МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

Кафедра протидії кіберзлочинності факультету №4

МЕТОДИЧНІ МАТЕРІАЛИ ДО ЛАБОРАТОРНИХ ЗАНЯТЬ

з навчальної дисципліни "Теорія інформації та кодування"
обов’язкових компонент
освітньої програми першого рівня вищої освіти

125 "Кібербезпека" (Протидія кіберзлочинності, Безпека інформаційних та комунікаційних систем)

Харків 2021

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 26.08.2021 № 7

СХВАЛЕНО
Вченою радою факультету №4
Протокол від 25.08.2021 № 7

ПОГОДЖЕНО
Секцією науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 26.08.2021 № 7

Розглянуто на засіданні кафедри протидії кіберзлочинності (протокол від 25.08.2021 № 15)

Розробники:

завідувач кафедри протидії кіберзлочинності ХНУВС, к.т.н., доцент
Гнусов Ю.В.,

викладач кафедри протидії кіберзлочинності ХНУВС Калякін С.В.

Рецензенти:

завідувач кафедри інформаційних управляючих систем ХНУРЕ, д.т.н., професор Петров К.Е.

доцент кафедри кібербезпеки та DATA-технологій факультету № 6 ХНУВС, к.т.н., доцент Тулупов В.В.

1. Розподіл часу навчальної дисципліни за темами

Номер та назва навчальної теми	Кількість годин відведених на вивчення навчальної дисципліни					Вид контролю
	Всього	з них:				
		лекції	Практичні заняття	Лабораторні заняття	Самостійна робота	
Семестр №4						
Тема №1. Основні поняття теорії інформації	44	8	-	8	28	**залік**
Тема №2. Кодування в дискретних каналах зв’язку	106	16	-	28	62	
Всього за дисципліною	**150**	**24**	**-**	**36**	**90**	

2. Методичні вказівки до лабораторних занять

Тема №1. Основні поняття теорії інформації

Лабораторна робота 1. Розрахунок характеристик дискретних джерел інформації

Навчальна мета заняття: навчитися оцінювати і розраховувати характеристики дискретних джерел інформації

Час проведення: 4 год.

Навчальні питання

Вступ

1. Розрахунок характеристик дискретного джерела інформації
2. Розрахунок характеристик сукупності немарковських дискретних джерел інформації

Висновки

Література: [3, л.1, 2], [4, 5, 6].

Матеріально-технічне забезпечення: комп’ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

I. Порядок проведення вступу до заняття.

Провести письмове опитування за контрольними питаннями лекцій 1 і 2. Нагадати основні визначення і вирази для:

- ентропії джерела повідомлення і кількості інформації в повідомленні,
- первинних характеристик дискретного джерела інформації,

- для двох дискретних немарковських джерел інформації:
  - умовної частинної ентропії;
  - середньої або повної умовної ентропії;
  - сумісної ентропії;
  - повної взаємної інформації.

ІІ. Порядок проведення основної частини заняття.

Навести дані задач. Дати час для самостійного розв'язання задач. Розібрати зразкове розв'язання задач.

1. Розрахунок характеристик дискретного джерела інформації.

Задача 1.1.

Розподіл ймовірностей появи символів на виході немарківського джерела з алфавітом X потужності $M=5$ є таким:

$$p(x_1)=p(x_2)=0{,}1; \quad p(x_3)=0{,}15; \quad p(x_4)=0{,}2; \quad p(x_5)=0{,}45.$$

Тривалості символів $\tau_1=\tau_2=\tau_3=2\ мс; \quad \tau_4=1 мс; \ \tau_5=3 мс.$

Розрахувати ентропію, продуктивність та надмірність джерела.

Розв'язання. Користуючись виразами $H=-\sum_{i=1}^{M} p(x_i)\cdot log\, p(x_i)$,

$H = H_{max} = log_2 M$, $\overline{H} = H/\tau$, $R = 1 - H/\log_2 M$, знаходимо:

1) ентропія

$H=(-0{,}1\cdot log_2 0{,}1)\cdot 2-0{,}15\cdot log_2 0{,}15-0{,}2\cdot log_2 0{,}2-0{,}45\cdot log_2 0{,}45\approx 2{,}058 біт;$

2) середня тривалість символу

$\tau=2\cdot(0{,}1+0{,}1+0{,}15)+1\cdot 0{,}2+3\cdot 0{,}45=2{,}25 мс$;

3) продуктивність

$\overline{H}=2{,}058/(2.25\cdot 10^{-3})\approx 914{,}67 біт/с;$

4) надмірність

$$R = 1 - 2{,}058 / log_2 5 = 0{,}114 .$$

2. Розрахунок характеристик сукупності немарківських дискретних джерел інформації.

Задача 1.2.

Маємо два дискретних немарківських джерела інформації з алфавітами $X=\{x_1,x_2,x_3\}$ та $Y=\{y_1,y_2,y_3\}$ з такими розподілами ймовірностей появи символів:

$p(x_1)=0{,}7; \quad p(x_2)=0{,}2; \quad p(x_3)=0{,}1;$

$p(y_1)=0{,}4; \quad p(y_2)=0{,}35; \quad p(y_3)=0{,}25$

Не розраховуючи ентропії джерел, дати відповідь, яке з них має більшу ентропію.

Розв'язання. Оскільки розподіл імовірностей появи символів на виході джерела з алфавітом Y є більш близьким до рівноймовірного, ентропія цього джерела буде більшою, ніж джерела з алфавітом X.

Розрахунки підтверджують цей висновок:

$H(Y)=1{,}56>H(X)=1{,}16.$

Задача 1.3.

Матриця ймовірностей сумісної появи символів на виходах двох немарківських джерел з алфавітами $X=\{x_1,x_2,x_3\}$ та $Y=\{y_1,y_2,y_3\}$ має вигляд:

$$\begin{bmatrix} p(x_1,y_1) & p(x_2,y_1) & p(x_3,y_1) \\ p(x_1,y_2) & p(x_2,y_2) & p(x_3,y_2) \\ p(x_1,y_3) & p(x_2,y_3) & p(x_3,y_3) \end{bmatrix} = \begin{bmatrix} 0{,}0336 & 0{,}0264 & 0{,}0200 \\ 0{,}3150 & 0{,}2475 & 0{,}1875 \\ 0{,}0714 & 0{,}0561 & 0{,}0425 \end{bmatrix}.$$

Визначити, яке з джерел має більшу ентропію та чи є джерела статистично незалежними.

Розв'язання. Для відповіді на перше запитання розрахуємо, користуючись виразами $p(y_k)=\sum_{i=1}^{M} p(x_i,y_k);\quad p(x_i)=\sum_{k=1}^{N} p(x_i,y_k)$, безумовні ймовірності появи символів на виходах першого та другого джерел:

$p(x_1)$ = 0,0336 + 0,3150 + 0,0714 = 0,42;

$p(x_2)$ = 0,0264 + 0,2475 + 0,0561 = 0,33;

$p(x_3)$ = 0,0200 + 0,1875 + 0,0425 = 0,25;

$p(y_1)$ = 0,0336 + 0,0264 + 0,0200 = 0,08;

$p(y_2)$ = 0,3150 + 0,2475 + 0,1875 = 0,75;

$p(y_3)$ = 0,0714 + 0,0561 + 0,0425 = 0,17.

Тепер можемо знайти ентропії джерел за виразом (1.1):

$H(X)=1{,}553\,біт$; $H(Y)=1{,}037\,біт.$

Таким чином, джерело з алфавітом X має більшу ентропію, ніж джерело з алфавітом Y.

Відповідь на друге запитання можна отримати різними способами. По-перше, оскільки вже відомі значення ентропій $H(X)$ та $H(Y)$, доцільно перевірити, чи виконується рівність $H(X,Y)=H(X)+H(Y)$. Для цього розрахуємо сумісну ентропію $H(X,Y)$. Підставивши чисельні значення ймовірностей у вираз $H(X,Y)=-\sum_{i=1}^{M}\sum_{k=1}^{N} p(x_i,y_k)\cdot log_2\, p(x_i,y_k)$., отримаємо:

$H(X,Y)=2{,}59\,біт.$

Оскільки $H(X)+H(Y)=1{,}533+1{,}037=2{,}59=H(X,Y)$, джерела є статистично незалежними.

Другий спосіб базується на перевірці виконання співвідношень $p(x_i,y_k)=p(x_i)\cdot p(y_k)$ для всіх пар символів:

$p(x_1)\cdot p(y_1)$ = 0,42·0,08 = 0,0336;

$p(x_2)\cdot p(y_1) = 0{,}33\cdot 0{,}08 = 0{,}0264$;
$p(x_3)\cdot p(y_1) = 0{,}25\cdot 0{,}08 = 0{,}0200$;
$p(x_1)\cdot p(y_2) = 0{,}42\cdot 0{,}75 = 0{,}3150$;
$p(x_2)\cdot p(y_2) = 0{,}33\cdot 0{,}75 = 0{,}2475$;
$p(x_3)\cdot p(y_2) = 0{,}25\cdot 0{,}75 = 0{,}1875$;
$p(x_1)\cdot p(y_3) = 0{,}42\cdot 0{,}17 = 0{,}0714$;
$p(x_2)\cdot p(y_3) = 0{,}33\cdot 0{,}17 = 0{,}0561$;
$p(x_3)\cdot p(y_3) = 0{,}25\cdot 0{,}17 = 0{,}0561$.

Як і слід було очікувати, розраховані ймовірності цілком збігаються із відповідними значеннями ймовірностей $p(x_i, y_k)$ сумісної появи символів, що наведені в умовах задачі.

Найбільш універсальним способом оцінки статистичної залежності джерел є обчислення повної взаємної інформації $I(X,Y)$. Аналізуючи вираз $I(X,Y) = \sum_{i=1}^{M}\sum_{k=1}^{N} p(x_i, y_k)\cdot log_2 \dfrac{p(x_i, y_k)}{p(x_i)\cdot p(y_k)}$, легко зрозуміти, що для джерел цієї задачі $I(X,Y)=0$, оскільки для усіх пар x_i, y_k

$$log_2 \frac{p(x_i, y_k)}{p(x_i)p(y_k)} = log_2 1 = 0 .$$

Ще один спосіб розв'язання задачі базується на аналізі матриці умовних імовірностей. Розрахуємо, наприклад, умовні ймовірності $p(x_i / y_k)$, користуючись виразом $p(x_i / y_k) = p(x_i, y_k) / p(y_k)$:

$$\begin{bmatrix} p(x_1/y_1) & p(x_2/y_1) & p(x_3/y_1) \\ p(x_1/y_2) & p(x_2/y_2) & p(x_3/y_2) \\ p(x_1/y_3) & p(x_2/y_3) & p(x_3/y_3) \end{bmatrix} = \begin{bmatrix} 0{,}42 & 0{,}33 & 0{,}25 \\ 0{,}42 & 0{,}33 & 0{,}25 \\ 0{,}42 & 0{,}33 & 0{,}25 \end{bmatrix}.$$

Всі елементи кожного стовпця однакові і дорівнюють безумовній ймовірності $p(x_i)$ появи відповідного символу x_i. Це означає, що ймовірність появи символу на виході першого джерела не залежить від символу на виході другого джерела. Можна переконатись, що і в матриці умовних ймовірностей $p(y_k / x_i)$ всі елементи кожного стовпця будуть однаковими і дорівнювати $p(y_k)$.

Задача 1.4.

Маємо три дискретних немарківських джерела інформації з алфавітами $X=\{x_1, x_2, x_3\}$, $Y=\{y_1, y_2\}$, $Z=\{z_1, z_2\}$. Матриці ймовірностей сумісної появи пар символів є такими:

$$\begin{bmatrix} p(x_1,y_1) & p(x_2,y_1) & p(x_3,y_1) \\ p(x_1,y_2) & p(x_2,y_2) & p(x_3,y_2) \end{bmatrix} = \begin{bmatrix} 0{,}28 & 0{,}08 & 0{,}04 \\ 0{,}42 & 0{,}12 & 0{,}06 \end{bmatrix},$$

$$\begin{bmatrix} p(x_1,z_1) & p(x_2,z_1) & p(x_3,z_1) \\ p(x_1,z_2) & p(x_2,z_2) & p(x_3,z_2) \end{bmatrix} = \begin{bmatrix} 0{,}50 & 0{,}05 & 0 \\ 0{,}20 & 0{,}15 & 0{,}10 \end{bmatrix},$$

$$\begin{bmatrix} p(y_1,z_1) & p(y_2,z_1) \\ p(y_1,z_2) & p(y_2,z_2) \end{bmatrix} = \begin{bmatrix} 0{,}35 & 0{,}15 \\ 0{,}05 & 0{,}45 \end{bmatrix}.$$

Визначити, між якими джерелами статистичний зв'язок найбільший, а між якими найменший.

Розв'язання. Для відповіді на поставлене запитання треба знайти значення повної взаємної інформації для всіх пар джерел, та порівняти їх. Найпростіше в даному разі користуватись виразом

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

Щоб обчислити безумовні ентропії кожного з джерел, знайдемо безумовні ймовірності появи символів на виході джерел за виразами $p(y_k) = \sum_{i=1}^{M} p(x_i, y_k)$;

$$p(x_i) = \sum_{k=1}^{N} p(x_i, y_k):$$

$p(x_1) = 0{,}7$; $p(x_2) = 0{,}2$; $p(x_3) = 0{,}1$;

$p(y_1) = 0{,}4$; $p(y_2) = 0{,}6$;

$p(z_1) = 0{,}5$; $p(z_2) = 0{,}5$.

Слід зазначити, що значення кожної з ймовірностей можна отримати двома шляхами. Так $p(y_i)$, $i = 1{,}2$ є сумою елементів відповідних рядків першої матриці, або елементів стовпців третьої матриці. Це означає, що матриці, наведені в завданні, відповідним чином узгоджені.

Розрахуємо ентропії джерел, користуючись $H = -\sum_{i=1}^{M} p(x_i) \cdot log\, p(x_i)$:

$$H(X) = 1{,}157\ біт;\ H(Y) = 0{,}971\ біт;\ H(Z) = 1{,}0\ біт.$$

Далі за виразом $H(X,Y) = -\sum_{i=1}^{M}\sum_{k=1}^{N} p(x_i, y_k) \cdot log_2\, p(x_i, y_k)$ знаходимо сумісні ентропії:

$H(X,Y) = 2{,}218$ *біт*; $H(X,Z) = 1{,}923$ *біт*;

$H(Y,Z) = 1{,}675$ *біт.*

Нарешті отримаємо:

$I(X,Y) = 1{,}157 + 0{,}971 - 2{,}128 = 0$ *біт*;

$I(X,Z) = 1{,}157 + 1{,}0 - 1{,}923 = 0{,}234$ *біт*;

$I(Y,Z) = 0{,}971 + 1{,}0 - 1{,}675 = 0{,}296$ *біт.*

Рівність нулю $I(X,Y)$ означає, що джерела з алфавітами X та Y статистично незалежні. Найбільший статистичний зв'язок має місце між джерелами з алфавітами Y та Z, оскільки $I(Y,Z)$ має найбільше значення.

Задача 1.5.

Маємо три дискретних немарківських джерела з алфавітами $X=\{x_1,x_2\}$, $Y=\{y_1,y_2\}$, $Z=\{z_1,z_2\}$. Ймовірності сумісної появи символів мають такі значення:

$p(x_1, y_1, z_1) = 0{,}048;$
$p(x_1, y_1, z_2) = 0{,}012;$
$p(x_1, y_2, z_1) = 0{,}072;$
$p(x_1, y_2, z_2) = 0{,}162;$
$p(x_2, y_1, z_1) = 0{,}272;$
$p(x_2, y_1, z_2) = 0{,}068;$
$p(x_2, y_2, z_1) = 0{,}300;$
$p(x_2, y_2, z_2) = 0{,}060.$

Знайти ентропії кожного з джерел, системи трьох джерел, а також повну взаємну інформацію для кожної пари джерел.

Розв'язання. Щоб знайти ентропію кожного з джерел, розрахуємо ймовірності появи символів на виході джерел згідно з виразами:

$$p(x_1) = \sum_{k=1}^{2}\sum_{j=1}^{2} p(x_1, y_k, z_j); \qquad p(x_2) = 1 - p(x_1);$$

$$p(y_1) = \sum_{i=1}^{2}\sum_{j=1}^{2} p(x_i, y_1, z_j); \qquad p(y_2) = 1 - p(y_1);$$

$$p(z_1) = \sum_{i=1}^{2}\sum_{k=1}^{2} p(x_i, y_k, z_1); \qquad p(z_2) = 1 - p(z_1).$$

Маємо такі значення:

$$p(x_1) = 0{,}3; \quad p(x_2) = 0{,}7; \quad p(y_1) = 0{,}4;$$
$$p(y_2) = 0{,}6; \quad p(z_1) = 0{,}692; \quad p(z_2) = 0{,}308.$$

Знаходимо ентропії джерел:

$$H(X) = 1{,}8813 \text{ біт}; \; H(Y) = 0{,}971 \text{ біт}; \; H(Z) = 0{,}8909 \text{ біт}.$$

Щоб обчислити повну взаємну інформацію, знайдемо ентропії $H(X,Y), H(X,Z), H(Y,Z)$, для чого розрахуємо ймовірності сумісної появи пар символів, користуючись виразами типу:

$$p(x_i, y_k) = \sum_{j=1}^{2} p(x_i, y_k, z_j).$$

Маємо

$$\begin{bmatrix} p(x_1,y_1) & p(x_2,y_1) \\ p(x_1,y_2) & p(x_2,y_2) \end{bmatrix} = \begin{bmatrix} 0{,}06 & 0{,}34 \\ 0{,}24 & 0{,}36 \end{bmatrix}, \quad \begin{bmatrix} p(y_1,z_1) & p(y_2,z_1) \\ p(y_1,z_2) & p(y_2,z_2) \end{bmatrix} = \begin{bmatrix} 0{,}32 & 0{,}372 \\ 0{,}08 & 0{,}228 \end{bmatrix},$$

$$\begin{bmatrix} p(x_1,z_1) & p(x_2,z_1) \\ p(x_1,z_2) & p(x_2,z_2) \end{bmatrix} = \begin{bmatrix} 0{,}12 & 0{,}572 \\ 0{,}18 & 0{,}128 \end{bmatrix}.$$

За виразом $H(X,Y) = -\sum_{i=1}^{M}\sum_{k=1}^{N} p(x_i, y_k) \cdot log_2 p(x_i, y_k)$ обчислюємо ентропії кожної із систем двох джерел:

$$H(X,Y) = 1{,}7975 \text{ біт};$$

$$H(X,Z) = 1{,}653\ біт;$$
$$H(Y,Z) = 1{,}8345\ біт.$$

Тепер знаходимо значення повної взаємної інформації для всіх пар джерел:
$I(X,Y) = H(X) + H(Y) - H(X,Y) = 0{,}0548\,біт,$

Аналогічно
$I(X,Z) = 0{,}1192\,біт$; $I(Y,Z) = 0{,}0274\,біт.$

Для обчислення ентропії системи трьох джерел скористуємось виразом $H(X_1, X_2,...,X_S) = H(X_1) + H(X_2/X_1) + H(X_3/X_2, X_1) + ... + H(X_S/X_{S-1}, X_{S-2},...,X_2, X_1)$, коли $S = 3,\ X_1 = X,\ X_2 = Y,\ X_3 = Z$:
$H(X,Y,Z) = H(X) + H(Y/X) + H(Z/X,Y).$

Із виразу $H(X,Y) = H(X) + H(Y/X)$ отримаємо
$H(Y/X) = H(X,Y) - H(X) = 0{,}9162\ біт.$

Щоб знайти $H(Z/Y,X)$, необхідно розрахувати умовні ймовірності типу $p(z_i / x_j, y_k)$. Для цього скористаємось виразами:

$$p(z_1/x_j, y_k) = \frac{p(x_j, y_k, z_1)}{p(x_j, y_k)}; \qquad p(z_2/x_j, y_k) = 1 - p(z_1/x_j, y_k).$$

Отримаємо
$p(z_1/x_1, y_1) = 0{,}8;$ $\qquad p(z_2/x_1, y_1) = 0{,}2;$
$p(z_1/x_2, y_1) = 0{,}8;$ $\qquad p(z_2/x_2, y_1) = 0{,}2;$
$p(z_1/x_1, y_2) = 0{,}3;$ $\qquad p(z_2/x_1, y_2) = 0{,}7;$
$p(z_1/x_2, y_2) = 0{,}8333;$ $\qquad p(z_2/x_2, y_2) = 0{,}1667.$

Далі знаходимо частинні умовні ентропії

$$H(Z/x_1, y_1) = -\sum_{k=1}^{2} p(z_k/x_1, y_1) \cdot log_2 p(z_k/x_1, y_1) = 0{,}7219\ біт,$$

аналогічно
$H(Z/x_2, y_1) = 0{,}7219\ біт,$
$H(Z/x_1, y_2) = 0{,}8813\ біт,$
$H(Z/x_2, y_2) = 0{,}6501\ біт.$

Тепер обчислимо повну умовну ентропію:

$$H(Z/X,Y) = -\sum_{k=1}^{2}\sum_{i=1}^{2} H(Z/x_i, y_k) \cdot p(x_i, y_k) = 0{,}7343\ біт.$$

Нарешті
$H(X,Y,Z) = 0{,}8813 + 0{,}9162 + 0{,}7343 = 2{,}5316\,біт.$

III. Порядок проведення заключної частини заняття.

Перевірити у декількох курсантів результати розв’язання задач, виставити відповідні оцінки. Зазначити перелік задач для їх розв’язання на самостійній роботі, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Лабораторна робота 2. Дослідження інформаційних характеристик дискретних джерел інформації

Навчальна мета заняття: сформувати уміння розраховувати і автоматизувати розрахунки інформаційних характеристик дискретних джерел інформації

Час проведення: 4 год.

Навчальні питання

Вступ

1. Розрахунок інформаційних характеристик дискретних джерел інформації

Висновки

Література: [3, л.1, 2], [4, 5, 6].

Матеріально-технічне забезпечення: комп’ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

I. Порядок проведення вступу до заняття.

Провести письмове опитування за контрольними питаннями:

1. Що таке джерело повідомлень?
2. Що таке ансамбль повідомлень?
3. Як визначається кількість інформації в одному повідомленні?
4. Що таке ентропія та які її властивості?
5. За яких умов ентропія джерела стає максимальною?
6. Чим визначається продуктивність дискретного джерела?

II. Порядок проведення основної частини заняття.

Виконання завдань роботи здійснюється або вручну, або у будь-якому обчислювальному середовищі (MS Excel, MathCad, MatLab, і т.д.).

1. **Розрахунок інформаційних характеристик дискретних джерел інформації.**

Завдання 2.1.

1. Задати два дискретних джерела повідомлень без пам'яті, що вибирають повідомлення $a_{\downarrow}k\ (A$ та $b_{\downarrow}k\ (B$ де A, B – множини літер прізвища, імені, по-батькові українською та англійською мовою відповідно.
2. Розрахувати ансамблі для кожного джерела повідомлень, пов'язавши з кожним дискретним повідомленням a_i та b_i ймовірність p_i його вибору джерелом.
3. Визначити кількість інформації, що містить кожне повідомлення, та ентропію обох джерел.
4. Визначити продуктивність обох джерел припустивши, що вони вибирають всі свої повідомлення за один і той самий проміжок часу .
5. Порівняти джерела за інформативністю та продуктивністю.

Приклад виконання 2.1.

Перше джерело повідомлень

Джерело повідомлень без пам'яті вибирає повідомлення з множини літер прізвища, імені, по-батькові українською мовою

ІВАНОВ_ІВАН_ІВАНОВИЧ N=20

Розрахунок ансамблю джерела повідомлень

$$A = \{І, В, А, Н, О, И, Ч, \_\}$$

Кількість різних повідомлень або абетка джерела повідомлень k=8.

$$p_i = \frac{n_i}{N}, \qquad \sum_{i=1}^{k} p_i = 1$$

літера	**І**	**В**	**А**	**Н**	**О**	**И**	**Ч**	**_**
a_i	1	2	3	4	5	6	7	8
n_i	3	5	3	3	2	1	1	2
p_i	0.15	0.25	0.15	0.15	0.10	0.05	0.05	0.10

Кількість інформації, що містить кожне повідомлення $I(a_i) = -\log_2 p_i$

a_i	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
p_i	0.15	0.25	0.15	0.15	0.10	0.05	0.05	0.10
$I(a_i)$	2.737	2.000	2.737	2.737	3.322	4.322	4.322	3.322

Ентропія джерела

$$H(A) = \sum_{i=1}^{k} p_i I(a_i), \qquad H(A) = 2.828$$

Продуктивність джерела

$$\bar{H}(A) = \frac{H(A)}{\tau}, \qquad \bar{H}(A) = 2.828$$

Друге джерело повідомлень

Джерело повідомлень без пам'яті вибирає повідомлення з множини літер прізвища, імені, по-батькові англійською мовою

IVANOV_IVAN_IVANOVICH N=21

Розрахунок ансамблю джерела повідомлень

$$B = \{I, V, A, N, O, C, H, \_\}$$

Кількість різних повідомлень k=8 .

$$p_i = \frac{n_i}{N}, \qquad \sum_{i=1}^{k} p_i = 1$$

літера	**I**	**V**	**A**	**N**	**O**	**C**	**H**	**_**
b_i	1	2	3	4	5	6	7	8
n_i	4	5	3	3	2	1	1	2
p_i	0.19	0.24	0.14	0.14	0.10	0.05	0.05	0.10

Кількість інформації, що містить кожне повідомлення $I(b_i) = -\log_2 p_i$

b_i	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
p_i	0.19	0.24	0.14	0.14	0.10	0.05	0.05	0.10
$I(b_i)$	2.392	2.070	2.807	2.807	3.392	4.392	4.392	3.392

Ентропія джерела

$$H(B) = \sum_{i=1}^{k} p_i I(b_i), \qquad H(B) = 2.815$$

Продуктивність джерела

$$\bar{H}(B) = \frac{H(B)}{\tau}, \qquad \bar{H}(B) = 2.815$$

Висновки

Джерело _ є більш інформативним та більш продуктивним порівняно з джерелом _.

Завдання 2.2.

1. Задати два дискретних джерела повідомлень із пам'яттю, що вибирають повідомлення $a_{\downarrow}k$ (А та $b_{\downarrow}k$ (В де A, B – множини пар літер (диграм) прізвища, імені, по-батькові українською та англійською мовою відповідно.
2. Розрахувати ансамблі для кожного джерела повідомлень, пов'язавши з кожним дискретним повідомленням a_i та b_i ймовірність p_i його вибору джерелом.
3. Визначити кількість інформації, що містить кожне повідомлення, та ентропію обох джерел.
4. Визначити продуктивність обох джерел припустивши, що вони вибирають всі свої повідомлення за один і той самий проміжок часу .
5. Порівняти джерела за інформативністю та продуктивністю.

Приклад виконання 2.2 для першого джерела повідомлень

Джерело повідомлень із пам'яттю вибирає диграми повідомлення з множини диграм літер прізвища, імені, по-батькові українською мовою

ІВАНОВ_ІВАН_ІВАНОВИЧ N=19

Розрахунок ансамблю джерела повідомлень

$$A = \{\text{ІВ}, \text{ВА}, \text{В\_}, \text{ВИ}, \text{АН}, \text{НО}, \text{Н\_}, \text{ОВ}, \text{\_І}, \text{ИЧ}\}$$

Кількість різних повідомлень k=10.

$$p_i = \frac{n_i}{N}, \qquad \sum_{i=1}^{k} p_i = 1$$

диграма	ІВ	ВА	В_	ВИ	АН	НО	Н_	ОВ	_І	ИЧ
a_i	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
n_i	3	3	1	1	3	2	1	2	1	1
p_i	0,158	0,158	0,053	0,053	0,158	0,134	0,053	0,134	0,053	0,053

Кількість інформації, що містить кожне повідомлення

$$I(a_i) = -\log_2 p_i$$

a_i	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
p_i	0,158	0,158	0,053	0,053	0,158	0,134	0,053	0,134	0,053	0,053
$I(a_i)$	2,663	2,663	4,248	4,248	2,663	2,900	4,248	2,900	4,248	4,248

Ентропія джерела

$$H(A) = \sum_{i=1}^{k} p_i I(a_i), \qquad H(A) = 3{,}156$$

Продуктивність джерела

$$\bar{H}(A) = \frac{H(A)}{\tau}, \qquad \bar{H}(A) = 3{,}156$$

Висновки

Джерело _ є більш інформативним та більш продуктивним порівняно з джерелом _.

Завдання 2.3.

За результатами виконання завдань 2.1 і 2.2 знайти умовні імовірності $p_i(j)$ для дискретних джерел повідомлень, тобто ймовірностей того, що за літерою i слідує літера j. Індекси i та j пробігають значення для всіх можливих символів. Частоти літер $p(i)$ (ймовірності літери i), умовні імовірності $p_i(j)$ та ймовірності діграм $p(i,j)$ пов'язані такими співвідношеннями:

$$p(i) = \sum_j p(i,j) = \sum_i p(j,i) = \sum_j p(j) p_j(i).$$

$$p(i,j) = p(i) p_i(j).$$

$$\sum_j p_i(j) = \sum_i p(i) = \sum_{i,j} p(i,j) = 1.$$

Приклад виконання завдання 2.3

$p_i(j)$	**І**	**В**	**А**	**Н**	**О**	**И**	**Ч**	**_**
І	0	**1**	0	0	0	0	0	0
В	0	0	**0,6**	0	0	**0,2**	0	**0,2**
А	0	0	0	**1**	0	0	0	0
Н	0	0	0	0	**0,6**	0	0	**0,4**
О	0	**1**	0	0	0	0	0	0
И	0	0	0	0	0	0	**1**	0
Ч	0	0	0	0	0	0	0	0
_	**1**	0	0	0	0	0	0	0

Висновки

III. Порядок проведення заключної частини заняття.

Перевірити результати виконання задач, виставити відповідні оцінки. Зазначити перелік задач для їх розв'язання на самостійній роботі, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №2. Кодування в дискретних каналах зв'язку

Лабораторна робота 3. Оптимальне кодування

Навчальна мета заняття: сформувати уміння здійснювати та оцінювати оптимальне кодування дискретних повідомлень

Час проведення: 4 год.

Навчальні питання

Вступ

1. Побудова оптимальних кодів дискретних повідомлень

Висновки

Література: [3, л.4], [5, 7, 11]].

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

I. Порядок проведення вступу до заняття.

Провести письмове опитування за контрольними питаннями:

1. Якою є ціль оптимального кодування джерела повідомлень?
2. Якою є умова кодування без втрат?
3. Якою повинна бути довжина кодового ланцюга для здійснення кодування без втрат?
4. Яке мінімально можливе значення може приймати середня довжина коду при оптимальному кодуванні?
5. Які існують шляхи зменшення середньої довжини коду при оптимальному кодуванні?
6. Як визначається мінімально середня довжини коду, якщо при цьому забезпечено рівна ймовірність появи знаків вторинного алфавіту?
7. Як визначається відносна надмірність коду?
8. Що стверджує перша теорема Шеннона?
9. Якою є умова Фано для префіксних кодів?
10. Які виконуються процедури при побудові префіксного коду Шеннона-Фано?
11. Які виконуються процедури при побудові проміжного алфавіту префіксного коду Хаффмена?
12. У чому особливість префіксного коду Хаффмена?

ІІ. Порядок проведення основної частини заняття.

Виконання завдань роботи здійснюється або вручну, або у будь-якому обчислювальному середовищі (MS Excel, MathCad, MatLab, і т.д.).

1. **Побудова оптимальних кодів дискретних повідомлень**

Завдання 3.1.

1. Задати дискретне джерело повідомлень без пам'яті, що вибирає повідомлення $a_{\downarrow}k$ (A та $b_{\downarrow}k$ (B де A, B – множини літер прізвища, імені, по-батькові українською мовою відповідно.
2. Розрахувати ансамбль джерела повідомлень, пов'язавши з кожним дискретним повідомленням a_i ймовірність p_i його вибору джерелом.
3. Розрахувати ентропію джерела.

Приклад виконання завдання 1.1

ІВАНОВ_ІВАН_ІВАНОВИЧ А = {І, В, А, Н, О, И, Ч, _}

літера	**І**	**В**	**А**	**Н**	**О**	**И**	**Ч**	**_**
p_i	0,15	0,25	0,15	0,15	0,10	0,05	0,05	0,10

$$H(A) = -\sum_{i=1}^{k} p_i \log_2 p_i, \qquad H(A) = 3{,}156 \text{ біт}$$

Завдання 3.2.

Для ансамблю повідомлень побудувати рівномірний двійковий код з мінімальною довжиною.

Приклад виконання завдання 3.2

Кількість різних повідомлень, що генерує джерело, $k = 8$. Тому для рівномірного двійкового коду мінімальна довжина кодового слова складає

$$n = \log_2 k$$

Кодова таблиця має вигляд

літера	**код**
І	**000**
В	**001**
А	**010**
Н	**011**
О	**100**
И	**101**
Ч	**110**
_	**111**

Завдання 3.3.

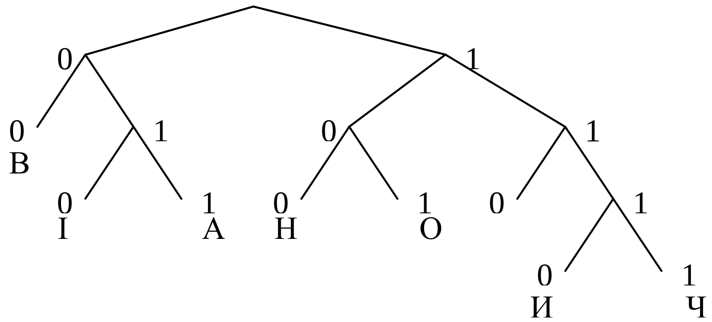
1. Для ансамблю повідомлень побудувати кодову таблицю та кодове дерево коду Шеннона-Фано.
2. Перевірити оптимальність коду відносно довжини кодових комбінацій.

Приклад виконання завдання 3.3.

Кодова таблиця має вигляд

<table>
<tr><th rowspan="2">літера</th><th rowspan="2">p_i</th><th colspan="4">Поділ на групи</th><th rowspan="2">Код</th></tr>
<tr><th>перша</th><th>друга</th><th>третя</th><th>четверта</th></tr>
<tr><td>В</td><td>0,25</td><td rowspan="3">0,55</td><td colspan="3">0,25</td><td>00</td></tr>
<tr><td>І</td><td>0,15</td><td rowspan="2">0,30</td><td colspan="2">0,15</td><td>010</td></tr>
<tr><td>А</td><td>0,15</td><td colspan="2">0,15</td><td>011</td></tr>
<tr><td>Н</td><td>0,15</td><td rowspan="5">0,45</td><td rowspan="2">0,25</td><td colspan="2">0,15</td><td>100</td></tr>
<tr><td>О</td><td>0,10</td><td colspan="2">0,10</td><td>101</td></tr>
<tr><td>_</td><td>0,10</td><td rowspan="3">0,20</td><td colspan="2">0,10</td><td>110</td></tr>
<tr><td>И</td><td>0,05</td><td rowspan="2">0,10</td><td>0,05</td><td>1110</td></tr>
<tr><td>Ч</td><td>0,05</td><td>0,05</td><td>1111</td></tr>
</table>

Кодове дерево має вигляд



Для того щоб перевірити оптимальність коду відносно довжини кодових комбінацій, визначаємо середню довжину кодової комбінації. У разі оптимальності ця довжина не повинна перевищувати довжину рівномірного коду, яким можна закодувати $k = 8$ повідомлень, тобто $q^n = 2^n = 8$ $(n = 3)$:

$$n_{\text{сер}} = 0{,}25 \times 2 + (0{,}15 + 0{,}15 + 0{,}15 + 0{,}10 + 0{,}10) \times 3 +$$
$$+(0{,}05 + 0{,}05) \times 4 = 2{,}85 < 3$$

Завдання 3.4.

1. Для ансамблю повідомлень побудувати нерівномірний префіксний код Хаффмена із використанням:
   a. кодової таблиці;
   b. кодового дерева.
2. Перевірити оптимальність коду відносно довжини кодових комбінацій.

Приклад виконання завдання 3.4.

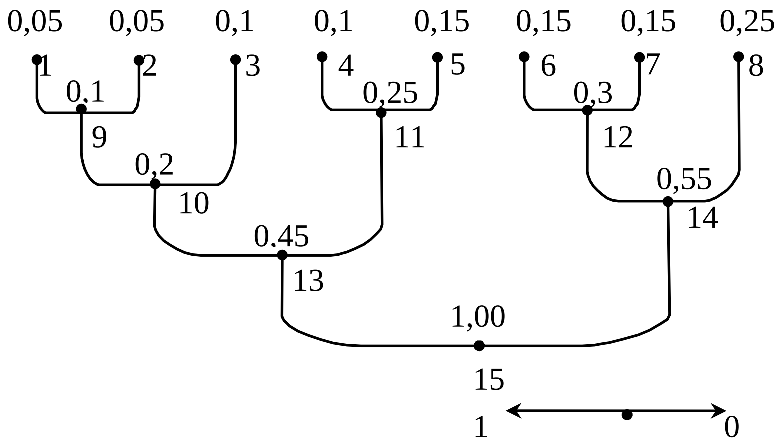
Кодова таблиця має вигляд

Літера	Ймовірності														
			Проміжні алфавіти												
	pi	Код	A(1)		A(2)		A(3)		A(4)		A(5)		A(6)		A(7)
В	0,25	**01**	0,25	01	0,25	01	0,25	01	**0,3**	00	**0,45**	1	**0,55**	0	**1**
І	0,15	**000**	0,15	000	**0,2**	11	**0,25**	10	0,25	01	0,3	00	0,45	1	
А	0,15	**001**	0,15	001	0,15	000	0,2	11	0,25	10	0,25	01			
Н	0,15	**100**	0,15	100	0,15	001	0,15	000	0,2	11					
О	0,1	**101**	0,1	101	0,15	100	0,15	001							
_	0,1	**110**	0,1	110	0,1	101									
И	0,05	**1110**	**0,1**	111											
Ч	0,05	**1111**													

Кодове дерево.

Процес побудови кодового дерева є таким. Кожному символу дерева поставимо у відповідність кінцевий вузол кодового дерева. Разом з позначенням символу напишемо біля вузла значення ймовірності його появи. Для зручності пояснення вузли дерева занумеровані. Кінцеві вузли мають номери з 1-го по 8-ий. Далі вибираємо два вузли, яким відповідають найменші значення ймовірностей (це вузли 1 та 2), об'єднуємо (склеюємо) їх, в результаті чого отримуємо новий вузол (номер 9), котрому приписуємо ймовірність, що дорівнює сумі ймовірностей об'єднаних вузлів. Знову вибираємо два вузли з найменшими ймовірностями, але тепер не враховуємо вузли, що були об'єднанні (тобто вузли 1 та 2), а беремо до уваги вузол, який з'явився (вузол 9). В даному випадку це вузли 3 та 9. Об'єднуємо їх у вузол 10, та приписуємо ймовірність 0,02. Повторюємо процедуру об'єднання вузлів з найменшими ймовірностями доки не утвориться кореневий вузол. Таким чином отримуємо кодове дерево. Гілки дерева можуть перехрещуватись.

И	**Ч**	**О**	**_**	**І**	**Н**	**А**	**В**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
0,05	0,05	0,10	0,10	0,15	0,15	0,15	0,25



И	**Ч**	**О**	**_**	**І**	**Н**	**А**	**В**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
0,05	0,05	0,10	0,10	0,15	0,15	0,15	0,25
1111	1110	110	101	100	011	010	00

Для перевірки оптимальності коду відносно довжини кодових комбінацій визначаємо середню довжину $n_{\text{сер}}$ кодової комбінації

$$n_{\text{сер}} = 0{,}25 \times 2 + (0{,}15 + 0{,}15 + 0{,}15 + 0{,}10 + 0{,}10) \times 3 +$$
$$+(0{,}05 + 0{,}05) \times 4 = 2{,}85 < 3$$

Висновки

Серед наведених кодів найменшу середню довжину кодової комбінації мають ____ і ____ коди, крім того, код ___ дає можливість ____, отже він і є найбільш оптимальним для заданого джерела.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити результати виконання задач, виставити відповідні оцінки. Зазначити перелік задач для їх розв'язання на самостійній роботі, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Лабораторна робота 4. Побудова двійкових кодів, що виявляють помилки

Навчальна мета заняття: навчитися будувати двійкові коди, що виявляють помилки

Час проведення: 4 год.

Навчальні питання

Вступ

1. Побудова двійкових кодів, що виявляють помилки

Висновки

Література: [1, л.5], [8, с. 121 – 126].

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Провести письмове опитування за контрольними питаннями лекції 5. Нагадати класифікацію кодів та основні їх характеристики, принципи побудови кодів:

- з перевіркою на парність;
- з перевіркою на непарність;
- з простим повторенням;
- Бауера;
- кореляційних;
- Бергера;
- з постійною вагою;
- з числом одиниць у комбінації, кратним трьом.

ІІ. Порядок проведення основної частини заняття.

Навести видані задачі. Дати час для самостійного розв'язання задач. Розібрати зразкове розв'язання задач.

1. Побудова двійкових кодів, що виявляють помилки

Закодувати комбінацію *A* двійкового простого коду двійковими кодами, що виявляють помилки, згідно варіанта, поданого в таблиці 1. Показати на прикладі виявлення помилок, кількість яких визначається заданим варіантом, та порівняти надмірності цих кодів.

Таблиця 1.

№ варі-анта	Первинна кодова комбінація *A* двійкового простого коду	Двійковий код, що виявляє помилки	Кількість помилок, яка виявляється першим / другим кодом
1	100101010100	ПРП, КБ	1/1
2	11101101101	ПРН, ПП	1/1
3	11011010	КК, КБ	1/1
4	0000011100	ПВ(4), ПП	1/1
5	0000011000	ПВ(3), ОК3	1/1
6	10111101011	ІК, КБ	3/1
7	11101010101	ІК, ПП	3/1
8	0011101100	ІК, КК	3/1
9	11000010100	ІК, ПВ(5)	3/1
10	00101010100	ПВ(6), ПРП	1/1
11	100101010100	ПВ(5), ПРН	1/1
12	101111010	КК, ПП	1/1
13	1110010111	КК, КБ	1/1
14	100101011110	ПРП, ПП	1/1
15	100101010100	ПРН, ОК3	1/1
16	110000101011	ІК, КБ	3/1
17	010101010101	ІК, ПП	3/1
18	1011101101	ІК, КБ	3/1
19	1100001011	ІК, ПВ(5)	3/1
20	1000000101	ПВ(4), ПРП	1/1
21	1001010101	ПВ(7), ПРН	1/1
22	10111	КК, ПП	1/1
23	11100101	КК, ОК3	1/1
24	100101011110	ПРП, ПП	1/1
25	100101010100	ПРН, ОК3	1/1

Умовні позначення двійкових кодів, що виявляють помилки: ПРП – з перевіркою на парність; ПРН – з перевіркою на непарність; ПП – з простим повторенням; ІК – інверсний; КК – кореляційний; КБ – Бергера; ОК3 – з числом одиниць, кратним трьом; ПВ(w) – з постійною вагою w.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити результати виконання задач, виставити відповідні оцінки. Зазначити перелік задач для їх розв’язання на самостійній роботі, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Лабораторна робота 5. Побудова двійкових кодів, що виправляють однократні помилки

Навчальна мета заняття: навчитися будувати двійкові коди, що виправляють однократні помилки

Час проведення: 4 год.

Навчальні питання

Вступ

1. Побудова двійкових кодів, що виправляють однократні помилки

Висновки

Література: [3, л.6], [8, с. 131 – 142].

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

I. Порядок проведення вступу до заняття.

Провести письмове опитування за контрольними питаннями лекції 6. Нагадати принципи побудови систематичних кодів, що виправляють однократні помилки:

- Хеммінга,
- ітеративний (Елайеса),
- з багатократним повторенням,
- інверсний,
- Бергера.

II. Порядок проведення основної частини заняття.

Навести виПланні дані задачі. Дати час для самостійного розв'язання задач. Розібрати зразкове розв'язання задач.

1. Побудова двійкових кодів, що виправляють однократні помилки

Завдання 5.1. Побудувати твірну матрицю двійкового систематичного (групового) коду, який має N_0 дозволених кодових комбінацій та здатен виправляти всі однократні помилки (згідно з варіантом таблиці 5.1). Навести приклад кодування за допомогою твірної матриці.

Таблиця 5.1

№ варіанту	**Кількість дозволених комбінацій N_0**
1	8
2	16
3	32
4	64
5	128

Завдання 5.2. Визначити, які з наведених комбінацій двійкового групового (7,4)-коду (згідно з варіантом таблиці 5.2), містять помилку, якщо відомо, що код побудований за твірною матрицею:

$$G_{7,4} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Таблиця 5.2

№ варіанту	Комбінації двійкового групового коду
1	1010110, 1110010, 0001111
2	0101010, 1111111, 0011011
3	0011101, 0010110, 1101110
4	1100000, 1100110, 1010101
5	0100010, 0100101, 1001011
6	1110000, 0000101, 0100000

Завдання 5.3. Визначити, які з комбінацій двійкового групового (7,4)-коду містять помилку (згідно з варіантом таблиці 5.3), якщо відомо, що перевірочна матриця коду має вигляд:

$$H_{7,3} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

Таблиця 5.3

№ варіанту	Комбінації двійкового групвого коду
1	0010110, 1110010, 1001111
2	0101110, 1111111, 1011001
3	1011111, 0010110, 1101110
4	0100011, 1100110, 0010101
5	0100011, 0100101, 1101011

Завдання 5.4. Побудувати перевірочну матрицю традиційного двійкового коду Хеммінга з заданими d_{min} та k (згідно з варіантом таблиці 5.4). За допомогою одержаної матриці закодувати кодом Хеммінга комбінації двійкового простого коду A_1 та A_2.

Показати на прикладі виправлення будь-якої однократної помилки (для коду з $d_{min} = 3$) або виявлення будь-якої трикратної помилки (для коду з $d_1(\min) = 4$) в отриманих кодових комбінаціях коду Хеммінга і визначити надмірність коду.

Таблиця 5.4

№ варіанту	$\boldsymbol{d_{min}}$	$\boldsymbol{k}$	$\boldsymbol{A_1}$	$\boldsymbol{A_2}$

№ варіанту	d_{min}	k	A_1	A_2
1	3	4	0011	1010
2	3	5	11001	00110
3	3	7	0101010	1110000
4	3	11	01110001010	00011100011
5	3	12	001100110010	111000111000
6	3	14	00010001000100	10010010010010
7	4	4	1110	0011
8	4	7	0100101	1110001
9	4	11	01110111000	11001100111
10	4	15	100011100101011	010100010100001

Завдання 5.5. Закодувати комбінації двійкового простого коду A_1 та A_2 довжиною k (згідно з варіантом таблиці 5.5) двійковим кодом з багатократним повторенням, здатним виправляти помилки кратності s. Показати процес виправлення помилок на прикладі і визначити надмірність коду.

Таблиця 5.5

№ варіанту	k	s	A_1	A_2
1	3	2	001	100
2	4	1	1100	0110
3	4	2	0011	0010
4	5	1	11100	00111
5	5	2	11001	00111
6	6	1	001000	110111
7	6	2	111011	010010
8	7	1	0100101	0110100
9	7	2	0111011	0010011
10	8	1	10001110	11100001

Завдання 5.6. Закодувати інформаційну послідовність двійкових елементів (згідно з варіантом таблиці 5.6) двійковим двомірним ітеративним кодом, здатним виправляти однократні помилки. Показати процес виправлення будь-якої однократної помилки і визначити надмірність коду.

Таблиця 5.6

№ варіанту	Послідовність двійкових елементів
1	0010110111001010
2	111111110110
3	1011111001011011
4	0100011110011000

5	0100011010010111
6	110111001010
7	000100110111
8	111110010110
9	1100101101011011
10	1100111010110110

III. Порядок проведення заключної частини заняття.

Перевірити результати виконання задач, виставити відповідні оцінки. Зазначити перелік задач для їх розв’язання на самостійній роботі, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Лабораторна робота 6. Коди, що виправляють помилки

Навчальна мета заняття: сформувати уміння формувати коди, що виправляють помилки, та порівнювати їх характеристики

Час проведення: 4 год.

Навчальні питання

Вступ

1. Побудова та оцінка кодів, що виправляють помилки

Висновки

Література: [3, л.7], [8, с. 153 - 165].

Матеріально-технічне забезпечення: комп’ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

I. Порядок проведення вступу до заняття.

Провести письмове опитування за контрольними питаннями:

1. Як утворюється код Хеммінга?
2. Як утворюються вкорочені систематичні (групові) коди?
3. Як утворюється розширений код Хеммінга?
4. Як утворюються циклічні коди з $d_{min} = 3$?
5. Як утворюються коди Боуза-Чоудхурі-Хоквінгема (БЧХ)?

II. Порядок проведення основної частини заняття.

Виконання завдань роботи здійснюється або вручну, або у будь-якому обчислювальному середовищі (MS Excel, MathCad, MatLab, і т.д.).

1. Побудова та оцінка кодів, що виправляють помилки

Завдання 6.1.

1. Задати дискретне джерело повідомлень без пам'яті, що вибирає повідомлення a_k (A та b_k (B де A,B – множини літер прізвища, імені, по-батькові українською мовою відповідно.

2. Розрахувати ансамбль джерела повідомлень, пов'язавши з кожним дискретним повідомленням a_i ймовірність p_i його вибору джерелом.
3. Розрахувати ентропію джерела.

Приклад виконання завдання 6.1.

ІВАНОВ_ІВАН_ІВАНОВИЧ   А = {І, В, А, Н, О, И, Ч, _}

літера	І	В	А	Н	О	И	Ч	_
p_i	0,15	0,25	0,15	0,15	0,10	0,05	0,05	0,10

$$H(A) = -\sum_{i=1}^{k} p_i \log_2 p_i, \qquad H(A) = 3{,}156 \text{ біт}$$

Завдання 6.2.

1. Для ансамблю повідомлень побудувати двійковий лінійний систематичний груповий (блоковий) код та код Хеммінга, здатний виправляти поодинокі помилки.
2. Продемонструвати виявлення та виправлення помилки при передачі повідомлення.

Приклад виконання завдання 6.2.

Побудова твірної матриці та визначення комбінацій лінійного систематичного двійкового групового коду, здатного виправляти поодинокі помилки ($s = 1$) .

Через те що $N = 2^k = 2^3 = 8$, маємо $k = 3$. Отже, кількість рядків твірної матриці $G_{n,k}$ дорівнює , а кількість її стовпців визначається довжиною коду $n = k + r$. Кількість перевірочних розрядів $r = 3$ (урахувавши, що $d_{\min} \geq 2s + 1 = 3$). Тоді кількість стовпців підматриці $C_{r,k}$ дорівнює , а твірної матриці $G_{n,k}$ - .

Згідно з правилом побудови підматриці $C_{r,k}$ кількість одиниць у кожному її рядку має бути не меншою ніж $d_{\min} - 1 = 3 - 1 = 2$, а кодова відстань між рядками — не меншою ніж $d_{\min} - 2 = 3 - 2 = 1$. Тому з триелементних комбінацій для підматриці $C_{r,k}$ вибираємо тільки ті, які задовольняють ці умови, тобто $101, 011, 110$.

Оскільки як інформаційна підматриця E_k твірної матриці $G_{n,k}$ вибирається одинична підматриця, дописавши до неї перевірну підматрицю, дістанемо твірну матрицю лінійного систематичного групового коду, здатного виправляти однократні помилки:

$$G_{(6,3)} = \begin{bmatrix} 1 & 0 & 0 & & 1 & 0 & 1 \\ 0 & 1 & 0 & & 0 & 1 & 1 \\ 0 & 0 & 1 & & 1 & 1 & 0 \end{bmatrix}$$

За допомогою цієї матриці визначаємо всі вісім комбінацій даного коду:

1. 000000
2. 100101
3. 010011
4. 001110
5. 110110(2 ⊕ 3);
6. 101011 (2 ⊕ 4);
7. 011101 (3 ⊕ 4);
8. 111000(2 ⊕ 3 ⊕ 4).

Для побудови перевірної матриці лінійного систематичного двійкового групового коду, здатного виправляти однократні помилки, скористаємось твірною матрицею.

Перевірна матриця H повинна мати r=3 рядки та n=6 стовпців. Вона складається з двох підматриць: $D_{(3,3)}$, що містить по три стовпці та рядки, кожний рядок якої відповідає стовпцю перевірної підматриці $C_{(3,3)}$ твірної матриці $G_{(6,3)}$; одиничної підматриці $E_{(3)}$. Отже,

$$H_{(6,3)} = \begin{bmatrix} 1 & 0 & 1 & & 1 & 0 & 0 \\ 0 & 1 & 1 & & 0 & 1 & 0 \\ 1 & 1 & 0 & & 0 & 0 & 1 \end{bmatrix}$$

Перевірні елементи коду згідно з цією матрицею визначаються як $b_1=a_1 \oplus a_3$; $b_2=a_2 \oplus a_3$; $b_3=a_1 \oplus a_2$.

Користуючись перевірною матрицею $H_{(6,3)}$, виконуємо кодування повідомлень.

Кодова таблиця має вигляд

літера	рівномірний двійковий код	перевірні розряди $b_1=a_1 \oplus a_3$ $b_2=a_2 \oplus a_3$ $b_3=a_1 \oplus a_2$	лінійний систематичний груповий код
І	000	000	000000
В	001	110	001110
А	010	011	010011
Н	011	101	011101
О	100	101	100101
И	101	011	101011
Ч	110	110	110110
_	111	000	111000

Надмірність коду

$R_{над}$=1-k/n $R_{над}$=1-3/6=0,5

Повідомлення для передачі перших трьох літер прізвища

C = 000000 001110 010011

Виявлення та виправлення помилки при передачі повідомлення.

Нехай в комбінації коду виникла однократна помилка, вектор якої E=000000 000000 001000. Тоді сума $C \oplus E$=000000 001110 011011.

На приймальному боці для виявлення та виправлення однократної помилки в прийнятій кодовій комбінації виконується перевірка — визначається синдром помилки. Для матриці $H_{(6,3)}$ маємо

$S_1=a_1\oplus a_3\oplus b_1$; $S_2=a_2\oplus a_3\oplus b_2$; $S_3=a_1\oplus a_2\oplus b_3$

000000 $S_1=0\oplus 0\oplus 0=0$; $S_2=0\oplus 0\oplus 0=0$; $S_3=0\oplus 0\oplus 0=0$ - без помилок;

001110 $S_1=0\oplus 1\oplus 1=0$; $S_2=0\oplus 1\oplus 1=0$; $S_3=0\oplus 0\oplus 0=0$ - без помилок;

011011 $S_1=0\oplus 1\oplus 0=1$; $S_2=1\oplus 1\oplus 1=1$; $S_3=0\oplus 1\oplus 1=0$ - помилка.

Синдром має вигляд 110, що відповідає третьому стовпцю перевірної матриці $H_{(6,3)}$, тобто помилка знаходиться в третьому розряді прийнятої кодової комбінації. Для її виправлення інвертуємо значення цього розряду. Виправлена комбінація матиме вигляд 010011.

Код Хеммінга

Для розрахунку основних параметрів коду Хеммінга використаємо співвідношення $2^n \ge (n+1)\cdot 2^k$, $n=k+r$. Звідки $k=3$, $n=6$, $r=3$

Характерна особливість перевірної матриці коду з $d_{\min}=3$ полягає у тому, що її стовпці є різними ненульовими комбінаціями завдовжки r.

$$H_{(6,3)} = \begin{array}{c} \left[\begin{array}{cccccc} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ b_1 & b_2 & a_1 & b_3 & a_2 & a_3 \end{array}\right] \begin{array}{c} S_1 \\ S_2 \\ S_3 \\ \end{array} \end{array}$$

Перевірні розряди розміщуються між інформаційними так, щоб номер i-го стовпця матриці H і номер розряду кодової комбінації відповідали двійковому поданню числа i. Тоді синдром, знайдений з перевірних рівнянь, буде двійковим поданням номера розряду кодової комбінації, в якій виникла помилка. Для цього перевірні розряди мають знаходитися не в кінці кодової комбінації, а на номерах позицій, які подаються степенем двійки (2^0, 2^1, 2^2, 2^3,..., 2^{r-1}).

Згідно з матрицею формуємо систему перевірних рівнянь, за допомогою яких знаходимо перевірні розряди:

$b_1=a_1\oplus a_2$, $b_2=a_1\oplus a_3$, $b_3=a_2\oplus a_3$.

Кодова таблиця має вигляд

літера	рівномірний двійковий код u_3, u_5, u_6	перевірні розряди $b_1=a_1\oplus a_2$ $b_2=a_1\oplus a_3$ $b_3=a_2\oplus a_3$	код Хеммінга
І	000	000	000000
В	001	011	010101
А	010	101	100110
Н	011	110	110011
О	100	110	111000
И	101	101	101101
Ч	110	011	011110
_	111	000	001011

Надмірність коду

$R_{\text{над}}$=1-k/n $R_{\text{над}}$=1-3/6=0,5

Повідомлення для передачі перших трьох літер прізвища

C=000000 010101 100110

Виявлення та виправлення помилки при передачі повідомлення.

Нехай в комбінації коду виникла однократна помилка, вектор якої E=000000 000000 001000. Тоді сума $C \oplus E$=000000 010101 101110.

На приймальному боці для виявлення та виправлення однократної помилки в прийнятій кодовій комбінації виконується перевірка — визначається синдром помилки.

$$S_1=b_3 \oplus a_2 \oplus a_3;\ S_2=b_2 \oplus a_1 \oplus a_3;\ S_3=b_1 \oplus a_1 \oplus a_2$$

000000S_1=0⊕0⊕0=0; S_2=0⊕0⊕0=0; S_3=0⊕0⊕0=0 - без помилок;

010101S_1=1⊕0⊕1=0; S_2=1⊕0⊕1=0; S_3=0⊕0⊕0=0 - без помилок;

101110S_1=1⊕1⊕0=0; S_2=0⊕1⊕0=1; S_3=1⊕1⊕1=1 - помилка.

Синдром має вигляд 011, тобто помилка знаходиться в третьому розряді прийнятої кодової комбінації. Для її виправлення інвертуємо значення цього розряду. Виправлена комбінація матиме вигляд 100110.

Завдання 6.3.

1. Для ансамблю повідомлень побудувати двійковий циклічний код.
2. Продемонструвати виявлення та виправлення помилки при передачі повідомлення.

Приклад виконання завдання 6.3.

Щоб побудувати циклічний код, необхідно вибрати твірний поліном $P(x)$. Його степінь визначається кількістю r перевірних елементів у комбінації циклічного коду, причому значення r при $d_{\min}$=3 можна знайти з виразу $2^r-1 \geq n$ або $2^r \geq k+r+1$. Отже, при k=3 маємо r=3, твірний поліном: $P(x)=x^3+x+1$.

Для побудови твірної матриці (формування її рядків) беремо комбінації $Q(x)$ двійкового простого коду, які містять одиницю в одному розряді $Q_i(x)$, де $i=1,2,\ldots,k$. Ці комбінації множимо на x^r і знаходимо остачу від ділення $x^r Q_i(x)/P(x)$, що дорівнює $R_i(x)$.

Отже, для циклічного (6,3)-коду з n=6, k=3 і твірним поліномом $P(x)=x^3+x+1$, беремо триелементні одиничні комбінації Q_i двійкового простого коду: $Q_1(x)=1$ (001); $Q_2(x)=x$ (010); $Q_3(x)=x^2$ (100). Вибрані комбінації $Q_i(x)$ множимо на x^3 ($r=n-k$=6-3=3), ділимо на $P(x)=x^3+x+1$ і знаходимо остачі:

$$\begin{array}{l|l} x^3 & x^3+x+1 \\ \hline \oplus\ x^3+x+1 & 1 \\ \hline x+1 & \end{array}$$

$$\frac{1x^3}{x^3+x+1} \to R_1(x)=x+1 \to 011$$

$$\begin{array}{l|l} x^4 & x^3+x+1 \\ \hline \oplus\ x^4+x^2+x & x \\ \hline x^2+x & \end{array}$$

$$\frac{xx^3}{x^3+x+1} \to R_2(x)=x^2+x \to 110$$

$$
\begin{array}{l|l}
x^5 & x^3+x+1 \\
\oplus\, \underline{x^5+x^3+x^2} & x^2+1 \\
\quad x^3+x^2 & \\
\oplus\, \underline{x^3+x+1} & \\
\quad x^2+x+1 &
\end{array}
$$

$$\frac{x^2x^3}{x^3+x+1} \to R_3(x)=x^2+x+1 \to 111$$

Твірна матриця матиме вигляд

$$G_{(6,3)}=\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

Перевірна матриця H повинна мати r=3 рядки та n=6 стовпців. Вона складається з двох підматриць: $D_{(3,3)}$, що містить по три стовпці та рядки, кожний рядок якої відповідає стовпцю перевірної підматриці $C_{(3,3)}$ твірної матриці $G_{(6,3)}$; одиничної підматриці $E_{(3)}$. Отже,

$$H_{(6,3)}=\begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Перевірні елементи коду згідно з цією матрицею визначаються як $b_1=a_1\oplus a_2$; $b_2=a_1\oplus a_2\oplus a_3$; $b_3=a_1\oplus a_3$.

Користуючись перевірною матрицею $H_{(6,3)}$, виконуємо кодування повідомлень.

Кодова таблиця має вигляд

літера	рівномірний двійковий код	перевірні розряди $b_1=a_1\oplus a_2$ $b_2=a_1\oplus a_2\oplus a_3$ $b_3=a_1\oplus a_3$	циклічний код
І	000	000	000000
В	001	011	001011
А	010	110	010110
Н	011	101	011101
О	100	111	100111
И	101	100	101100
Ч	110	001	110001
_	111	010	111010

Надмірність коду

$R_{над}=1-k/n$ $\qquad\qquad$ $R_{над}$=1-3/6=0,5

Повідомлення для передачі перших трьох літер прізвища

C=000000 001011 010110

<u>Виявлення та виправлення помилки при передачі повідомлення.</u>

Нехай в комбінації коду виникла однократна помилка, вектор якої E=000000 000000 001000. Тоді сума $C\oplus E$=000000 001011 011110.

На приймальному боці для виявлення та виправлення однократної помилки в прийнятій кодовій комбінації виконується перевірка — визначається синдром помилки.

$S_1=a_1\oplus a_2\oplus b_1$; $S_2=a_1\oplus a_2\oplus a_3\oplus b_2$; $S_3=a_1\oplus a_3\oplus b_3$

000000 $S_1=0\oplus 0\oplus 0=0$; $S_2=0\oplus 0\oplus 0\oplus 0=0$; $S_3=0\oplus 0\oplus 0=0$ - без помилок;

001011 $S_1=0\oplus 0\oplus 0=0$; $S_2=0\oplus 0\oplus 1\oplus 1=0$; $S_3=0\oplus 1\oplus 1=0$ - без помилок;

011110 $S_1=0\oplus 1\oplus 1=0$; $S_2=0\oplus 1\oplus 1\oplus 1=1$; $S_3=0\oplus 1\oplus 0=1$ - помилка.

Синдром має вигляд 011, що відповідає третьому стовпцю перевірної матриці $H_{(6,3)}$, тобто помилка знаходиться в третьому розряді прийнятої кодової комбінації. Для її виправлення інвертуємо значення цього розряду. Виправлена комбінація матиме вигляд 010011.

Виявлення та виправлення помилки при передачі повідомлення, що ґрунтується на застосуванні твірного полінома $P(x)$.

Поліном прийнятої комбінації циклічного коду $F'(x)=F(x)+E(x)$.

На приймальному боці декодер виконує перевірне ділення комбінації $F'(x)$ на поліном $P(x)$, використаний при кодуванні інформації:

$$\begin{array}{l|l} 000000 & \underline{1011} \\ \underline{\oplus\ 0000} & 0 \\ \quad 0 \rightarrow 0 & \end{array} \qquad \begin{array}{l|l} 001011 & \underline{1011} \\ \underline{\oplus\ 1011} & 001 \\ \quad 0 \rightarrow 0 & \end{array} \qquad \begin{array}{l|l} 011110 & \underline{1011} \\ \underline{\oplus\ 1011} & 010 \\ \quad 1000 \rightarrow x^3 & \end{array}$$

Оскільки остача від ділення в третій кодовій комбінації не дорівнює нулю, робимо висновок про наявність помилки в прийнятій кодовій комбінації.

Для визначення місця помилки користуємося методом гіпотез:

• будуємо гіпотезу про помилку в молодшому розряді комбінації $F'(x)$, тобто вважаємо, що вектор помилки $E_1(x)=1\rightarrow E_1=000001$. Виконавши додавання $F'\oplus E_1$ поділивши результат на поліном $P(x)$ з метою підтвердження (в разі нульової остачі) або спростування (в разі ненульової остачі) гіпотези, дістанемо

$$\begin{array}{l} 011110 \\ \underline{\oplus\ 000001} \\ \ 011111 \end{array} \qquad \begin{array}{l|l} 011111 & \underline{1011} \\ \underline{\oplus\ 1011} & 010 \\ \quad 1001 \rightarrow R(x)=x^3+1 & \end{array}$$

тобто остача ненульова й гіпотеза відкидається;

• будуємо гіпотезу про помилку в п'ятому розряді комбінації $F'(x)$, тобто вважаємо, що вектор помилки $E_2(x)=2\rightarrow E_2=000010$. Виконавши додавання $F'\oplus E_2$ та поділивши результат на поліном $P(x)$ з метою підтвердження або спростування гіпотези, матимемо

$$\begin{array}{l} 011110 \\ \underline{\oplus\ 000010} \\ \ 011100 \end{array} \qquad \begin{array}{l|l} 011100 & \underline{1011} \\ \underline{\oplus\ 1011} & 010 \\ \quad 1010 \rightarrow R(x)=x^3+x & \end{array}$$

тобто остача ненульова й гіпотеза відкидається;

• будуємо гіпотезу про помилку в четвертому розряді комбінації $F'(x)$, тобто вважаємо, що вектор помилки $E_3(x)=3\rightarrow E_3=000100$. Виконавши додавання $F'\oplus E_3$ та поділивши результат на поліном $P(x)$ з метою підтвердження або спростування гіпотези, знайдемо

$$
\begin{array}{r}
011110 \\
\oplus\ \underline{000100} \\
011010
\end{array}
\qquad
\begin{array}{rl}
011010 & |\ \underline{1011} \\
\oplus\ \underline{1011\ \ } & |\ 011 \\
1100 & \\
\oplus\ \underline{1011\ \ } & \\
0111 \rightarrow R(x)=x^2+x+1 &
\end{array}
$$

тобто остача ненульова й гіпотеза відкидається;

• будуємо гіпотезу про помилку в третьому розряді комбінації $F'(x)$, тобто вважаємо, що вектор помилки $E_4(x)=4 \rightarrow E_4=001000$. Виконавши додавання $F' \oplus E_4$ та поділивши результат на поліном $P(x)$ з метою підтвердження або спростування гіпотези, дістанемо

$$
\begin{array}{r}
011110 \\
\oplus\ \underline{001000} \\
010110
\end{array}
\qquad
\begin{array}{rl}
010110 & |\ \underline{1011} \\
\oplus\ \underline{1011\ \ } & |\ 010 \\
0 \rightarrow R(x)=0 &
\end{array}
$$

тобто помилка дійсно є в третьому розряді, а початкова комбінація циклічного коду має вигляд $F=010110 \rightarrow F(x)=x^4+x^2+x$.

Завдання 6.4.

1. Для ансамблю повідомлень побудувати двійковий код БЧХ, здатний виправляти поодинокі помилки.
2. Продемонструвати виявлення та виправлення помилки при передачі повідомлення.

Приклад виконання завдання 6.4.

Довжину n комбінації кодів БЧХ можна визначити так: $n = 2^h - 1$ або $n = (2^h - 1)/g$, де $h>0$ — ціле число; g — непарне додатне число, при діленні на яке n стає цілим непарним числом. Таким чином, довжина n може дорівнювати 3, 7, 15, 31 розрядам і т.д. Кількість перевірних елементів коду визначається виразом

$$r \le \frac{h(d-1)}{2} = \left[\log_2(n+1)\right]\frac{d-1}{2},$$

а кількість інформаційних елементів — виразом

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

Отже, при n=7 маємо r=3, k=4, твірний поліном: $P(x)=x^3+x+1$.

Для побудови твірної матриці (формування її рядків) беремо комбінації $Q(x)$ двійкового простого коду, які містять одиницю в одному розряді $Q_i(x)$, де $i=1,2,\ldots,k$. Ці комбінації множимо на x^r і знаходимо остачу від ділення $x^r Q_i(x)/P(x)$, що дорівнює $R_i(x)$.

Отже, беремо чотириелементні одиничні комбінації Q_i двійкового простого коду: $Q_1(x)=1$ (0001); $Q_2(x)=x$ (0010); $Q_3(x)=x^2$ (0100); $Q_4(x)=x^3$ (1000). Вибрані комбінації $Q_i(x)$ множимо на x^3 ($r=n-k=7-4=3$), ділимо на $P(x)=x^3+x+1$ і знаходимо остачі:

$$
\begin{array}{rl}
x^3 & |\ \underline{x^3+x+1} \\
\oplus\ \underline{x^3+x+1} & |\ 1 \\
x+1 &
\end{array}
\qquad
\frac{1x^3}{x^3+x+1} \rightarrow R_1(x) = x+1 \rightarrow 011
$$

$$
\begin{array}{l|l}
x^4 & \underline{x^3+x+1} \\
\underline{\oplus\, x^4+x^2+x} & x \\
\quad x^2+x &
\end{array}
\qquad
\frac{xx^3}{x^3+x+1} \to R_2(x) = x^2 + x \to 110
$$

$$
\begin{array}{l|l}
x^5 & \underline{x^3+x+1} \\
\underline{\oplus\, x^5+x^3+x^2} & x^2+1 \\
\quad x^3+x^2 & \\
\quad \underline{\oplus x^3+x+1} & \\
\qquad x^2+x+1 &
\end{array}
\qquad
\frac{x^2x^3}{x^3+x+1} \to R_3(x) = x^2 + x + 1 \to 111
$$

$$
\begin{array}{l|l}
x^6 & \underline{x^3+x+1} \\
\underline{\oplus\, x^6+x^4+x^3} & x^3+x+1 \\
\quad x^4+x^3 & \\
\underline{\oplus\, x^4+x^2+x} & \\
\quad x^3+x^2+x & \\
\underline{\oplus\, x^3+x+1} & \\
\qquad x^2+x+1 &
\end{array}
\qquad
\frac{x^3x^3}{x^3+x+1} \to R_4(x) = x^2 + x + 1 \to 111
$$

Твірна матриця матиме вигляд

$$
G = \begin{bmatrix}
1 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 1
\end{bmatrix}
$$

Перевірна матриця H повинна мати r=3 рядки та n=7 стовпців.

$$
H = \begin{bmatrix}
1 & 1 & 1 & 0 & 1 & 0 & 0 \\
1 & 1 & 1 & 1 & 0 & 1 & 0 \\
1 & 1 & 0 & 1 & 0 & 0 & 1
\end{bmatrix}
$$

Перевірні елементи коду згідно з цією матрицею визначаються як $b_1=a_1\oplus a_2\oplus a_3$; $b_2=a_1\oplus a_2\oplus a_3\oplus a_4$; $b_3=a_1\oplus a_2\oplus a_4$.

Користуючись перевірною матрицею, виконуємо кодування повідомлень.

Кодова таблиця має вигляд

літера	рівномірний двійковий код	перевірні розряди $b_1=a_1\oplus a_2\oplus a_3$ $b_2=a_1\oplus a_2\oplus a_3\oplus a_4$ $b_3=a_1\oplus a_2\oplus a_4$	код БЧХ
І	0000	000	0000000
В	0001	011	0001011
А	0010	110	0010110
Н	0011	101	0011101
О	0100	111	0100111
И	0101	100	0101100
Ч	0110	001	0110001
_	0111	010	0111010

Надмірність коду $R_{над}$=1-3/7=0,65

(один інформаційний розряд не використовується)

Повідомлення для передачі перших трьох літер прізвища

C=0000000 0001011 0010110

Виявлення та виправлення помилки при передачі повідомлення виконується як для циклічних кодів.

Інший варіант n=7, r=3, k=4, s=1, твірний поліном: $P(x)=x^3+x^2+1$.

Для побудови твірної матриці (формування її рядків) беремо комбінації $Q(x)$ двійкового простого коду, які містять одиницю в одному розряді $Q_i(x)$, де i=1,2,…,k. Ці комбінації множимо на x^r і знаходимо остачу від ділення $x^rQ_i(x)/P(x)$, що дорівнює $R_i(x)$.

Отже, беремо чотириелементні одиничні комбінації Q_i двійкового простого коду: $Q_1(x)=1$ (0001); $Q_2(x)=x$ (0010); $Q_3(x)=x^2$ (0100); $Q_4(x)=x^3$ (1000). Вибрані комбінації $Q_i(x)$ множимо на x^3 ($r=n-k$=7-4=3), ділимо на $P(x)=x^3+x^2+1$ і знаходимо остачі:

$$\begin{array}{l|l} x^3 & \underline{x^3+x^2+1} \\ \underline{\oplus\, x^3+x^2+1} & 1 \\ x^2+1 & \end{array}$$

$$\frac{1x^3}{x^3+x^2+1} \to R_1(x)=x^2+1 \to 101$$

$$\begin{array}{l|l} x^4 & \underline{x^3+x^2+1} \\ \underline{\oplus\, x^4+x^3+x} & x+1 \\ x^3+x & \\ \underline{\oplus\, x^3+x^2+1} & \\ x^2+x+1 & \end{array}$$

$$\frac{xx^3}{x^3+x^2+1} \to R_2(x)=x^2+x+1 \to 111$$

$$\begin{array}{l|l} x^5 & \underline{x^3+x^2+1} \\ \underline{\oplus\, x^5+x^4+x^2} & x^2+x+1 \\ x^4+x^2 & \\ \underline{\oplus\, x^4+x^3+x} & \\ x^3+x^2+x & \\ \underline{\oplus\, x^3+x^2+1} & \\ x+1 & \end{array}$$

$$\frac{x^2x^3}{x^3+x^2+1} \to R_3(x)=x+1 \to 011$$

$$\begin{array}{l|l} x^6 & \underline{x^3+x^2+1} \\ \underline{\oplus\, x^6+x^5+x^3} & x^3+x^2+x+1 \\ x^5+x^3 & \\ \underline{\oplus\, x^5+x^4+x^2} & \\ x^4+x^3+x^2 & \\ \underline{\oplus\, x^4+x^3+x} & \\ x^2+x & \end{array}$$

$$\frac{x^3x^3}{x^3+x^2+1} \to R_4(x)=x^2+x \to 110$$

Твірна матриця матиме вигляд

$$G=\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

Перевірна матриця H повинна мати r=3 рядки та n=7 стовпців.

$$H=\begin{bmatrix}1&1&0&1&&1&0&0\\0&1&1&1&&0&1&0\\1&1&1&0&&0&0&1\end{bmatrix}$$

Перевірні елементи коду згідно з цією матрицею визначаються як $b_1=a_1\oplus a_2\oplus a_4$; $b_2=a_2\oplus a_3\oplus a_4$; $b_3=a_1\oplus a_2\oplus a_3$.

Користуючись перевірною матрицею, виконуємо кодування повідомлень.

Кодова таблиця має вигляд

літера	рівномірний двійковий код	перевірні розряди $b_1=a_1\oplus a_2\oplus a_4$ $b_2=a_2\oplus a_3\oplus a_4$ $b_3=a_1\oplus a_2\oplus a_3$	код БЧХ
І	0000	000	0000000
В	0001	110	0001110
А	0010	011	0010011
Н	0011	101	0011101
О	0100	111	0100111
И	0101	001	0101001
Ч	0110	100	0110100
_	0111	010	0111010

Надмірність коду $R_{над}$=1-3/7=0,65

(один інформаційний розряд не використовується)

Повідомлення для передачі перших трьох літер прізвища

C=0000000 0001110 0010011

Висновки

Серед наведених кодів найменшу надмірність мають ____ і ____ коди, крім того, код ___ дає можливість ____, отже він і є найбільш оптимальним для заданого джерела.

III. Порядок проведення заключної частини заняття.

Перевірити результати виконання задач, виставити відповідні оцінки. Зазначити перелік задач для їх розв’язання на самостійній роботі, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Лабораторна робота 7. Недвійкові коди

Навчальна мета заняття: навчитися будувати недвійкові коди.

Час проведення: 4 год.

Навчальні питання

Вступ

1. Недвійкові коди, що виявляють помилки
2. Узагальнений код Хеммінга

3. Код Ріда-Соломона

Висновки

Література: [3, л.8], [8, с. 178-190].

Матеріально-технічне забезпечення: комп’ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

I. Порядок проведення вступу до заняття.

Провести письмове опитування за контрольними питаннями лекції 8. Нагадати принципи побудови недвійкових кодів, що виявляють помилки:

- код з багатократним повторенням;
- код з простим повторенням та перевіркою за *mod q*;
- узагальнений код Хеммінга УКХ;
- код Ріда-Соломона (РС);

II. Порядок проведення основної частини заняття.

Навести виПланні дані задачі. Дати час для самостійного розв’язання задач. Розібрати зразкове розв’язання задач.

1. Недвійкові коди, що виявляють помилки

7.1. Згідно з варіантом, поданим в таблиці 7.1, закодувати комбінацію *A* недвійкового коду з алфавітом потужності *q* недвійковими кодами, що виявляють помилки: з перевіркою за *mod q* та з простим повторенням. Показати процес виявлення однократної помилки, визначити та порівняти надмірності цих кодів.

Таблиця 7.1

№ варіанту	Потужність алфавіту коду, *q*	Комбінація первинного коду, *A*
1	4	1032
2	5	4310
3	6	34512
4	7	21563
5	8	032745
6	9	674831
7	10	5479802
8	12	479*A*0*B*1
9	14	391*A*2*C*84
10	16	*D*17*A*2*EFB*

7.2. Згідно з варіантом поданим в таблиці 7.2, закодувати недвійковим кодом: з багатократним повторенням комбінацію *A* первинного змінно-якісного коду з алфавітом потужності *q*. Визначити надмірність одержаного коду та показати процес виправлення будь-якої помилки кратності *s*.

Таблиця 7.2

№ варіанту	Потужність алфавіту коду, *q*	Кратність помилки, *s*	Комбінація первинного коду, *A*
1	3	2	1012

2	4	2	0130
3	5	2	42301
4	7	1	20235436
5	8	1	32310167

7.3. Згідно з варіантом поданим в таблиці 7.3, закодувати недвійковим кодом з простим повторенням та перевіркою за *mod q* комбінацію *A* первинного змінно-якісного коду з алфавітом потужності *q*. Визначити надмірність одержаного коду та показати процес виправлення будь-якої однократної помилки.

Таблиця 7.3

№ варіанту	Потужність алфавіту коду, *q*	Комбінація первинного коду, *A*
1	3	2012
2	4	02131
3	6	14510215
4	7	012354362
5	8	202310176

2. Узагальнений код Хеммінга

7.4. Згідно з варіантом, поданим в таблиці 7.4, закодувати узагальненим кодом Хеммінга (УКХ) з алфавітом потужності *q* та ненульовою компонентою δ кодову комбінацію первинного коду *A*. Показати процес виправлення однократної помилки.

Таблиця 7.4

№ варіанту	Потужність алфавіту коду, *q*	Ненульова компонента, δ	Комбінація первинного коду, *A*
1	8	2	7501032
2	8	3	4741310
3	8	4	345021
4	8	5	21563
5	8	6	0327450145
6	8	7	5012674831
7	16	1	*A*0*B*5471
8	16	2	479*A*0*B*6
9	16	4	31*A*2*CE*
10	16	1	*D*13457*A*2*EFB*

3. Код Ріда-Соломона

7.5. Згідно з варіантом, поданим в таблиці 7.5, закодувати кодом Ріда-Соломона, що виправляє помилки кратності *s*, комбінацію шістнадцяткового первинного коду *Q*(0,*F*) з *k* інформаційними елементами.

Таблиця 7.5.

№ варіанту	Потужність алфавіту коду, q	Кратність помилки, s	Кількість інформаційних елементів, k	Комбінація первинного коду $Q(0,F)$
1	16	1	11	$D3AB1221384$
2	16	1	7	$F38D110$
3	16	1	8	$1100EFAA$
4	16	1	9	$CC5BAF301$
5	16	1	10	$BB335711A0$
6	16	2	11	$229ABB11244$
7	16	2	8	$100215AF$
8	16	2	9	$369AB0206$
9	16	2	10	$32745AC821$
10	16	3	11	$AA0CC142670$

III. Порядок проведення заключної частини заняття.

Перевірити результати виконання задач, виставити відповідні оцінки. Зазначити перелік задач для їх розв'язання на самостійній роботі, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Лабораторна робота 8. Інформаційні характеристики дискретного каналу зв'язку

Навчальна мета заняття: навчитися оцінювати інформаційні характеристики дискретного каналу зв'язку.

Час проведення: 8 год.

Навчальні питання

Вступ

1. Розрахунок і оцінка інформаційних характеристик дискретного каналу зв'язку

Висновки

Література: [3, л.9], [8, с. 65 - 77].

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

I. Порядок проведення вступу до заняття.

Провести письмове опитування за контрольними питаннями лекції 9. Нагадати визначення інформаційних характеристик дискретного каналу зв'язку.

II. Порядок проведення основної частини заняття.

Навести вихідні дані задачі. Дати час для самостійного розв'язання задач. Розібрати зразкове розв'язання задач.

1. Розрахунок і оцінка інформаційних характеристик дискретного каналу зв'язку

8.1. Знайти пропускну здатність трійкового стаціонарного каналу без пам'яті, який має таку матрицю перехідних ймовірностей

$$\begin{bmatrix} p(y_1/x_1) & p(y_2/x_1) & p(y_3/x_1) \\ p(y_1/x_2) & p(y_2/x_2) & p(y_3/x_2) \\ p(y_1/x_3) & p(y_2/x_3) & p(y_3/x_3) \end{bmatrix} = \begin{bmatrix} 0{,}9 & 0{,}07 & 0{,}03 \\ 0{,}03 & 0{,}9 & 0{,}07 \\ 0{,}07 & 0{,}03 & 0{,}9 \end{bmatrix}.$$

Швидкість передачі символів по каналу v_0=100 *Бод*.

Знайти середню кількість інформації, що переноситься одним символом, та швидкість передачі інформації по такому каналу від дискретного немарковського джерела інформації з алфавітом $X = \{x_1, x_2, x_3\}$, якщо ймовірності виникнення символів

$$p(x_1) = 0{,}6; p(x_2) = 0{,}3; p(x_3) = 0{,}1.$$

Часові характеристики джерела та каналу узгоджені, тобто тривалість кожного символу на виході джерела $\tau_i = T = 1/v_0 = 0{,}01$с.

8.2. Для каналу, який має матрицю переПланних ймовірностей

$$\begin{bmatrix} p(y_1/x_1) & p(y_2/x_1) & p(y_3/x_1) \\ p(y_1/x_2) & p(y_2/x_2) & p(y_3/x_2) \\ p(y_1/x_3) & p(y_2/x_3) & p(y_3/x_3) \end{bmatrix} = \begin{bmatrix} 0{,}9 & 0{,}07 & 0{,}03 \\ 0{,}03 & 0{,}9 & 0{,}07 \\ 0{,}07 & 0{,}03 & 0{,}9 \end{bmatrix}$$

знайти середню кількість інформації, що переноситься одним символом $I(Y, X)$, та швидкість передачі інформації по каналу $\bar{I}$, якщо до входу каналу підключене марковське стаціонарне дискретне джерело інформації з алфавітом $X = \{x_1, x_2, x_3\}$ та глибиною пам'яті $h = 1$ описується такою матрицею умовних ймовірностей $p(x_i / x_k)$ виникнення символу x_i при умові, що йому передував символ x_k:

$$\begin{bmatrix} p(x_1/x_1) & p(x_2/x_1) & p(x_3/x_1) \\ p(x_1/x_2) & p(x_2/x_2) & p(x_3/x_2) \\ p(x_1/x_3) & p(x_2/x_3) & p(x_3/x_3) \end{bmatrix} = \begin{bmatrix} 0{,}8 & 0{,}1 & 0{,}1 \\ 0{,}7 & 0{,}2 & 0{,}1 \\ 0{,}6 & 0{,}2 & 0{,}2 \end{bmatrix}.$$

8.3. Отримати вирази для пропускної здатності симетричного в посиленому значенні каналу без пам'яті для довільної потужності M алфавіту та для біноміального каналу. Проаналізувати залежність пропускної здатності біноміального каналу від ймовірності p помилки в каналі.

8.4. Маємо трійковий стаціонарний канал без пам'яті та без витирання. Ймовірності $p(x_i, y_k)$ сумісного виникнення символу x_i на вході каналу та символу y_k – на його виході для різних варіантів наведені у другому стовпці таблиці 5.1. Знайти середню кількість $I(Y, X)$ інформації, що переноситься одним символом, швидкість $\bar{I}$ передачі інформації по каналу та пропускну здатність C каналу. Чисельні значення швидкості v_0 передачі символів по каналу (в *Бодах*) наведені у третьому стовпці таблиці 8.1.

Таблиця 8.1

№ варіанту	$\begin{bmatrix} p(x_1,y_1) & p(x_2,y_1) & p(x_3,y_1) \\ p(x_1,y_2) & p(x_2,y_2) & p(x_3,y_2) \\ p(x_1,y_3) & p(x_2,y_3) & p(x_3,y_3) \end{bmatrix}$	v_0, *Бод*
1	$\begin{bmatrix} 0{,}170 & 0{,}015 & 0{,}050 \\ 0{,}020 & 0{,}255 & 0{,}025 \\ 0{,}010 & 0{,}030 & 0{,}425 \end{bmatrix}$	50
2	$\begin{bmatrix} 0{,}360 & 0{,}016 & 0{,}012 \\ 0{,}024 & 0{,}360 & 0{,}008 \\ 0{,}016 & 0{,}024 & 0{,}180 \end{bmatrix}$	75
3	$\begin{bmatrix} 0{,}075 & 0{,}020 & 0{,}100 \\ 0{,}020 & 0{,}300 & 0{,}025 \\ 0{,}005 & 0{,}080 & 0{,}375 \end{bmatrix}$	100
4	$\begin{bmatrix} 0{,}200 & 0{,}015 & 0{,}060 \\ 0{,}025 & 0{,}120 & 0{,}060 \\ 0{,}025 & 0{,}015 & 0{,}480 \end{bmatrix}$	120
5	$\begin{bmatrix} 0{,}255 & 0{,}007 & 0{,}048 \\ 0{,}024 & 0{,}085 & 0{,}042 \\ 0{,}021 & 0{,}008 & 0{,}51 \end{bmatrix}$	150
6	$\begin{bmatrix} 0{,}105 & 0{,}025 & 0{,}120 \\ 0{,}030 & 0{,}175 & 0{,}060 \\ 0{,}015 & 0{,}050 & 0{,}420 \end{bmatrix}$	200
7	$\begin{bmatrix} 0{,}276 & 0{,}010 & 0{,}015 \\ 0{,}009 & 0{,}184 & 0{,}025 \\ 0{,}015 & 0{,}006 & 0{,}460 \end{bmatrix}$	300
8	$\begin{bmatrix} 0{,}255 & 0{,}015 & 0{,}040 \\ 0{,}030 & 0{,}255 & 0{,}020 \\ 0{,}015 & 0{,}030 & 0{,}340 \end{bmatrix}$	600
9	$\begin{bmatrix} 0{,}045 & 0{,}018 & 0{,}030 \\ 0{,}003 & 0{,}405 & 0{,}020 \\ 0{,}002 & 0{,}027 & 0{,}450 \end{bmatrix}$	1200
10	$\begin{bmatrix} 0{,}450 & 0{,}015 & 0{,}020 \\ 0{,}120 & 0{,}225 & 0{,}005 \\ 0{,}030 & 0{,}060 & 0{,}075 \end{bmatrix}$	2400

№ варіанту	$\begin{bmatrix} p(x_1,y_1) & p(x_2,y_1) & p(x_3,y_1) \\ p(x_1,y_2) & p(x_2,y_2) & p(x_3,y_2) \\ p(x_1,y_3) & p(x_2,y_3) & p(x_3,y_3) \end{bmatrix}$	v_0, *Бод*
11	$\begin{bmatrix} 0{,}280 & 0{,}020 & 0{,}045 \\ 0{,}035 & 0{,}160 & 0{,}045 \\ 0{,}035 & 0{,}020 & 0{,}360 \end{bmatrix}$	50
12	$\begin{bmatrix} 0{,}425 & 0{,}021 & 0{,}016 \\ 0{,}040 & 0{,}255 & 0{,}014 \\ 0{,}035 & 0{,}024 & 0{,}170 \end{bmatrix}$	75
13	$\begin{bmatrix} 0{,}385 & 0{,}015 & 0{,}060 \\ 0{,}110 & 0{,}105 & 0{,}030 \\ 0{,}055 & 0{,}030 & 0{,}210 \end{bmatrix}$	100
14	$\begin{bmatrix} 0{,}552 & 0{,}015 & 0{,}003 \\ 0{,}018 & 0{,}276 & 0{,}005 \\ 0{,}030 & 0{,}009 & 0{,}092 \end{bmatrix}$	120
15	$\begin{bmatrix} 0{,}170 & 0{,}035 & 0{,}010 \\ 0{,}020 & 0{,}595 & 0{,}005 \\ 0{,}010 & 0{,}070 & 0{,}085 \end{bmatrix}$	150
16	$\begin{bmatrix} 0{,}405 & 0{,}006 & 0{,}024 \\ 0{,}027 & 0{,}135 & 0{,}016 \\ 0{,}018 & 0{,}009 & 0{,}360 \end{bmatrix}$	200
17	$\begin{bmatrix} 0{,}075 & 0{,}025 & 0{,}080 \\ 0{,}020 & 0{,}375 & 0{,}020 \\ 0{,}005 & 0{,}100 & 0{,}300 \end{bmatrix}$	300
18	$\begin{bmatrix} 0{,}280 & 0{,}015 & 0{,}050 \\ 0{,}035 & 0{,}120 & 0{,}050 \\ 0{,}035 & 0{,}015 & 0{,}400 \end{bmatrix}$	600
19	$\begin{bmatrix} 0{,}170 & 0{,}021 & 0{,}040 \\ 0{,}016 & 0{,}255 & 0{,}035 \\ 0{,}014 & 0{,}024 & 0{,}425 \end{bmatrix}$	1200
20	$\begin{bmatrix} 0{,}245 & 0{,}035 & 0{,}060 \\ 0{,}070 & 0{,}245 & 0{,}030 \\ 0{,}035 & 0{,}070 & 0{,}210 \end{bmatrix}$	2400

8.5. Розрахувати пропускну здатність C двійкового стаціонарного симетричного по входу каналу без пам'яті із витиранням. Вихідні дані, а саме, ймовірності

- правильного прийому двійкового символу q;
- помилки при його передачі по каналу $p_П$;
- витирання символу $p_В$,

а також швидкість v_0 передачі символів по каналу (в *Бодах*) для різних варіантів наведені у таблиці 8.2.

Таблиця 8.2

№ варіанту	q	$p_П$	$p_В$	v_0	№ варіанту	q	$p_П$	$p_В$	v_0
1	0,90	0,02	0,08	100	11	0,90	0,03	0,07	200
2	0,87	0,01	0,12	120	12	0,95	0,01	0,04	300
3	0,95	0,01	0,04	150	13	0,87	0,03	0,10	600
4	0,88	0,03	0,09	200	14	0,84	0,04	0,12	1200
5	0,83	0,03	0,14	300	15	0,94	0,01	0,05	2400
6	0,80	0,02	0,18	600	16	0,81	0,02	0,17	50
7	0,92	0,02	0,06	1200	17	0,88	0,02	0,10	75
8	0,80	0,05	0,15	2400	18	0,86	0,03	0,11	100
9	0,91	0,01	0,08	50	19	0,93	0,01	0,06	120
10	0,88	0,02	0,10	75	20	0,89	0,01	0,10	150

ІІІ. Порядок проведення заключної частини заняття.

Перевірити результати виконання задач, виставити відповідні оцінки. Зазначити перелік задач для їх розв'язання на самостійній роботі, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

3. Рекомендована література (основна, допоміжна), інформаційні ресурси в Інтернеті

Основна

1. Носов В.В. Електронний курс лекцій "Теорія інформації та кодування". Харків, ХНУВС, 2018 р.
2. Жураковський Ю. П., Гніліцький В. В. Теорія інформації та кодування в задачах: Навчальний посібник. – Житомир: ЖІТІ, 2002. – 255с.
3. Майданюк В. П. Кодування та захист інформації. Навчальний посібник. - Вінниця: ВНТУ, 2009. - 164 с.

Допоміжна

4. Подлевський Б.М., Рикалюк Р.Є. Теорія інформації в задачах: підручник. – Київ «Центр учбової літератури», 2017, - 271 с.
5. Тулякова Н. О. Теорія інформації : навч. посібник / Н. О. Тулякова. – Суми : Вид-во СумДУ, 2008. – 212 с.
6. Shannon C.E. A Mathematical Theory of Communication // Bell System Technical Journal. — 1948. — T. 27. — C. 379-423, 623–656.

7. Кожевников В.Л., Кожевников А.В. Теорія інформації та кодування : навч. посібник – Д.: Національний гірничий університет, 2011. – 108 с.
8. Решетник В.Я. Введення в теорію інформації: Навч. посібник. – Тернопіль.: ТДТУ., 2002. – 130 с.
9. Курко А.М., Решетник В.Я. Введення в теорія інформації : Навч. посібник.– Тернопіль : Тернопільський національний технічний університет імені Івана Пулюя, 2017. – 108 с.

Інформаційні ресурси

10. https://www.khanacademy.org/computing/computer-science/informationtheory
11. http://edyo.ru
12. http://www.intuit.ru/