Міністерство освіти і науки України
Центральноукраїнський національний технічний університет
Кафедра «Автоматизація виробничих процесів»

Т Е О Р І Я І Н Ф О Р М А Ц І Ї

МЕТОДИЧНІ ВКАЗІВКИ

до виконання контрольної роботи

для студентів спеціальності

151 «Автоматизація та комп’ютерно – інтегровані техології»

заочної форми навчання

Затверджено на засіданні кафедри
«Автоматизація виробничих процесів»
Протокол № 3 від 26 вересня 2018 р.

Кропивницький
2018

Теорія інформації. Методичні вказівки до виконання контрольної роботи для студентів спеціальності 151 «Автоматизація та комп`ютерно інтегровані технології» заочної форми навчання

/Укл.: Осадчий С.І., Березюк І.А., Зубенко В.О. – Кропивницький: ЦНТУ, 2018. – 74 с.

Укладачі: Осадчий С.І. – доктор технічних наук, професор

Березюк І.А. – кандидат технічних наук, доцент

Зубенко В.О. – кандидат технічних наук, доцент

Рецензент: Каліч В. М., кандидат технічних наук, професор.

ЗМІСТ

1 КІЛЬКІСНА ОЦІНКА ІНФОРМАЦІЇ

Загальне число повідомлень, що не повторюються, яке може бути складене з алфавіту *m* шляхом комбінування по *n* символів в повідомленні

$$N = m^n \tag{1}$$

Невизначеність, що приходиться на символ первинного (кодованого) алфавіту, складеного з рівноймовірних і взаємонезалежних символів

$$H = \log m \tag{2}$$

Основа логарифму впливає лише на зручність обчислення. У разі оцінювання ентропії:

а) у двійкових одиницях

$$H = \log_2 m \ \ біт/символ;$$

б) у десяткових одиницях

$$H = \lg m \ \ біт/символ,$$

де $\log_2 3{,}32 \lg m, 1 біт \approx 0{,}693 нат$;

в) у натуральних одиницях

$$H = \ln m \ нат/символ,$$

де $\log_2 m = 1{,}443 \ \ln m, 1 \ біт \approx 0{,}693 \ нат.$

Оскільки інформація є невизначеність, що знімається при отриманні повідомлення, то кількість інформації може бути представлена як добуток загального числа повідомлень *k* на середню ентропію *H*, що приходиться на одне повідомлення:

$$I = kH \ \ біт. \tag{3}$$

Для випадків рівноймовірних і взаємонезалежних символів первинного алфавіту кількість інформації в *k* повідомленнях алфавіту *m* дорівнює

$$I = k \log_2 m \ , біт.$$

Для нерівноймовірних алфавітів ентропія на символ алфавіту

$$H = \sum_{i=1}^{m} p_i \log_2 \frac{1}{p_i} = -\sum_{i=1}^{m} p_i \log_2 \ p_i \quad біт/символ, \tag{4}$$

а кількість інформації в повідомленні, складеному з *k* нерівноймовірних

символів

$$I = -k\sum p_i \log_2 p_i \quad бiт. \tag{5}$$

Кількість інформації визначається виключно характеристиками первинного алфавіту, об'єм – характеристиками вторинного алфавіту. Об'єм інформації

$$Q = kl_{ср} \tag{6}$$

де $l_{ср}$ – середня довжина кодових слів вторинного алфавіту. Для рівномірних кодів (всі комбінації коду містять однакову кількість розрядів)

$$Q = kn,$$

де n – довжина коду (число елементарних посилок в коді). Згідно (3), об'єм дорівнює кількості інформації, якщо $l_{ср}=H$, тобто у разі максимального інформаційного навантаження на символ повідомлення. В іншому випадку $I < Q$.

Наприклад, якщо кодувати в коді Бодо деякий рівноймовірний алфавіт, що складається з 32 символів, то

$$I = kH = k\log_2 m = k\log_2 32 = k*5 \quad бiт;$$
$$Q = kl_{ср} = k*5.$$

Якщо закодувати в коді Бодо російський 32-літерний алфавіт, то без урахування кореляції між літерами кількість інформації

$$I = kH = k*4{,}358 \; бiт; \; Q = k*5; \; Q > I,$$

тобто якщо в коді існує надмірність і $H \neq H_{макс}$,то об'єм в бітах завжди більше кількості інформації в тих же одиницях.

Задача 1.1: Припустимо, є набір з 3-х літер А, В, С. а) Скласти максимальну кількість повідомлень, комбінуючи по дві літери в повідомленні. б) Яка кількість інформації приходиться на одне таке повідомлення?

Розв'язок:

а) АА, ВА, СА, АВ, ВВ, СВ, АС, ВС, СС;

б) $N = m^n$; $N = 3^2 = 9$.

Задача 1.2: Символи алфавіту володіють двома якісними ознаками (m = 2, символів первинного алфавіту). а) Яку кількість повідомлень можна отримати, комбінуючи по 3, 4, 5 і 6 елементів в повідомленнях? б) Яка кількість інформації приходиться на один елемент таких повідомлень?

Розв'язок:

а) $N = m^n$; $m = 2$;

$N_1 = 2^3 = 8; \quad N_2 = 2^4 = 16; \quad N_3 = 2^5 = 32; \quad N_4 = 2^6 = 64;$

б $I = \log_2 N;$

$I_1 = \log_2 8 = 3$ *біт*, $\quad I_2 = \log_2 16 = 4$ *біт*, $\quad I_3 = \log_2 32 = 5$ *біт*, $\quad I_4 = \log_2 64 = 6$ *біт*.

2. УМОВНА ЕНТРОПІЯ І ЕНТРОПІЯ ОБ'ЄДНАННЯ

Поняття умовної ентропії в теорії інформації використовується при визначенні взаємозалежності між символами кодованого алфавіту, для визначення втрат при передачі інформації по каналах зв'язку, при обчисленні ентропії об'єднання.

У всіх випадках при обчисленні умовної ентропії в тому або іншому вигляді використовується умовна ймовірність.

Якщо при передачі n повідомлень символ A з'явився m разів, символ B з'явився l разів, а символ A разом з символом B – k разів, то ймовірність появи символу A - $p(A)=\frac{m}{n}$; ймовірність появи символу B - $p(B)=\frac{l}{n}$; ймовірність сумісної появи символів A і B $p(AB)=\frac{k}{n}$; умовна ймовірність появи символу A відносно символу B і умовна ймовірність появи символу B відносно символу A

$$p(A/B)=\frac{p(AB)}{p(B)}=\frac{k}{l};\quad p(B/A)=\frac{p(AB)}{p(A)}=\frac{k/n}{m/n}=\frac{k}{m}. \tag{7}$$

Якщо відома умовна ймовірність, то можна легко визначити і ймовірність сумісної появи символів A і B, використовуючи вирази (7)

$$p(AB)=p(B)p(A/B)=p(A)p(B/A). \tag{8}$$

Від класичного виразу (4) формула умовної ентропії відрізняється тим, що в ній ймовірність - умовна:

$$H(b_j/a_i)=-\sum_j p(b_j/a_i)\log p(b_j/a_i); \tag{9}$$

$$H(a_i/b_j)=-\sum_i p(a_i/b_j)\log p(a_i/b_j), \tag{10}$$

де індекс i вибраний для характеристики довільного стану джерела повідомлення А, індекс j вибраний для характеристики довільного стану адресата В.

Розрізняють поняття часткової і загальної умовної ентропії. Вирази (9) і (10) є частковими умовними ентропіями. *Загальна умовна ентропія*

повідомлення B відносно повідомлення A характеризує кількість інформації, що міститься в будь-якому символі алфавіту, і визначається усереднюванням по всіх символах, тобто по всіх станах з урахуванням ймовірністі появи кожного із станів, і дорівнює сумі ймовірністі появи символів алфавіту на невизначеність, яка залишається після того, як адресат прийняв сигнал

$$H(B/A) = -\sum_i p(a_i) H(b_j / a_i) = -\sum_i \sum_j p(a_i)\, p(b_j / a_i) \log p(b_j / a_i) \qquad (11)$$

Вираз (11) є загальним виразом для визначення кількості інформації на один символ повідомлення для випадку нерівномірних і взаємонезалежних символів.

Оскільки $p(a_i)\, p(b_j / a_i)$ є ймовірністю сумісної появи двох подій $p(a_i, b_j)$, то формулу (11) можна записати таким чином:

$$H(B/A) = -\sum_i \sum_j p(a_i, b_j) \log p(b_j / a_i). \qquad (12)$$

Поняття загальної і частинної умовної ентропії широко використовується при обчисленні інформаційних втрат в каналах зв'язку з шумами.

У загальному випадку, якщо ми передаємо *m* сигналів *A* і чекаємо отримати *m* сигналів *B*, вплив перешкод в каналі зв'язку повністю описується *канальною матрицею*, яку наведено нижче:

B A	b_1 b_2 … b_j … b_m
a_1	$p(b_1/a_2)$, $p(b_2/a_1)$, ..., $p(b_j/a_1)$, ..., $p(b_m/a_1)$
a_2	$p(b_1/a_2)$, $p(b_2/a_2)$, ..., $p(b_j/a_2)$, ..., $p(b_m/a_2)$
…	.....
a_i	$p(b_1/a_i)$, $p(b_2/a_i)$, ..., $p(b_j/a_i)$, ..., $p(b_m/a_2)$
…	.....
a_m	$p(b_1/a_m)$, $p(b_2/a_m)$, ..., $p(b_j/a_m)$, ..., $p(b_m/a_m)$

Ймовірності, які розташовані по діагоналі, визначають правильний

прийом, інші - помилковий. Значення цифр, що заповнюють колонки канальної матриці, зазвичай зменшуються по мірі їх віддалення від головної діагоналі і при повній відсутності перешкод всіх, окрім цифр, розташованих на головній діагоналі, дорівнюють нулю.

Якщо описувати канал зв'язку з боку джерела повідомлень, то проходження даного виду сигналу в даному каналі зв'язку описується розподілом умовної ймовірності вигляду $p(b_j / a_i)$, то для сигналу a_i розподілом вигляду

$$p(b_1 / a_1) + p(b_2 / a_1) + ... + p(b_j / a_i) + ... + p(b_m / a_1). \quad (13)$$

Сума ймовірностей розподілу (13) завжди дорівнює 1. Втрати інформації, які припадають на частку сигналу a_1 описуються за допомогою *частковою умовною ентропією* вигляду

$$H(b_j / a_1) = -\sum_j p(b_j / a_1) \log p(b_j / a_1) \quad (14)$$

Сумування проводиться по *j*, оскільки *і-й* стан (у даному випадку перший) залишається постійним.

Щоб врахувати втрати при передачі всіх сигналів по даному каналу зв'язку, слід підсумувати всі часткові умовні ентропії, тобто провести подвійне підсумовування по *i* та *j*. При цьому у разі рівноймовірної появи сигналів на виході джерела повідомлень

$$H(B / A) = -\frac{1}{m} \sum_j p(b_j / a_i) \log p(b_j / a_i) \quad (15)$$

(на *m* ділимо, оскільки ентропія є невизначеність на один символ).

У разі нерівноімовірної появи символів джерела повідомлень слід врахувати вірогідність появи кожного символу, помноживши на неї відповідну власну умовну ентропію. При цьому загальна умовна ентропія

$$H(B / A) = -\sum_i p(a_i) \sum_j p(b_j / a_i) \log p(b_j / a_i) \quad (16)$$

Якщо ми досліджуємо канал зв'язку з боку приймача повідомлень, то з отриманням сигналу b_j припускаємо, що був відправлений якійсь з сигналів

$a_1, a_2, ..., a_i, ..., a_m$. При цьому канальна матриця матиме вигляд

B / A	b_1	b_2	…	b_j	…	b_m
a_1	$p(a_1/b_2)$,	$p(a_2/b_1)$, ...,		$p(a_1/b_j)$,	...,	$p(a_1/b_m)$
a_2	$p(a_1/b_2)$,	$p(a_2/b_2)$, ...,		$p(a_2/b_j)$,	...,	$p(a_1/b_m)$
…	.....					
a_i	$p(a_i/b_1)$,	$p(a_i/b_2)$, ...,		$p(a_i/b_j)$,	...,	$p(a_i/b_m)$
…	.....					
a_m	$p(a_m/b_1)$,	$p(a_m/b_2)$, ...,		$p(a_m/b_j)$, ...,		$p(a_m/b_m)$

В цьому випадку одиниці повинні дорівнювати суми умовної імовірності не по рядках, а по стовбцях канальної матриці

$$p(a_1/b_j) + p(a_2/b_j) + ... + p(a_i/b_j) + ... + p(a_m/b_j) = 1.$$

Часткова умовна ентропія

$$H = (a_i/b_j) = -\sum_{i=1}^{m} p(a_i/b_j) \log p(a_i/b_j), \tag{17}$$

а загальна умовна ентропія

$$H(A/B) = -\sum_j p(b_j) \sum_i p(a_i/b_j) \log p(a_i/b_j). \tag{18}$$

Оскільки

$$p(a_i)\, p(b_j/a_i) = p(a_i, b_j),$$

то для обчислення загальної умовної ентропії нарівні з виразом (16) може бути використаний наступний вираз:

$$H(B/A) = -\sum_i \sum_j p(a_i, b_j) \log p(b_j/a_i). \tag{19}$$

Якщо задані канальна матриця вигляду $p(b_j/a_i)$ (частинна умовна ентропія в цьому випадку відповідає (14)) і безумовна ймовірність вигляду $p(a_i)$, то безумовну ймовірність приймача $p(b_j)$ знаходимо як $\sum_i p(a_i)\, p(b_j/a_i)$, тобто якщо задані безумовна ймовірність джерела і канальна матриця, то може бути обчислена ентропія приймача

$$H(B) = -\sum_j p(b_j) \log p(b_j),$$

і навпаки, якщо задана ймовірність вигляду $p(b_j)$ і канальна матриця, що описує канал зв'язку з боку приймача повідомлень (частинна умовна ентропія при цьому відповідає виразу (17)), то $p(a_i) = \sum_j p(b_j)\, p(a_i / b_j)$, а значить може бути визначена ентропія джерела повідомлень

$$H(A) = -\sum_i p(a_i) \log p(a_i).$$

Якщо взаємозалежність зв'язує 3 елементи a_i, a_j, a_k, то умовна ентропія обчислюється за формулою

$$H(A / B, K) = -\sum_i \sum_j \sum_k p(a_i, a_j, a_k) \log p(a_i, a_j, a_k),$$

аналогічно і для 4, 5,…, n елементів.

Ентропія об'єднання використовується для обчислення ентропії сумісної появи статистично залежних повідомлень. Наприклад, передавши сто разів цифру 5 по каналу зв'язку з перешкодами, відмітимо, що цифра 5 була прийнята 90 разів, цифра 6 – 8 разів і цифра 4 – 2 рази. Невизначеність виникнення комбінацій вигляду 5 – 4, 5 – 5, 5 – 6 при передачі цифри 5 може бути описана за допомогою ентропії об'єднання $H(A,B)$ - невизначеність того, що буде послано *A,* а прийнято *B*. Для ансамблів переданих повідомлень *A* і прийнятих повідомлень *B* ентропія об'єднання є сумою вигляду

$$H(A,B) = -\sum_i \sum_j p(a_i, b_j) \log p(a_i, b_j) \;\; \textit{біт / два символа.} \qquad (20)$$

Ентропія об'єднання і умовна ентропія зв'язані між собою наступними співвідношеннями:

$$H(A,B) = H(A) + H(B/A) = H(B) + H(A/B),$$
$$H(B/A) = H(A,B) - H(A); \quad H(A/B) = H(A,B) - H(B).$$

Ентропія об'єднання може бути підрахована за допомогою матриці вигляду

$$p(a_i, b_j) = \begin{vmatrix} p(a_1, b_1) & p(a_1, b_2) & \dots & p(a_1, b_m) \\ p(a_2, b_1) & p(a_2, b_2) & \dots & p(a_2, b_m) \\ \dots\dots\dots & \dots\dots\dots & \dots & \dots\dots\dots \\ p(a_m, b_1) & p(a_m, b_2) & \dots & p(a_m, b_m) \end{vmatrix}$$

Така матриця володіє натупною властивістю: $\sum_i p(a_i, b_j) = p(b_j)$; $\sum p(a_i, b_j) = p(a_i)$, при цьому $\sum_i p(a_i) = \sum_j p(b_j) = 1$. Ця властивість, у свою чергу, дозволяє обчислювати ентропію як джерела, так і приймача повідомлень безпосередньо по канальній матриці

$$H(A) = -\sum_i \sum_j p(a_i, b_j) \log \sum_j p(a_i, b_j), \tag{21}$$

$$H(B) = -\sum_i \sum_j p(b_j, a_i) \log \sum_i p(b_j, a_i) \tag{22}$$

Умовні ймовірності вигляду $p(a_i / b_j)$ і $p(b_j / a_i)$ обчислюються як

$$p(a_i, b_j) = \frac{p(a_i, b_j)}{\sum_i p(a_i, b_j)}; \quad p(b_j / a_i) = \frac{p(a_i, b_j)}{\sum_j p(a_i, b_j)}.$$

Кількість інформації на символ повідомлення, переданого по каналу зв'язку, в якому вплив перешкод описується за допомогою ентропії об'єднання, розраховується таким чином

$$I(A, B) = H(A) + H(B) - H(B, A).$$

Задача 2.1: В результаті статистичних випробувань встановлено, що при передачі кожних 100 повідомлень завдовжки по 5 символів в повідомленні символ *К* зустрічається 50 разів, а символ *Т* – 30 разів. Разом з символом *К* символ Т зустрічається 10 разів. Визначити умовні ентропії *H(K/T)* і *H(T/K).*

Розв'язок:

Загальна кількість переданих символів

$$n = 100 * 5 = 500$$

Ймовірності появи символів *Т* та *К*

$$p(K) = \frac{50}{500} = 0{,}1; \; p(T) = \frac{30}{500} = 0{,}06.$$

Ймовірність сумісної появи символу *К* і *Т*

$$p(KT) = \frac{10}{500} = 0{,}02.$$

Оскільки $p(KT) = p(T)p(K/T) = p(K)p(T/K)$, то умовна ймовірність появи символу K відносно T

$$p(K/T) = \frac{p(KT)}{p(T)} = \frac{0{,}02}{0{,}06} = 0{,}33.$$

Умовна ймовірність появи символу T відносно символу K

$$p(T/K) = \frac{p(KT)}{p(K)} = \frac{0{,}02}{0{,}1} = 0{,}2.$$

Умовна ентропія символу K відносно T

$$H(K/T) = -\sum p(b_j/a_i)\log_2 p(b_j/a_i) = -\{p(K/T)\log_2 p(K/T) +$$

$$+[1-p(K/T)]\log_2[1-p(K/T)]\} = -(0{,}33\log_2 0{,}33 +$$
$$+0{,}67\log_2 0{,}67) = 0{,}9149\ \textit{біт/символ}.$$

Умовна ентропія появи символу T відносно K

$$H(T/K) = -(0{,}2\log_2 0{,}2 + 0{,}8\log_2 0{,}8) = 0{,}7219\ \textit{біт/символ}.$$

3. ОБЧИСЛЕННЯ ІНФОРМАЦІЙНИХ ВТРАТ ПРИ ПЕРЕДАЧІ ПОВІДОМЛЕНЬ ПО КАНАЛАХ ЗВ'ЯЗКУ З ШУМАМИ

Втрати інформації в каналах зв'язку з шумами зазвичай описують за допомогою умовної ентропії і ентропії об'єднання.

Якщо перешкод немає або їх рівень настільки низький, що вони не в змозі знищити сигнал або імітувати корисний сигнал у відсутність передачі, то при передачі ми будемо твердо упевнені, що отримаємо - сигнал, що відповідає переданому a_i сигналу. Події А і В статистично жорстко зв'язані, умовна ймовірність максимальна, а умовна ентропія

$$H(A/B) = -\sum p(b_j / a_i)\log p(b_j / a_i) = 0, \qquad (23)$$

оскільки $\log p(b_j / a_i) = \log 1 = 0.$ У цьому випадку кількість інформації, що міститься в прийнятому ансамблі повідомлень В, дорівнює ентропії повідомлень, що передаються, ансамблю А, тобто I(B, A)= H (A).

При високому рівні перешкод будь-який з прийнятих сигналів b_j може відповідати будь-якому прийнятому сигналу a_i, статистичний зв'язок між переданими і прийнятими сигналами відсутній. В цьому випадку ймовірність $p(a_i)$ і $p(b_j)$ є ймовірність незалежних подій і

$$p(b_j / a_i) = p(b_j);\ \log p(a_i / b_j) = p(a_i).$$

$$H(A/B) = -\sum_i \sum_j p(b_j)\, p(a_i / b_j)\log p(a_i / b_j) =$$

$$= -\sum_i \sum_j p(b_j)\, p(a_i)\log p(a_i) = \sum_j p(b_j) H(A) = H(A)$$

оскільки $\sum_j p(b_j) = 1,$ тобто умовна ентропія дорівнює безумовній, а кількість інформації, що міститься у B, відносно A дорівнює нулю:

$$I(A,B) = H(A) - H(A/B) = 0$$

Інформаційні характеристики реальних каналів зв'язку лежать між цими двома граничними випадками. При цьому втрати інформації при передачі k символів по даному каналу зв'язку

$$\Delta I = kH(A/B).$$

Не дивлячись на те, що частина інформації вражається перешкодами, між прийнятими і переданими повідомленнями існує статистична залежність. Це дозволяє описувати інформаційні характеристики реальних каналів зв'язку за допомогою ентропії об'єднання статистично залежних подій. Оскільки

$$H(A,B) = H(A) + H(B/A) = H(B) + H(A/B), \tag{24}$$

то втрати в каналі зв'язку можуть бути враховані за допомогою ентропії об'єднання таким чином:

$$I(B,A) = H(A) + H(B) - H(B,A), \tag{25}$$

а з використанням умовної ентропії

$$I(B,A) = H(A) - H(A/B) = H(B) - H(B/A).$$

Для обчислення середньої кількості інформації, що міститься в прийнятому ансамблі повідомлень B відносно передаваного ансамблю повідомлень A в умовах дії перешкод, користуються наступними виразами, виведеними безпосередньо з виразу (25):

$$I(B,A) = \sum_i \sum_j p(a_i)\, p(b_j/a_i) \log \frac{p(b_j/a_u)}{p(b_j)}, \tag{26}$$

$$I(B,A) = \sum_i \sum_j p(b_j)\, p(a_i/b_j) \log \frac{p(a_i/b_j)}{p(a_i)}, \tag{27}$$

$$I(B,A) = I(A,B) = \sum_i \sum_j p(a_i,b_j) \log \frac{p(b_j/a_u)}{p(b_j)} = \sum_i \sum_j p(b_j,a_i) \log \frac{p(a_i/b_j)}{p(a_i)} =$$
$$= \sum_i \sum_j p(a_i,b_j) \log \frac{p(a_i,b_j)}{p(a_i)\,p(b_j)}. \tag{28}$$

Для обчислення часто зручно застосовувати вирази (26-28) у вигляді

$$I(A,B) = \sum_j p(b_j) \sum_i [p(a_i/b_j) \log p(a_i/b_j) - p(a_i/b_j) \log p(a_i)],$$
$$I(B,A) = \sum_i p(a_i) \sum_j [p(b_j/a_i) \log p(b_j/a_i) - p(b_j/a_i) \log p(b_j)],$$
$$I(A,B) = I(B,A) = \sum_i \sum_j p(a_i,b_j) \log p(a_i,b_j) - \sum_i \sum_j p(a_i,b_j) \log p(a_i)\,p(b_j).$$

Для повного і всестороннього опису каналу зв'язку необхідно задати: канальну матрицю вигляду $p(a_i/b_j)$ і безумовну ймовірність вигляду $p(b_j)$

або канальну матрицю вигляду $p(b_j / a_i)$ і безумовну ймовірність вигляду $p(a_i)$ або канальну матрицю вигляду $p(a_i, b_j)$. У останньому випадку сума значень матриці по стовпцях дає безумовну ймовірність вигляду $p(b_j)\left(\sum_j p(b_j) = 1\right)$, а сума по рядках дає безумовну ймовірність вигляду $p(a_i)\left(\sum_i p(a_i) = 1\right)$. Умовна ймовірність може бути знайденою з виразів:

$$p(a_i / b_j) = \frac{p(b_j, a_i)}{p(b_j)}; \quad p(b_j / a_i) = \frac{p(a_i, b_j)}{p(a_i)}.$$

Знаючи умовну і безумовну ймовірність, можна знайти *H(A), H(B), H(A/B)* і *H(B/A).*

Якщо рівень перешкод настільки високий, що з рівною імовірністю можна чекати перехід будь-якого символу джерела повідомлення в довільний символ первинного алфавіту, то ентропія каналу зв'язку буде дорівнювати $\log_2 m$, а кількість інформації $I = H(A) - \log_2 m \le 0$ при цьому значення *I* може бути від'ємною величиною, що означає, що канал зв'язку вносить дезінформацію.

Задача 3.1: Використовуючи ентропію об'єднання, визначити кількість інформації при передачі повідомлень, побудованих з алфавіту 1, 2, 3, якщо апріорна ймовірність появи символів первинного алфавіту рівна між собою, а в результаті дії перешкод 5% символів передаваних повідомлень можуть з рівною імовірністю перейти в будь-який інший символ даного алфавіту.

Розв'язок:

$$\begin{array}{l|l|l} p_1 = 0{,}333; & p(1/1) = p(2/2) = p(3/3) = & p(1,1) = p(2,2) = p(3,3) = \\ & = 0{,}95 & = 0{,}333 * 0{,}95 = 0{,}3166; \\ p_2 = 0{,}333; & p(2/1) = p(3/1) = p(1/3) = & p(1,2) = p(1,3) = p(2,3) = \\ p_3 = 0{,}333. & = p(2/3) = p(1/2) = p(3/2) = & = p(3,1) = p(2,1) = p(3,2) = \\ & = 0{,}025. & = 0{,}333 * 0{,}025 = 0{,}008325. \end{array}$$

$H(A) = \log_2 3 = 1{,}58$ *біт / символ.*

Канальна матриця має вигляд

$$p(b/a) = \begin{vmatrix} 0,95 & 0,025 & 0,025 \\ 0,025 & 0,95 & 0,025 \\ 0,025 & 0,025 & 0,95 \end{vmatrix}.$$

$$H(A/B) = H(B/A) = [-0,333(0,95\log_2 0,95 + 2*0,025\log_2 0,025)]*3 =$$
$$= 0,07 + 0,266 = 0,336 \quad \textit{біт/символ.}$$
$$H(A,B) = -[p(1,1)\log_2 p(1,1) + p(2,2)\log_2 p(2,2) + p(3,3)\log_2 p(3,3) +$$
$$+ p(1,2)\log_2 p(1,2) + p(2,1)\log_2 p(2,1) + p(1,3)\log_2 p(1,3) + p(3,1)\log_2 p(3,1) +$$
$$+ p(3,2)\log_2 p(3,2) + p(2,3)\log_2 p(2,3)] = (3*0,3166\log_2 0,3166 +$$
$$+ 6*0,008325\log_2 0,008325) = 1,5762 + 0,3438 = 1,92 \quad \textit{біт/два символа},$$

або

$$H(A,B) = H(A) + H(B/A) = 1,58 + 0,336 = 1,916 \quad \textit{біт/два символа.}$$
$$I(A,B) = H(A) - H(A/B) = 1,58 - 0,336 = 1,244 \quad \textit{біт},$$

або $I(A,B) = H(A) + H(B) - H(A,B) = 3,16 - 1,92 = 1,24 \quad \textit{біт.}$

4. ВИЗНАЧЕННЯ НАДМІРНОСТІ ПОВІДОМЛЕНЬ. ОПТИМАЛЬНЕ КОДУВАННЯ

Якщо ентропія джерела повідомлень не дорівнює максимальній ентропії для алфавіту з даною кількістю якісних ознак (маються на увазі якісні ознаки алфавіту, за допомогою яких складаються повідомлення), то це перш за все означає, що повідомлення даного джерела могли б нести більшу кількість інформації. Абсолютна недовантаженість на символ повідомлень такого джерела $\Delta D = (H_{макс} - H)$ *біт / символ* .

Для визначення кількості «зайвої» інформації, яка закладена в структурі алфавіту або в природі коду, вводиться поняття надмірності. Надмірність, з якою ми маємо справу в теорії інформації, не залежить від змісту повідомлення і зазвичай заздалегідь відома із статистичних даних.

Інформаційна надмірність показує відносну недовантаженість на символ алфавіту і є безрозмірною величиною:

$$D = \frac{H_{макс} - H}{H_{макс}} = 1 - \frac{H}{H_{макс}}, \qquad (29)$$

де $\frac{H}{H_{макс}} = \mu$ — коефіцієнт стиснення (відносна ентропія). H і $H_{макс}$ беруться відносно одного і того ж алфавіту.

Окрім загального поняття надмірності існують частинні види надмірності.

Надмірність, обумовлена нерівноімовірним розподілом символів в повідомленні

$$D_p = 1 - \left(\frac{-\sum_i p_i \log_2 p_i}{\log_2 m} \right). \qquad (30)$$

Надмірність, викликана статистичним зв'язком між символами повідомлення

$$D_s = 1 - \left[\frac{-\sum_i \sum_j p(a_i)\, p(b_j / a_i) \log_2 p(b_j / a_i)}{-\sum_i p_i \log_2 p_i} \right]. \qquad (31)$$

Повна інформаційна надмірність

$$D = D_s + D_P - D_s D_p. \qquad (32)$$

Так при передачі десяткових цифр двійковим кодом максимально завантаженими бувають тільки ті символи вторинного алфавіту, які передають значення, що є цілочисельними степенями двійки. У решті випадків тією ж кількістю символів може бути передане більша кількість цифр (повідомлень). Наприклад, трьома двійковими розрядами ми можемо передати і цифру 5, і цифру 8, тобто на передачу п'яти повідомлень витрачається стільки ж символів, скільки витрачається і на вісім повідомлень.

Фактично для передачі повідомлення досить мати довжину кодової комбінації

$$L \geq \frac{\log_2 N}{\log_2 m},$$

де N - загальна кількість передаваних повідомлень.

L можна представити і як

$$L \geq \frac{\log_2 m_1}{\log_2 m_2},$$

де m_1 і m_2 —відповідно якісні ознаки первинного і вторинного алфавітів. Тому для цифри 5 в двійковому коді можна записати

$$L \geq \frac{\log_2 5}{\log_2 2} = 2{,}32 \; \textit{дв. символа.}$$

Проте цю цифру необхідно округляти до найближчого цілого числа, оскільки довжина коду не може бути виражена дробовим числом. Округлення, природно, проводиться у більшу сторону. У загальному випадку, надмірність від округлення

$$D_0 = \frac{k - \varphi}{k},$$

де $\varphi = \frac{\log_2 m_1}{\log_2 m_2}$, k - зокруглене до найближчого цілого числа значення φ.

Для нашого прикладу

$$D_0 = \frac{3 - 2{,}32}{3} \approx 0{,}227.$$

Надмірність - не завжди небажане явище. Для підвищення перешкодостійкості кодів надмірність необхідна і її вводять штучно у вигляді додаткових n_k символів. Якщо в коді всього n розрядів і n_i з них несуть інформаційне навантаження, то $n_k = n - n_i$ характеризує абсолютну коректуючу надмірність, а величина $D_k = \frac{n - n_i}{n_i}$ характеризує відносну коректуючу надмірність.

Інформаційна надмірність – явище природнє, і вона закладена в первинному алфавіті. Корректуюча надмірність - явище штучне, закладена вона в кодах**,** представлених у вторинному алфавіті.

Найбільш ефективним способом зменшення надмірності повідомлення є побудова оптимальних кодів.

Оптимальні коди - коди з практично нульовою надмірністю. Оптимальні коди мають мінімальну середню довжину кодових слів - L. Верхня і нижня межі L визначаються з нерівності

$$\frac{H}{\log m} \le L \le \frac{H}{\log m} + 1, \qquad (33)$$

де H - ентропія первинного алфавіту, m - число якісних ознак вторинного алфавіту.

У разі поблокового кодування, де кожен з блоків складається з M незалежних літер $a_1, a_2, ..., a_M$ мінімальна середня довжина кодового блоку лежить в межах

$$\frac{MH}{\log m} \le L_M \le \frac{MH}{\log m} + 1, \qquad (34)$$

Загальний вираз середнього числа елементарних символів на літеру повідомлення при блоковому кодуванні

$$\frac{H}{\log m} \le L \le \frac{H}{\log m} + \frac{1}{M}, \qquad (35)$$

Суть блокового кодування можна з'ясувати на прикладі представлення десяткових цифр в двійковому коді. Так, при передачі цифри 9 в двійковому коді необхідно витратити 4 символи, тобто 1001. Для передачі цифри 99 якщо кодувати по літері - 8, при поблочному - 7, оскільки 7 двійкових знаків достатні для передачі будь-якої цифри від 0 до 123; при передачі цифри 999 співвідношення буде 12 - 10, при передачі цифри 9999 співвідношення буде 16 - 13 і так далі В загальному випадку «вигода» блокового кодування виходить і за рахунок того, що в блоках відбувається вирівнювання ймовірності окремих символів, що веде до підвищення інформаційного навантаження на символ.

При побудові оптимальних кодів найбільше розповсюдження знайшли методики Шеннона - Фано і Хаффмена.

Згідно методики Шеннона - Фано побудова оптимального коду ансамблю з повідомлень зводиться до виконання наступних кроків:

1-й крок. Множина з повідомлень розташовується в порядку спадання ймовірності.

2-й крок. Первинний ансамбль кодованих сигналів розбивається на дві групи так, щоб сумарна ймовірность повідомлень обох груп була по можливості рівна. Якщо рівної ймовірності в підгрупах не можна досягти, то їх ділять так, щоб у верхній частині (верхній підгрупі) залишалися символи, сумарна ймовірность яких менше сумарної ймовірності символів в нижній частині (у нижній підгрупі).

3-й крок. Першій групі присвоюється символ 0, другій групі символ 1.

4-й крок. Кожну з утворених підгруп ділять на дві частини так, щоб сумарна ймовірность знов утворених підгруп була по можливості рівна.

5-й крок. Першим групам кожної з підгруп знов присвоюють 0, а другим - 1. Таким чином, ми отримуємо інші цифри коду. Потім кожна з чотирьох груп знов ділиться на рівні (з огляду на сумарну ймовірність)

частини до тих пір, поки в кожній з підгруп не залишиться по одній літері.

Відповідно до методики Хаффмена, для побудови оптимального коду N символи первинного алфавіту виписуються в порядку спадання ймовірності. Останні n_0 символів, де $2 \le n_0 \le m$ і $\frac{N-n_0}{m-1}$ - ціле число, об'єднують в деякий новий символ з ймовірностю, яка дорівнює сумі ймовірностей об'єднаних символів. Останні символи з урахуванням отриманого символу знов об'єднують, отримують новий, допоміжний символ, знову виписують символи в порядку спадання ймовірності з урахуванням допоміжного символу і так далі, до тих пір, доки сума ймовірностей символів, що залишилися, після $\frac{N-n_0}{m-1}$-го виписування в порядку спадання ймовірності не дасть в сумі ймовірность, яка дорівнює 1. На практиці зазвичай, не проводять багатократного виписування ймовірності символів з урахуванням ймовірності допоміжного символу, а обходяться елементарними геометричними побудовами, суть яких зводиться до того, що символи кодованого алфавіту попарно об'єднуються в нові символи, починаючи з символів, що мають найменшу ймовірность. Потім з урахуванням знов отриманих символів, яким привласнюється значення сумарної ймовірності двох попередніх, будують кодове дерево, у вершині якого стоїть символ з ймовірностю 1. При цьому відпадає необхідність у впорядковуванні символів кодованого алфавіту в порядку спадання ймовірності.

Побудовані по вказаних вище (або подібним) методиках коди з нерівномірним розподілом символів, що мають мінімальну середню довжину кодового слова, називають оптимальними, нерівномірними, кодами (ОНК). Рівномірні коди можуть бути оптимальними тільки для передачі повідомлень з рівноймовірним розподілом символів первинного алфавіту, при цьому число символів первинного алфавіту повинно дорівнювати цілій степені числа, яке дорівнює кількості якісних ознак

вторинного алфавіту, а у разі двійкового коду - цілої степені двох.

Максимально ефективними будуть ті ОНК, у яких

$$\log_2 m\sum_{i=1}^{N} p_i l_i = l_{ср} = H.$$

Для двійкових кодів

$$\sum_{i=1}^{N} p_i l_i = -\sum_{i=1}^{N} p_i \log_2 p_i, \tag{36}$$

оскільки $\log_2 2 = 1$. Очевидно, що рівність (36) задовольняється за умови, що довжина коду у вторинному алфавіті

$$l_i = -\log_2 p_i = \log_2 \frac{1}{p_i}.$$

Величина l_i точно дорівнює Н, якщо $p_i = 2^{-n_i}$ де *n* - будь-яке ціле число. Якщо *n* не є цілим числом для всіх значень літери первинного алфавіту, то $l_{ср} > H$ і, відновідно до основної теоремі кодування, середня довжина кодового слова наближається до ентропії джерела повідомлень по мірі укрупнення кодованих блоків.

Ефективність ОНК оцінюють за допомогою коефіцієнта статистичного стиснення:

$$K_{с.с} = \frac{H_{макс}}{l_{ср}} = \frac{\log_2 N}{\log_2 m\sum_{i=1}^{N} p_i l_i}, \tag{37}$$

який характеризує зменшення кількості двійкових знаків на символ повідомлення при застосуванні ОНК в порівнянні із застосуванням методів нестатистичного кодування, і коефіцієнта відносної ефективності

$$K_{о.э} = \frac{H}{l_{ср}}, \tag{38}$$

який показує, наскільки використовується статистична надмірність повідомлення, що передається.

Для найбільш загального випадку нерівноімовірних і взаємонезалежних символів

$$K_{о.э} = \frac{-\sum_{i=1}^{N} p_i \log_2 p_i}{\log_2 m \sum_{i=1}^{N} p_i l_i}.$$

Для випадку нерівноімовірних і взаємозалежних символів

$$K_{о.э} = \frac{-\sum_i \sum_j p_i p(j/i) \log_2 p(j/i)}{\log_2 m \sum_{i=1}^{N} p_i l_i}.$$

Задача 4.1: Повідомлення складається з алфавіту a, b, c, d. Ймовірність появи літери алфавіту в текстах рівна відповідно: $p_a = 0{,}2;\ p_b = 0{,}3;\ p_c = 0{,}4;\ p_d = 0{,}1.$ Знайти надмірність повідомлень, складених з даного алфавіту.

Розв'язок. Надмірність, згідно (29)

$$D = \frac{H_{макс} - H}{H_{макс}} = 1 - \frac{H}{H_{макс}}.$$

Для алфавіту з чотирьох літер максимальна ентропія

$$H_{макс} = \log_2 m = \log_2 4 = 2\ , біт/символ.$$

Середня ентропія на символ повідомлення

$$H = -\sum_i p_i \log p_i = -(0{,}2\log_2 0{,}2 + 0{,}3\log_2 0{,}3 + 0{,}4\log_2 0{,}4 + 0{,}1\log_2 0{,}1) =$$

$$= 0{,}4644 + 0{,}5211 + 0{,}5288 + 0{,}3322 = 1{,}8465\ біт/символ$$

Тоді надмірність

$$D = 1 - \frac{1{,}8465}{2} = 1 - 0{,}9232 = 0{,}07688.$$

Задача 4.2: Побудувати оптимальний код повідомлення, в якому ймовірність появи літер первинного алфавіту, що складається з 8 символів, ім-ті появи яких дорівнює 1/4; 1/4; 1/8; 1/8; 1/16; 1/16

Розв'язок: Побудова оптимального коду ведеться по методиці Шеннона-Фано. Результати побудови відображені в таблиці 4.1:

Таблиця 4.1

Побудова оптимального коду методом Шеннона-Фано

Літери	Ймовірність появи літери	Кодове слово	Число знаків в кодовому слові	$p_i l_i$
A1	1/4	00	2	0,5
A2	1/4	01	2	0,5
A3	1/8	100	3	0,375
A4	1/8	101	3	0,375
A5	1/16	1100	4	0,25
A6	1/16	1101	4	0,25
A7	1/16	1110	4	0,25
A8	1/16	1111	4	0,25

Перевірка:

$$L = \sum_{i=1}^{N} p_i l_i = 2*0{,}5 + 2*0{,}375 + 4*0{,}25 = 2{,}75;$$

$$H = -\sum p_i \log_2 p_i = 2*0{,}85\log_2 0{,}85 + 2*0{,}125\log_2 0{,}125 + 4*0{,}0625\log_2 0{,}0625 =$$

$$= 1 + 2*0{,}375 + 4*0{,}25 = 2{,}75 \quad \textit{біт / символ.}$$

Примітка. Кодові слова однакової ймовірності появи мають однакову довжину.

5. ВИЯВЛЕННЯ І ВИПРАВЛЕННЯ ПОМИЛОК В ПОВІДОМЛЕННЯХ

5.1. Поняття про корекцію помилок

Для того, щоб в прийнятому повідомленні можна було виявити помилку це повідомлення повинне володіти деякою надмірною інформацією, що дозволяє відрізнити помилковий код від правильного. Наприклад, якщо передане повідомлення складається з трьох абсолютно однакових частин, то в прийнятому повідомленні відділення правильних символів від помилкових може бути здійснене за наслідками накопичення посилок одного вигляду, наприклад 0 або 1. Для двійкових кодів цей метод можна проілюструвати наступним прикладом:

10110 - передана кодова комбінація;

10010 - 1-а прийнята комбінація;

10100 - 2-а прийнята комбінація;

00110 - 3-а прийнята комбінація;

10110 - накопичена комбінація.

Як бачимо, не дивлячись на те, що у всіх трьох прийнятих комбінаціях були помилки, накопичена не містить помилок[8].

Прийняте повідомлення може також складатися з коду і його інверсії. Код і інверсія посилаються в канал зв'язку як одне ціле. Помилка на приймальному кінці виділяється при зіставленні коду і його інверсії.

Для того, щоб спотворення будь-якого з символів повідомлення призвело до забороненої комбінації, необхідно в коді виділити комбінації, що відрізняються один від одної у ряді символів, частину з цих комбінацій заборонити і тим самим ввести в код надмірність. Наприклад, в рівномірному блоковому коді вважати дозволеними кодові комбінації з постійним співвідношенням нулів і одиниць в кожній кодовій комбінації. Такі коди отримали назву *кодів з постійною вагою.* Для двійкових кодів число кодових комбінацій в кодах з постійною вагою завдовжки в *n* символів дорівнює

$$N = C_n^l = \frac{n!}{l!(n-l)!}, \tag{39}$$

де l - число одиниць в кодовому слові. Якби не існувало умови постійної ваги, то число комбінацій коду могло б бути набагато більшим, а саме 2^n. Прикладом коду з постійною вагою може служити стандартний телеграфний код № 3. Комбінації цього коду побудовані таким чином, що на 7 тактів, протягом яких повинна бути прийнята одна кодова комбінація, завжди приходяться три струмові і чотири безструмові посилки. Збільшення або зменшення кількості струмових посилок говорить про наявність помилки.

Ще одним прикладом введення надмірності в код є метод, суть якого полягає в тому, що до початкових кодів додаються нулі або одиниці так, щоб сума їх завжди. була парною або непарною. Збій будь-якого одного символу завжди порушить умову парності (непарності), і помилка буде виявлена. В цьому випадку комбінації одна від одної повинні відрізнятися мінімум в двох символах, тобто рівно половина комбінацій коду є забороненою (забороненими є всі непарні комбінації при перевірці на парність або навпаки).

У всіх згаданих вище випадках повідомлення володіють надмірною інформацією. Надмірність повідомлення говорить про те, що воно могло б містити більшу кількість інформації, коли б не багатократне повторення одного і того ж коду, не додавання до коду його інверсії, що не несе ніякої інформації, коли б не штучна заборона частин комбінацій коду і так далі . Але всі перераховані види надмірності доводиться вводити для того, щоб можна було відрізнити помилкову комбінацію від правильної.

Коди без надмірності виявляти, а тим більше виправляти помилки не можуть Мінімальна кількість символів, в яких будь-які дві комбінації коду відрізняються одна від одної, називається *кодовою відстанню.* Мінімальна кількість символів, в яких всі комбінації коду відрізняються одна від одної, називається *мінімальною кодовою відстанню.* Мінімальна

кодова відстань - параметр, що визначає перешкодостійкість коду і закладену в коді надмірність. Мінімальною кодовою відстанню визначаються властивості коректуючого коду.

У загальному випадку для виявлення *r* помилок мінімальна кодова відстань

$$d_0 = r + 1. \tag{40}$$

Мінімальна кодова відстань, яка необхідна для одночасного виявлення і виправлення помилок

$$d_0 = r + s + 1, \tag{41}$$

де s - число помилок, що виправляються.

Для кодів, що тільки виправляють помилки

$$d_0 = 2s + 1. \tag{42}$$

Для того, щоб визначити кодову відстань між двома комбінаціями двійкового коду, досить підсумувати ці комбінації за модулем 2 і підрахувати число одиниць в отриманій комбінації.

Якщо кодова комбінація двійкового коду *A* відстоіть від кодової комбінації *B* на відстань *d,* то це означає, що в коді *A* потрібно *d* символів замінити на зворотні, щоб отримати код, але це не означає, що потрібно *d* додаткових символів, щоб код володів даними корректуючими властивостями. У двійкових кодах для виявлення одиночної помилки досить мати 1 додатковий символ незалежно від числа інформаційних розрядів коду, а мінімальна кодова відстань $d_0 = 0.$

Для виявлення і виправлення одиночної помилки співвідношення між числом інформаційних розрядів n_i і числом коректуючих розрядів n_k повинно задовольняти наступним умовам:

$$2^{n_k} \geq n + 1, \tag{43}$$

$$2^{n_i} \leq \frac{2^n}{n+1}, \tag{44}$$

при цьому мається на увазі, що загальна довжина кодової комбінації

(45)

$$n = n_i + n_k$$

Для практичних розрахунків при визначенні числа контрольних розрядів коду з мінімальною кодовою відстанню $d_0 = 3$ зручно користуватися виразами:

$$n_{k_{1(2)}} = [\log_2 (n+1)], \tag{46}$$

якщо відома довжина повної кодової комбінації *n,* і

$$n_{k_{1(2)}} = [\log_2 \{(n_i + 1) + [\log_2 (n_i + 1)]\}], \tag{47}$$

якщо при розрахунках зручніше виходити із заданого числа інформаційних символів n_i .Для кодів, що виявляють всі триразові помилки $(d_0 = 4)$,

$$n_{k_{1(3)}} \geq 1 + \log_2 (n+1), \tag{48}$$

або

$$n_{k_{1(3)}} \geq 1 + \log_2 [(n_u + 1) + \log_2 (n_i + 1)]. \tag{49}$$

Для кодів завдовжки в *n* символів, що виправляють одну або дві помилки $(d_0 = 5)$,

$$n_{k_2} \geq \log_2 (C_n^2 + C_n^1 + 1). \tag{50}$$

Для практичних розрахунків можна користуватися виразом

$$n_{k_2} = \left[\log_2 \frac{n^2 + n + 1}{2} \right]. \tag{51}$$

Для кодів, що виправляють 3 помилки $(d_0 = 7)$,

$$n_{k_3} = \left[\log_2 \frac{n^3 + n^2 + n + 1}{6} \right]. \tag{52}$$

Для кодів, які виправляють s помилок $(d_0 = 2s + 1)$,

$$\log_2 (C_n^s + C_n^{s-1} + ... + 1) < n_{k_s} < \log_2 (C_{n-1}^{2s-1} + C_{n-1}^{2s-2} + ... + 1). \tag{53}$$

Вираз зліва відомий як нижня межа Хеммінга, а вираз справа - як верхня межа Варшамова - Гільберта.

Для наближених розрахунків можна користуватися виразом

$$n_{k_s} = \left[\log_2 \frac{n^s + n^{s-1} + ... + 1}{s!} \right]. \tag{54}$$

Можна припустити, що значення n_k наближатиметься до верхньої межі залежно від того, наскільки вираз під знаком логарифма наближається до цілого ступеня два.

Задача 5.1: Визначити кількість перевірочних розрядів для побудови систематичного коду, що виправляє одиночну помилку і містить 5 інформаційних розрядів.

Розв'язок:

$$2^{n_i} \le \frac{2^n}{n+1}, \quad \text{òî .å.} \quad 2^5(n+1) \le 2^n;$$

при n = 6, 192 + 32 > 64;

при n = 7, 224 + 32 > 128;

при n = 8, 288 + 32 >256;

при n = 9, 288 + 32 < 512

тобто n = 9.

$$n_k = n - n_i = 9 - 5 = 4.$$

Задача 5.2. Визначити максимальну кількість інформаційних розрядів систематичного коду, що виправляє одиночну помилку, якщо допустима довжина всього коду 10 символів.

Розв'язок:

1) $n = n_i + n_k = 10; \quad 2^{n_k} \ge n+1; \quad n_k = 4;$

2) $n_i = n - n_k = 10 - 4 = 6.$

Задача 5.3. Визначити мінімально можливу довжину кодової комбінації систематичного коду, що виправляє одиночну помилку, якщо кількість інформаційних розрядів n_i=11.

Розв'язок:

$$2^{n_i}(n+1) \le 2^n; \quad 2^{11}(n+1) \le 2^n;$$

при n = 12; $2^{11}(12+1) > 2^{12}$

при n = 13; $2^{11}(13+1) > 2^{13}$

при n = 14; $2^{11}(14+1) > 2^{14}$

при n = 15; $2^{11}(15+1) > 2^{15}$

тобто n = 15.

Задача 5.4: Визначити кількість коректуючих розрядів, для побудови коду, що виявляє всі триразові помилки, якщо допустима довжина коду n=15.

Розв'язок:

$n_k \geq 1 + \log_2(n+1); \quad n_k = 1 + \log_2 16 = 5.$

5.2. Лінійні групові коди

Лінійними називаються коди, в яких перевірочними символами є лінійні комбінації інформаційних символів.

Для двійкових кодів як лінійна операція використовують додавання за модулем 2.

Правила додавання за модулем 2 визначаються наступною рівністю:

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

Послідовність нулів і одиниць, що належать даному коду, називається *кодовим вектором.*

Властивість лінійних кодів: сума (різниця) кодових векторів лінійного коду дає вектор, що належить даному коду.

Лінійні коди утворюють групу алгебри по відношенню до операції додавання за модулем 2.

Властивість групового коду: мінімальна кодова відстань між кодовими векторами групового коду дорівнює мінімальній вазі ненульових кодових векторів.

Вага кодового вектора (кодова комбінації) дорівнює числу його ненульових компонентів.

Відстань між двома кодовими векторами дорівнює вазі вектора,

отриманого в результаті додавання початкових векторів за модулем 2. Таким чином, для даного групового коду

$$W_{iií} = d_0.$$

Групові коди зручно задавати матрицями, розмірність яких визначається параметрами коду n_i і n_k. Число рядків матриці дорівнює n_i,число стовпців дорівнює $n_i + n_k = n$:

$$C_{n;n_i} = \begin{Vmatrix} a_{11}a_{12} & \dots & a_{1n_i}p_{11}p_{12} & \dots & p_{1n_k} \\ a_{21}a_{22} & \dots & a_{2n_i}p_{21}p_{22} & \dots & p_{2n_k} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n_i1}a_{n_i2} & \dots & a_{n_in_i}p_{n_i1}p_{n_i2} & \dots & p_{n_in_k} \end{Vmatrix} \quad (55)$$

Коди, що породжуються цими матрицями, відомі як $(n;k)$-*коди,* де $k = n_i$ а відповідні ним матриці називають *породжувальними, твірними.*.

Породжувальна (твірна) матриця С може бути представлена двома матрицями *I* та *П* (інформаційною і перевірочною). Число стовпців матриці *П* дорівнює n_k число стовпців матриці *I* довівнює n_i:

$$C_{n;n_i} = \begin{Vmatrix} a_{11}a_{12} & \dots & a_{1n_i} \\ a_{21}a_{22} & \dots & a_{2n_i} \\ \dots & \dots & \dots \\ a_{n_i1}a_{n_i2} & \dots & a_{n_in_i} \end{Vmatrix} \begin{Vmatrix} p_{11}p_{12} & \dots & p_{1n_k} \\ p_{21}p_{22} & \dots & p_{2n_k} \\ \dots & \dots & \dots \\ p_{n_i1}p_{n_i2} & \dots & p_{n_kn_k} \end{Vmatrix} = \|I\| \|\ddot{I}\ \|. \quad (56)$$

Теорією і практикою встановлено, що в якості як матриці *I* зручно брати одиничну матрицю в канонічній формі:

$$I_{n_i} = \begin{Vmatrix} 100...0 \\ 010...0 \\ ..... \\ 000...1 \end{Vmatrix}.$$

При виборі матриці *П* виходять з наступних міркувань: чим більше одиниць в розрядах перевірочної матриці *П*, тим ближче відповідний породжуваний код до оптимального, з іншого боку, число одиниць в матриці *П* визначає число суматорів за модулем 2 в шифраторі і дешифраторі, тобто чим більше одиниць в матриці *П*, тим складніше апаратура.

Вага кожного рядка матриці *П* повинна бути не менше $W_{\ddot{I}} \geq d_0 - W_i$, де W_i - вага відповідного рядка матриці *I*. Оскільки матриця I - одинична, то $W_I = 1$ (зручність вибору матриці I як одиничної очевидна: при $W_I > 1$ ускладнилася б як побудова кодів, так і їх технічна реалізація).

При дотриманні перерахованих умов будь-яку твірну матрицю групового коду, можна привести до наступного вигляду:

$$C_{n;\,n_i} = \begin{Vmatrix} a_1 & a_2 & a_3 & \dots & a_{n_i} & p_1 & p_2 & \dots & p_{n_i} \\ 1 & 0 & 0 & \dots & 0 & p_{11} & p_{12} & \dots & p_{1(n-n_i)} \\ 0 & 1 & 0 & \dots & 0 & p_{21} & p_{22} & \dots & p_{2(n-n_i)} \\ 0 & 0 & 1 & \dots & 0 & p_{31} & p_{32} & \dots & p_{3(n-n_i)} \\ . & . & . & \dots & . & . & . & \dots & . \\ 0 & 0 & 0 & \dots & 1 & p_{k1} & p_{k2} & \dots & p_{k(n-n_i)} \end{Vmatrix} = \|I\ddot{I}\ \|,$$

Який називається лівою канонічною формою породжувальної матриці .

Для кодів з d_0=2 породжувальна матриця *C* має вигляд

$$C_{n;\,n_i} = \begin{Vmatrix} 100...01 \\ 010...01 \\ 001...01 \\ ..... \\ 000...11 \end{Vmatrix} = \overbrace{\begin{Vmatrix} 100...0 \\ 010...0 \\ 001...0 \\ ..... \\ 000...1 \end{Vmatrix}}^{I} \quad \overbrace{\begin{Vmatrix} 1 \\ 1 \\ 1 \\ ... \\ 1 \end{Vmatrix}}^{\ddot{I}}.$$

У всіх комбінаціях коду, побудованого за допомогою такої матриці, парне число одиниць.

Для коду з $d_0 \geq 3$ твірна матриця, не може бути представлена у формі, загальній для всіх кодів з даним d_0. Вид матриці залежить від конкретних вимог до породжуваного коду. Цими вимогами можуть бути або мінімум коректуючи розрядів, або максимальна простота апаратури.

Коректуючі коди з мінімальною кількістю надмірних розрядів називають *щільно упакованими* або *досконалими кодами.* Для кодів з $d_0 = 3$ співвідношення *n* і n_k. наступні: (3; 1), (7;4), (15; 11), (31; 26), (63; 57) і так далі.

Щільно упаковані коди, оптимальні з погляду мінімуму надмірних

символів, виявляють максимально можливу кількість варіантів помилок кратністю r + 1; r + 2 і так далі $d_0 \le 6$ і $n \le 40$ були досліджені Д. Слепяном. Для отримання цих кодів матриця $П$ повинна мати комбінації з максимальною вагою. Для цього при побудові кодів з $d_0 \ge 3$ послідовно використовуються вектори довжиною n-n_i вагою $W_П = n_k$, $n_k - 1, ..., d_0 - 1$. Тим же Слепяном були досліджені *нещільно упаковані коди з малою щільністю перевірок на парність*. Ці коди економні з погляду простоти апаратури і містять мінімальне число одиниць в коректуючих розрядах твірної матриці. При побудові кодів з максимально простими шифраторами і дешифраторами послідовно вибираються вектори вагою $W_П$ = 2, 3 ..., n_k. Якщо число комбінацій, що є коректуючими розрядами коду, і що задовольняють умові $W_П \ge d_0 - 1$ більше n_i, то в першому випадку не використовують набори з найменшою вагою, а в другому - з найбільшим.

Рядки твірної матриці C є n_i комбінацій шуканого коду. Решта комбінацій коду будується за допомогою твірної матриці за наступним правилом: коректуючі символи, призначені для виявлення або виправлення помилки в інформаційній частині коду, знаходяться шляхом підсумовування за модулем 2 тих рядків матриці $П$, номери яких співпадають з номерами розрядів, що містять одиниці в кодовому векторі, що представляє інформаційну частину коду. Отриману комбінацію приписують справа до інформаційної частини коду і отримують вектор повного коректуючого коду. Аналогічну процедуру проробляють з другою, третьою і подальшими інформаційними кодовими комбінаціями, поки не буде побудований коректуючий код для передачі всіх символів первинного алфавіту.

Алгоритм утворення перевірочних символів по відомій інформаційній частині коду може бути записаний таким чином:

$$
\begin{aligned}
&p_1 = p_{11}a_1 \oplus p_{21}a_2 \oplus ... \oplus p_{n_u 1}a_{n_u},\\
&p_2 = p_{12}a_1 \oplus p_{22}a_2 \oplus ... \oplus p_{n_u 2}a_{n_u},\\
&.....\\
&p_{n_u} = p_{1n_k}a_1 \oplus p_{2n_k}a_2 \oplus ... \oplus p_{n_u n_k}a_{n_u},\\
&\textit{або}\\
&p_{ij} = p_{1j}a_1 \oplus p_{2j}a_2 \oplus ... \oplus p_{n_u j}a_{n_u} = \sum p_{ij}a_i.
\end{aligned}
\qquad (57)
$$

В процесі декодування здійснюються перевірки, ідея яких в загальному вигляді може бути представлена таким чином:

$$
p_i \oplus \sum_{i=1}^{n_u} p_{ij}a_1 = S_j, \quad j = 1, 2, ..., n_k. \qquad (58)
$$

Для кожної конкретної матриці існує своя, одна-єдина система перевірок. Перевірки проводяться за наступним правилом: у першу перевірку разом з перевірочним розрядом p_1 входять інформаційні розряди, які відповідають одиницям першого стовпця перевірочної матриці *П*; у другу перевірку входить другий перевірочний розряд p_2 і інформаційні розряди, відповідні одиницям другого стовпця перевірочної матриці, і так далі число перевірок дорівнює числу перевірочних розрядів коректуючого коду n_k.

В результаті здійснення перевірок утворюється *перевірочний вектор* $S_1, S_2, ..., S_{n_k}$, який називають *синдромом.* Якщо вага синдрому дорівнює нулю, то прийнята комбінація вважається безпомилковою. Якщо хоч би один розряд перевірочного вектора містить одиницю, то прийнята комбінація містить помилку. Виправлення помилки проводиться по вигляду синдрому, оскільки кожному помилковому розряду відповідає один-єдиний перевірочний вектор.

Вид синдрому для кожної конкретної матриці може бути визначений за допомогою перевірочної матриці *Н,* яка є транспонованою матрицею *П*, доповненою одиничною матрицею I_{n_k} число стовпців якої дорівнює числу перевірочних розрядів коду:

$$H = \left\| \Pi^T I_{n_k} \right\|.$$

Стовпці такої матриці є значенням синдрому для розряду, відповідного номеру стовпця матриці *H*.

Процедура виправлення помилок в процесі декодування групових кодів зводиться до наступного.

Будується кодова таблиця. У першому рядку таблиці розташовуються всі кодові вектори A_i. У першому стовпці другого рядка розміщується вектор e_1, вага якого дорінює 1.

Решта позицій другого рядка заповнюється векторами, отриманими в результаті підсумовування за модулем 2 вектору e_1 з вектором A_i розташованим у відповідному стовпці першого рядка. У першому стовпці третього рядка записується вектор e_2 , вага якого також дорівнює 1, проте, якщо вектор e_1 містить одиницю в першому розряді, то e_2- у другому. У решту позицій третього рядка записують суми A_i і e_2.

Аналогічно поступають до тих пір, поки не будуть підсумовані з векторами A_i всі вектори e_j вагою 1, з одиницями в кожному з *n* розрядів. Потім підсумовуються за модулем 2 вектори e_j вагою 2, з послідовним перекриттям всіх можливих розрядів. Вага вектора e_j визначає число помилок, що виправляються. Число векторів e_j визначається можливим числом синдромів, що не повторюються, і дорівнює $2^{n_k} - 1$ (нульова комбінація говорить про відсутність помилки). Умова неповторюваності синдрому дозволяє по його вигляду визначати один-єдиний відповідний йому вектор e_j . Вектори e_j, є вектори помилок, які можуть бути виправлені даним груповим кодом.

По вигляду синдрому прийнята комбінація може бути віднесена до того або іншого суміжного класу, утвореного сумуванням за модулем 2 кодових комбінації A_i з вектором помилки e_j, тобто до певного рядка кодової табл. 5.2

Таблиця 5.2

A / e	A_1	A_2	•••	$A_{2^{n_k}-1}$
e_1 e_2 ... $e_{2^{n_k}-1}$	$e_1 \oplus A_1$ $e_2 \oplus A_1$ ... $e_{2^{n_k}-1} \oplus A_1$	$e_1 \oplus A_2$ $e_2 \oplus A_2$ ... $e_{2^{n_k}-1} \oplus A_2$	... ...	$e_1 \oplus A_{2^{n_k}-1}$ $e_2 \oplus A_{2^{n_k}-1}$ ... $e_{2^{n_k}-1} \oplus A_{2^{n_k}-1}$

Прийнята кодова комбінація A_x^n порівнюється з векторами, записаними в рядку, відповідному отриманому в результаті перевірок синдрому. Дійсний код буде розташований в першому рядку тієї ж колонки таблиці. Процес виправлення помилки полягає в заміні на зворотне значення розрядів, відповідних одиницям у векторі помилок e_j.

Вектори $e_1, e_2, ..., e_{2^{n_k}-1}$ не повинні дорівнювати жодному з векторів $A_1, A_2, ..., A_{2^{n_k}-1}$ інакше в таблиці з'явилися б нульові вектори.

Завдання 5.5: Визначити мінімальну кодову відстань між двійковими векторами: 1100011; 1001111; 1010101.

Розв'язок:

$$\begin{array}{r} 1100011 \\ \oplus\ 1001111 \\ \hline 0101100 \end{array} \quad d_0 = W = 3; \qquad \begin{array}{r} 1100011 \\ \oplus\ 1010101 \\ \hline 0110110 \end{array} \quad d_0 = W = 4;$$

$$\begin{array}{r} 1001111 \\ \oplus\ 1010101 \\ \hline 0011010 \end{array} \quad d_0 = W = 3; \qquad \begin{array}{r} 1001111 \\ \oplus\ 1100011 \\ \hline 0101100 \end{array} \quad d_0 = W = 3.$$

Таким чином $d_{мин} = 3.$

Завдання 5.6: Визначити коректуючі властивості наступного коду: 001; 010; 111.

Розв'язок:

1) $\oplus\begin{matrix}111\\001\\\hline 110\end{matrix}$ $\oplus\begin{matrix}111\\100\\\hline 011\end{matrix}$ $\oplus\begin{matrix}111\\010\\\hline 101\end{matrix}$ 2) $\oplus\begin{matrix}001\\100\\\hline 101\end{matrix}$ $\oplus\begin{matrix}001\\111\\\hline 110\end{matrix}$ $\oplus\begin{matrix}001\\010\\\hline 011\end{matrix}$

3) $\oplus\begin{matrix}100\\111\\\hline 011\end{matrix}$ $\oplus\begin{matrix}100\\001\\\hline 101\end{matrix}$ $\oplus\begin{matrix}100\\010\\\hline 110\end{matrix}$ 4) $\oplus\begin{matrix}010\\111\\\hline 101\end{matrix}$ $\oplus\begin{matrix}010\\001\\\hline 011\end{matrix}$ $\oplus\begin{matrix}010\\100\\\hline 110\end{matrix}$

$d_{мин} = 2.$ Код здатний виявляти тільки одиночну помилку.

Завдання 5.7: Джерело передає повідомлення за допомогою 15 двійкових комбінацій. Скласти інформаційну //І// і перевірочну //П// матриці так, щоб повна твірна матриця С=// І П //, дозволяла отримати груповий код, що коректує одиночні збої.

Розв'язок:

$n_i = 4,$ оскільки 2^{n_i} повинно бути більше або дорівнювати 15;

$d_0 = 2r + 1 = 3;\quad W_{\bar{I}} \geq d_0 - W_I = 3 - 1 = 2.$

$$C_{7;4} = \left\| \begin{matrix} 1000011 \\ 0100110 \\ 0010101 \\ 0001111 \end{matrix} \right\|.$$

5.3. Тривіальні систематичні коди. Код Хеммінга

Систематичними кодами є такі коди, в яких інформаційні і коректуючі розряди розташовані за суворо визначеною системою і завжди займають суворо визначені місця в кодових комбінаціях. Систематичні коди є рівномірними, тобто всі комбінації коду із заданими коректуючими здібностями мають однакову довжину. Групові коди також є систематичними, але не всі систематичні коди можуть бути віднесені до групових.

Тривіальні систематичні коди можуть будуватися, як і групові, на основі твірної матриці. Зазвичай твірна матриця будується за допомогою

одиничної, ранг якої визначається числом інформаційних розрядів, і додаткової, число стовпців якої визначається числом контрольних розрядів коду. Кожен рядок додаткової матриці повинен містити не менше $d_0 - 1$ одиниць, а сума по модулю два будь-яких рядків не менше $d_0 - 2$ одиниць (де d_0 - мінімальна кодова відстань). Твірна матриця дозволяє знаходити решту всіх кодових комбінацій підсумовуванням за модулем два рядків твірної матриці в усіх можливих поєднаннях.

Код Хеммінга є типовим прикладом систематичного коду. Проте при його побудові до матриць зазвичай не вдаються. Для обчислення основних параметрів коду задається або кількість інформаційних символів, або кількість інформаційних комбінацій $N = 2^n i$. За допомогою (43) і (44) обчислюються n_i і n_k. Співвідношення між n, n_i, n_k для коду Хеммінга представлені в додатку Б. Знаючи основні параметри коректуючого коду визначають, які позиції сигналів будуть робочими, а які контрольними. Як показала практика, номери контрольних символів зручно вибирати згідно із законом 2^i де $i = 0, 1, 2$ і так далі - натуральний ряд чисел. Номери контрольних символів в цьому випадку будуть відповідно: 1, 2, 4, 8, 16, 32 і т.д.

Потім визначають значення контрольних коефіцієнтів (0 або 1), керуючись наступним правилом: *сума одиниць на контрольних позиціях повинна бути парною.* Якщо ця сума парна, то значення контрольного коефіцієнта - 0, в іншому випадку - 1.

Перевірочні позиції вибираються таким чином: складається таблиця для ряду натуральних чисел в двійковому коді. Число рядків таблиці

$$n = n_i + n_k.$$

Першому рядку відповідає перевірочний коефіцієнт a_1, другому a_2 і так далі. Потім виявляють перевірочні позиції, виписуючи коефіцієнти за наступним принципом: у першу перевірку входять коефіцієнти, які містять в молодшому розряді 1, тобто $a_1, a_3, a_5, a_7, a_9, a_{11}$ і т. д.; в другу - коефіцієнти,

що містять 1 в другому розряді, тобто a_2, a_3, a_6, a_7, a_{10}, a_{11} і т.д.; в третю перевірку - коефіцієнти, які містять 1 в третьому розряді, і так далі. Номери перевірочних коефіцієнтів відповідають номерам перевірочних позицій, що дозволяє скласти загальну таблицю перевірок (додаток Б). Старшинство розрядів визначається зліва направо, а при перевірці зверху вниз. Порядок перевірок показує також порядок проходження розрядів в отриманому двійковому коді.

Якщо в прийнятому коді є помилка, то результати перевірок по контрольних позиціях утворюють двійкове число, яке вказує номер помилкової позиції. Виправляють помилку, змінюючи символ помилкової позиції на зворотний.

Для виправлення одиничної і виявлення подвійної помилки, окрім перевірок по контрольних позиціях, слід проводити ще одну перевірку на парність для кожного коду. Щоб здійснити таку перевірку, слід до кожного коду в кінці кодової комбінації додати контрольний символ так, щоб сума одиниць в отриманій комбінації завжди була парною. Тоді у разі однієї помилки перевірки по позиціях вкажуть номер помилкової позиції, а перевірка на парність вкаже наявність помилки. Якщо перевірки позицій вкажуть на наявність помилки, а перевірка на парність не фіксує помилки, то це означає, що в коді дві помилки.

5.4. Циклічні коди

Циклічні коди названі так тому, що в них частина комбінацій коду або всі комбінації можуть бути отримані шляхом циклічного зсуву однієї або декількох комбінацій коду. Циклічний зсув здійснюється справа наліво, причому крайній лівий символ кожного разу переноситься в кінець комбінації. Циклічні коди, практично всі відносяться до систематичних кодів, в них контрольні і інформаційні розряди розташовані на суворо визначених місцях. Крім того, циклічні коди належать до *блокових кодів*.

Кожен блок (одна літера є окремим випадком блоку) кодується самостійно.

Ідея побудови циклічних кодів базується на використанні двійкових чисел багаточленів, що *не приводяться* в полі. Незвідними називаються багаточлени, які не можуть бути представлені у вигляді добутку многочленів нижчих ступенів з коефіцієнтами з того ж поля, так само, як прості числа не можуть бути представлені добутком інших чисел. Іншими словами незвідні многочлени, діляться без залишку тільки на себе або на одиницю.

Незвідні многочлени, в теорії циклічних кодів грають роль *створюючих* (генераторних, твірних) многочленів. Якщо задану кодову комбінацію помножити на вибраний незвідний многочлен, то отримаємо циклічний код, коректуючі здібності якого визначаються незвідним многочленом.

Припустимо, потрібно закодувати одну з комбінацій чотиризначної двійкового коду. Припустимо також, що ця комбінація - $U(x) = x^3 + x^2 + 1 \to 1101$. Поки не обгрунтовувавши свій вибір, беремо з таблиці незвідних многочленів, як створюючий многочлен $K(x) = x^3 + x + 1 \to 1011$. Потім помножимо $U(x)$ на одночлен того ж ступеня, що і створюючий многочлен. Від множення многочлена на одночлен ступеня n ступінь кожного члена многочлена підвищиться на n , що еквівалентно приписуванню n нулів з боку молодших розрядів многочлена. Оскільки ступінь вибраного незвідного многочлена, дорівнює трьом, то початкова інформаційна комбінація множиться на одночлен третього ступеня:

$$U(x) \cdot x^n = (x^3 + x^2 + 1)x^3 = x^6 + x^5 + x^3 = 110100.$$

Це робиться для того, щоб згодом на місці цих нулів можна було б записати корректуючі розряди.

Значення корректуючих розрядів, знаходять по результату від ділення $U(x) \cdot x^n$ на $K(x)$:

$$
\begin{array}{r}
x^6 + x^5 + 0 + x^3 + 0 + 0 + 0 \\
\underline{x^6 + 0 + x^4 + x^3} \\
x^5 + x^4 + 0 + 0 \\
\underline{x^5 + 0 + x^3 + x^2} \\
x^4 + x^3 + x^2 + 0 \\
\underline{x^4 + 0 + x^2 + x} \\
x^3 + 0 + x + 0 \\
\underline{x^3 + 0 + x + 1} \\
\end{array}
\quad
\begin{array}{l|l}
 & x^3 + x + 1 \\
\hline
x^3 + x^2 + x + 1 + \dfrac{1}{x^3 + x + 1} &
\end{array}
$$

або

$$
\begin{array}{r}
1101000 \\
\underline{1011} \\
1100 \\
\underline{1011} \\
1110 \\
\underline{1011} \\
1010 \\
\underline{1011} \\
001
\end{array}
\quad
\begin{array}{l|l}
 & 1011 \\
\hline
1111 + \dfrac{001}{1011} &
\end{array}
$$

Таким чином

$$\frac{U(x)\cdot x^3}{K(x)} = x^3 + x^2 + x + 1 + \frac{1}{x^3 + x + 1},$$

або в загальному вигляді

$$\frac{U(x)\cdot x^3}{K(x)} = Q(x) + \frac{R(x)}{K(x)}, \tag{59}$$

де $Q(x)$ - частка, а $R(x)$ - залишок від ділення $U(x)\cdot x^n$ на $K(x)$.

Оскільки в двійковій арифметиці $1 \oplus 1 = 0$, а значить $-1 = 1$, то можна при складанні двійкових чисел переносити складову з однієї частини рівност в іншу без зміни знаку (якщо це зручно), тому рівність вигляду $a \oplus b = 0$ можна записати і як $a = b$, і як $a - b = 0$. Всі три рівності в даному випадку означають, що або a і b дорівнює 0, або a і b дорівнюють 1, тобто мають однакову парність.

Таким чином, вираз (59) можна записати як

$$F(x) = Q(x) \cdot K(x) = U(x) \cdot x^n + R(x), \qquad (60)$$

що у разі нашого прикладу дасть

$$F(x) = (x^3 + x^2 + x + 1)(x^3 + x + 1) = (x^3 + x^2 + 1)x^3 + 1,$$

або

$$F(x) = 1111 \times 1011 = 1101000 + 001 = 1101001.$$

Многочлен 1101001 і є шукана комбінація, де 1101 - інформаційна частина, а 001 - контрольні символи. Відмітимо, що шукану комбінацію ми отримали б і як в результаті множення однієї з комбінацій повного чотиризначного двійкового коду (в даному випадку 1111) на створюючий многочлен, так і множенням заданої комбінації на одночлен, що має той же ступінь, що і вибраний створюючий многочлен (у нашому випадку таким чином була отримана комбінація 1101000) з подальшим додаванням до отриманого добутку залишку від ділення цього добутку на створюючий многочлен (у нашому прикладі залишок мав вигляд 001).

Таким чином, ми вже знаємо два способи утворення комбінацій лінійних систематичних кодів, до яких відносяться і циклічні коди, що нас цікавлять. Ці способи стали теоретичною базою для побудови кодуючих і декодуючих пристроїв.

Шифратори циклічних кодів, в тому або іншому вигляді, побудовані за принципом множення двійкових многочленів. Кодові комбінації отримують в результаті складання сусідніх комбінацій за модулем два, що, як ми побачимо нижче, еквівалентно множенню першої комбінації на двочлен $x+1$.

Отже, комбінації циклічних кодів можна представляти у вигляді многочленів, у яких показники ступеня x відповідають номерам розрядів, коефіцієнти при x дорівнюють 0 або 1 залежно від того, стоїть 0 або 1 в розряді кодової комбінації, яку представляє даний многочлен. Наприклад,

$$000101 \to 0\cdot x^5 + 0\cdot x^4 + 0\cdot x^3 + 1\cdot x^2 + 0\cdot x^1 + 1\cdot x^0 = x^2 + 1;$$
$$001010 \to 0\cdot x^5 + 0\cdot x^4 + 1\cdot x^3 + 0\cdot x^2 + 1\cdot x^1 + 0\cdot x^0 = x^3 + x;$$
$$010100 \to 0\cdot x^5 + 1\cdot x^4 + 0\cdot x^3 + 1\cdot x^2 + 0\cdot x^1 + 0\cdot x^0 = x^4 + x^2;$$
$$101000 \to 1\cdot x^5 + 0\cdot x^4 + 1\cdot x^3 + 0\cdot x^2 + 0\cdot x^1 + 0\cdot x^0 = x^5 + x^3;$$

Циклічний зсув кодової комбінації аналогічний множенню відповідного многочлена на *x:*

$$(x^2 + 1)\cdot x = x^3 + x \to 001010;$$
$$(x^3 + x)\cdot x = x^4 + x^2 \to 010100;$$
$$(x^4 + x^2)\cdot x = x^5 + x^3 \to 101000.$$

Якщо ступінь многочлена досягає розрядності коду, то відбувається «перенесення» в нульовий ступінь при x. У шифраторах циклічних кодів ця операція здійснюється шляхом з'єднання виходу комірки старшого розряду з входом комірки нульового розряду. Складання за модулем 2 будь-яких двох сусідніх комбінацій циклічного коду еквівалентно операції множення многочлена відповідного комбінації першого доданку на многочлен $x+1$, якщо приведення подібних членів здійснюється по модулю 2:

$$\begin{array}{r} 000101 \\ \oplus\ 001010 \\ \hline 001111 \end{array} \qquad \begin{array}{rl} & x^2 + 0 + 1 \to 000101 \\ \times & x + 1 \\ \hline & x^2 + 0 + 1 \\ & x^3 + 0 + x \to 001010 \\ \hline & x^3 + x^2 + x + 1 \to 001111 \end{array}$$

тобто існує принципова можливість отримання будь-якої кодової комбінації циклічного коду шляхом множення відповідним чином підібраного створюючого многочлена на деякий інший многочлен.

Проте мало побудувати циклічний код. Треба вміти виділити з нього можливі помилкові розряди, тобто ввести деякі пізнавачі помилок, які виділяли б помилковий блок зі всіх інших. Оскільки циклічні коди - блокові, то кожен блок повинен мати свій пізнавач. І тут вирішальну роль грають властивості створюючого многочлена $K(x)$. Методика побудови циклічного коду така, що створюючий многочлен бере участь в утворенні кожної кодової комбінації, тому будь-який многочлен циклічного коду

ділиться на створюючий без залишку. Але без залишку діляться тільки ті многочлени, які належать даному коду, тобто створюючий многочлен дозволяє вибрати дозволені комбінації зі всіх можливих. Якщо ж при діленні циклічного коду на створюючий многочлен буде отриманий залишок, то означає або в коді відбулася помилка, або це комбінація якогось іншого коду (заборонена комбінація), що для декодуючого пристрою не має принципової різниці. По залишку і виявляється наявність забороненої комбінації, тобто виявляється помилка. Залишки *від ділення многочленів є пізнавачами помилок циклічних кодів.*

З іншого боку, залишки від ділення одиниці з нулями на створюючий многочлен використовуються для побудови циклічних кодів (можливість цього видно з виразу (60)).

При діленні одиниці з нулями на створюючий многочлен слід пам'ятати, що довжина залишку повинна бути не менше числа контрольних розрядів, тому у разі браку розрядів в залишку до залишку приписують справа необхідне число нулів. Наприклад

```
10000000000 | 1011
1011        -------
-------     11111 + 11
  01100         1011
  1011
-------
  1110          Залишки
  1011          011
-------         110
  1010          111
  1011          101
-------         001
  1000          010
  1011          100
-------         011
    11          110
                і т.д.
```

починаючи з восьмого, залишки повторюватимуться.

Залишки від ділення використовують для побудови створюючих матриць, які, завдяки своїй наочності і зручності отримання похідних комбінацій, набули широкого поширення для побудови циклічних кодів. Побудова твірної матриці зводиться до складання одиничної транспонованої і додаткової матриці, елементами якої є залишки від ділення одиниці з нулями на створюючий многочлен $K(x)$. Нагадаємо, що одинична транспонована матриця є квадратною матрицею, всі елементи якої - нулі, окрім елементів, розташованих по діагоналі справа наліво зверху вниз (у нетранспонованій матриці діагональ з одиничними елементами розташована зліва направо зверху вниз). Елементи додаткової матриці приписуються праворуч від одиничної транспонованої матриці.

Проте не всі залишки від ділення одиниці з нулями на створюючий многочлен можуть бути використані як елементи додаткової матриці. Використовуватися можуть лише ті залишки, вага яких $W \geq d_0 - 1$, де d_0 - мінімальна кодова відстань. Довжина залишків повинна бути не менше кількості контрольних розрядів, а число залишків повинне дорівнювати числу інформаційних розрядів.

Рядками твірної матриці є перші комбінації шуканого коду. Решта комбінацій коду виходить в результаті підсумовування за модулем 2 всіляких поєднань рядків створюючої матриці

Описаний вище метод побудови твірних матриць не є єдиним. Твірна матриця може бути побудована в результаті безпосереднього множення елементів одиничної матриці на створюючий многочлен. Це часто буває зручнішим, ніж знаходження залишків від ділення. Отримані коди нічим не відрізняються від кодів, побудованих за твірними матрицями, в яких додаткова матриця складається із залишків від ділення одиниці з нулями на створюючий многочлен.

Твірна матриця може бути побудована також шляхом циклічного зсуву комбінації, отриманої в результаті множення рядка одиничної матриці

рангу n_i на створюючий многочлен.

На закінчення пропонуємо ще один метод побудови циклічного коду. Перевагою цього методу є виняткова простота схемних реалізації кодуючих і декодуючих пристроїв.

Для отримання комбінацій циклічного коду в цьому випадку досить провести циклічний зсув рядку твірної матриці і комбінації, що є її дзеркальним відображенням. При побудові коду з $d_0 = 3$ $n_i = 4$

Число ненульових комбінацій, що отримуються в результаті підсумовування за модулем 2 всіляких поєднань рядків твірної матриці

$$P_a = C_{n_i}^1 + C_{n_i}^2 + ... + C_{n_i}^{n_i-1} + C_{n_i}^{n_i}, \quad (61)$$

де n_i - число інформаційних розрядів коду.

Число ненульових комбінацій, що отримуються в результаті циклічного зсуву будь-якого рядку твірної матриці і дзеркальної до неї комбінації (62)

$$P_C = 2n,$$

де n - довжина кодової комбінації.

При числі інформаційних розрядів $n_i \geq 6$ число комбінацій від підсумовування рядків твірної матриці росте набагато швидше, ніж число комбінацій, що отримуються в результаті циклічного зсуву рядка твірної матриці і дзеркальної нею комбінації. У останньому випадку коди виходять надмірними (оскільки при тій же довжині коду можна іншим способом передати більшу кількість повідомлень), відповідно, падає відносна швидкість передачі інформації. У таких випадках доцільність застосування того або іншого методу кодування може бути визначена з конкретних технічних умов.

Помилки в циклічних кодах виявляються і виправляються за допомогою залишків від ділення отриманої комбінації на твірний многочлен. *Залишки від ділення є пізнавачами помилок,* але не указують безпосередньо на місце помилки в циклічному коді.

Ідея виправлення помилок базується на тому, що помилкова комбінація після певного числа циклічних зрушень “ підганяється ” під залишок таким чином, що в сумі із залишком вона дає виправлену комбінацію. Залишок при цьому є не що інше, як різниця між спотвореними і правильними символами, одиниці в залишку стоять якраз на місцях спотворених розрядів в підігнаній циклічними зрушеннями комбінації. Підганяють спотворену комбінацію до тих пір, поки число одиниць в залишку не буде дорівнювати числу помилок в коді. При цьому, природно, число одиниць може або дорівнювати числу помилок s що виправляються даним кодом (код виправляє 3 помилки і в спотвореній комбінації 3 помилки), або бути менше s (код виправляє 3 помилки, а в прийнятій комбінації - 1 помилка).

Місце помилки в кодовій комбінації не має значення. Якщо $n_k \geq \frac{n}{2}$, то після певної кількості зсувів всі помилки опиняться в зоні “разової” дії твірного многочлена, тобто досить отримати один залишок, вага якого $W \leq s$ і це вже буде досить для виправлення спотвореної комбінації. Розглянемо побудову і декодування конкретних циклічних кодів

I. Коди, що виправляють одиночну помилку $d_0 = 3$.

1. *Розрахунок співвідношення між контрольними і інформаційними символами коду* проводиться на підставі виразів (43) - (53).

Якщо задано число інформаційних розрядів n_i, то число контрольних розрядів n_k знаходимо з виразу

$$n_k = [\log_2\{(n_i + 1) + [\log_2(n_i + 1)]\}].$$

Загальне число символів коду

$$n = n_i + n_k.$$

Якщо задана довжина коду n_i,то число контрольних розрядів

$$n_k = [\log_2(n + 1)].$$

Співвідношення числа контрольних і інформаційних символів для коду з

$$d_0 = 3.$$

2. *Вибір створюючого многочлена* проводиться по таблицях двійкових многочленів, що не приводяться.

Твірний многочлен $K(x)$ слід вибирати якомога коротшим, але ступінь його повинна бути не менше числа контрольних розрядів n_k, а число ненульових членів - не менше мінімальної кодової відстані d_0.

3. *Вибір параметрів одиничної транспонованої матриці* походить з умови, що число стовпців (рядків) матриці визначається числом інформаційних розрядів, тобто ранг одиничної матриці рівний n_i.

4. *Визначення елементів додаткової матриці* проводиться по залишках від ділення останнього рядка транспонованої матриці (одиниці з нулями) на твірний многочлен. Отримані залишки повинні задовольняти наступним вимогам:

а) число розрядів кожного залишку повинно дорівнювати числу контрольних символів n_k, отже, число розрядів додаткової матриці повинне бути рівне ступеню створюючого многочлена;

б) число залишків повинне бути не менше числа рядків одиничної транспонованої матриці, тобто повинно дорівнювати числу інформаційних розрядів n_i;

в) число одиниць кожного залишку, тобто його вага, повинна бути не менше величини $r = d_0 - 1$, де d_0 - мінімальна кодова відстань, не менша числа помилок, що виявляються;

г) кількість нулів, що приписуються до одиниці з нулями при діленні її на вибраний многочлен, що не приводиться, повинна бути такою, щоб дотримувалися умови а), б), в).

5. *Твірна матриця* складається дописуванням елементів додаткової матриці праворуч від одиничної транспонованої матриці або множенням елементів одиничної матриці на створюючий многочлен.

6. *Комбінаціями шуканого коду* є рядки твірної матриці і всі можливі суми за модулем 2 різних поєднань рядків твірної матриці.

7. *Виявлення і виправлення помилок* проводиться по залишках від ділення прийнятої комбінації $F(x)$ на твірний многочлен $K(x)$. *Якщо прийнята комбінація ділиться на твірний многочлен без залишку, то код прийнятий безпомилково.* Залишок від ділення свідчить про наявність помилки, але не вказує, якої саме. Для того, щоб знайти помилковий розряд і виправити його в циклічних кодах, здійснюють наступні операції:

а) прийняту комбінацію ділять на твірний многочлен,

б) підраховують кількість одиниць в залишку (вага залишку).

Якщо $W \le s$, де s - допустиме число помилок, що виправляються даним кодом, то прийняту комбінацію додають за модулем 2 до отриманого залишку. Сума дасть виправлену комбінацію. Якщо $W \le s$ то

в) проводять циклічний зсув прийнятої комбінації $F(x)$ вліво на один розряд. Комбінацію, отриману в результаті циклічного зсуву, ділять на $K(x)$. Якщо в результаті цього повторного ділення $W \le s,$,то ділиме підсумовують із залишком;

г) проводять циклічний зсув вправо на один розряд комбінації, отриманої в результаті підсумовування останнього ділимого з останнім залишком. Отримана в результаті комбінація вже не містить помилок. Якщо після першого циклічного зсуву і подальшого ділення залишок виходить таким, що його вага $W > s$,то

д) повторюють операцію пункту в) до тих пір, поки не буде $W \le s,$. В цьому випадку комбінацію, отриману в результаті останнього циклічного зсуву, підсумовують із залишком від ділення цієї комбінації на створюючий многочлен, а потім

е) проводять циклічний зсув вправо рівно на стільки розрядів, на скільки була зрушена підсумовувана з останнім залишком комбінація щодо прийнятої комбінації. В результаті отримаємо виправлену комбінацію.

II. Коди, що виявляють триразові помилки $d_0 = 4$.

1. *Вибір числа коректуючих розрядів,* проводиться із співвідношення

$$n_k \geq 1 + \log_2(n+1),$$

або

$$n_k \geq 1 + \log_2[(n_i + 1) + \log_2(n_i + 1)].$$

2. *Вибір створюючого многочлена* проводять, виходячи з таких міркувань: для виявлення триразової помилки

$$d_0 = r + 1 = 3 + 1 = 4,$$

тому ступінь твірного многочлена не може бути менше чотирьох; многочлен третього ступеня, який має число ненульових членів, більше або рівне трьом, дозволяє виявляти всі подвійні помилки, многочлен першого ступеня $(x+1)$ виявляє будь-яку кількість непарних помилок, отже, многочлен четвертого ступеня, що отримується в результаті множення цих многочленів, володіє їх властивостями, що коректують: може виявляти дві помилки, а також одну і три, тобто всі триразові помилки.

3. *Побудову твірної матриці* проводять або знаходженням залишків від ділення одиниці з нулями на твірний многочлен, або множенням рядків одиничної матриці на твірний многочлен.

4. *Решту комбінацій коректуючого коду,* знаходять підсумовуванням за модулем 2 всіляких поєднань рядків створюючої матриці.

5. *Виявлення помилок* проводиться по залишках від ділення прийнятої комбінації $F(x)$ на створюючий многочлен $K(x)$. Якщо залишку немає, то контрольні розряди відкидаються і інформаційна частина коду використовується за призначенням. Якщо в результаті ділення виходить залишок, то комбінація бракується. Відмітимо, що такі коди можуть виявляти 75% будь-якої кількості помилок, оскільки окрім подвійної помилки виявляються всі непарні помилки, але гарантована кількість помилок, яку код ніколи не пропустить, дорівнює 3.

Приклад: Початкова кодова комбінація - 0101111000, прийнята - 0001011001 (тобто відбувся потрійний збій). Показати процес виявлення помилки, якщо відомо, що комбінації коду були утворені за допомогою многочлена 101111.

Рішення:

$$\begin{array}{r} 0001011001 \\ 101111 \\ \hline 0000111 \end{array} \quad \underline{|101111}$$

Залишок не нульовий, комбінація бракується. Вказати помилкові розряди при триразових спотвореннях такі коди не можуть.

III. Циклічні коди, що виправляють дві і більше помилок $d_0 \geq 5$.

Методика побудови циклічних кодів з $d_0 \geq 5$ відрізняється від методики побудови циклічних кодів з $d_0 < 5$ тільки у виборі створюючого многочлена. У літературі ці коди відомі як коди БЧХ (перші букви прізвищ Боуз, Чоудхурі, Хоквінхем - авторів методики побудови циклічних кодів з $d_0 \geq 5$.).

Побудова створюючого многочлена залежить, в основному, від двох параметрів: від довжини кодового слова n і від числа помилок s, що виправляються. Решта параметрів, що беруть участь в побудові створюючого многочлена, залежно від заданих n і s можуть бути визначені за допомогою таблиць і допоміжних співвідношень, про які буде сказано нижче.

Для виправлення числа помилок $s \geq 2$ ще не достатньо умови, щоб між комбінаціями коду мінімальна кодова відстань $d_0 = 2s + 1$ необхідно також, щоб довжина коду n задовольняла умові

$$n = 2^h - 1, \tag{63}$$

при цьому n завжди буде непарним числом. Величина h визначає вибір числа контрольних символів n_k і пов'язана з n_k і s наступним співвідношенням:

$$n_k \le hs = [\log_2 (n+1)]s. \qquad (64)$$

З іншого боку, число контрольних символів визначається твірним многочленом і дорівнює його ступеню. При великих значеннях h довжина коду n стає дуже великою, що викликає цілком певні труднощі при технічній реалізації кодуючих і декодуючих пристроїв. При цьому частина інформаційних розрядів деколи залишається невикористаною. У таких випадках для визначення h зручно користуватися виразом

$$2^h - 1 = nC, \qquad (65)$$

де C є одним із співмножників, на які розкладається число n.

Співвідношення між n ,l і h можуть бути зведені в наступну таблицю

№ п/п	h	$n = 2^h - 1$	C
1	3	7	1
2	4	15	5; 3
3	5	31	1
4	6	63	7; 3; 3
5	7	127	1
6	8	255	17; 5; 3
7	9	511	7; 3; 7
8	10	1023	31; 11; 3
9	11	2047	89; 23
10	12	4095	3; 3; 5; 7; 13

Наприклад, при h = 10 довжина кодової комбінації може дорівнювати 1023 $(C = 1)$ і 341 (l = 3), і 33 (l =31), і 31 (l = 33), зрозуміло, що n не може бути менше $n_k \ge hs.$ Величина C впливає на вибір порядкових номерів мінімальних многочленів, оскільки індекси спочатку вибраних многочленів множаться на С.

Побудова твірного многочлена $K(x)$ проводиться за допомогою так званих мінімальних многочленів $M(x)$, які є простими неприводими многочленами. Твірним многочленом є добуток непарних мінімальних многочленів і є їх найменшим загальним кратним (НЗК). Максимальний порядок ρ визначає номер останнього з вибираних табличних мінімальних многочленів.

6. ВАРІАНТИ КОНТРОЛЬНОЇ РОБОТИ

Варіант 1

1. Відомо, що одне з *m* можливих повідомлень, які передаються рівномірним двійковим кодом, несе 3 біта інформації. Чому дорівнює N?

2. Чому дорівнює ентропія системи, стан якої описується дискретною величиною з наступними розподілами ймовірності:

x_i	x_1	x_2	x_3	x_4
p_i	0,1	0,2	0,3	0,4

3. В результаті статистичних випробувань встановлено, що при передачі кожних 100 повідомлень завдовжки по 5 символів в повідомленні символ *К* зустрічається 50 разів, а символ *Т* – 30 разів. Разом з символом *К* символ *Т* зустрічається 10 разів. Визначити умовні ентропії H(K/T) і H(T/K).

4. Чому дорівнюють інформаційні втрати в каналі зв'язку, описаного за допомогою наступної канальної матриці:

$$P(a/b) = \begin{vmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{vmatrix}$$

5. Визначити надмірність повідомлень, побудованих з алфавіту з наступним розподілом імовірності появи символів в повідомленнях: pa = 0,03; pb = 0,26; pc = =0,09; pd = 0,05; pe = 0,16; pf = 0,1; pg=0,09; ph = 0,22.

6. Чому дорівнює мінімальна довжина кодових слів для передачі 16, 128, 57, 10, 432 повідомлень у вісімковому і двійковому кодах?

7. Кількісна оцінка інформації. Формули Шеннона та Хартли для знаходження середньої кількості інформації.

Варіант 2

1. Символи алфавіту володіють двома якісними ознаками (m = 2, символи первинного алфавіту). а) Яку кількість повідомлень можна отримати, комбінуючи по 3, 4. 5 і 6 елементів в повідомленні? б) Яка кількість

інформації приходиться на один елемент таких повідомлень?

2. Повідомлення складене з рівномірного алфавіту, що містить *m=128* якісних ознак. Чому дорівнює кількість символів в прийнятому повідомленні, якщо відомо, що воно містить 42 біта інформації? Чому дорівнює ентропія цього повідомлення?

3. Визначити загальну умовну ентропію повідомлень, складених з алфавіту A, B, якщо ймовірність появи символів в повідомленні рівна p_A=0,6; p_B=0,4. Умовна ймовірність переходів одного символу в іншій рівна p(B/A)=0,15; p(A/B)=0,1.

4. Визначити інформаційні втрати в каналі зв'язку, який описується наступною матрицею:

$$P(a/b) = \begin{vmatrix} 0{,}99 & 0{,}01 & 0 \\ 0{,}01 & 0{,}98 & 0 \\ 0 & 0{,}01 & 1 \end{vmatrix}$$

5. Ймовірність появи букв первинного алфавіту на виході джерела повідомлень дорівнює: pa = 0,1; pb = 0,05; pc = 0,04; pd = 0,01; pe = 0,2; pf = 0,5; pg=0,07; ph = 0,03. Визначити ентропію, коефіцієнт стиснення, надмірність і недовантаженість символів повідомлень, побудованих з даного алфавіту.

6. Визначити мінімальну кодову відстань між векторами 1100011 та 1001111.

7. Часткова ентропія. Кількість та об’єм інформації.

Варіант 3

1. В алфавіті три літери A, B, C. а) Скласти максимальну кількість повідомлень, комбінуючи по 3 букви в повідомленні? б) Яка кількість інформації приходиться на одне таке повідомлення? в) Чому дорівнює кількість інформації на символ первинного алфавіту?
2. Визначити ентропію системи, що складається з 6 елементів, кожен з яких може бути в одному з чотирьох станів рівноімовірно.

3. При передачі повідомлень по каналу зв'язку з шумами була отримана наступна статистика: частота f1 з 100 разів була прийнята 97 разів, 2 рази була прийнята частота f2 і 1 раз частота f3; при передачі f2: 98 разів прийнята f2, двічі – f1; при передачі f3: 96 разів прийнята f3, двічі - f2 і двічі – f4; при передачі f4 99 разів прийнята f4 і один раз - f3.

а) Скласти канальну матрицю, що описує даний канал зв'язку з погляду умов проходження частот f1, – f4. б) Визначити загальну умовну ентропію повідомлень алфавітом, яких є частоти f1 - f4, якщо ймовірність появи цих частот в повідомленнях, що передаються, відповідно дорівнює: p(f1)= 0,5, p(f2)=0,2 p(f3)=0,15, p(f4)=0,15.

4. По каналу зв'язку передаються повідомлення, що являють послідовність шістнадцятирічних цифр імовірності яких відповідно дорівнюють:

$$p(a_1)=0,1;\ p(a_2)=0,4;\ p(a_3)=0,5.$$

Канальна матриця, що визначає втрати інформації в каналі зв'язку має вигляд:

$$P(b/a)=\begin{bmatrix} p(b_1/a_1) & p(b_2/a_1) & p(b_3/a_1) \\ p(b_1/a_2) & p(b_2/a_2) & p(b_3/a_2) \\ p(b_1/a_3) & p(b_2/a_2) & p(b_3/a_3) \end{bmatrix}=\begin{bmatrix} 1 & 0 & 0 \\ 0,25 & 0,75 & 0 \\ 0 & 0,2 & 0,8 \end{bmatrix}$$

Визначити ентропію об’єднання H(A, B).

5. Визначити середню надмірність на 200-літерний текст, побудований з алфавіту A, B, C, D з наступним розподілом ймовірності: pa= 0,1; pb= 0,25; pc= 0,35; pd= 0,3.
6. Представити у вигляді поліному наступні кодові комбінації циклічного коду 0111110, 0011111, 1001111.
7. Характеристики дискретних джерел.

Варіант 4

1. Генератор виробляє чотири частоти f1, f2, f3, f4. У шифраторі частоти комбінуються по три частоти в кодовій комбінації. а) Чому дорівнює максимальна кількість комбінацій, складених з цих частот? б) Чому дорівнює кількість інформації на одну кодову посилку цих кодів?

2. Визначити ентропію словосполучення, складеного з англійських літер Lemon tea. Ймовірність появи літер в англійському тексті наступна:
L-0,29; E-0,1105: M-0,021; O-0,065; N-0,059; T-0,072; A-0,063.

3. В результаті статистичних випробувань встановлено, що при передачі кожних 100 повідомлень завдовжки по 5 символів в повідомленні символ *К* зустрічається 25 разів, а символ *Т* – 60 разів. Разом з символом *К* символ *Т* зустрічається 15 разів. Визначити умовні ентропії Н(К/Т) і Н(Т/К).

4. Визначити середню кількість інформації, що міститься в прийнятому ансамблі повідомлень відносно переданого, якщо повідомлення складені з алфавіту А, Б, В. Ймовірністі появи літер в алфавіті на виході джерела повідомлень $p(A_i)$=0,25, $p(B_i)$=0,25, $p(C_i)$ = 0,5. Умовна ймовірність виникнення пар виду a_i/ b_i наступна:
p(A/A)= 0,97; p(A/B)= 0,02; p(A/C)= 0,01; p(B/A)= 0,015; p(B/B)= 0,97; p(B/C)= 0,01; p(C/A)= 0,015; p(C/B)= 0,01; p(C/C)= 0,98.

5. Визначити загальну і часткову надмірності деякого восьмилітерного алфавіту, якщо відомо, що з урахуванням нерівноімовірності розподілу символів його ентропія дорівнює Н’=2,7 біт/символ, а з урахуванням взаємозалежності літер ентропія цього алфавіту зменшується на 0,25 біт/символ.

6. Необхідно передати в двійковому коді 9 числа: 5, 7, 17, 31, 33, 127, 128, 129. Представити ці числа в двійковому коді.

7. Види і класифікація каналів зв’язку.

Варіант 5

1. Відомо, що одне з m можливих повідомлень, які передаються рівномірним двійковим кодом, несе 4 біта інформації. Чому дорівнює N?

2. Чому дорівнює ентропія системи, стан якої описується дискретною величиною з наступними розподілами імовірностей:

x_i	x_1	x_2	x_3	x_4
p_i	0,25	0,25	0,3	0,2

3. Визначити загальну умовну ентропію повідомлень, складених з алфавіту A, B, якщо ймовірність появи символів в повідомленні дорівнює pA=0,8; pB=0,2. Умовна ймовірність переходів одного символу в інший дорівнює p(B/A)=0,35; p(A/B)=0,2.

4. Визначити інформаційні втрати в каналі зв'язку, який описується наступною канальною матрицею:

$$P(a/b)= \begin{vmatrix} 0,99 & 0,02 & 0 & 0 \\ 0,01 & 0,98 & 0,01 & 0,01 \\ 0 & 0 & 0,98 & 0,02 \\ 0 & 0 & 0,01 & 0,97 \end{vmatrix}$$

Ймовірність появи символів A, B, C, D на виході джерела повідомлень відповідно дорівнюють: p(A) = p(B) = p(C) = p(D) =0,25. Визначити також середню кількість інформації в прийнятих повідомленнях відносно переданих.

5. З урахуванням частоти появи літер в текстах, ентропія англійської, німецької, французької і іспанської мов дорівнюють відповідно: $H_{англ}$ =4,03 біт/символ; $H_{фр}$ = 3,96 біт/символ; $H_{ісп}$ = 3,98 біт/символ; $H_{нем}$ = 4,1 біт/символ. Визначити часткову надмірність виду Dp для вказаних вище мов.

6. Закодувати традиційним двійковим кодом Хеммінга комбінацію двійкового простого коду 10110 і показати на прикладі процес виправлення будь-якої однократної помилки. Визначити надмірність коду.

7. Характеристики каналів зв’язку. Характеристики неперервних каналів зв’язку.

Варіант 6

1. Символи алфавіту володіють двома якісними ознаками (m = 2, символи первинного алфавіту). а) Яку кількість повідомлень можна отримати, комбінуючи по 2, 3, 7 і 8 елементів в повідомленні? б) Яка кількість інформації приходиться на один елемент таких повідомлень?

2. Повідомлення складене з рівномірного алфавіту, що містить $m=128$ якісних ознак. Чому рівна кількість символів в прийнятому повідомленні, якщо відомо, що воно містить 42 біта інформації? Чому дорівнює ентропія цього повідомлення?

3. При передачі повідомлень по каналу зв'язку з шумами була отримана наступна статистика: частота f1 з 100 разів була прийнята 97 разів, 2 рази була прийнята частота f2 і 1 раз частота F3; при передачі f2 98 разів прийнята f2, двічі – f1; при передачі f3 96 разів прийнята f3, двічі - f2 і двічі – f4; при передачі f4 99 разів прийнята f4 і один раз - f3.

А) Скласти канальну матрицю, що описує даний канал зв'язку з погляду умов проходження частот f1, – f4.

Б) Визначити загальну умовну ентропію повідомлень алфавітом яких є частоти f1 - f2,если ймовірність появи цих частот в передаваних повідомленнях відповідно рівна: p(f1)=0,2, p(f2)=0,4, p(f3)=0,25, p(f4)=0,15.

4. Визначити надмірність повідомлень, побудованих з алфавіту з наступним розподілом ймовірністі появи символів в повідомленнях: pa = 0,07; pb = 0,03; pc = 0,09; pd = 0,01; pe = 0,3; pf = 0,11; pg=0,09; ph = 0,3.

5. Повідомлення складені з п’яти якісних ознак. Тривалість елементарної посилки складає τ=20 мсек. Чому дорівнює швидкість передачі сигналів?

6. Визначити мінімальну кодову відстань, яка необхідна для виправлення в коді потрійної помилки.

7. Швидкість передачі інформації та пропускна здатність дискретного каналу без завад.

Варіант 7

1. У алфавіті три літери D, E, F. а) Скласти максимальну кількість повідомлень, комбінуючи по 2 літери в повідомленні? б) Яка кількість інформації приходиться на одне таке повідомлення? у) Чому дорівнює кількість інформації на символ первинного алфавіту?

2. Визначити максимальну ентропію системи, що складається з 8 елементів, кожен з яких може бути в одному з п'яти станів рівноімовірно.

3. В результаті статистичних випробувань встановлено, що при передачі кожних 100 повідомлень завдовжки по 5 символів в повідомленні символ *К* зустрічається 30 разів, а символ *Т* – 40 разів. Разом з символом *К* символ *Т* зустрічається 20 разів. Визначити умовні ентропії H(K/T) і H(T/K).

4. Визначити кількість інформації в прийнятому ансамблі повідомлень, якщо задана умовна імовірність переходу одного сигналу в інший і імовірності появи сигналів на виході джерела повідомлень: p(a) = 0,2; p(b) = 0,3; p(c) = 0,5; p(a/a)= p(b/b)= p(c/c)= 0,97; p(b/a)= p(c/a)= p(a/b)= p(c/b)= p(a/c)= p(b/c)= 0,015.

5. Ймовірність появи літер первинного алфавіту на виході джерела повідомлень дорівнює: pa = 0,2; pb = 0,03; pc = 0,06; pd = 0,02; pe = 0,1; pf = 0,5; pg=0,06; ph = 0,03. Визначити ентропію, коефіцієнт стиснення, надмірність і недовантаженість символів повідомлень, побудованих з даного алфавіту.

6. Побудувати оптимальний код повідомлення, в якому імовірність появи літер підпорядковується закону $p_i=(1/2)^i$.

7. Швидкість передачі інформації та пропускна здатність дискретного каналу з завадами.

Варіант 8

1. Яка кількість інформації приходиться на літеру алфавіту, що складається з 16, 25, 32 літер?

2. Визначити ентропію словосполучення, отриманого з російських літер – «Яблони цветут». Ймовірність появи літер в російському тексті наступна:
Я – 0,018; Б – 0,014; Л – 0,035; О – 0,09; Н – 0,053; И – 0,062; Ц – 0,004; В - 0,038; Е – 0,072; Т – 0,053; У – 0,021.

3. Визначити загальну умовну ентропію повідомлень, складених з алфавіту A, B, якщо ймовірність появи символів в повідомленні дорівнює pA=0,3; pB=0,7. Умовна вірогідність переходів одного символу в інший дорівнює p(B/A)=0,25; p(A/B)=0,15.

4. Визначити інформаційні втрати в каналі зв'язку, який описується наступною канальною матрицею:

$$P(a,b) = \begin{vmatrix} 0{,}1 & 0{,}1 & 0 \\ 0 & 0{,}2 & 0{,}1 \\ 0 & 0{,}2 & 0{,}3 \end{vmatrix}$$

5. Визначити середню надмірність на 200-літерний текст, побудований з алфавіту A, B, C, D з наступним розподілом ймовірностей: pa = 0,2; pb = 0,25; pc = 0,45; pd = 0,1.

6. Побудувати модель кода Хеммінга для комбінації 0101.

7. Класифікація завадостійких кодів. Основні принципи завадостійкого кодування.

Варіант 9

1. Відомо, що одне з m можливих повідомлень, передаваних рівномірним двійковим кодом, несе 9 біт інформації. Чому дорівнює N?

2. Визначити максимум ентропії системи, що складається з 9 елементів,

кожен з яких може бути в одному з трьох станів рівноімовірно.

3. При передачі повідомлень по каналу зв'язку з шумами була отримана наступна статистика: частота f1 з 100 разів була прийнята 97 разів, 2 рази була прийнята частота f2 і 1 раз частота f3; при передачі f2 98 разів прийнята f2, двічі – f1; при передачі f3 96 разів прийнята f3, двічі - f2 і двічі – f4; при передачі f4 99 разів прийнята f4 і один раз - f3.

а) Скласти канальну матрицю, що описує даний канал зв'язку з погляду умов проходження частот f1 – f4.

б) Визначити загальну умовну ентропію повідомлень, алфавітом яких є частоти f1 - f2, якщо ймовірність появи цих частот в передаваних повідомленнях відповідно рівна: p(f1) =0,17, p(f2)=0,33, p(f3)=0,23, p(f4)=0,27.

4. Визначити ентропію приймача повідомлень H(B), умовну ентропію H(B/A), якщо канальна матриця має вигляд

$$p(b/a) = \begin{vmatrix} 0{,}99 & 0{,}01 & 0 \\ 0{,}01 & 0{,}98 & 0{,}01 \\ 0 & 0{,}03 & 0{,}97 \end{vmatrix}$$

а імовірності появи символів на виході джерела повідомлень p(a1)=0,8; p(a2)=0,05;p(a3)=0,15.

5. Визначити загальну і часткову надмірності деякого чотирьохлітерногоалфавіту, якщо відомо, що з урахуванням нерівноімовірності розподілу символів його ентропія дорівнює H=1,7 біт/символ, а з урахуванням взаємозалежності літер ентропія цього алфавіту зменшується на 0,15 біт/символ.

6. Закодувати двійковим циклічним кодом, що виправляє однократні помилки, кодову комбінацію двійкового простого коду 1110.

7. Побудова кодів з заданою виправляючою здатністю. Показники якості корегуючого коду.

Варіант 10

1. Символи алфавіту володіють двома якісними ознаками (m = 2, символи первинного алфавіту). а) Яку кількість повідомлень можна отримати, комбінуючи по 3, 4. 9 і 11 елементів в повідомленні? б) Яка кількість інформації приходиться на один елемент таких повідомлень?

2. Повідомлення складене з рівномірного алфавіту, *т, що* містить = 256 якісних ознак. Чому дорівнює кількість символів в прийнятому повідомленні, якщо відомо, що воно містить 42 біта інформації? Чому дорівнює ентропія цього повідомлення?

3. При передачі текстових повідомлень статистичні спостереження показали, що для слів з середньою довжиною в 6 букв на кожних 100 повідомлень літера А зустрічається 80 разів, літера В зустрічається 50 разів, літера А і В разом зустрічаються 10 разів. Визначити умовну ентропію появи А, якщо в слові присутня В, і умовну ентропію В, якщо в слові присутній А.

4. Визначити інформаційні втрати в каналі зв'язку, описаному наступною канальною матрицею:

$$P(a,b) = \begin{vmatrix} 0{,}1 & 0 & 0{,}1 \\ 0 & 0{,}1 & 0{,}2 \\ 0 & 0{,}3 & 0{,}2 \end{vmatrix}$$

5. З урахуванням частоти появи букв в текстах, ентропія англійської, німецької, французької і іспанської мов дорівнюють відповідно: $H_{англ}$ =4,03 біт/символ; $H_{фр}$ = 3,96 біт/символ; $H_{ісп}$ = 3,98 біт/символ; $H_{нем}$ = 4,1 біт/символ. Визначити частинну надмірність виду D_p для вказаних вище мов.

6. Визначити ентропію фізичної системи В, яка може знаходитись в одному з 10 станів:

B	b1	b2	b3	b4	b5	b6	b7	b8	b9	b10
	0.01	0.07	0.035	0.035	0.35	0.07	0.14	0.07	0.15	0.07

7. Побудова циклічних кодів.

7. ОСНОВНІ ВИМОГИ ДО ОФОРМЛЕННЯ КОНТРОЛЬНОЇ РОБОТИ

Контрольна робота повинна містити титульний лист (див. додаток ІІ), умову завдання і докладне її рішення. При описі рішення необхідно указувати:

1. назви формул;
2. формули;
3. опис змінних, використовуваних у формулах;
4. назва методів, які використовуються при рішення конкретної задачі;
5. всю послідовність виконання розрахунків;
6. результати обчислень і, якщо необхідно, зробити висновок.

Варіант контрольної роботи уточнюється у викладача (по списках).

8. ЕКЗАМЕНАЦІЙНІ ПИТАННЯ

1. Що розуміють під інформаційними системами?
2. Що таке інформація, повідомлення, сигнал ?
3. Який зв'язок між поняттями інформація, повідомлення, сигнал?
4. В чому полягає предмет і метод теорії інформації?
5. Що розуміють під ефективністю і завадостійкістю інформаційних систем?
6. В чому полягає процес перетворення повідомлень в сигнал ?
7. Які способи представлення моделей сигналів вам відомі ?
8. В чому полягають переваги частотного методу представлення сигналів?
9. За яких умов періодична функція може бути представлена рядом Фур'є ?
10. Як визначити спектр амплітуд та фаз періодичного сигналу?
11. Які характерні особливості спектрів періодичного сигналу?
12. Умови представлення неперіодичної функції рядом Фур'є ?
13. Які властивості спектральної щільності неперіодичного сигналу?
14. Сформулювати визначення та властивості випадкового сигналу.
15. Головні числові характеристики випадкового сигналу.
16. Що таке ергодична стаціонарна випадкова функція ?
17. Поясніть сутність поняття ентропії.
18. Сформулюйте основні властивості ентропії.
19. Як визначається ентропія дискретної системи з рівномірними і нерівноімовірними станами ?
20. Чому дорівнює ентропія при нерівномірному і взаємозалежному розподілі елементів системи?
21. Що таке умовна ентропія?
22. Якими узагальненими характеристикам визначаються сигнал і канал передачі інформації?
23. Що розуміють під об'ємом сигналу і ємністю каналу передачі інформації?
24. Чим обумовлена необхідність узгодження сигналу з каналом передачі інформації ?

25. Сформулюйте необхідні і достатні умови узгодження сигналу з каналом передачі інформації.
26. Поясніть , як можна передати широкополосний сигнал через вузькополосний канал без спотворень?
27. Що розуміють під швидкістю передачі інформації і пропускною здатністю каналу?
28. Якими факторами визначаються швидкість передачі інформації та пропускна здатність каналу?
29. В чому полягає сутність теореми Шеннона для дискретного каналу без завад?
30. Яким чином обчислюється швидкість передачі інформації по дискретному каналу з завадами і без завад?
31. Яким чином визначається пропускна здатність дискретного каналу з завадами і без завад?
32. В чому полягає сутність теореми Шеннона для дискретного каналу з завадами ?

9. ЛІТЕРАТУРА

1. Кузин Л. Т. Основи кібернетики. Т. 1. Математичні основи кібернетики. Навчальний посібник для студентів вузів. М.: “Енергія”, 1973.
2. Теорія інформації і кодування. Цимбал В. П. Київ, Видавниче об'єднання “Вища школа”, 1977, 288 с.
3. Задачник по теорії інформації і кодуванню. Цимбал В. П. Видавниче об'єднання “Вища школа”, 1976, 276 с.
4. Тарасенко Ф. П. Введення в курс теорії інформації. Університет Томська, 1963 р.
5. М. Н. Аршинів, Л. Е. Садовський Коди і математика (розповіді про кодування).- М.: Наука, Головна редакція фізико-математичної літератури, 1983.
6. Марков А. А. Введення в теорію кодування. -М.: Наука, 1982.
7. Шенон К. Работи по теорії інформації і кібернетики, М.: видавництво іноз. літ., 1963г.
8. Хеммінг Р. В. Коди з виявленням і виправленням помилок. Під ред. Трофімова До. Н., М.: Воєніздат, 1970.

Додаток А

Таблиця логарифмів

p	$-p\log_2 p$	p	$-p\log_2 p$	p	$-p\log_2 p$
0.00	-	0.35	0.5301	0.70	0.3602
0.01	0.0664	0.36	0.5306	0.71	0.3508
0.02	0.1129	0.37	0.5307	0.72	0.3412
0.03	0.1517	0.38	0.5304	0.73	0.3314
0.04	0.1857	0.39	0.5298	0.74	0.3215
0.05	0.2161	0.40	0.5288	0.75	0.3113
0.06	0.2435	0.41	0.5274	0.76	0.3009
0.07	0.2686	0.42	0.5256	0.77	0.2903
0.08	0.2915	0.43	0.5236	0.78	0.2796
0.09	0.3127	0.44	0.5211	0.79	0.2687
0.10	0.3322	0.45	0.5184	0.80	0.2575
0.11	0.3503	0.46	0.5153	0.81	0.2462
0.12	0.3671	0.47	0.5120	0.82	0.2348
0.13	0.3826	0.48	0.5083	0.83	0.2231
0.14	0.3971	0.49	0.5043	0.84	0.2113
0.15	0.4105	0.50	0.5000	0.85	0.1993
0.16	0.4230	0.51	0.4954	0.86	0.1871
0.17	0.4346	0.52	0.4906	0.87	0.1748
0.18	0.4453	0.53	0.4854	0.88	0.1623
0.19	0.4552	0.54	0.4800	0.89	0.1496
0.20	0.4644	0.55	0.4744	0.90	0.1368
0.21	0.4728	0.56	0.4684	0.91	0.1238
0.22	0.4806	0.57	0.4623	0.92	0.1107
0.23	0.4877	0.58	0.4558	0.93	0.0974

0.24	0.4941	0.59	0.4491	0.94	0.0839
0.25	0.5000	0.60	0.4422	0.95	0.0703
0.26	0.5053	0.61	0.4350	0.96	0.0565
0.27	0.5100	0.62	0.4276	0.97	0.0426
0.28	0.5142	0.63	0.4199	0.98	0.0286
0.29	0.5179	0.64	0.4121	0.99	0.0140
0.30	0.5211	0.65	0.4040		
0.31	0.5238	0.66	0.3957		
0.32	0.5260	0.67	0.3871		
0.33	0.5278	0.68	0.3784		
0.34	0.5292	0.69	0.3694		

Додаток Б

Таблиця Б.1

Співвідношення між n, n_i, n_k для коду Хеммінга

n	n_i	n_k	n	n_i	n_k
1	0	1	9	5	4
2	0	2	10	6	4
3	1	2	11	7	4
4	1	3	12	8	4
5	2	3	13	9	4
6	3	3	14	10	4
7	4	3	15	11	4
8	4	4	16	11	5

Таблиця Б.2

Загальна таблиця перевірок

№ перевірки	Перевірочні позиції	№ контрольного символу
1	1, 3, 5, 7, 9, 11...	1
2	2, 3, 6, 7, 12, 13, 14, 15, 20, 21, 22, 23, 27, 30, 31...	2
3	4, 5, 6, 7, 12, 13, 14, 15, 20, 21, 22, 23, 28, 29, 30, 31..	3
4	8, 9, 10, 11, 12, 13, 14, 15, 24, 25, 26, 27, 28, 29, 30, 31, 40, 41, 42, 43, 44, 45, 46...	4

Додаток В

Твірні поліноми циклічних кодів

Кількість перевірочних елементів *r*	Твірний поліном *P(x)*	Двійковий запис полінома
3	$x^3 \oplus x \oplus 1 \oplus$	1011
3	$x^3 \oplus x^2 \oplus 1$	1101
4	$x^4 \oplus x \oplus 1$	10011
4	$x^4 \oplus x^3 \oplus 1$	11001
5	$x^5 \oplus x^2 \oplus 1$	100101
5	$x^5 \oplus x^3 \oplus 1$	101001
5	$x^5 \oplus x^3 \oplus x^2 \oplus x \oplus 1$	101111
5	$x^5 \oplus x^4 \oplus x^2 \oplus x \oplus 1$	110111
6	$x^6 \oplus x^5 \oplus x^4 \oplus 1$	1110001
8	$x^8 \oplus x^7 \oplus x^6 \oplus x^5 \oplus x^2 \oplus x \oplus 1$	111100111
9	$x^9 \oplus x^5 \oplus x^3 \oplus 1$	1000101001

Додаток Г

Титульний лист

Міністерство освіти та науки України

Центральноукраїнський національний технічний університет

Кафедра «АВП»

К О Н Т Р О Л Ь Н А Р О Б О Т А

з курсу «ТЕОРІЯ ІНФОРМАЦІЇ»

Варіант № ____

Розробив: студент гр. *шифр групи*

прізвище, ім'я, по-батькові студента

Перевірив: *вчений ступінь та звання, посада*

прізвище, ім'я, по-батькові викладача

Кропивницький 2018