Міністерство освіти і науки України
Ужгородський національний університет

І.В. Шапочка

АЛГЕБРАЇЧНА ТЕОРІЯ КОДУВАННЯ

Методична розробка

Ужгород 2002

УДК 519.95

Шапочка І.В. Алгебраїчна теорія кодування. – Ужгород: Ужгород. нац. ун-т, 2002. – 20 с.

Відповідальний за випуск:

доктор фізико-математичних наук, професор *П. М. Гудивок*

Рецензент:

кандидат фізико-математичних наук, доцент *Ф. Е. Гече*

Рекомендовано до друку методичною комісією математичного факультету (протокол №5 від 24.01.02)

©Шапочка І.В., 2002

Зміст

Вступ

Цей методичний посібник присвячений одному із методів розв'язання наступної важливої проблеми в теорії передачі інформації: двійкове кодування і декодування, що забезпечує надійну передачу по каналам з "шумом". Типова ситуація така: потрібно передати повідомлення, яке може бути рядком символів деякого скінченного алфавіту, наприклад, $\{0, 1\}$ або українські чи латинські букви, або арабські числа і т. п. Так чи інакше, передача даних зводиться до передачі по деякому каналу зв'язку знаків деякого скінченного алфавіту. Практично завжди цей канал зв'язку не ідеальний через різноманітні причини, наприклад, через збої, до яких схильне чутливе і складне електронне обладнання. Навіть, якщо ймовірність невірної передачі одного символу є досить малою, скажімо 10^{-6}, то при передачі довгих рядків ймовірність вірно послати необхідну інформацію може виявитися недопустимо малою.

Двійкові симетричні канали. При математичному аналізі систем зв'язку звично користуються спрощеними моделями. Для двійкового алфавіту $\{0, 1\}$ найпростіша достатньо реалістична модель називається *двійковим симетричним каналом*. Вона використовується найбільш часто.

Нехай двійкові сигнали 0, 1 послідовно передаються по каналу зв'язку на приймач. На рис. 1 зображена ситуація, коли кожний символ приймається вірно з ймовірністю p і помилково з ймовірністю $q = 1 - p$ (насправді одиниці перетворюються у нулі частіше ніж нулі — в одиницю). Більше того припускається, що помилки при передачі послідовних символів відбуваються незалежно у розумінні наступного означення.

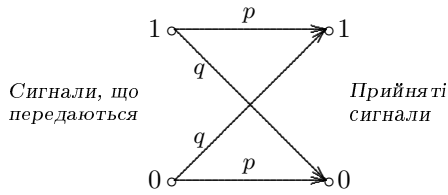

Рис. 1

Означення. Нехай $\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_3, \ldots$ — деяка послідовність випробувань, і нехай T — деяка подія, яка може відбутися при випробуванні $\mathcal{E}_i$ $(i \in \mathbb{N})$. Позначимо через p_i ймовірність події T, а через $q_i = 1 - p_i$ ймовірність того, що вона не відбудеться. Тоді випробування називаються *незалежними* по відношенню до події T, якщо для довільних підмножин I та J випробувань, що не перетинаються, ймовірність того, що при $\mathcal{E}_i \in I$ подія T відбудеться, а при $\mathcal{E}_j \in J$ не відбудеться,

дорівнює $\prod\limits_{\mathcal{E}_i \in I} p_i \prod\limits_{\mathcal{E}_j \in J} q_j$.

Приклад 1. Нехай ймовірність помилки при передачі одного двійкового символу 0 або 1 (одного *біта* інформації) дорівнює $q = 1\% = 0,01$ і, що ми хочемо бути впевнені в абсолютній точності передачі послідовностей із 1000 символів. Тоді при прямій передачі послідовності символа за символом вона буде вірно прийнята з дуже малою ймовірністю:

$$P_0 = (1 - 0,01)^{1000} \approx 10^{-4} \cdot 0,4 < 0,004\%.$$

Цей числовий результат є частинним випадком класичної формули Бернуллі для незалежних випробувань (див., наприклад, [5]). Позначимо

$$C_n^k = \frac{n!}{k!(n-k)!} = \frac{(n-k+1)\cdots(n-1)n}{1 \cdot 2 \cdot 3 \cdots k}.$$

Справедлива наступна теорема.

Теорема 1. *Нехай по двійковому симетричному каналу передається n-бітова послідовність. Ймовірність того, що вона буде прийнята з рівно k помилками, дорівнює*

$$P_k = C_n^k p^{n-k} q^k.$$

Загальна схема передачі числових даних зображена на рис. 2. Маємо інформацію, яка підлягає передачі по каналу, шум у каналі, прийом сигналу на фоні шуму, перекодування одержаних сигналів з шумом у двійкову послідовність, деякі знаки якої можуть виявитися помилковими через шум.

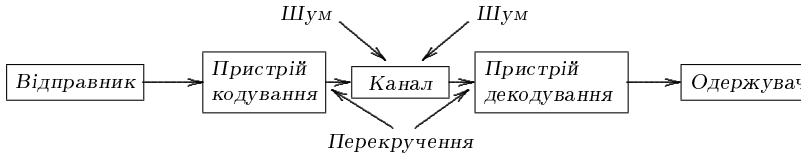

Рис. 2

Загальна задача, яка постає перед проектувальником такої системи зв'язку, полягає у наступному. Через фізичні обмеження, які накладаються на систему (максимальна потужність передавача, затухання сигналу у каналі зв'язку і неусувний шум), проектувальник

не може надіятися на точне відтворення приймачем переданого сигналу. Якщо перекручення великі, приймач буде робити помилки. Проектувальник повинен або свідомо прийняти визначену долю помилок, або придумати спосіб зменшити її.

§1. Кодування і декодування

В багатьох системах, які обробляють інформацію, подібних системам зв'язку з супутниками і великих обчислювальних систем, за помилки доводиться платити дорогою ціною. Тому важливо домогтися, щоб вони траплялися вкрай рідко. Збільшення надійності передачі інформації досягається за допомогою *систематичних кодів* різних типів.

Ідея, що покладена в основу кожного з систематичних кодів, полягає у наступному. Послідовності символів, які підлягають передачі, кодуються більш довгими послідовностями тих же символів за визначеною схемою *кодування*. Приймач здатний розпізнати і/або виправити помилки, що викликані шумом, аналізуючи додаткову інформацію, яка міститься в додаткових символах. Ці символи називають ще *перевірочними* символами. Прийнята довга послідовність декодується за схемою *декодування* у початково передану, тобто в послідовність до стадії кодування.

Означення. *Двійковим* (m, n)*-кодом* називається пара, яка складається із схеми кодування (відображення) $E : \mathbf{2}^m \to \mathbf{2}^n$ і схеми декодування (відображення) $D : \mathbf{2}^n \to \mathbf{2}^m$, де $\mathbf{2}^k$ — множина всіх двійкових послідовностей довжини k.

Відображення E і D вибираються таким чином, щоб добуток відображень DTE, де $T : \mathbf{2}^n \to \mathbf{2}^n$ — "відображення помилок з ймовірністю, що близька до одиниці, був тотожним відображенням. Таким чином, математичну модель системи зв'язку можна зобразити блок-схемою (рис. 3), де E, D — детерміновані відображення.

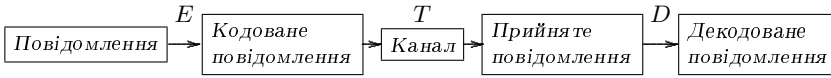

Рис. 3

Двійкові (m,n)-коди діляться на два великих класи. (m,n)-*коди з виправленням помилок* мають за мету відновити з ймовірністю, що близька до одиниці, послане повідомлення. (m,n)-*коди з виявленням помилок* мають за мету виявити з ймовірністю, що близька до одиниці, наявність помилок. Для ілюстрації наведемо два приклади.

Приклад 2. Простий $(m,m+1)$-код з виявленням помилок грунтуєтья на схемі *перевірки парності*, що застосовується до повідомлень $\mathbf{a} = (a_1, a_2, \ldots, a_m) = a_1 a_2 \ldots a_m \in \mathbf{2}^m$ довільної фіксованої довжини $m \in \mathbb{N}$. Схема кодування визначається таким чином:

$$E : (a_1, \ldots, a_m) = \mathbf{a} \to \mathbf{b} = (b_1, \ldots, b_{m+1}) \in \mathbf{2}^{m+1},$$

де

$$b_i = a_i \quad \text{при} \quad i = 1, \ldots, m; \tag{1}$$

$$b_{m+1} = \begin{cases} 0, & \text{якщо } \sum\limits_{i=1}^{m} a_i \text{ число парне;} \\ 1, & \text{якщо } \sum\limits_{i=1}^{m} a_i \text{ число непарне.} \end{cases} \tag{2}$$

Наприклад, у випадку $m = 2$ схема кодування E виглядає так:

$$E : 00 \to 000,\ 01 \to 011,\ 10 \to 101,\ 11 \to 110.$$

Із визначення (1) і (2) випливає, що для довільного повідомлення $\mathbf{a} \in \mathbf{2}^m$ кодоване повідомлення $\mathbf{b} = E(\mathbf{a})$ містить парне число одиниць.

Відповідна схема декодування така: якщо для одержаного повідомлення $\mathbf{b} = (b_1, \ldots, b_{m+1})$ сума $\sum_{i=1}^{m+1} b_i$ — число парне, то

$$D : (b_1, \ldots, b_m, b_{m+1}) = \mathbf{b} \to \mathbf{c} = (b_1, \ldots, b_m);$$

якщо ж вказана сума є непарним числом, то приймач вкаже на *наявність помилки*. Зрозуміло, якщо сума $\sum_{i=1}^{m+1} b_i$ є парним числом, ми не можемо бути впевнені, що помилка не відбулась. Але, скажімо, при $m = 2$ і при ймовірності q помилкового прийому одного символу доля невірно прийнятих символів буде складати $q^3 + 3q^2p + 3qp^2$ (відповідно три, дві, одна помилка). Тому доля помилкових повідомлень, що залишаться непоміченими, відносно всіх помилкових повідомлень буде складати

$$\frac{3q^2p}{q^3 + 3q^2p + 3qp^2} < \frac{q}{q+p} = q.$$

Отже, ймовірність пропуску помилки буде меншою за q.

Тепер докладніше розглянемо приклад коду з виправленням помилок. Найпростіший приклад такого кодування полягає у повторенні сигналу довільне фіксоване число разів.

Приклад 3. Розглянемо двійковий симетричний канал, описаний у вступі, для передачі рядків двійкової інформації та наступний $(m, 3m)$-код з *потрійним повторенням*. Любе повідомлення розбивається на блоки по m послідовних символів у кожному і кожний блок передається тричі: це визначає схему кодування E. Схема декодування D ж така. Одержаний рядок розбивається на блоки довжини $3m$. Якщо черговий блок складається із трьох однакових рядків символів довжини m, то цей рядок є результатом його декодування. У загальному випадку по трійці символів c_i, c_{i+m}, c_{i+2m} в цьому блоці відновлюється символ, що частіше за все (два або три рази) зустрічається у цій трійці, і ставиться на i-місце у декодованому блоці.

Ймовірність того, що символ у даній позиції буде прийнятий вірно тричі, дорівнює p^3. Ймовірність помилки тільки в перший раз дорівнює p^2q, отже, ймовірність рівно одної помилки дорівнює $3p^2q$. Тому ймовірність вірного прийому символу в даній позиції дорівнює p^3+3p^2q, а ймовірність помилкового прийому — $3pq^2+q^3$. Припустимо, що $q = 0,1$. Тоді в кожній позиції символ буде прийнятий тричі вірно з ймовірністю $0,729$ і двічі вірно з ймовірністю $0,243$. Він буде прийнятий двічі невірно з ймовірністю $0,027$ і тричі невірно з ймовірністю $0,001$. Таким чином, наш код зменшує ймовірність помилки на один символ з 10% до $2,8\%$.

Аналогічно п'ятикратна передача і декодування по принципу "більшості голосів" дає ймовірність помилки $q^5 + 5q^4p + 10q^3p^2 = = 0,00856$, тобто менше 1%. В результаті ймовірність вірної передачі рядку довжини 10 виросте із $(0,9)^{10} \simeq 35\%$ до $(0,972)^{10} \simeq 74\%$ при трикратних повтореннях і до $(0,99144)^{10} \simeq 92\%$ при п'ятикратних повтореннях.

На завершення зазначимо, що трикратне повторення забезпечує виправлення однієї помилки в кожній позиції за рахунок трикратного подовження часу передачі. У наступних параграфах наводяться приклади кодів, які виправляються помилки з такою ж надійністю з меншим часом передачі повідомлень.

В п р а в и

1. Нехай по двійковому симетричному каналу (рис. 1)передаються рядки довжини 14.

а) Яка ймовірність того, що рівно п'ять символів будуть прийняті невірно?

б) Скільки існує рядків, що відрізняються від даного не більше як в чотирьох позиціях?

2. Скільки існує двійкових $(3, 5)$-кодів?

§2. Блочні коди

Описані вище приклади належать до класу *блочних кодів*. За означенням, блочний код замінює кожний блок із m символів деяким більш довшим блоком із n символів, які після передачі підлягають декодуванню. Нижче ми будемо розглядати тільки такі коди.

Із міркувань простоти і надійності більшість систем зв'язку конструюють для передачі двійкових послідовностей. Блочний (m, n)-код, як це вже говорилось раніше, визначається двома відображеннями:

$$E : \mathbf{2}^m \to \mathbf{2}^n, \quad D : \mathbf{2}^n \to \mathbf{2}^m, \quad m \leq n$$

(випадок $m = n$ використовується у шифруванні, де мета кодування полягає в забезпеченні секретності сигналу). Повинно виконуватись умова, щоб добуток DE був тотожним відображенням, для того щоб повідомлення було прийняте вірно при відсутності перешкод.

Надалі будь-яку послідовність із n символів 0 або 1 будемо називати *словом довжини* n або *двійковим* n*-вимірним вектором*. Інформаційні символи за означенням додаються у відповідності з двійковими правилами: $0 + 0 = 0$, $0 + 1 = 1$, $1 + 0 = 1$, $1 + 1 = 0$.

Означення. *Сумою* слів $\mathbf{a} = (a_1, \ldots, a_n)$ і $\mathbf{b} = (b_1, \ldots, b_n)$ називається слово довжини n

$$\mathbf{a} + \mathbf{b} = (a_1 + b_1, \ldots, a_n + b_n). \tag{3}$$

Очевидно, множина $\mathbf{2}^n$ всіх слів довжини n відносно вказаної вище операції додавання є абелевою групою, яку позначатимемо через $\mathbb{Z}_2^n$.

Будь-яке слово довжини n, яке може бути передане кодером називається *кодовим словом*. Тобто кодовими словами є образи слів довжини m при відображенні $E : \mathbf{2}^m \to \mathbf{2}^n$. Оскільки, відображення E є ін'єктивним, то існує всього 2^m різних кодових слів довжини n.

Означення. *Вагою Геммінга* $w(\mathbf{a})$ слова $\mathbf{a} = (a_1, \ldots, a_n)$ називається число одиниць серед його компонент $a_1, \ldots, a_n$. *Відстанню*

Геммінга $d(\mathbf{a}, \mathbf{b})$ між словами $\mathbf{a}$ і $\mathbf{b}$ однакової довжини називається вага їх суми, тобто $d(\mathbf{a}, \mathbf{b}) = w(\mathbf{a} + \mathbf{b})$.

Очевидно, відстань Геммінга між словами $\mathbf{a} = (a_1, \ldots, a_n)$ і $\mathbf{b} = (b_1, \ldots, b_n)$ дорівнює порядку множини $\{i \in \{1, 2, \ldots, n\} \mid a_i \neq b_i\}$.

Теорема 2. *Для того, щоб (m, n)-код давав можливість виявити всі помилки в небільш як k позиціях, необхідно і досить, щоб найменша відстань Геммінга між двома різними кодовими словами дорівнювала $k + 1$.*

Доведення. Нехай кодове слово $\mathbf{b} = E(\mathbf{a})$, де $\mathbf{a} \in \mathbf{2}^m$, було передане як слово $\mathbf{b}^*$ з t помилками. Тоді відстань Геммінга $d(\mathbf{b}, \mathbf{b}^*)$ між цими словами дорівнює t. Оскільки $t \leq k$, то очевидно, що умова $d(E(\mathbf{a}), E(\mathbf{a}')) \geq k + 1$ для довільних $\mathbf{a}, \mathbf{a}' \in \mathbf{2}^m$ є необхідною і достатньою умовою виявлення помилки при передачі повідомлення.

Теорема 3. *Для того, щоб (m, n)-код давав можливість виправити всі помилки в небільш як k позиціях, необхідно і досить, щоб найменша відстань Геммінга між двома різними кодовими словами дорівнювала $2k + 1$.*

Доведення. Доведемо лише достатність теореми, залишивши інше читачеві. Припустимо, що найменша відстань Геммінга між двома кодовими словами дорівнювала $2k+1$. Нехай $\mathbf{b} = E(\mathbf{a})$ — кодове слово, що передається ($\mathbf{a} \in \mathbf{2}^m$), а $\mathbf{b}^*$ — одержане слово з t помилками. Тоді для будь-якого кодового слова $\mathbf{c}$ із нерівності трикутника (див. вправу 1 §2) слідує, що

$$d(\mathbf{c}, \mathbf{b}^*) \geq d(\mathbf{c}, \mathbf{b}) - d(\mathbf{b}, \mathbf{b}^*) \geq 2k + 1 - k = k + 1 > k \geq t = d(\mathbf{b}, \mathbf{b}^*).$$

Визначивши схему декодування D таким чином, що кожному слову $\mathbf{u} \in \mathbf{2}^n$ у відповідність ставиться прообраз найближчого кодованого слова до слова $\mathbf{u}$ при відображенні E, то одержане слово $\mathbf{b}^*$ буде вірно декодоване у $\mathbf{a}$. Це завершує доведення теореми.

Приклад 4. Для простого $(1, 3)$-коду з схемою кодування

$$E : 0 \to 000, 1 \to 111$$

схема декодування D має вигляд:

$$\begin{array}{llll} 000 \to 0, & 001 \to 0, & 010 \to 0, & 100 \to 0, \\ 111 \to 1, & 011 \to 1, & 101 \to 1, & 110 \to 1. \end{array}$$

Цей $(1, 3)$-код виправляє помилки тільки в одній позиції.

З точки зору групової структури зручно розглядати *слова помилок* ("шумові слова"). Дане повідомлення $\mathbf{a} = (a_1, \ldots, a_m)$ перекодується у кодове слово $\mathbf{b} = (b_1, \ldots, b_n)$. Канал зв'язку при передачі добавляє до нього слово помилок $\mathbf{e} = (e_1, \ldots, e_n)$, таким чином, що приймач одержує слово $\mathbf{r} = (r_1, \ldots, r_n)$, де $r_i = b_i + e_i$ $(i = 1, \ldots, n)$. Система, що виправляє помилки переводить слово $\mathbf{r}$ у найближче кодове слово $\mathbf{b}$. Система ж, яка перевіряє чи є одержане слово кодовим, повідомляє про наявність помилки, якщо це не так.

В п р а в и

1. Довести, що у n-вимірному векторному просторі над полем $\mathbb{Z}_2$ з двох елементів відстань Геммінга є метрикою, а вага Геммінга є нормою.

2. Завершити доведення теореми 3.

3. Побудувати двійковий $(m, 7)$-код такий, що відстань між довільними кодовими словами була б не менша 4.

4. Довести, що для того, щоб двійковий (m, n)-код давав можливість виправити всі комбінації від 1 до t помилок і мав можливість виявляти всі комбінації від $t+1$ до $t+s$ помилок необхідно, щоб найменша відстань Геммінга між двома різними кодовими словами була не меншою за $2t + s$.

§3. Лінійні коди

Раніше ми описували кожну із схем кодування і декодування таблицями. Для слів великої довжини ці таблиці є дуже великими і використовують великий об'єм пам'яті і є неекономічними. Набагато меншого об'єму пам'яті потрібно при використанні *лінійного кодування*. Почнемо розглядувати цей метод кодування із наступного прикладу.

Приклад 5. Нехай схема кодування E $(3, 6)$-коду визначається правилом: кожне слово $\mathbf{a} = (a_1, a_2, a_3) \in \mathbf{2}^3$ кодується словом $\mathbf{b} = (b_1, b_2, b_3, b_4, b_5, b_6)$, де

$$\begin{aligned} b_1 &= a_1, \quad b_4 = a_1 + a_3, \\ b_2 &= a_2, \quad b_5 = a_2 + a_3, \\ b_3 &= a_3, \quad b_6 = a_1 + a_2 + a_3. \end{aligned} \tag{4}$$

Якщо через $\mathcal{U}$ позначити матрицю

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix},$$

то рівності (4) можна переписати у матричній формі

$$\mathbf{b} = \mathbf{a}\mathcal{U}.$$

Матрицю $\mathcal{U}$ будемо називати *кодуючою матрицею*. З іншого боку із рівностей (4) випливає, що кодове слово $\mathbf{b}$ задовольняє умовам:

$$\begin{aligned} b_1 + b_3 + b_4 &= 0, \\ b_2 + b_3 + b_5 &= 0, \\ b_1 + b_2 + b_3 + b_6 &= 0, \end{aligned} \tag{5}$$

тобто є розв'язком системи лінійних однорідних рівнянь. А тому множина всіх кодових слів є підгрупою групи $\mathbb{Z}_2^6$. Далі, якщо через $\mathcal{V}$ позначити матрицю системи рівнянь (5), а через $\mathbf{b}^T$ — вектор-стовпець, який є транспонованим до вектора-рядка (слова) $\mathbf{b}$, то систему рівнянь (5) також можна переписати у матричні формі

$$\mathcal{V}\,\mathbf{b}^T = \mathbf{0},$$

де $\mathbf{0}$ — нульовий вектор-стовпець довжини 3.

Означення. Двійковий (m, n)-код називається *лінійним*, якщо існує така $s \times n$-матриця $\mathcal{V}$ над полем $\mathbb{Z}_2$ з двох елементів ($\mathbb{Z}_2 = \{0, 1\}$), що будь-яке кодове слово $\mathbf{b}$ задовольняє рівнянню $\mathcal{V}\,\mathbf{b}^T = \mathbf{0}$ ($\mathbf{0}$ — нульовий вектор-стовпець довжини s). Матриця $\mathcal{V}$ називається *перевірочною матрицею.*

Простий $(m, m+1)$-код з виявленням помилок та $(m, 3m)$-код з потрійним повторенням є лінінійними кодами відповідно з перевірочними $1 \times (m+1)$- та $2m \times 3m$-матрицями:

$$\begin{pmatrix} 1 & 1 & \dots & 1 \end{pmatrix}, \qquad \begin{pmatrix} E_m & E_m & 0 \\ E_m & 0 & E_m \end{pmatrix},$$

де E_m і 0 — відповідно одинична і нульова матриці порядку m.

Означення. Двійковий (m, n)-код називається *груповим*, якщо множина всіх кодових слів є групою відносно операції додавання слів.

Будь-який лінійний (m, n)-код з перевірочною матрицею $\mathcal{V}$ є груповим, оскільки для довільних кодових слів $\mathbf{b}$ і $\mathbf{c}$ цього коду

$$\mathcal{V}(\mathbf{b} + \mathbf{c})^T = \mathcal{V}\,\mathbf{b}^T + \mathcal{V}\,\mathbf{c}^T = \mathbf{0} + \mathbf{0} = \mathbf{0}.$$

Теорема 4. *Якщо (m,n)-код є груповим, то найменша відстань Геммінга між двома різними кодовими словами дорівнює найменшій вазі ненульового кодового слова.*

Доведення теореми відразу випливає із означення відстані Геммінга між кодовими словами.

Найменша вага ненульового кодового слова у прикладі 5 дорівнює 3 (див. таблицю 1). Отже, мінімальна відстань Геммінга також дорівнює 3, і вказаний (3,6)-код здатен виправляти однократну помилку і виявляти подвійну.

Неважко визначити, які помилки залишаться непоміченими; для групових кодів вони в точності відповідають тим словам, які самі є кодовими словами. Так, у прикладі 5 слово помилок $\mathbf{e} = 100101$ переводить довільне кодове слово у кодове слово.

Розглянемо тепер проблему декодування лінійного (m,n)-коду з схемою кодування E, яка визначається матрицею кодування $\mathcal{U}$, і з перевірочною матрицею $\mathcal{V}$. Потрібно підібрати схему декодування D таким чином, щоб ймовірність того, що $D(E(\mathbf{a})) \neq \mathbf{a}$, була найменшою для довільних інформаційних повідомлень $\mathbf{a} \in \mathbf{2}^m$.

Нехай $\mathbf{b}$ — передане кодове слово, а $\mathbf{c}$ — слово, одержане після передачі $\mathbf{b}$. Називатимемо *синдромом слова* $\mathbf{c}$ слово $\mathbf{s}$, яке визначається рівністю $\mathbf{s}^T = \mathcal{V}\,\mathbf{c}^T$. Множина всеможливих слів помилок при одержанні слова $\mathbf{c}$ співпадає з множиною всіх слів довжини n, що мають такий же синдром, як і слово $\mathbf{c}$. Дійсно, якщо слово $\mathbf{s}$ не є синдромом слова $\mathbf{e}$, тобто $\mathcal{V}\,\mathbf{c}^T \neq \mathcal{V}\,\mathbf{e}^T$, то $\mathcal{V}(\mathbf{c}-\mathbf{e})^T \neq \mathbf{0}$. Отже, $\mathbf{c}-\mathbf{e}$ не є переданим кодовим словом. Навпаки, якщо $\mathcal{V}\,\mathbf{c}^T = \mathcal{V}\,\mathbf{e}^T$, то $\mathcal{V}(\mathbf{c}-\mathbf{e})^T = \mathbf{0}$, і слово помилок може співпадати з словом $\mathbf{e}$, якщо $\mathbf{b}+\mathbf{e} = \mathbf{c}$.

Припустимо, наприклад, що прийняте слово $\mathbf{c}$ є кодовим, тобто $\mathcal{V}\,\mathbf{c}^T = \mathbf{0}$. Тоді слово помилок $\mathbf{e} = \mathbf{c}-\mathbf{b}$ також є кодовим, оскільки множина всіх кодових слів є групою відносно операції додавання слів.

Таким чином, нами показано, що множина всіх слів довжини n, які мають один і тот же синдром, є суміжним класом групи $\mathbb{Z}_2^n$ за підгрупою всіх кодових слів довжини n. Отже, декодер може відразу виключити з розгляду всі слова помилок, які не лежать в одному суміжному класі з прийнятим словом. Однак всі слова, які належать цьому суміжному класу, можуть бути словами помилок. Ні одна із цих можливостей не може бути повністю виключена з розглядання. Але, оскільки помилки в каналі відносно досить рідкі, то деякі із слів помилок у межах даного суміжного класу набагато менш ймовірні

чим інші. Звичайно найбільш ймовірно словом помилок буде слово з найменшою вагою Геммінга. Слово найменшої ваги у межах даного суміжного класу називається *лідером суміжного класу.*

Суміжні класи для розглянутого вище прикладу 5 виписані у вигляді рядків таблиці 1. Перший рядок є суміжним класом з нульовим синдромом, тобто множиною всіх кодових слів. Лідер кожного з суміжних класів виписаний у другому стовпці. Слово, що розміщене в i-му рядку і j-му стовпцю, дорівнює сумі j-го кодового слова і i-го лідера.

Таблиця 1.

Синдром	Слова							
000	000000	100101	010011	011100	001111	101010	110110	111001
100	000100	100001	010111	011000	001011	101110	110010	111101
010	000010	100111	010001	011110	001101	101000	110100	111011
001	000001	100100	010010	011101	001110	101011	110111	111000
011	010000	110101	000011	001100	011111	111010	100110	101001
101	100000	000101	110011	111100	101111	001010	010110	011001
110	000110	100011	010101	011010	001001	101100	110000	111111
111	001000	101101	011011	010100	000111	100010	111110	110001

Підсумуємо все вище сказане у вигляді теореми.

Теорема 5. *Якщо* $\mathbf{c}$ *— прийняте слово довжини* n*, то множина можливих слів помилок співпадає з суміжним класом групи* $\mathbb{Z}_2^n$ *за підгрупою всіх кодових слів, який містить слово* $\mathbf{c}$*. Найбільш ймовірним словом помилок є лідер цього суміжного класу. Схема декодування* D *лінійного* (m, n)*-коду може бути побудована наступним чином: обчислюємо синдром прийнятого слова, знаходимо лідер суміжного класу, якому відповідає цей синдром, і, віднімаючи знайдений лідер від прийнятого слова, одержуємо найбільш ймовірне передане кодове слово.*

В п р а в и

1. Нехай

$$\mathcal{U} = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

— кодуюча матриця двійкового $(2, 5)$-коду. Знайти його перевірочну матрицю, множину всіх кодових слів і лідери суміжних класів для цього коду.

2. Скільки кодових слів містить двійковий код, що визначається перевірочною матрицею

$$\mathcal{V} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}?$$

3. Нехай $\mathcal{V}$ — перевірочна матриця лінійного (m, n)-коду. Довести, що суміжний клас з синдромом $\mathbf{s}$ містить слово вагою Геммінга w тоді і тільки тоді, коди деяка лінійна комбінація w стовпців матриці $\mathcal{V}$ дорівнює $\mathbf{s}$.

4. Довести, що кодові слова двійкового групового коду або всі мають парну вагу Геммінга, або половина — парну, а інша — непарну.

§4. Коди Геммінга

Нехай $\mathbf{x}$ — довільне слово з групи слів $\mathbb{Z}_2^n$ довжини n і r — довільне натуральне число. Підмножину $S_r(\mathbf{x}) \subset \mathbb{Z}_2^n$ всіх слів, відстань Геммінга від яких до слова $\mathbf{x}$ не перевищує r, називається *кулею радіуса* r з центром в $\mathbf{x}$.

Теорема 6. *Якщо (m, n)-код, який має s кодових слів, може виправляти всі комбінації t або менше помилок, то*

$$s \leq \frac{2^n}{\sum_{i=0}^{t} C_n^i}.$$

Доведення. Нехай $\mathbf{u}_1, \ldots, \mathbf{u}_s$ — всі кодові слова (m, n)-коду. Для довільного кодового слова розглянемо кулю $S_t(\mathbf{u}_i)$ радіуса t з центром в $\mathbf{u}_i$ $(i \in \{1, \ldots, s\})$. Оскільки (m, n)-код виправляє до t помилок включно, то із теореми 3 випливає, що кулі $S_t(\mathbf{u}_i)$, $S_t(\mathbf{u}_j)$ $(i \neq j)$ не перетинаються. Кожна куля $S_t(\mathbf{u}_i)$ містить всі слова, які відрізняються від кодового слова $\mathbf{u}_i$ в 0, 1, $\ldots t$ позиціях, а отже, число всіх цих слів дорівнює

$$1 + C_n^1 + C_n^2 + \cdots + C_n^t = \sum_{i=0}^{t} C_n^i.$$

Тому у всіх s кулях міститься $s \sum_{i=0}^{t} C_n^i$ слів. Це число не перевищує числа всіх слів довжини n, тобто 2^n. Звідси випливає доведення теореми.

Означення. Якщо (m, n)-код, що може виправляти всі комбінації t або менше помилок, має

$$\frac{2^n}{\sum_{i=0}^{t} C_n^i}$$

кодових слів, то цей (m, n)-код називається *досконалим*.

Теорема 7. *Найменша відстань Геммінга між різними кодовими словами лінійного (m, n)-коду з перевірочною матрицею $\mathcal{V}$ дорівнює найбільшому серед чисел w, для яких будь-які $w-1$ стовпці матриці $\mathcal{V}$ утворюють лінійно незалежну систему векторів m-вимірного векторного простору над полем з двох елементів.*

Доведення. Нехай найменша відстань Геммінга між кодовими словами лінійного (m, n)-коду дорівнює w. Тоді із теореми 4 слідує, що w є найменшою вагою ненульового кодового слова. Звідси відразу випливає існування лінійно залежної системи w стовпців матриці $\mathcal{V}$. Покажемо, що будь-які $w-1$ із стовпців $\mathbf{h}_1, \ldots, \mathbf{h}_n$ матриці $\mathcal{V}$ утворюють лінійно незалежну систему. Припустимо протилежне. Нехай система стовпців $\mathbf{h}_{i_1}, \ldots, \mathbf{h}_{i_{w-1}}$ $(i_1 < i_2 < \ldots < i_{w-1})$ є лінійно залежною, тобто існує система елементів $\alpha_{i_1}, \ldots, \alpha_{i_{w-1}} \in \{0, 1\}$, хоча б один з яких не дорівнює нулю, що

$$\alpha_{i_1}\mathbf{h}_{i_1} + \cdots + \alpha_{i_{w-1}}\mathbf{h}_{i_{w-1}} = \mathbf{0}.$$

Тоді для слова $\mathbf{x} = (\alpha_1, \ldots, \alpha_n)$ $(\alpha_j = 0$ при $j \notin \{i_1, \ldots i_{w-1}\})$ справедлива рівність $\mathcal{V}\mathbf{x}^T = \mathbf{0}$. Отже, слово $\mathbf{x}$ є кодовим з вагою, що не перевищує $w-1$. Одержана суперечність завершує доведення теореми.

Оскільки два m-вимірні вектори векторного простору над полем $\mathbb{Z}_2$ з двох елементів утворюють лінійно незалежну систему тоді і тільки тоді, коли вони ненульові і різні, то із теорем 3 і 7 випливає наступна теорема.

Теорема 8. *Лінійний (m, n)-код дозволяє виправляти всі поодинокі помилки тоді і тільки тоді, коли всі стовпці його перевірочної матриці відмінні від нульового і попарно різні.*

Означення. Лінійний (m, n)-код називається *кодом Геммінга*, якщо всі стовпці його перевірочної матриці представляють собою всі ненульові вектори $(n-m)$-вимірного векторного простору над полем $\mathbb{Z}_2$.

Легко видно, що для довільного натурального числа $r \geq 2$ існує $(2^r - r - 1, 2^r - 1)$-код Геммінга. Цей код дозволяє виправляти поодиноку помилку у кожній позиції і є досконалим кодом. Більше того, оскільки будь-який ненульовий синдром дорівнює деякому стовпцю перевірочної матриці, то ніколи не відбувається відмова від декодування. Процедура декодування поодиноких помилок є повною. Вага лідера кожного класу суміжності помилок дорівнює нулю або одиниці. Жоден вектор помилок ваги ≥ 2 не може бути виявленим або виправленим. Для того щоб виправляти конфігурації таких помилок, потрібно будувати коди з більшим числом перевірочних позицій, які природньо будуть менш швидкісними ніж коди Геммінга.

Приклад 6. Розглянемо $(4, 7)$-код Геммінга з перевірочною матрицею

$$\mathcal{V} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Припустимо, що одержано слово $\mathbf{b} = 0110100$. Обчислимо синдром $\mathbf{s}$ цього слова:

$$\mathcal{V}\,\mathbf{b}^T = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}.$$

Отже, $\mathbf{s} = 110$, а тому слово $\mathbf{b}$ не є кодовим. Бачимо, що синдром $\mathbf{s}$ співпадає з четвертим стовпцем матриці $\mathcal{V}$. Покладемо $\mathbf{e} = 0001000$. Тоді

$$\mathcal{V}(\mathbf{b} + \mathbf{e})^T = \mathcal{V}\,\mathbf{b}^T + \mathcal{V}\,\mathbf{e}^T = \mathbf{s} + \mathbf{s} = \mathbf{0}.$$

Тому, якщо припустити, що була допущена лише одна помилка у каналі, то слово $\mathbf{e}$ є словом помилок, а переданим кодовим словом є слово $\mathbf{b} + \mathbf{e} = 0111100$.

В п р а в и

1. За допомогою $(4, 7)$-коду Геммінга з перевірочною матрицею

$$\mathcal{V} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

закодуєте повідомлення 01101010. Крім цього, припускаючи, що трапилась не більше як одна помилка у зашумленому каналі при передачі слова, декодуйте слова $\mathbf{a} = 1100000$, $\mathbf{b} = 1001010$, $\mathbf{c} = 1101011$.

2. Покажіть, що $(2^r - r - 1, 2^r - 1)$-код Геммінга є досконалим.

3. Розглянемо три $(4, 7)$-коди Геммінга відповідно з перевірочними матрицями

$$\mathcal{V}_1 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}, \quad \mathcal{V}_2 = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

$$\mathcal{V}_3 = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Показати, що дві із вказаних матриць задають однакові множини кодових слів.

Література

1. *Акритас А.* Основы компьютерной алгебры с приложениями. – М.: Мир, 1994.
2. *Биркгоф Г., Барти Т.* Современная прикладная алгебра. – М.: Мир, 1976.
3. *Берлекэмп Э.* Алгебраическая теория кодирования. – М.: Мир, 1971.
4. *Ван дер Варден Б.Л.* Алгебра. – М.: Наука, 1979.
5. *Гнеденко Б.В.* Курс теории вероятностей. – М.: Наука, 1967.
6. *Каргаполов М.И., Мерзляков Ю.И.* Основы теории групп. – М.: Наука, 1982.
7. *Кострикин А.И.* Введение в алгебру. – М.: Наука, 1977.
8. *Курош А.Г.* Теория групп. – М.: Наука, 1967.
9. *Курош А.Г.* Курс высшей алгебры. – М.: Наука, 1971.
10. *Фаддеев Д.К.* Лекции по алгебре. – М.: Наука, 1984.

ШАПОЧКА Ігор Валерійович

АЛГЕБРАЇЧНА ТЕОРІЯ КОДУВАННЯ

Методична розробка

Підписано до друку 06.02.02 Формат $60 \times 84/16$. Офсетний друк.
Умов. друк. арк. 1,19. Облік.-вип. арк. 0,94. Замовлення №351
Тираж 100 екз.

Видавництво Ужгородського національного університету
м. Ужгород, вул. Капітульна, 18