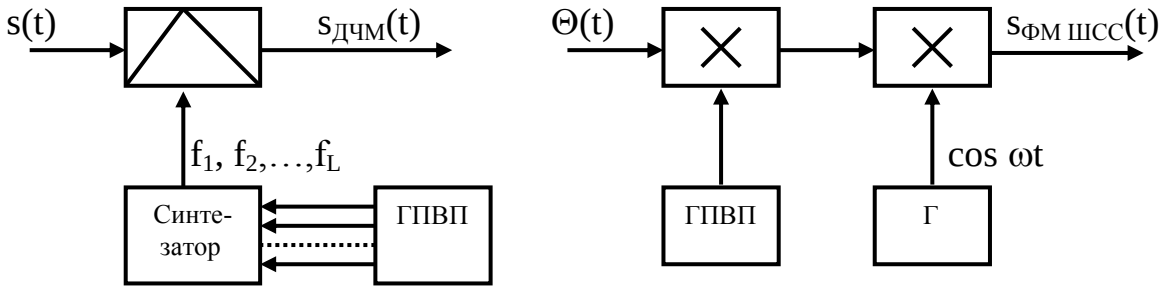


Рис. 5.8

Смуга частот, яку займає сигнал з швидкою ППЧ, дорівнює $\Delta f_c = [L+1]\cdot\Delta f$, де Δf – крок квантування за частотою.

Оскільки $\Delta f = 1/T_0$, $T_0 = T/L$, $\Delta f = L/T$, то для бази ДЧМ-сигналу маємо: $B = \Delta f_c / \Delta F = (L+1)\cdot\Delta f / (2/T) = (L+1)\cdot L / T\cdot(2/T) = L\cdot(L+1)/2$.

При ФМ-ШСС ширина спектра сигналу безпосередньо визначається тривалістю елемента сигналу T_0. Можливо забезпечити значення T_0 порядку десятків наносекунд, тобто розширити спектр до декількох десятків МГц. Подальше розширення спектра ускладнюється необхідністю розробки пристроїв зі швидкодією (часом переключення) в одиниці наносекунд.

При ППЧ досить просто сформувати сигнал з шириною смуги частот у сотні МГц. Однак потрібно враховувати, що з ростом кількості частот і швидкості їх зміни ускладнюється синтезатор частот.

Усі переваги широкосмугових сигналів можуть бути реалізовані лише при їх оптимальному прийомі. Тому пристрої обробки ШСС будують або на основі кореляторів, або узгоджених фільтрів.

При кореляційній обробці ШСС демодуляція здійснюється у два етапи (рис. 5.9).

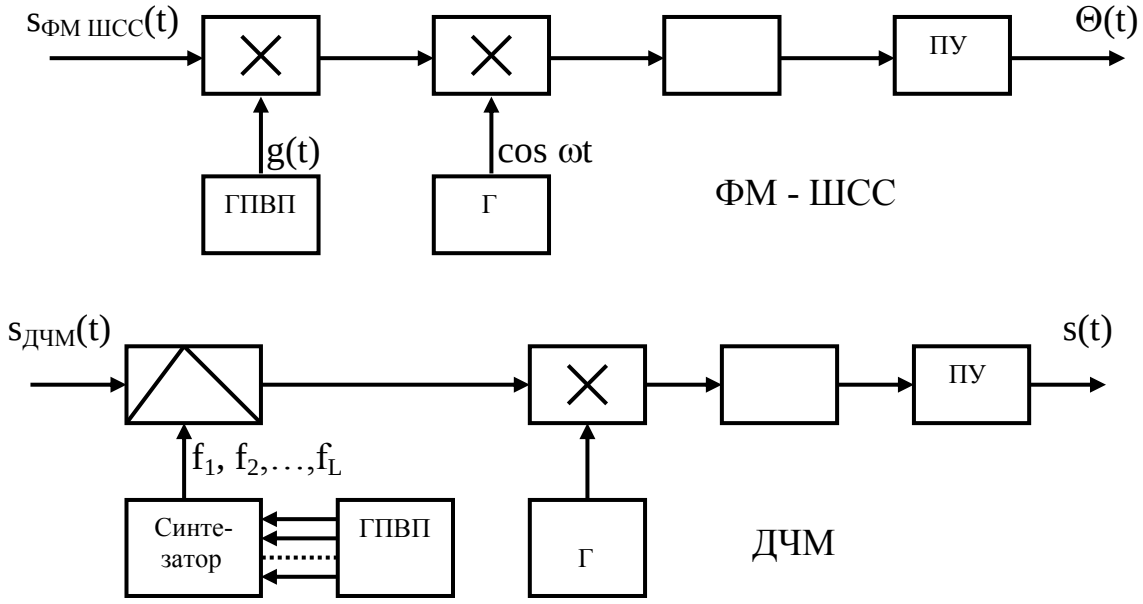


Рис. 5.9

На першому етапі знімається широкосмугова модуляція сигналів (модуляція псевдовипадковою послідовністю або стрибкоподібна зміна частоти). Це здійснюється множенням ФМ-ШСС, що приймається, на зразкову ПВП, який формується у приймачі, або гетеродинуванням ДЧМ сигналу (рис. 5.9). При цьому відбувається “звуження” смуги частот ШСС,

тобто перетворення у вузькосмуговий сигнал, ширина спектра якого визначається інформаційним параметром, який модулює.

На другому етапі відбувається виділення інформації, що міститься у сигналі. Після першого етапу ШСС перетворюється у вузькосмуговий сигнал з одним із звичайних видів маніпуляції (наприклад, ВФМн, ЧМн). Тому тут використовують оптимальні демодулятори таких сигналів.

Основна привабливість узгоджених фільтрів пов'язана з їх інваріантністю щодо затримки сигналу. При будь – якій затримці УФ працює однаково і буде реагувати на сигнал тільки з тією різницею, що момент досягнення максимуму напруги на виході фільтра буде змінюватися (рис. 5.10).

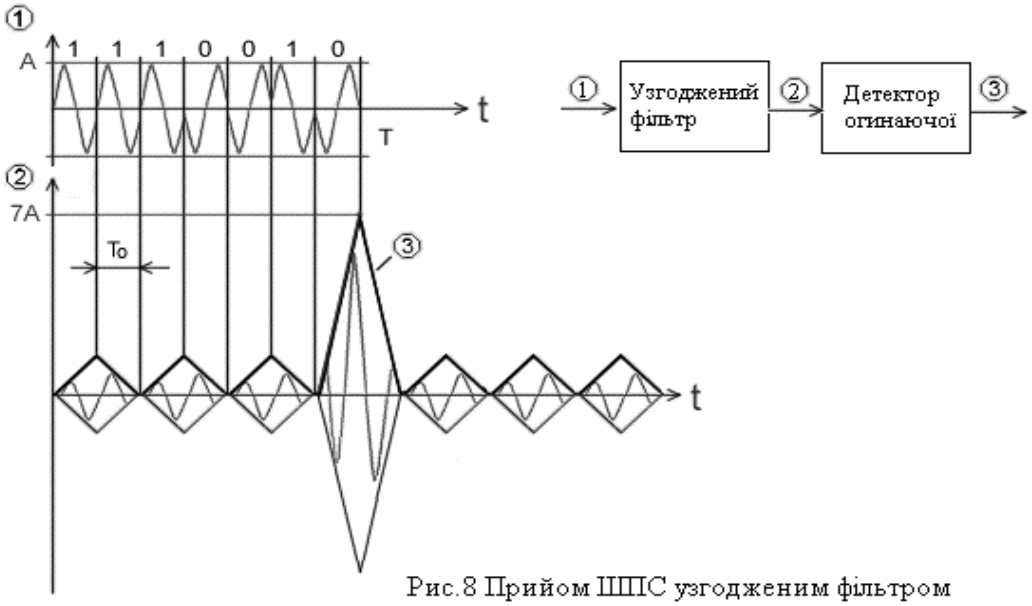


Рис.8 Прийом ШПС узгодженим фільтром

Рис. 5.10

На відміну від кореляційної обробки, при узгодженій фільтрації здійснюється стискання сигналу не за спектром, а за часом. Сигнал на виході узгодженого фільтра має приблизно ту ж ширину спектра, але три-валість його зменшується в *B* разів. Напруга на виході фільтра повторює у масштабі реального часу кореляційну функцію сигналу. З метою спрощення подальшої обробки на вихід узгодженого фільтра включають детектор обвідної. Відмітимо, що інваріантність до затримки сигналу суттєво полегшує входження у синхронізм при прийомі ШСС. Дійсно, момент максимального значення вихідного сигналу узгодженого фільтра є оптимальною оцінкою моменту зміни значень дискретного інформаційного параметра.

ШСС знайшли широке використання в системах стільникового і космічного зв'язку та завадозахищених системах передачі даних.

СПИСОК
ВИКОРИСТАНОЇ ТА РЕКОМЕНДУЄМОЇ ЛІТЕРАТУРИ

1. Жураковський Ю.П., Полторак В.П. Теорія інформації та кодування. – К.: Вища шк., 2001. – 255с.

2. Блейхут Р. Теория и практика кодов, контролирующих ошибки. – М.: Мир, 1986. – 576с.

3. Касами Т., Токура Н., Ивадари Е., Инагаки Я. Теория кодирования. – М.: Мир, 1978. – 576с.

4. Габидулин Э.М., Афанасьев В.Б. Кодирование в радиоэлектронике. – М.: Радио и связь, 1986. – 176с.

5. Кларк Дж. мл., Кейн Дж. Кодирование с исправлением ошибок в системах цифровой связи. – М.: Радио и связь, 1987. – 392с.

6. Гаранин М.В., Журавлев В.И., Кунегин С.В. Системы и сети передачи информации. – М.: Радио и связь, 2001. – 336с. (с.96 – 167).

7. Величкин А.И., Азаров Г.С., Саютин Ю.В. Средства связи и системы передачи данных ВВС. – М.: ВВИА, 1985. – 326с. (с.105 – 134).

8. Авиационные радиосвязные устройства. Под ред. В.И. Тихонова. – М.: ВВИА, 1986. – 442с. (с.149 – 190, 234 – 265).

9. Пенин П.И., Филиппов Л.И. Радиотехнические системы передачи информации. – М.: Радио и связь, 1984. – 256с. (с.176 – 191).

10. Аблазов В. И., Гупал В.И., Згурский А.В. Преобразование, запись и воспроизведение речевых сигналов. – К.: Лыбидь, 1991. – 208с. (с.165 – 188).

З М І С Т

Редактор Л.П. Мусієнко
Обсяг ум. друк. арк. 7,25
Друк. ХІ ВПС. Зам._____ Тир. 50 прим.
Безкоштовно