Министерство образования Республики Беларусь

Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Факультет информационных технологий и управления

Кафедра систем управления

Н. И. Сорока, Г. А. Кривинченко

ТЕОРИЯ ПЕРЕДАЧИ ИНФОРМАЦИИ.
СБОРНИК ЗАДАЧ

Рекомендовано УМО по образованию в области информатики и радиоэлектроники в качестве пособия для специальности 1-53 01 07 «Информационные технологии и управление в технических системах»

Минск БГУИР 2015

УДК 621.391.3(076.1)
ББК 32.811я73
С65

Р е ц е н з е н т ы:
кафедра информационных технологий
Белорусского государственного университета
(протокол №8 от 20.05.2014);

доцент кафедры управления информационными ресурсами
Академии управления при Президенте Республики Беларусь,
кандидат технических наук, доцент Н. И. Белодед

Сорока, Н. И.

С65 Теория передачи информации. Сборник задач : пособие / Н. И. Сорока, Г. А. Кривинченко. – Минск : БГУИР, 2015. – 68 с.
ISBN 978-985-543-104-7.

Содержит задачи по расчёту информационных характеристик источников и каналов связи, кодированию информации в каналах связи с помехами и без помех, сжатию информации и криптографическому закрытию информации. В начале каждого раздела приводятся основные расчётные формулы и примеры решения задач. В приложениях приведены необходимые справочные данные. Материалы могут быть использованы в курсовом и дипломном проектировании.

УДК 621.391.3(076.1)
ББК 32.811я73

ISBN 978-985-543-104-7

СОДЕРЖАНИЕ

1. КОЛИЧЕСТВЕННАЯ ОЦЕНКА ИНФОРМАЦИИ

1.1. Основные формулы

Ёмкость устройства, состоящего из n ячеек, каждая из которых может находиться в одном из m равновероятных состояний:

$$C = I = \log N = n \log m. \tag{1.1}$$

Энтропия дискретного источника, имеющего m равновероятных состояний:

$$H = \log m. \tag{1.2}$$

Количество информации при неполной достоверности результатов опыта:

$$I = \log(\frac{P_2}{P_1}), \tag{1.3}$$

где P_2 и P_1 – апостериорная и априорная вероятности соответственно.

Энтропия ансамбля:

$$H = I_{\text{ср}} = -\sum_{i=1}^{m} P_i \log P_i, \tag{1.4}$$

где P_i – вероятность того, что источник находится в i-м состоянии.

Средняя неопределённость, приходящаяся на одно состояние ансамбля Y при известном состоянии ансамбля X (условная энтропия):

$$H(Y/X) = -\sum_{i=1}^{n} P(x_i) \sum_{j=1}^{m} P(y_j / x_i) \log P(y_j / x_i). \tag{1.5}$$

Энтропия объединения двух статистически связанных ансамблей X и Y:

$$H(X,Y) = H(X) + H(Y/X); \tag{1.6}$$

$$H(Y,X) = H(Y) + H(X/Y); \tag{1.7}$$

$$H(X,Y) = H(Y,X) = -\sum_{i=1}^{n} \sum_{j=1}^{m} P(x_i, y_j) \log P(x_i, y_j). \tag{1.8}$$

Энтропия статистически независимых ансамблей:

$$H(X,Y) = H(Y,X) = H(X) + H(Y). \tag{1.9}$$

Точные количества неопределённости в совместном событии x_i и y_j:

$$H(x_i, y_j) = -\log P(x_i, y_j).$$

Точные значения неопределённостей в наступления события y_j при известном исходе некоторого события x_i:

$$H(y_j / x_i) = -\log(y_j / x_i).$$

Основные соотношения между вероятностями:

$$P(x_i) = \sum_{j=1}^{m} P(x_i, y_j); \tag{1.10}$$

$$P(y_j) = \sum_{i=1}^{n} P(x_i, y_j); \tag{1.11}$$

$$P(x_i, y_j) = P(x_i)P(y_j / x_i) = P(y_j)P(x_i / y_j); \tag{1.12}$$

$$\sum_{i=1}^{n}\sum_{j=1}^{m} P(x_i, y_j) = 1; \tag{1.13}$$

$$\sum_{i=1}^{n} P(x_i) = 1; \quad \sum_{j=1}^{m} P(y_j) = 1. \tag{1.14}$$

Если неопределённость передачи некоторого сигнала X до опыта $H(X)$, а после опыта $H(X/Y)$, то количество информации, имеющееся в Y о X:

$$I = (Y, X) = H(X) - H(X / Y); \tag{1.15}$$

$$I(Y, X) = H(Y) - H(Y / X); \tag{1.16}$$

$$I(Y, X) = \sum_{i=1}^{m}\sum_{j=1}^{m} P(x_i, y_j)\log\frac{P(x_i, y_j)}{P(x_i)P(y_j)}. \tag{1.17}$$

Пример 1.1. Опыт X имеет два исхода x_1, x_2 с соответственными вероятностями $P(x_1)$ = 0,3, $P(x_2)$ = 0,7. Найти точные и среднее количества информации, несомые исходами x_1 и x_2. Вычислить дисперсию случайной величины $I = -\log P(x_i)$ и величину отклонения от своего среднего значения $\bar{I}(X)$.

Решение. Точные количества информации, несомые исходами x_1, x_2, равны:

$$I(x_1) = -\log P(x_1) = -\log 0{,}3 = 1{,}737 \text{ бит};$$

$$I(x_2) = -\log P(x_2) = -\log 0{,}7 = 0{,}515 \text{ бит}.$$

Так как числа $I(x_1) = 1{,}737$ и $I(x_2) = 0{,}515$ появляются с соответственными вероятностями 0,7 и 0,3, среднее количество информации по К. Шеннону будет иметь значение

$$\bar{I}(X) = H(X) = -\sum_{i=1}^{2} P(x_i) \cdot \log P(x_i) = 0{,}3 \cdot 1{,}737 + 0{,}7 \cdot 0{,}515 = 0{,}88 \text{ бит.}$$

Дисперсию случайной величины $I = -\log P(x_i)$ вычислим из выражения

$$D(I) = \sum_{i-1}^{2} (I(x_i) - \bar{I}(X))^2 \cdot P(x_i) = (1{,}737 - 0{,}88)^2 \cdot 0{,}3 + (0{,}515 - 0{,}88)^2 \cdot 0{,}7 = 0{,}86.$$

Таким образом, случайная величина $I(x_i)$ отклоняется от своего значения $\bar{I}(X)$ в среднеквадратичном на величину $\sigma_i = \sqrt{D(I)} = \sqrt{0{,}86} = 0{,}92$.

Пример 1.2. Вероятности совместного появления $P(x_i, y_j)$ объединения двух статистически зависимых ансамблей заданы в виде табл. 1.1.

Таблица 1.1

Вероятности совместного появления $P(x_i, y_j)$

y_j	x_i	
	x_1	x_2
y_1	0,20	0,35
y_2	0, 0	0,05

Определить точные и среднее количества неопределенности совместного наступления событий x_i и y_j, а также точные и средние количества неопределенности в y_j при известном исходе x_i.

Решение. Точные количества неопределенности в совместном наступлении событий x_i и y_j находим из формулы

$$H(x_i, y_j) = -\log P(x_i, y_j).$$

Подставляя в данное выражение $P(x_i, y_j)$ из табл. 1.1, получим точные количества $H(x_i, y_j)$, которые помещены в табл. 1.2.

Таблица 1.2

Точные количества $H(x_i, y_j)$

y_j	x_i	
	x_1	x_2
y_1	2,32	1,51
y_2	1,32	4,32

Среднее количество неопределенности в любом совместном наступлении событий x_i, y_j равно

$$H(X, Y) = -\sum_{i=1}^{2} \sum_{j=1}^{2} P(x_i, y_j) \cdot \log P(x_i, y_j) =$$

$$= \sum_{i=1}^{2} \sum_{j=1}^{2} H(x_i, y_j) \cdot P(x_i, y_j) =$$

$$= 2{,}32 \cdot 0{,}20 + 1{,}32 \cdot 0{,}40 + 1{,}51 \cdot 0{,}35 + 4{,}32 \cdot 0{,}05 =$$

$$= 0{,}46 + 0{,}53 + 0{,}53 + 0{,}22 = 1{,}74 \text{ бит.}$$

Найдём точные значения неопределенностей в наступлении события y_j при известном исходе некоторого события x_i. Для этого необходимо знать условные вероятности $P(y_j / x_i)$, а затем воспользоваться формулой

$$H(y_j / x_i) = -\log P(y_j / x_i).$$

Найдём сначала безусловные вероятности $P(x_i)$ и $P(y_j)$ по формулам полной вероятности:

$$P(x_i) = \sum_{j=1}^{2} P(x_i, y_j);\ P(y_j) = \sum_{i=1}^{2} P(x_i, y_j).$$

В результате вычислений получим:

$$P(x_1) = 0{,}6;\ P(x_2) = 0{,}4;$$

$$P(y_1) = 0{,}55;\ P(y_2) = 0{,}45.$$

Наконец, по формуле умножения вероятностей вычислим

$$P(y_j / x_i) = \frac{P(x_i, y_j)}{P(x_i)}.$$

Результаты вычислений представлены в табл. 1.3.

Таблица 1.3

Условные вероятности $P(y_j / x_i)$

y_j	x_i	
	x_1	x_2
y_1	0,33	0,87
y_2	0,67	0,13

Результаты расчета $H(y_j / x_i)$ представлены в табл. 1.4.

Таблица 1.4

Точные условные энтропии $H(y_j / x_i)$

y_j	x_i	
	x_1	x_2
y_1	1,6	0,20
y_2	0,58	2,94

Найдём частные условные энтропии путём усреднения точных условных энтропий:

$$H(Y / x_i) = \sum_{j=1}^{2} P(y_j / x_i) \cdot H(y_j / x_i).$$

Результаты расчёта следующие:

$$H(Y / x_1) = 1,6 \cdot 0,33 + 0,58 \cdot 0,67 = 0,53 + 0,39 = 0,92;$$

$$H(Y / x_2) = 0,20 \cdot 0,87 + 2,94 \cdot 0,13 = 0,17 + 0,38 = 0,55.$$

Эти результаты образуют случайную величину, значения которой наступают с вероятностью $P(x_i)$. Поэтому только среднее $H(Y / x_i)$, усреднённое с весом $P(x_i)$, не случайно, а именно:

$$H(Y / X) = \sum_{i=1}^{2} H(Y / x_i) \cdot P(x_i) = -\sum_{i=1}^{2}\sum_{j=1}^{2} P(x_i, y_j) \cdot \log P(y_j / x_i) =$$
$$= 0,92 \cdot 0,6 + 0,55 \cdot 0,4 = 0,55 + 0,22 = 0,77\ \frac{\text{бит}}{\text{сообщ.}}.$$

Если испытания будут независимы, то энтропия объединения будет

$$H^*(X,Y) = H(X) + H(Y) = -\sum_{i=1}^{2} P(x_i) \cdot \log P(x_i) - \sum_{j=1}^{2} P(y_j) \cdot \log P(y_j) =$$
$$= -(0,6 \cdot \log 0,6 + 0,4 \cdot \log 0,4) - (0,55 \cdot \log 0,55 + 0,45 \cdot \log 0,45) =$$
$$= 0,44 + 0,53 + 0,47 + 0,52 = 1,96\ \text{бит}.$$

Таким образом,

$$H(X,Y) = 1,74\ \text{бит} < H^*(X,Y) = H(X) + H(Y) = 1,96\ \text{бит}.$$

1.2. Задачи и упражнения

1.2.1. В некотором городе 25 % населения составляют студенты. Среди студентов 50 % юношей. Всего юношей в городе 35 %. Сколько дополнительной информации содержится в сообщении, что встреченный юноша – студент.

Ответ: I = 1,486 бит.

1.2.2. Определить минимальное число взвешиваний, которое необходимо произвести на равноплечных весах, чтобы среди 27 внешне неотличимых монет найти одну фальшивую, более лёгкую. Указать алгоритм определения фальшивой монеты.

Ответ: 3.

1.2.3. Опыт X имеет три исхода x_1, x_2, x_3 с соответственными вероятностями $P(x_1) = 0,2$; $P(x_2) = 0,5$; $P(x_3) = 0,3$. Найти точные и средние количества информации, несомые исходами x_1, x_2, x_3.

Ответ: 1,49 бит.

1.2.4. По условию предыдущей задачи вычислить дисперсию $D(I)$ случайной величины $I = -\log P(x_i)$ и величину отклонения δ_i.

Ответ: $D(I) = 0,277$; $\delta_i = \sqrt{D(I)} = 0,525.$

1.2.5. Вероятности совместного появления $P(x_i,\ y_j)$ объединения двух статистически зависимых ансамблей заданы в табл. 1.5. Определить точные и средние количества неопределённости в совместном наступлении событий x_i и y_j, а также точные и средние количества неопределённости в y_j при известном исходе x_i.

Таблица 1.5

Вероятности совместного появления, $P(x_i,\ y_j)$

y_j	x_i		
	x_1	x_2	x_3
y_1	0,1	0,15	0,05
y_2	0,05	0,03	0,02
y_3	0,3	0,2	0,1

Ответ: точные количества $H(x_1,y_1) = 3{,}32$; $H(x_2,y_1) = 2{,}74$; $H(x_3,y_1) = 4{,}32$; $H(x_1,y_2) = 4{,}32$; $H(x_2,y_2) = 5{,}06$; $H(x_3,y_2) = 5{,}64$; $H(x_1,y_3) = 1{,}74$; $H(x_2,y_3) = 2{,}32$; $H(x_3,y_3) = 3{,}32$; среднее количество $H(X,Y) = 2{,}76\ \dfrac{\text{бит}}{\text{сообщ.}}$; точные количества условных энтропий $H(y_1/x_1) = 2{,}171$; $H(y_1/x_2) = 1{,}361$; $H(y_1/x_3) = 1{,}766$; $H(y_2/x_1) = 3{,}171$; $H(y_2/x_2) = 3{,}662$; $H(y_2/x_3) = 3{,}074$; $H(y_3/x_1) = 0{,}584$; $H(y_3/x_2) = 0{,}908$; $H(y_3/x_3) = 0{,}766$; среднее количество $H(Y\,/\,X) = 1{,}274\ \dfrac{\text{бит}}{\text{сообщ.}}$.

1.2.6. По условию задачи 1.2.5 определить энтропию объединения, когда источники независимы.

Ответ: $H(X,Y) = 2{,}78\ \dfrac{\text{бит}}{\text{сообщ.}}$.

1.2.7. Известно, что телеизмеряемая величина должна быть в пределах от 21 до 40 В. Измерение произвели прибором, который показал 30 В, но он имеет погрешность ± 2 В. Определить количество информации, полученной в результате опыта.

Ответ: $I = 2$ бита.

1.2.8. Студент может сдать зачёт по теории передачи информации с вероятностью α, не проработав весь материал, и с вероятностью β, проработав весь материал курса; или не сдать зачёт с вероятностью γ, не проработав весь материал, и с вероятностью δ, проработав весь материал курса $(\alpha + \beta + \gamma + \delta) = 1$. Определить среднее количество информации, которое может получить преподаватель, о подготовленности студента по результатам сдачи зачёта.

Ответ:

$$I(X,Y) = \beta \log \frac{\beta}{(\alpha+\beta)(\beta+\delta)} + \alpha \log \frac{\alpha}{(\alpha+\beta)(\alpha+\gamma)} + \delta \log \frac{\delta}{(\delta+\gamma)(\beta+\delta)} + \gamma \log \frac{\gamma}{(\delta+\gamma)(\alpha+\gamma)}.$$

1.2.9. По линии связи с помехами передаётся одно из двух сообщений x_1 или x_2 с вероятностями соответственно p и g, причём $p + g = 1$. На приёмном конце канала сигналу x_1 соответствует y_1, а сигналу x_2 соответствует y_2. Заданы условные вероятности правильного приёма $P(y_1/x_1) = \Delta$ и $P(y_2/x_2) = \delta$. Определить количество информации $I(Y, X)$, содержащееся в Y о X.

Ответ:

$$I(Y,X) = p\Delta \log \frac{\Delta}{p\Delta + g(1-\delta)} + p(1-\Delta)\frac{1-\Delta}{g\delta + p(1-\Delta)} + g(1-\delta)\log\frac{1-\delta}{p\Delta + g(1-\delta)} + g\delta\log\frac{\delta}{g\delta + p(1-\Delta)}.$$

1.2.10. По каналу связи передаётся один из двух сигналов x_1 или x_2 с одинаковыми вероятностями. На выходе канала сигналы x_1 и x_2 преобразуются в сигналы y_1 и y_2, причём из-за помех, которым одинаково подвержены сигналы x_1 и x_2, в передачу вносится ошибка, так что в среднем один сигнал из ста принимается неверно. Определить среднее количество информации на один символ. Сравнить её с количеством информации при отсутствии помех.

Ответ: при отсутствии помех $I(X,Y) = 1$ бит; при наличии помех $I(Y,X) = 0{,}919$ бит.

1.2.11. Из выражения для количества информации

$$I(Y,X) = \sum_{i=1}^{n}\sum_{j=1}^{m} P(x_i, y_j)\log\frac{P(x_i, y_j)}{P(x_i), P(y_j)}$$

получить выражение для точного количества информации, содержащегося в сообщении y_j, о сообщении x_i.

Ответ: $I(y_j, x_i) = \log\dfrac{P(x_i/y_j)}{P(x_i)}$.

1.2.12. По цели может быть произведено n независимых выстрелов, вероятность поражения цели при каждом выстреле равна P. После k-го выстрела $(1 \le k \le n)$ производится разведка, сообщающая, поражена или не поражена цель. Если поражена, стрельба прекращается. Определить k из условия, что количество информации, доставляемое разведкой, было максимальным.

Ответ: $k = -\dfrac{1}{\log(1-p)}$.

1.2.13. На вход линии связи, в которой действует помеха, поступает сообщение X в двоичном коде 11111000. На выходе линии связи зафиксирована последовательность 11100001. Определить точное и среднее количество информации, содержащееся в Y о X.

Указание. Для удобства расчётов обозначить $X = AAAAABBB$ и $Y = CCCDDDDC$.

Ответ: точные количества информации $I(A, C) = I(C, A) = 0{,}263$ бит, $I(A, D) = I(D, A) = –0{,}322$ бит, $I(B, D) = I(D, B) = 0{,}415$ бит, $I(B, C) = I(C, B) =$ $= –0{,}585$ бит, среднее количество информации $I(Y, X) = 0{,}049$ бит.

1.2.14. Сигнал состоит из семи двоичных элементов. Определить количество информации в сигнале, когда элементы равновероятны, т. е. $P_1 = P_2 = 1/2$, и когда $P_1 = 3/4$, а $P_2 = 1/4$.

Ответ: $I_{РВ} = 7$ бит; $I_{НРВ} = 5,67$ бит.

1.2.15. Определить энтропии *H(X), H(Y), H(X/Y), H(X,Y),* если задана матрица вероятностей состояний системы, объединяющей источники *X* и *Y*:

$$P(x_i, y_j) = \begin{vmatrix} 0,4 & 0,1 & 0 \\ 0 & 0,2 & 0,1 \\ 0 & 0 & 0,2 \end{vmatrix}.$$

Ответ: $H(X)$ = 1,485 дв.ед.; $H(Y)$ = 1,57 дв.ед.; $H(X/Y)$ = 0,55 дв.ед.; $H(X,Y)$ = 2,12 дв.ед.

1.2.16. Известны энтропии двух зависимых источников $H(X)$ = 5 дв.ед., $H(Y)$ = 10 дв.ед. Определить, в каких пределах будет изменяться условная энтропия $H(Y/X)$ при изменении $H(X/Y)$ в максимально возможных пределах.

Указание. Использовать графическое отображение связи между энтропиями.

Ответ: $H(Y/X)$ будет уменьшаться до значения $H(Y) – H(X)$ = 5 дв.ед.

1.2.17. Ансамбли событий *X* и *Y* объединены. Вероятности совместных событий (*x*, *y*) описываются матрицей, представленной ниже.

	x_1	x_2	x_3
y_1	0,1	0,2	0,3
y_2	0,25	0	0,15

Определить:
1) энтропию ансамблей *X* и *Y*;
2) энтропию объединённого ансамбля (*X,Y*);
3) условные энтропии ансамблей;
4) количество информации, содержащейся в событиях *y* относительно *x*.

Ответ: $H(X) = 1,512\ \frac{\text{дв.ед.}}{\text{сообщ.}}$; $H(Y) = 0,971\ \frac{\text{дв.ед.}}{\text{сообщ.}}$; $H(X,Y) = 2,228\ \frac{\text{дв.ед.}}{\text{сообщ.}}$; $H(X/Y) = 1,257\ \frac{\text{дв.ед.}}{\text{сообщ.}}$; $H(Y/X) = 0,716\ \frac{\text{дв.ед.}}{\text{сообщ.}}$; $I(Y,X)$ = 0,255 дв.ед.

2. ИСТОЧНИКИ ДИСКРЕТНЫХ СООБЩЕНИЙ

2.1. Основные формулы

Энтропия источника сообщений при наличии связей между двумя соседними символами:

$$H(X) = -\sum_{k=1}^{n} P(x_k) \sum_{l=1}^{n} P(x_l/x_k) \log P(x_l/x_k) = \\ = \sum_{k=1}^{n} \sum_{l=1}^{n} P(x_k, x_l) \log P(x_l/x_k) \quad \frac{\text{дв.ед.}}{\text{символ}}. \tag{2.1}$$

Энтропия источника сообщений, когда коррелятивные связи имеются между тремя символами:

$$H(X) = -\sum_{h=1}^{n} \sum_{j=1}^{n} P(x_h, x_j) \sum_{i=1}^{n} P(x_i/x_h, x_j) \log P(x_i/x_h, x_j) = \\ = \sum_{h=1}^{n} \sum_{j=1}^{n} \sum_{i=1}^{n} P(x_h, x_j, x_i) \log P(x_i/x_h, x_j) \quad \frac{\text{дв.ед.}}{\text{символ}}. \tag{2.2}$$

Число типичных последовательностей длиной M:

$$N_T = 2^{MH(X)}, \tag{2.3}$$

где $H(X)$ – энтропия эргодического источника.

Число всевозможных последовательностей, которое можно составить из n букв:

$$N = n^M. \tag{2.4}$$

Число последовательностей, у которых из M мест n_A мест предоставлено букве A, равно числу сочетаний из M элементов n_A:

$$C_M^{n_A} = \frac{M!}{n_A!(M - n_A)!}. \tag{2.5}$$

Вероятность того, что в выработанной источником последовательности длиной M содержится n_A символов A, определяется из биномиального закона:

$$P_{M,n_A} = C_M^{n_A} P^{n_A} (1 - P)^{M - n_A}. \tag{2.6}$$

Избыточность источника:

$$R = \frac{H_{\max}(X) - H(X)}{H_{\max}(X)}. \tag{2.7}$$

Скорость создания сообщений или поток информации

$$\overline{H}(X) = \frac{H(X)}{\overline{\tau}} \ \frac{\text{дв.ед.}}{\text{с}}, \qquad (2.8)$$

где $\overline{\tau}$ – средняя длительность, которая определяется формулой

$$\overline{\tau} = \sum_i \tau_i P(x_i). \qquad (2.9)$$

Пример 2.1. Источник, используя алфавит из двух символов x_1 и x_2, вырабатывает последовательности $x_1\ x_2\ x_2\ x_1\ x_2\ x_1\ x_2\ x_1$ и т. д. Вероятностные связи в данной последовательности имеют место между тремя символами. Определить все возможные состояния источника и порядок их следования в данной последовательности.

Решение. В условии задан эргодический источник второго порядка $(r = 2)$. Поэтому число различных состояний источника равно $2^2 = 4$. Выпишем их, нумеруя состояния соответствующими индексами:

$$x_1x_1 - S_{11};$$
$$x_1x_2 - S_{12};$$
$$x_2x_1 - S_{21};$$
$$x_2x_2 - S_{22}.$$

Чтобы установить, в каком состоянии находится источник, необходимо подождать, пока он выработает два символа. Поэтому в последовательности $x_1\,x_2\,x_2\,x_1\,x_2\,x_1\,x_2\,x_1$ и т. д. первым состоянием является S_{12}. Затем источник после появления символа x_2 переходит в состояние S_{22} и т. д. Получается следующая последовательность состояний, проходимая источником:

$$S_{12} \to S_{22} \to S_{21} \to S_{12} \to S_{21} \to S_{12} \to S_{21} \dots .$$

Пример 2.2. Источник сообщений вырабатывает три различных символа x_1, x_2, x_3 с соответственными вероятностями 0,2; 0,5; 0,3.

Вероятности появления пар заданы в табл. 2.1. Определить энтропию и сравнить её с энтропией источника, у которого отсутствуют вероятностные связи. Определить избыточность источника.

Таблица 2.1

Вероятности появления пар символов $P(x_i, x_j)$

$x_i\ x_j$	$x_1\ x_1$	$x_1\ x_2$	$x_1\ x_3$	$x_2\ x_1$	$x_2\ x_2$	$x_2\ x_3$	$x_3 x_1$	$x_3\ x_2$	$x_3\ x_3$
$P(x_i, x_j)$	0,2	0	0	0,1	0,3	0,1	0,1	0,2	0

Решение. Энтропию найдём из выражения

$$H(X) = -\sum_{i=1}^{3}\sum_{j=1}^{3} P(x_i, x_j)\cdot \log P(x_i / x_j)\,. \tag{2.10}$$

Для этого вычислим условные вероятности по формуле

$$P(x_i / x_j) = \frac{P(x_i, x_j)}{P(x_j)}.$$

Результаты расчёта сведём в табл. 2.2.

Таблица 2.2

Условные вероятности $P(x_i / x_j)$

x_i / x_j	x_1 / x_1	x_1 / x_2	x_1 / x_3	x_2 / x_1	x_2 / x_2	x_2 / x_3	x_3 / x_1	x_3 / x_2	x_3 / x_3
$P(x_i / x_j)$	0,5	0	0	0,25	0,6	1	0,25	0,4	0

Подставляя полученные значения вероятностей $P(x_i, x_j)$ и $P(x_i / x_j)$ в формулу (2.10), получим:

$$H(X) = -(0{,}2\cdot\log 0{,}5 + 0{,}1\cdot\log 0{,}25 + 0{,}3\cdot\log 0{,}6 + 0{,}1\cdot\log 1 +$$
$$+\,0{,}1\cdot\log 0{,}25 + 0{,}2\cdot\log 0{,}4) = 0{,}2\cdot 1 + 0{,}1\cdot 2 + 0{,}3\cdot 0{,}737 +$$
$$+\,0{,}1\cdot 0 + 0{,}1\cdot 2{,}0 + 0{,}2\cdot 1{,}32 = 1{,}08 \text{ бит}\,.$$

Энтропия источника, у которого вероятностные связи между символами отсутствуют:

$$H^*(X) = -\sum_{i=1}^{3} P(x_i)\cdot\log P(x_i) = -(0,2\cdot\log 0,2 + 0,5\cdot\log 0,5 + 0,3\cdot\log 0,3) =$$
$$= 0,46 + 0,5 + 0,52 = 1,48 \text{ бит}\,.$$

Энтропия источника с независимым появлением равновероятных символов равна

$$H^{**}(X) = \log 3 = 1{,}58\,\text{бит}\,.$$

Находим избыточность с учётом статистических связей:

$$R = \frac{H\max(X) - H(X)}{H\max(X)} = \frac{H^{**}(X) - H(X)}{H^{**}(X)} = \frac{1,58 - 1,08}{1,58} = 0,32\,.$$

Избыточность из-за неравновероятности появления символов равна

$$R^* = \frac{H^{**}(X) - H^*(X)}{H^{**}(X)} = \frac{1{,}58 - 1{,}48}{1{,}58} = 0{,}06\,.$$

Следовательно, наличие коррелятивных (статистических) связей между символами также приводит к уменьшению энтропии и увеличению избыточности.

Пример 2.3. Источник вырабатывает два символа A и B с вероятностью $P(A) = 0{,}4$ и $P(B) = 0{,}6$. Определить количество возможных последовательностей, содержащих n_A символов A, причём $n_A + n_B = M = 4$. Определить вероятность события, которое заключается в том, что в выработанной источником последовательности длиной M содержится n_A символов A.

Решение. Число всевозможных последовательностей, которое можно составить из двух букв, по M букв в каждой, $N = 2^M$. Число последовательностей, у которых из M мест n_A мест предоставлено букве A, равно числу сочетаний из M элементов по n_A:

$$C_M^{n_A} = \frac{M!}{(M - n_A)!\,n_A!}.$$

Вероятность того, что в выработанной источником последовательности длиной M содержится n_A символов A, определяется из биномиального закона

$$P_{M,n_A} = C_M^{n_A} P^{\,n_A} (1 - P)^{\,M - n_A}.$$

Более подробно рассмотрим работу данного источника для $M = 4$. Тогда $N = 2^4 = 16$. Выпишем эти 16 возможных последовательностей, вычислив для каждой из них $C_M^{n_A}$ и P_{M,n_A}.

Возможные последовательности	n_A	n_B	$C_M^{n_A}$	P_M, n_A
AAAA	4	0	1	0,0256
AAAB *AABA* *ABAA* *BAAA*	3	1	4	0,154
AABB *ABBA* *BBAA* *BAAB* *BABA* *ABAB*	2	2	6	0,346
BBBA *BBAB* *BABB* *ABBB*	1	3	4	0,346
BBBB	0	4	1	0,130

Из таблицы видно, что источник чаще вырабатывает последовательности, содержащие одинаковое число символов *A* и *B*, а также три символа *B*.

Пример 2.4. Эргодический источник с энтропией $H = 2$ бита вырабатывает 8 различных символов. Оценить, какую долю общего числа возможных последовательностей следует учитывать в практических расчётах, если длина последовательностей $M = 30$.

Решение. Всевозможное число последовательностей равно

$$N = n^M = 8^{30} = 2^{90}$$

Найдем число типичных последовательностей:

$$N_T = 2^{MH(X)} = 2^{30 \cdot 2} = 2^{60},$$

откуда

$$\frac{N_T}{N} = \frac{2^{60}}{2^{90}} = \frac{1}{2^{30}} \cong \frac{1}{10^9}.$$

Следовательно, к типичным последовательностям относится только одна миллиардная доля всевозможных реализаций.

2.2. Задачи и упражнения

2.2.1. Источник, используя алфавит из двух символов x_1 и x_2, вырабатывает последовательность $x_1\, x_2\, x_2\, x_1\, x_2\, x_1\, x_2\, x_1$ и т. д. Вероятностные связи в данной последовательности имеют место между четырьмя символами. Определить все возможные состояния источника и порядок их следования в данной последовательности.

Ответ: $x_1 x_1 x_1$ $x_1 x_1 x_2$ $x_1 x_2 x_1$ $x_2 x_1 x_1$ $x_1 x_2 x_2$ $x_2 x_1 x_2$ $x_2 x_2 x_1$ $x_2 x_2 x_2$;

$$S_{122} \to S_{221} \to S_{212} \to S_{121} \to S_{212} \to S_{121} \to \ldots .$$

2.2.2. Источник сообщений вырабатывает три различных символа $x_1\, x_2\, x_3$ с соответственными вероятностями 0,4; 0,5; 0,1.

Вероятности появления пар заданы в табл. 2.3. Определить энтропию и сравнить её с энтропией источника, у которого отсутствуют вероятностные связи и вероятность появления символов одинакова.

Таблица 2.3

x_i, x_j	x_1x_1	x_1x_2	x_1x_3	x_2x_1	x_2x_2	x_2x_3	x_3x_1	x_3x_2	x_3x_3
$P(x_i,x_j)$	0,1	0,2	0,1	0,2	0,3	0	0,1	0	0

Ответ: $H(X)$ = 1,086 бит; $H'(X)$ = 1,36 бит; $H''(X)$ = 1,58 бит.

2.2.3. Источник сообщений вырабатывает символы a и b. Условные вероятности $P(a/b)$ = 0,1; $P(b/b)$ = 0,9; $P(b/a)$ = 0,7; $P(a/a)$ = 0,3. Определить энтропию источника.

Ответ: $H(X) = 0{,}51 \dfrac{\text{бит}}{\text{символ}}.$

2.2.4. Источник генерирует два равновероятных символа x_1 и x_2, условные вероятности $P(x_1/x_1) = P(x_2/x_2) = 0{,}7$; $P(x_1/x_2) = P(x_2/x_1) = 0{,}3$. Определить энтропию и избыточность источника.

Ответ: $H(X) = 0{,}883 \dfrac{\text{бит}}{\text{символ}};\ R = 0{,}12.$

2.2.5. Элементы сигнала принимают два состояния m_1 и m_2. Определить количество информации (энтропию) и избыточность, если две полные и четыре условные вероятности имеют следующие значения: $P(m_1)$ = 3/4; $P(m_2)$ = 1/4; $P(m_1/m_1)$ = 2/3; $P(m_2/m_2)$ = 0; $P(m_1/m_2)$ = 1; $P(m_2/m_1)$ = 1/3, т. е. после m_2 всегда следует m_1.

Ответ: $H(X) = 0{,}685 \dfrac{\text{бит}}{\text{символ}};\ R = 0{,}315.$

2.2.6. Вероятности появления символов источника равны $P(x_1)$ = 1/2, $P(x_2)$ = 1/4, $P(x_3) = P(x_4)$ = 1/8. Коррелятивные связи имеют место между двумя соседними символами, которые описываются в табл. 2.4. Определить энтропию и избыточность источника.

Таблица 2.4

x_i, x_j	$P(x_i,x_j)$	x_i, x_j	$P(x_i,x_j)$	x_i, x_j	$P(x_i, x_j)$	x_i, x_j	$P(x_i,x_j)$
x_1x_1	13/32	x_2x_1	1/32	x_3x_1	0	x_4x_1	1/16
x_1x_2	3/32	x_2x_2	1/8	x_3x_2	0	x_4x_2	1/32
x_1x_3	0	x_2x_3	3/32	x_3x_3	0	x_4x_3	1/32
x_1x_4	0	x_2x_4	0	x_3x_4	1/8	x_4x_4	0

Ответ: $H(X) = 0{,}886 \dfrac{\text{бит}}{\text{символ}};\ \ R = 0{,}557.$

2.2.7. Эргодический источник с энтропией $H(X)$ = 1,9 бит вырабатывает четыре различных символа. Найти отношение числа типичных к общему числу всевозможных последовательностей длиной M = 100 символов.

Ответ: $\dfrac{N_T}{N} = 1 \cdot 10^{-3}.$

2.2.8. Источник вырабатывает с одинаковой вероятностью два символа A и B. Определить количество возможных последовательностей, содержащих n_A символов A, причём $n_A + n_B = M = 4$. Определить вероятность события, которое заключается в том, что в выработанной источником последовательности длиной M содержится n_A символов A.

Ответ: $C_M^{n_A} = \dfrac{M!}{n_A!(M - n_A)!}$; $P_{M,n_A} = C_M^{n_A}(1/2)^M$; $C_4^4 = 1$, $P_{4,4} = 1/16$; $C_4^3 = 4$, $P_{4,3} = 4/16$; $C_4^2 = 6$, $P_{4,2} = 6/16$; $C_4^1 = 4$, $P_{4,1} = 4/16$; $C_4^0 = 1$, $P_{4,0} = 1/16$.

2.2.9. Источник вырабатывает три различных символа x_1, x_2, x_3 с вероятностями 0,5; 0,3; 0,2 соответственно. Заданы возможные длительности символов $\tau_1 = 10$ с, $\tau_2 = 4$ с, $\tau_3 = 2$ с. Подобрать такое соответствие заданных длительностей символам источника, чтобы поток информации был максимальным.

Ответ: $\bar{\tau}_{\min} = 4{,}2$ с; $\bar{H}_{\max} = 0{,}354\ \dfrac{\text{бит}}{\text{с}}$.

2.2.10. Оценить, какую долю общего числа возможных последовательностей следует учитывать в практических расчётах, если эргодический источник, имеющий энтропию $H(X)$ = 3,5 дв.ед., вырабатывает n = 16 различных символов, а длина последовательностей M = 50.

Ответ: $\dfrac{N_T}{N} = \dfrac{2^{175}}{2^{200}} = \dfrac{1}{30 \cdot 10^6}$.

2.2.11. На контролируемом пункте имеются три объекта, каждый из которых может находиться в одном из двух положений («включён» или «выключен»). С контролируемого пункта передаются сообщения об изменении положений объектов. Наблюдением в течение длительного отрезка времени установлено, что из 100 переданных сообщений 70 относятся к первому объекту, 20 – ко второму и 10 – к третьему. Определить количество информации, содержащееся в одном сообщении.

Ответ: $H(X) = 2{,}156\ \dfrac{\text{дв.ед.}}{\text{сообщ.}}$.

2.2.12. На контролируемом пункте, аналогичном описанному в задаче 2.2.11, производится периодический контроль состояния объектов. Количество сообщений, передаваемых о состоянии каждого объекта, одинаково. Наблюдением установлено, что в среднем объект 1 включён в течение 98 % всего времени, объект 2 – 80 %, а объект 3 – 0,6 %. В остальное время объекты отключены. Определить количество информации, содержащееся в одном сообщении.

Ответ: $H(X) = 1{,}88\ \dfrac{\text{дв.ед.}}{\text{сообщ.}}$.

2.2.13. Определить избыточность источников информации для условий задач 2.2.11 и 2.2.12.

Ответ: для условия задачи 2.2.11 R = 0,167; для условия задачи 2.2.12 R = 0,272.

3. ИСТОЧНИК НЕПРЕРЫВНЫХ СООБЩЕНИЙ

3.1. Основные формулы

Дифференциальная энтропия источника:

$$H_{\Delta}(X) = -\int_{-\infty}^{\infty} W(x) \log W(x) dx. \tag{3.1}$$

Относительная дифференциальная условная энтропия источника:

$$H_{\Delta}(X/Y) = \int_{-\infty}^{\infty} \int_{\infty}^{\infty} W(x, y) \log \frac{W(x, y)}{W(y)} dxdy. \tag{3.2}$$

Эпсилон-энтропия источника:

$$H(X)_{\varepsilon} = \min I(Y, X) = H_{\Delta}(X) - \max H_{\Delta}(X/Y). \tag{3.3}$$

Эпсилон-энтропия для одного независимого отсчёта при гауссовском процессе $X(t)$ и $E(t)$:

$$\max H(X)_{\varepsilon} = 0,5 \log(\sigma_X^2 / \sigma_E^2), \tag{3.4}$$

где σ_X и σ_E – среднеквадратичное значение сигнала и помехи соответственно.

Эпсилон-производительность источника при дискретном времени:

$$H'(X)_{\varepsilon} = V_{\tau} H(X)_{\varepsilon} = V_{\tau} \left(H_{\Delta}(X) - \log \sqrt{2\pi e \varepsilon_0^2} \right) \frac{\text{бит}}{\text{с}}, \tag{3.5}$$

где $V_{\tau} = 1/\Delta t$ – скорость передачи отсчетов;

$\Delta t = 1/2\Delta F$ – интервал дискретизации;

ΔF – полоса частот сигнала $X(t)$.

Если время непрерывное, то

$$H'(X)_{\varepsilon} = 2\Delta F (H_{\Delta}(X) - \log \sqrt{2\pi e \varepsilon_0^2}) \frac{\text{бит}}{\text{с}}. \tag{3.6}$$

Максимальное значение эпсилон-производительности имеет место, когда сигнал $X(t)$ является гауссовским:

$$\max H'(X)_{\varepsilon} = \frac{V_{\tau}}{2} \log(\sigma_X^2 / \varepsilon_0^2) \frac{\text{бит}}{\text{с}}; \tag{3.7}$$

$$\max H'(X)_{\varepsilon} = \Delta F \log(\sigma_X^2 / \varepsilon_0^2) \frac{\text{бит}}{\text{с}}, \tag{3.8}$$

где ε_0^2 – максимальная мощность помехи.

Объём информации, выдаваемый источником за время T:

$$\max V = \max H'(X)_{\varepsilon} \cdot T = \Delta F T \log(\sigma_X^2 / \varepsilon_0^2) \text{ бит}. \tag{3.9}$$

Избыточность источника

$$R_X = 1 - \frac{H_\Delta(X) - \log\sqrt{2\pi e \varepsilon_0^2}}{0{,}5\log(\sigma_X^2/\varepsilon_0^2)}. \tag{3.10}$$

Количество информации, содержащееся в одной непрерывной случайной величине, относительно другой:

$$I(X,Y) = H_\Delta(X) - H_\Delta(X/Y) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} W(x,y)\log\frac{W(x,y)}{W(x)W(y)}dxdy. \tag{3.11}$$

Пример 3.1. Определить энтропию случайных величин, равномерно распределённых на интервале с шириной $\varepsilon=\beta-\alpha$..

Решение. Из условия задачи следует, что плотность вероятности $W(x) = \frac{1}{\varepsilon}$, а энтропия

$$H_\Delta(X) = -\int_\alpha^\beta W(x)\log W(x)dx = -\int_\alpha^\beta \frac{1}{\varepsilon}\log\frac{1}{\varepsilon}dx = \log(\beta-\alpha).$$

Пример 3.2. Вычислить дисперсию равномерного распределения на интервале (α,β).

Решение. На основании определения дисперсии имеем

$$\sigma_x = \int_\alpha^\beta (x(t) - m(x))^2 W(x)dx = \int_\alpha^\beta (x - \frac{\alpha+\beta}{2})^2 \frac{1}{\beta-\alpha}dx = \frac{(\beta-\alpha)^2}{12}.$$

3.2. Задачи и упражнения

3.2.1. Определить выигрыш в мощности при использовании источника с гауссовской плотностью распределения по сравнению с источником, имеющим в интервале (α,β) равномерную плотность распределения.

Ответ: $\sigma_P^2 = 1{,}42\sigma_\Gamma^2$, т. е. 42 %.

3.2.2. Определить энтропию случайной величины, распределённой по экспоненциальному закону:

$$W(X) = \begin{cases} ce^{-cx}, x \ge 0; \\ 0, x \le 0; c > 0. \end{cases}$$

Ответ: $H_\Delta(X) = \log\frac{e}{c}$.

3.2.3. Определить количество информации $I(X, Y)$ для системы (X, Y) гауссовских случайных величин:

$$W(x, y) = \frac{1}{2\pi\sigma_x\sigma_y\sqrt{1-\gamma^2}}\exp\left(-\frac{1}{2(1-\gamma^2)}\left(\frac{x^2}{\sigma_x^2} - \frac{2\gamma \cdot xy}{\sigma_x\sigma_y} + \frac{y^2}{\sigma_y^2}\right)\right).$$

Ответ: $I(X,Y) = -\log\sqrt{1-\gamma^2}$.

3.2.4. Определить производительность источника ε, формирующего со скоростью $V_\tau = \alpha$ некоррелированные отсчёты стационарного нормального случайного сигнала с дисперсией σ_x^2.

Ответ: $H'(X)_{\varepsilon_0} = \dfrac{\alpha}{2}\log\dfrac{\sigma_x^2}{\varepsilon_0^2}$.

4. ИНФОРМАЦИОННЫЕ ХАРАКТЕРИСТИКИ НЕПРЕРЫВНЫХ КАНАЛОВ

4.1. Основные формулы

Пропускная способность канала с дискретным временем:

$$C = 0,5V_\tau \log(1 + \sigma_X^2/\sigma_E^2). \qquad (4.1)$$

Пропускная способность канала с непрерывным временем:

$$C = \Delta F \log\left(1 + \sigma_X^2/\sigma_E^2\right). \qquad (4.2)$$

Число уровней, которое может быть различимо без ошибок:

$$M = \sqrt{1 + \frac{\sigma_X^2}{\sigma_E^2}} = \sqrt{1 + \frac{P_X}{P_{\text{ш}}}\Big/\sigma_E^2}, \qquad (4.3)$$

где P_X и $P_{\text{ш}}$ – мощность полезного сигнала и шума соответственно.

Приёмник не различает изменения входного сигнала меньше чем корень квадратный из мощности шума, т. е.

$$\delta = \sqrt{P_{\text{Ш}}}\ . \qquad (4.4)$$

Наибольшее количество информации, переносимое импульсом, имеющим M различных уровней:

$$I = \frac{1}{2}\log\left(1 + \frac{P_X}{P_{\text{ш}}}\right). \qquad (4.5)$$

Пример 4.1. Аналоговый сигнал с амплитудой 2 В передаётся по каналу связи, в котором отношение сигнал/шум равно 20 дБ. Определить абсолютную погрешность телеизмерения.

Решение. Если сигнал смешан с помехой, то амплитуда сигнала может быть измерена с точностью до эффективного значения напряжения. При этом погрешность оценки точного значения амплитуды равна $\sqrt{P_{\text{ш}}}$.

Из соотношения

$$10 \lg \frac{P_{\text{С}}}{P_{\text{ш}}} = 20 \text{ дБ}$$

определим мощность шума

$$\lg \frac{P_{\text{С}}}{P_{\text{ш}}} = 2, \quad P_{\text{ш}} = \frac{P_{\text{С}}}{100} = 1 \cdot 10^{-2} \text{ Вт.}$$

Тогда погрешность

$$\delta = \sqrt{P_{\text{ш}}} = \sqrt{0,01} = 0,1 \text{ В.}$$

Пример 4.2. Определить пропускную способность канала связи при условии, что сигнал $C(t) = 5\sin 1000\pi t$ должен быть восстановлен с погрешностью, не большей чем 1 В.

Решение. Из условия задачи известно, что амплитуда сигнала $u_{\text{С}} = 5$ В, а полоса частот $\Delta F\text{с} = 500$ Гц. Тогда пропускная способность

$$C = \Delta F_{\text{С}} \log\left(1 + \frac{P_{\text{С}}}{P_{\text{ш}}}\right) = \Delta F_{\text{С}} \log\left(1 + \frac{u_{\text{С}}^2}{\delta^2}\right) = 500 \log\left(1 + \frac{25}{1}\right) =$$
$$= 500 \log(26) \cong 500 \cdot 4,7 = 2350 \ \frac{\text{дв.ед.}}{\text{с}}.$$

4.2. Задачи и упражнения

4.2.1. Определить объём информации, содержащейся в изображении из 500 строк по 500 элементов в каждой. Яркость каждого элемента передаётся восемью квантованными уровнями. Различные градации яркости равновероятны, а яркости разных элементов не коррелированы.

Ответ: $H(X) = 750000 \ \frac{\text{дв.ед.}}{\text{изобр.}}$.

4.2.2. Изображение задачи 4.2.1 должно быть передано по радиолинии, на входе которой действует белый гауссовский шум с удельной мощностью $P_{\text{ош}} = 10^{-4}$ Вт/Гц. Ширина полосы пропускания приёмного устройства $\Delta F_{\text{С}} = 1000$ Гц. Время передачи 1 час. Определить минимально возможное значение мощности полезного сигнала на входе приёмника.

Ответ: $P_X = 155 \cdot 10^{-4}$ Вт.

4.2.3. Определить длину магнитной ленты для записи одного изображения, если энтропия изображения $H(X)_{\text{И}} = 600000\ \frac{\text{дв.ед.}}{\text{изобр.}}$, а по ширине ленты записывается 30 дв.ед. информации при плотности записи $10\ \frac{\text{дв.ед.}}{\text{мм}}$.

Ответ: L = 2000 мм.

4.2.4. Сигнал с амплитудой 1 В передаётся по каналу связи, в котором отношение сигнал/шум равно 10 дБ. Определить абсолютную погрешность телеизмерений.

Ответ: δ = 0,31 В.

4.2.5. По непрерывному каналу передаётся сигнал, спектр которого ограничен полосой частот 30 Гц. Определить пропускную способность канала связи таким образом, чтобы погрешность передаваемого сигнала не превышала 1 %.

Ответ: $C = 400\ \frac{\text{дв.ед.}}{\text{с}}$.

4.2.6. Непрерывный канал связи с пропускной способностью $40\ \frac{\text{дв.ед.}}{\text{с}}$ предназначен для передачи квантованного сигнала с полосой частот 5 Гц. Определить число различных уровней измеряемого сигнала и погрешность измерений.

Ответ: M = 16, δ = 6,3 %.

4.2.7. По радиолинии, на входе которой действует гауссовский шум с удельной мощностью 10^{-8} Вт/Гц, передаётся 1024 сообщения в течение $1 \cdot 10^{-1}$ с. Определить минимальную мощность полезного сигнала на входе приёмника, если полоса пропускания приёмника равна 100 Гц.

Ответ: $P_{\text{C min}} = 10^{-6}$ Вт.

4.2.8. Отношение сигнал/шум в линии связи равно 10^{-1}, а полоса пропускания канала связи 1 кГц. Определить пропускную способность канала связи.

Ответ: $C = 140\ \frac{\text{дв.ед.}}{\text{с}}$.

4.2.9. Определить пропускную способность канала связи при условии, что сигнал $\sin 500\pi t$ должен быть восстановлен с погрешностью, не большей чем 0,57 В.

Ответ: $C = 500\ \frac{\text{дв.ед.}}{\text{с}}$.

5. ИНФОРМАЦИОННЫЕ ХАРАКТЕРИСТИКИ ДИСКРЕТНЫХ КАНАЛОВ СВЯЗИ

5.1. Основные формулы

Скорость передачи информации:

$$R_t = \frac{H(X) - H(X/Y)}{\tau} = \frac{I(X,Y)}{\tau}, \tag{5.1}$$

где τ – длительность передаваемых сигналов.

Пропускная способность канала связи:

$$C = \frac{\max I(X,Y)}{\tau} = \frac{H_{\max}(X) - H(X/Y)}{\tau}. \tag{5.2}$$

Пропускная способность бинарного канала связи:

$$C = \frac{1}{\tau}(1 + P\log P + (1-P)\log(1-P)), \tag{5.3}$$

где P – вероятность перехода одного символа в другой.

Объём сигнала:

$$V_X = T_X \cdot F_X \cdot H_X. \tag{5.4}$$

где $H_X = \log(P_X / P_\varepsilon)$ – превышение сигнала над помехой;

T_X – время передачи сигнала;

F_X – полоса частот сигнала.

Объём канала:

$$V_K = T_K \cdot F_K \cdot H_K, \tag{5.5}$$

где T_K – время использования канала;

F_K – полоса пропускания канала;

$H_K = \log(P_{X\max} / P_\varepsilon)$ – допустимая энергетическая нагрузка.

Пример 5.1. По каналу связи передаются двоичные 8-разрядные сообщения, вероятность появления нулей $P(0)$ = 0,6. Время передачи одного сообщения $T = 10^{-3}$ с. Определить скорость передачи и пропускную способность канала связи.

Решение. Пропускная способность будет определяться выражением

$$C = \frac{n\log m}{\tau} = \frac{8\log 2}{10^{-3}} = 8000\ \frac{\text{дв.ед.}}{\text{с}}.$$

Скорость передачи сообщений с учётом вероятности состояния каждого элемента будет равна

$$R_t = \frac{-n\sum_{i=1}^{2} P_i \cdot \log P_i}{\tau} = \frac{-8(0,6 \cdot \log 0,6 + 0,4 \cdot \log 0,4)}{10^{-3}} =$$

$$= \frac{8 \cdot (0,4422 + 0,5288)}{10^{-3}} \cong 7768 \quad \frac{\text{дв.ед.}}{\text{с}}.$$

Пример 5.2. Количество сообщений, передаваемых с контролируемого пункта, о состоянии четырёх объектов одинаково. Наблюдением установлено, что в среднем объект 1 включен в течение 80 % всего времени, объект 2 – 40 %, объект 3 – 60 %, объект 4 – 20 %. В остальное время объекты отключены. Определить скорость передачи информации и пропускную способность канала связи, если длительность одного сообщения 10^{-3} с.

Решение. Исходя из одинакового количества сообщений о состоянии объектов, можно записать, что $P(x_1) = P(x_2) = P(x_3) = P(x_4) = \frac{1}{4}$. Из статистики наблюдений можно записать выражения для определения вероятности того, что объекты находятся во включенном состоянии:

$$P(x_{1B}) = 0,8P(x_1);\ P(x_{2B}) = 0,4P(x_2);\ P(x_{3B}) = 0,6P(x_3);\ P(x_{4B}) = 0,2P(x_4).$$

Результаты расчёта вероятностей того, что объекты находятся во включённом или отключённом состоянии, сведём в табл. 5.1.

Таблица 5.1

Вероятности $P(x_{iB})$ и $P(x_{iO})$

x_i	x_{1B}	x_{1O}	x_{2B}	x_{2O}	x_{3B}	x_{3O}	x_{4B}	x_{4O}
$P(x_i)$	0,2	0,05	0,1	0,15	0,15	0,1	0,05	0,2

Тогда скорость передачи информации будет равна

$$R_t = V_\tau \cdot (H(X)) = \frac{1}{10^{-3}} \cdot (-0,2 \cdot \log 0,2 - 0,05 \cdot \log 0,05 - 0,1 \cdot \log 0,1 -$$

$$-0,15 \cdot \log 0,15 - 0,15 \cdot \log 0,15 - 0,1 \cdot \log 0,1 - 0,05 \cdot \log 0,05 - 0,2 \cdot \log 0,2) =$$

$$= \frac{1}{10^{-3}} \cdot (0,464 + 0,216 + 0,332 + 0,410 + 0,410 + 0,332 + 0,216 + 0,464) = 2844 \quad \frac{\text{дв.ед.}}{\text{с}}.$$

Пропускная способность в этом случае будет равна

$$C = V_\tau \cdot \max H(X) = V_\tau \log M = 10^3 \cdot 3 = 3000 \quad \frac{\text{дв.ед.}}{\text{с}},$$

где M = 8 – общее число состояний системы (четырёх объектов).

Пример 5.3. По дискретному каналу связи с помехами передаётся кодовое сообщение 1110011110. Вероятность искажения одиночных сигналов

$$P = P_{10} = P_{01} = 10^{-2},$$

а длительность элемента кода 10^{-3} с. Определить скорость передачи и пропускную способность канала связи.

Решение. Пропускную способность канала связи определим из выражения

$$C = V_{\tau} \cdot (1 + P\log P + (1-P)\cdot\log(1-P)) = 10^{3}(1 + 0,01\cdot\log 0,01 + 0,99\cdot\log 0,99) =$$

$$= 1000\cdot(1 - 0,066 - 0,014) \cong 1000\cdot 0,92 \;= 920\ \frac{\text{дв.ед.}}{\text{с}}.$$

Скорость передачи

$$R_t = V_{\tau}\cdot\left(-\sum_{i=1}^{2} P_i\log P_i + P\log P + (1-P)\cdot\log(1-P)\right) =$$

$$= 10^{3}(-0,3\log 0,3 - 0,7\log 0,7 + 0,01\log 0,01 + 0,99\log 0,99) =$$

$$= 1000\cdot(0,521 + 0,360 - 0,066 - 0,014) = 1000\cdot 0,801 = 801\ \frac{\text{дв.ед.}}{\text{с}},$$

где $P(0) = \dfrac{n(0)}{n} = \dfrac{3}{10} = 0{,}3,\quad P(1) = \dfrac{n(1)}{n} = \dfrac{7}{10} = 0{,}7.$

5.2. Задачи и упражнения

5.2.1. В информационном канале используется алфавит с четырьмя различными символами. Длительность всех символов одинакова и равна τ = 1 мс. Определить пропускную способность канала при отсутствии шумов.

Ответ: $C = 2000\ \dfrac{\text{дв.ед.}}{\text{с}}$.

5.2.2. В информационном канале используется сменно-качественный код, при котором запрещается передача подряд двух одинаковых символов. Алфавит кода состоит из четырёх различных символов. Вероятности передачи всех разрешённых пар символов одинаковы. Длительности всех символов также одинаковы и равны τ = 1 мс. Определить скорость передачи информации.

Ответ: $R_t = 1585\ \dfrac{\text{дв.ед.}}{\text{с}}$.

5.2.3. В дискретном канале для передачи сообщений используются три различных символа с длительностями $\tau_1 = \tau_2$ = 10 мс и τ_3 = 20 мс. Определить пропускную способность канала.

Ответ: $C = 127\ \frac{\text{дв.ед.}}{\text{с}}$.

5.2.4. В канал связи передаются сообщения длиной n = 10 элементов, каждый из которых может принимать m = 4 состояния с вероятностями P_1 = 0,2; P_2 = 0,3; P_3=0,1; P_4 = 0,4. Время передачи одного сообщения τ = 0,1 с. Определить скорость передачи информации и пропускную способность канала связи.

Ответ: $R_t = 185\ \frac{\text{дв.ед.}}{\text{с}}$, $C = 200\ \frac{\text{дв.ед.}}{\text{с}}$.

5.2.5. По бинарному каналу передаются сообщения: 1110011101, 1110000001. Длительность каждого элемента сообщения τ = 10 мс. Определить скорость передачи каждого сообщения и пропускную способность двоичного канала.

Ответ: $R_{t1} = 88\ \frac{\text{дв.ед.}}{\text{с}}$, $R_{t2} = 97\ \frac{\text{дв.ед.}}{\text{с}}$, $C = 100\ \frac{\text{дв.ед.}}{\text{с}}$.

5.2.6. В канал связи передаются сообщения от эргодического источника, вырабатывающего m = 3 элемента. В кодовых комбинациях запрещена передача двух одинаковых элементов. Вероятность передачи всех разрешённых кодовых комбинаций длиной n = 3 одинакова. Длительность каждого элемента τ = 10 мс. Определить скорость передачи информации и пропускную способность канала связи.

Ответ: $R_t = C = 300\ \frac{\text{дв.ед.}}{\text{с}}$.

5.2.7. В бинарном канале вероятности подавления и воспроизведения ложного сигнала одинаковы и равны $P_{10} = P_{01} = P = 10^{-3}$. Длительности символов одинаковы и равны τ = 1 мс. Определить пропускную способность бинарного симметричного канала.

Ответ: $C = 11{,}3\ \frac{\text{дв.ед.}}{\text{с}}$.

5.2.8. По линии связи с помехами передаётся четыре сообщения. Ансамбль объединения описывается в табл. 5.2. Длительность сообщения τ = 2 мс. Определить скорость передачи сообщений и пропускную способность канала связи.

Таблица 5.2

y_j	x_i			
	x_1	x_2	x_3	x_4
y_1	0,1	0,05	0,05	0,15
y_2	0,03	0,05	0,1	0,04
y_3	0,07	0,03	0,05	0,06
y_4	0	0,07	0,05	0,1

Ответ: $R_t = 13{,}5\ \frac{\text{дв.ед.}}{\text{с}}$, $C = 34{,}5\ \frac{\text{дв.ед.}}{\text{с}}$.

5.2.9. По дискретному каналу связи с помехами передаётся кодовое сообщение 1100110011. Вероятность искажёния одиночных символов $P_{10} = P_{01} = P = 10^{-1}$, а длительность элемента кода $\tau = 1 \cdot 10^{-2}$ с. Определить скорость передачи и пропускную способность канала связи.

Ответ: $R_t = 72\ \dfrac{\text{дв.ед.}}{\text{с}},\ C = 92\ \dfrac{\text{дв.ед.}}{\text{с}}$.

5.2.10. С контролируемого пункта передаются сообщения об изменении положения объектов. Каждый объект может находиться в одном из двух положений: «включён» или «выключен». Наблюдением установлено, что из 50 переданных сообщений 40 относится к первому объекту, 2 – ко второму и 8 – к третьему. Объекты работают независимо друг от друга, а положения объектов равновероятны. Определить скорость передачи информации и пропускную способность дискретного канала, если длительность каждого сообщения 1 мс.

Ответ: $R_t = 1864\ \dfrac{\text{дв.ед.}}{\text{с}},\ C = 2585\ \dfrac{\text{дв.ед.}}{\text{с}}$.

5.2.11. Количество сообщений, передаваемых с контролируемого пункта, о состоянии трёх объектов, одинаково. Наблюдением установлено, что в среднем объект 1 «включён» в течение 60 % всего времени, объект 2 – 30 %, а объект 3 – 40 %. В остальное время объекты «отключены». Определить скорость передачи информации и пропускную способность канала связи, если длительность одного сообщения 5 мс.

Ответ: $R_t = 504\ \dfrac{\text{дв.ед.}}{\text{с}},\ C = 517\ \dfrac{\text{дв.ед.}}{\text{с}}$.

6. КОДИРОВАНИЕ ИНФОРМАЦИИ ПРИ ПЕРЕДАЧЕ ПО ДИСКРЕТНОМУ КАНАЛУ БЕЗ ПОМЕХ

6.1. Основные формулы

Средняя длина кодового слова:

$$L = \sum_{i=1}^{n} \mu_i P(x_i), \tag{6.1}$$

где μ_i – длина кодового слова, сопоставляемая x_i сообщению.

При кодировании сообщений x_i в алфавите, насчитывающем m символов, при условии отсутствия шумов средняя длина кодового слова определяется формулой

$$L \geq \frac{H(X)}{\log m}, \tag{6.2}$$

где $H(X)$ – энтропия сообщения.

Пример 6.1. Определите среднюю длину кодового слова и её нижнюю границу, а также вероятность появления нулей $P(0)$ и единиц $P(1)$ при передаче сообщений длиной μ_i и вероятностями появления сообщений $P(x_i)$, указанными в табл. 6.1.

Таблица 6.1

Ансамбль сообщений

Сообщение	$P(x_i)$	Код	μ_i
x_1	0,4	11	2
x_2	0,3	10	2
x_3	0,2	010	3
x_4	0,1	0001	4

Решение. Среднюю длину кодового слова определим из выражения

$$L = \sum_{i=1}^{4} \mu_i P(x_i).$$

Подставив значения μ_i и $P(x_i)$ из таблицы, получим

$$L = 2\cdot 0{,}4 + 2\cdot 0{,}3 + 3\cdot 0{,}2 + 4\cdot 0{,}1 = 0{,}8 + 0{,}6 + 0{,}6 + 0{,}4 = 2{,}4 \text{ символа.}$$

Среднее число нулей

$$L(0) = \sum_{i=1}^{4} \mu_{i0} P(x_i) = 1\cdot 0{,}3 + 2\cdot 0{,}2 + 3\cdot 0{,}1 = 0{,}3 + 0{,}4 + 0{,}3 = 1 \text{ символ.}$$

Вероятность появления нулей $P(0) = L(0)/L = 1/2{,}4 = 0{,}417$.

Среднее число единиц $L(1) = \sum_{i=1}^{4} \mu_{i1} P(x_i) = 2\cdot 0{,}4 + 1\cdot 0{,}3 + 1\cdot 0{,}2 + 1\cdot 0{,}1 =$ $= 0{,}8 + 0{,}3 + 0{,}2 + 0{,}1 = 1{,}4$ символа.

Вероятность появления единиц $P(1) = L(1)/L = 1{,}4/2{,}4 = 0{,}583$.

Определим нижнюю границу средней длины кодового слова из выражения (6.2):

$$L \ge \frac{H(X)}{\log m} = \frac{-(0{,}4\log 0{,}4 + 0{,}3\log 0{,}3 + 0{,}2\log 0{,}2 + 0{,}1\log 0{,}1)}{\log 2} =$$

$$= \frac{0{,}529 + 0{,}521 + 0{,}464 + 0{,}332}{1} = 1{,}846 \text{ символа}.$$

6.2. Правила построения эффективных кодов

6.2.1. Для построения кода Шеннона – Фано все сообщения выписываются в порядке убывания их вероятностей. Записанные таким образом сообщения затем разбиваются на две по возможности равновероятные подгруппы. Всем сообщениям первой подгруппы присваивают цифру 1 в качестве первого кодового символа, а сообщениям второй подгруппы – цифру 0. Аналогичное деление на подгруппы продолжается до тех пор, пока в каждую подгруппу не попадёт по одному сообщению.

6.2.2. Для получения кода Хаффмана все сообщения выписывают в порядке убывания их вероятностей. Две наименьшие вероятности объединяют скобкой и одной из них присваивают символ 1, а другой – 0. Затем эти вероятности складывают, результат записывают в промежутке между ближайшими вероятностями. Процесс объединения двух сообщений с наименьшими вероятностями продолжают до тех пор, пока суммарная вероятность двух оставшихся сообщений не станет равной единице. Код для каждого сообщения строится при записи двоичного числа справа налево путём обхода по линиям вверх направо, начиная с вероятности сообщения, для которого строится код.

6.2.3. Универсальный код при неизвестной статистике сообщений для k-й группы состоит из двух частей: префикса и суффикса. Префикс содержит $\log(n+1)$ двоичных знаков. Он указывает, к какой группе сообщений принадлежит кодируемый блок. Суффикс содержит $\log C_n^k$ двоичных символов и указывает номер блока в группе. Суффикс вычисляется по правилу

$$N(X) = C_{i_1-1}^{1} + C_{i_2-1}^{2} + \ldots + C_{i_r-1}^{r}. \tag{6.3}$$

Для нахождения $N(X)$ используется таблица биномиальных коэффициентов (треугольник Паскаля):

$$\begin{array}{lllllllll}
8 & 7 & 21 & 35 & 35 & 21 & 7 & 1 & 0 \\
7 & 6 & 15 & 20 & 15 & 6 & 1 & 0 & \\
6 & 5 & 10 & 10 & 5 & 1 & 0 & & \\
5 & 4 & 6 & 4 & 1 & 0 & & & \\
4 & 3 & 3 & 1 & 0 & & & & \\
3 & 2 & 1 & 0 & & & & & \\
2 & 1 & 0 & & & & & & \\
1 & 0 & & & & & & &
\end{array} \tag{6.4}$$

Пример 6.2. Для передачи по каналу связи без шумов используется код, состоящий из двух букв a_1 и a_2, появляющихся с вероятностями $P(a_1) = 0{,}9$ и $P(a_2) = 0{,}1$ соответственно. Применить метод Шеннона – Фано к кодированию всевозможных однобуквенных, двухбуквенных и трёхбуквенных сообщений. Определить среднюю длину в каждом случае и результаты сравнить между собой.

Решение. Определим энтропию сообщений:

$$H(A) = -0{,}9 \cdot \log 0{,}9 - 0{,}1 \cdot \log 0{,}1 = 0{,}469\ \frac{\text{дв.ед.}}{\text{буква}}.$$

Применяя метод Шеннона – Фано к двухбуквенному алфавиту, получаем простейший код (табл. 6.2).

Таблица 6.2

Код Шеннона – Фано для однобуквенных сообщений

Буква	Вероятность	Код
a_1	0,9	1
a_2	0,1	0

Этот код требуется для передачи каждой буквы одного двоичного символа $(L=1)$, что на 53 % больше минимально возможного значения $H(A)=0{,}469\ \dfrac{\text{дв.ед.}}{\text{буква}}$.

Применим метод Шеннона – Фано к кодированию всевозможных двухбуквенных комбинаций (табл. 6.3).

Таблица 6.3

Код Шеннона – Фано для двухбуквенных сообщений

Сообщение	Вероятность	Код
a_1a_1	0,81	1
a_1a_2	0,09	01
a_2a_1	0,09	001
a_2a_2	0,01	000

Средняя длина кодового слова равна $L = 1\cdot0{,}81 + 2\cdot0{,}09 + 3\cdot0{,}09 + 3\cdot0{,}01 = 1{,}29$ бит.

Таким образом, на одну букву приходится 1,29/2 = 0,645 бит, что на лишь на 76 % больше значения 0,469.

Произведём кодирование всевозможных трёхбуквенных комбинаций (табл. 6.4).

Таблица 6.4

Сообщение	Вероятность	Код	Сообщение	Вероятность	Код
$a_1a_1a_1$	0,729	1	$a_1a_2a_2$	0,009	00011
$a_1a_1a_2$	0,081	011	$a_2a_1a_2$	0,009	00010
$a_1a_2a_1$	0,081	010	$a_2a_2a_1$	0,009	00001
$a_2a_1a_1$	0,081	001	$a_2a_2a_2$	0,001	00000

Средняя длина кодового слова здесь равна

$$L = 0{,}729 + 3\cdot0{,}081 + 3\cdot0{,}081 + 3\cdot0{,}081 + 5\cdot0{,}009 + 5\cdot0{,}009 + \\ + 5\cdot0{,}009 + 5\cdot0{,}009 = 1{,}598 \text{ бит.}$$

Таким образом, на одну букву текста приходится в среднем 1,598/3 = 0,532 бит, что только на 6,3 % больше значения $H(A)=0{,}469\ \dfrac{\text{бит}}{\text{буква}}$.

Ответ: кодирование блоками более выгодно, чем кодировать отдельные буквы.

Пример 6.3. Закодировать блок $X = x_2x_1x_2x_1x_1x_1x_1x_2$ префиксным кодом при неизвестной статистике сообщений, если символ x_1 появляется с вероятностью p, а x_2 – с вероятностью g.

Решение. Определим число разрядов префикса

$$E\log(n+1)=E\log(8+1)=4,$$

где E – знак округления в большую сторону.

Вероятность слова определяется формулой

$$P(X) = p^5 g^3.$$

Тогда префикс будет 0011.

Число символов x_1 $r = 5$, которые размещаются на местах: $i_1 = 2,$ $i_2 = 4,$ $i_3 = 5,$ $i_4 = 6,$ $i_5 = 7.$

Находим номер блока $N(X) = C_1^1 + C_3^2 + C_4^3 + C_5^4 + C_6^5.$

Слагаемые в $N(X)$ находим, используя таблицу дополнительных коэффициентов. Таким образом,

$$N(X)=1+3+4+5+6=19,$$

или в двоичной записи

$$N(X)=10011.$$

Следовательно, закодированный блок поступит в канал связи в виде

$$X = 001110011.$$

Пример 6.4. Из канала связи принята кодовая комбинация $X = 001110011$ в префиксном коде с неизвестной статистикой сообщений. Необходимо декодировать данную кодовую комбинацию, если известно, что длина передаваемого блока $n = 8,$ а разрядность префиксов равна четырём.

Решение. По префиксу находим, что число букв $x_2 = 3,$ а следовательно, число букв в $x_1 = 5.$ Находим максимальное число в пятом столбце треугольника Паскаля, не превосходящее число 19. Это $6 = C_{7-1}^5,$ следовательно, $i_5 = 7,$ находим разность 19 – 6 = 13. Далее находим максимальное число четвёртого столбца, не превосходящее 13. Это $5 = C_{6-1}^4,$ т. е. $i_4 = 6.$ Находим разность $13 - 5 = 8.$ Максимальным числом третьего столбца, не превосходящим 8, является $4 = C_{5-1}^3,$ т. е. $i_3 = 5.$ Находим разность 8 – 4 = 4. Максимальное число второго столбца, не превосходящее 4, – это $3 = C_{4-1}^2,$ т. е. $i_2 = 4.$ Находим разность 4 – 3 = 1. Максимальное число первого столбца, не превышающее 1, – это $1 = C_{2-1}^1,$ т. е. $i_1 = 2.$ Следовательно, декодируемое сообщение имеет вид

$$X = x_2 x_1 x_2 x_1 x_1 x_1 x_1 x_2,$$

что совпадает с условием примера 6.3.

6.3. Задачи и упражнения

6.3.1. Определить среднюю длину кодового слова при передаче x_i сообщений длиной μ_i и вероятностями появления $P(x_i)$, указанными в табл. 6.5.

Таблица 6.5

Сообщения	$P(x_i)$	Кодовые слова
x_1	0,35	11
x_2	0,25	10
x_3	0,20	010
x_4	0,15	0010
x_5	0,05	0001

Ответ: L = 2,6 символа.

6.3.2. По каналу связи без помех передаются пять сообщений с вероятностями $P(x_1)$ =0,30; $P(x_2)$ = 0,20; $P(x_3)$ = 0,40; $P(x_4)$ = $P(x_5)$ = 0,05 в двоичном коде. Определить нижнюю границу средней длины кодового слова.

Ответ: L= 1,95 символа.

6.3.3. По каналу связи без помех передаются в двоичном коде пять сообщений с вероятностями $P(x_1)$ = 1/2; $P(x_2)$ = 1/4; $P(x_3)$ = 1/8; $P(x_4)$ = 1/16, $P(x_5)$ =1/32. Определить нижнюю границу средней длины кодового слова и результаты сравнить с результатами задачи 6.3.2.

Ответ: L = 1,78; из сравнения следует, что если вероятности сообщений не являются целочисленными степенями числа m, точное достижение нижней границы невозможно.

6.3.4. Построить код Шеннона – Фано для восьми сообщений, имеющих следующие вероятности: 0,2; 0,2; 0,15; 0,13; 0,12; 0,10; 0,07; 0,03. Определить среднее число нулей, приходящихся на одно сообщение.

Ответ: L = 2,9 символа, что меньше, чем при равномерном кодировании (L = 3) и не очень далеко от энтропии: $H(X) = 2{,}806\ \frac{\text{дв.ед.}}{\text{сообщ.}}$.

6.3.5. Для передачи по каналу связи без шумов используется код, состоящий из двух букв a_1 и a_2, появляющихся с вероятностями $P(a_1)$ = 0,8 и $P(a_2)$ = 0,2. Применить метод Шеннона – Фано к кодированию всевозможных однобуквенных, двухбуквенных и трёхбуквенных сообщений. Определить среднюю длину в каждом случае и результаты сравнить между собой.

Ответ: $L(1)$ = 1; $L(2)$ = 0,78; $L(3)$ = 0,728; $H(A)$ = 0,722 $\frac{\text{бит}}{\text{буква}}$; кодирование блоками более выгодно, чем кодирование отдельных букв.

6.3.6. Построить код Хаффмана для восьми сообщений, имеющих следующие вероятности: 0,2; 0,2; 0,15; 0,13; 0,12; 0,10; 0,07; 0,03. Определить среднее число нулей и единиц, приходящихся на одно сообщение, и сравнить с результатами, полученными при решении задачи 6.3.4.

Ответ: L = 2,9; по экономичности в данном случае методы Шеннона – Фано и Хаффмана одинаковы.

6.3.7. Для передачи по каналу связи без шумов используется код, состоящий из двух букв a_1 и a_2, с вероятностями $P(a_1) = 0{,}8$ и $P(a_2) = 0{,}2$. Применить метод Хаффмана к кодированию всевозможных однобуквенных сообщений. Определить среднюю длину, скорость передачи, избыточность для каждого случая и сравнить их между собой, если длительности кодовых символов одинаковы и равны $\tau = 10^{-6}$ с.

Ответ: $L(1)$ = 1 бит; R_{t1} = 721900 бит/с; $R(1)$ = 0,2781; $L(2)$ = 0,78 бит; R_{t2} = 925513 бит/с; $R(2)$ = 0,0042; $L(3)$ = 0,728 бит; R_{t3} = 991620 бит/с; $R(3)$ = 0,002.

Кодирование трёхбуквенных комбинаций даёт возможность приблизиться к максимальной скорости передачи информации.

6.3.8. По каналу связи передаются четыре сообщения кодовыми комбинациями

x_1	x_2	x_3	x_4
001	01	0111	100

Определить, являются ли данные кодовые комбинации комбинациями префиксного кода.

Ответ: не являются.

6.3.9. По каналу связи передаётся последовательность 11011010110011001 0 комбинаций префиксного кода

x_1	x_2	x_3	x_4	x_5
11	10	011	010	001

Произвести декодирование данной последовательности.

Ответ: $x_1x_3x_4x_1x_5x_2x_4$.

6.3.10. Алфавит кода состоит из двух символов x_1 и x_2, появляющихся с вероятностями p и q. Построить префиксный код, если кодовые комбинации передаются блоками, состоящими из n = 3 символов.

Ответ: $\underline{00}$, $\underline{01}00$, $\underline{01}01$, $\underline{01}10$, $\underline{10}00$, $\underline{10}00$, $\underline{10}10$, $\underline{11}$, где подчеркнуты префиксы.

6.3.11. Закодировать блок $X = x_1x_2x_2x_1x_1x_1x_2x_1$ префиксным кодом при неизвестной статистике сообщений, если символы x_1 появляются с вероятностью p, а x_2 – с вероятностью q.

Ответ: X = 0011100001.

6.3.12. Из канала связи принята кодовая комбинация X = 0011100001 в префиксном коде с неизвестной статистикой сообщений. Декодировать данную кодовую комбинацию, если известно, что длина передаваемого блока равна n = 8, а разрядность префикса равна четырём.

Ответ: $X = x_1x_2x_2x_1x_1x_1x_2x_1$.

7. КОДИРОВАНИЕ ИНФОРМАЦИИ ПРИ ПЕРЕДАЧЕ ПО ДИСКРЕТНОМУ КАНАЛУ С ПОМЕХАМИ

7.1. Основные формулы

Число разрешённых кодовых комбинаций, если число информационных символов равно k:

$$N_1 = 2^k. \quad (7.1)$$

Общее число выходных кодовых комбинаций длиной n:

$$N_2 = 2^n. \quad (7.2)$$

Число запрещённых кодовых комбинаций (исправляемых ошибок):

$$N_3 = 2^n - 2^k. \quad (7.3)$$

Количество случаев появления необнаруживаемых ошибок

$$N_4 = 2^k(2^k - 1). \quad (7.4)$$

Количество случаев появления обнаруживаемых ошибок:

$$N_5 = 2^k(2^n - 2^k). \quad (7.5)$$

Общее количество возможных случаев передачи:

$$N_6 = 2^k \cdot 2^n. \quad (7.6)$$

Если производительность источника информации равна $\bar{H}(X)\,\dfrac{\text{бит}}{\text{с}}$, то скорость передачи после кодирования

$$V_k = \frac{\bar{H}(X)}{n}\,\frac{\text{бит}}{\text{с}}. \quad (7.7)$$

Минимальное кодовое расстояние для обнаружения ошибок кратностью m:

$$d_{\min} \geq m + 1. \quad (7.8)$$

Минимальное кодовое расстояние для исправления ошибок кратностью s:

$$d_{\min} \geq 2s + 1. \quad (7.9)$$

Минимальное кодовое расстояние для обнаружения и исправления ошибок:

$$d_{\min} \geq m + s + 1. \quad (7.10)$$

Число проверочных символов, если известна общая длина кодовой комбинации n:

$$r_{d=3} \geq E\log(n + 1), \quad (7.11)$$

$$r_{d=4} \geq E\log(2n). \qquad (7.12)$$

Число проверочных символов, если известно число информационных символов:

$$r_{d=3} = E\log((k+1) + E\log(k+1)), \qquad (7.13)$$

где E – знак округления в большую сторону.

Пример 7.1. Для передачи сообщения используется код Хэмминга $n = 7$, $k = 4$. Определить число разрешённых кодовых комбинаций, общее число n-разрядных кодовых комбинаций, число случаев появления необнаруженных ошибок, число случаев появления обнаруженных ошибок, число исправляемых ошибок и общее число возможных случаев передачи.

Решение. Число разрешённых кодовых комбинаций равно

$$N_1 = 2^k = 2^4 = 16.$$

Общее число кодовых комбинаций, которые могут быть представлены n-разрядным кодом:

$$N_2 = 2^n = 2^7 = 128.$$

Число случаев появления необнаруживаемых ошибок:

$$N_3 = 2^k \cdot (2^k - 1) = 2^4 \cdot (2^4 - 1) = 16 \cdot 15 = 240.$$

Число случаев обнаруживаемых ошибок:

$$N_4 = 2^k \cdot (2^n - 2^k) = 2^4 \cdot (2^7 - 2^4) = 16(128 - 16) = 1792.$$

Число случаев исправленных ошибок:

$$N_5 = (2^n - 2^k) = 2^7 - 2^4 = 128 - 16 = 112.$$

Общее число возможных случаев передачи:

$$N_6 = 2^k \cdot 2^n = 2^4 \cdot 2^7 = 16 \cdot 128 = 2048.$$

Пример 7.2. Определить минимальное кодовое расстояние d, если код должен обнаруживать ошибки кратностью $m = 2$, исправлять ошибки кратностью $S = 1$ или обнаруживать и исправлять ошибки указанной кратности.

Решение. При обнаружении ошибок кратностью $m = 2$

$$d_{\min} = m + 1 = 2 + 1 = 3.$$

При исправлении ошибок кратностью $S = 1$

$$d_{\min} = 2S + 1 = 2 \cdot 1 + 1 = 3.$$

При обнаружении и исправлении ошибок

$$d_{\min} = S + m + 1 = 1 + 2 + 1 = 4.$$

7.2. Общие правила построения корректирующих кодов

7.2.1. Образующая матрица M систематического кода состоит из единичной матрицы размерностью $k \times k$ и приписанной к ней справа матрицы дополнений размерностью $k \times r$. Причём вес каждой строки матрицы дополнений должен быть не меньше чем $d_{\min} - 1$.

$$M = \begin{Vmatrix} 1 & 0 & \cdots & 0 & b_{11} & b_{12} & \cdots & b_{1r} \\ 0 & 1 & \cdots & 0 & b_{21} & b_{22} & \cdots & b_{2r} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & b_{k1} & b_{k2} & \cdots & b_{kr} \end{Vmatrix}. \qquad (7.14)$$

Проверочная матрица N строится из образующей матрицы M следующим образом. Строками матрицы N являются столбцы матрицы дополнений образующей матрицы M. К полученной матрице дописывается справа единичная матрица размерностью $r \times r$.

$$N = \begin{Vmatrix} b_{11} & b_{21} & \cdots & b_{k1} & 1 & 0 & \cdots & 0 \\ b_{12} & b_{22} & \cdots & b_{k2} & 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ b_{1r} & b_{2r} & \cdots & b_{kr} & 0 & 0 & \cdots & 1 \end{Vmatrix}. \qquad (7.15)$$

Единицы, стоящие в каждой строке, однозначно определяют, какие символы должны участвовать в определении значения контрольного разряда. Причём единицы в единичной матрице N определяют номера контрольных разрядов.

Декодирование систематических кодов осуществляется с учётом правил кодирования.

7.2.2. Проверочные элементы в рекуррентном коде формируются путём сложения по модулю два двух информационных элементов, отстоящих друг от друга на шаг сложения, равный b.

b=2

Информационные элементы 0 0 0 0 1 1 1 0 1…

Проверочные элементы 0 0 1 1 0 1 0…

В данном коде после каждого информационного элемента следует проверочный элемент.

Процесс декодирования заключается в выработке проверочных элементов из информационных, поступивших на декодер, и их сравнении с проверочными символами, пришедшими из канала связи. В результате сравнения вырабатывается корректирующая последовательность, которая и производит исправление информационных элементов.

7.2.3. При построении свёрточных кодов поток данных разбивается на блоки длиной K_0 символов, которые называются кадрами информационных символов (КИС). КИС кодируются кадрами кодовых символов длиной n_0. При этом кодирование КИС в кадр кодового слова производится с учётом предшествующих m кадров информационных символов. Процедура кодирования, таким образом, связывает между собой последовательные кадры кодовых слов. Передаваемая последовательность становится одним полубесконечным кодовым словом.

Пример 7.3. Определить число контрольных символов в коде, позволяющем обнаруживать двойные ошибки, если число информационных символов $k = 7$.

Решение. Определим минимальное кодовое расстояние:

$$d_{\min} = m + 1 = 2 + 1 = 3.$$

Тогда число контрольных символов

$$r_{d=3} \geq E\log\big((k+1) + E\log(k+1)\big) = E\log\big((7+1) + E\log(7+1)\big) =$$
$$= E\log(8 + E\log 8) = E\log(8+3) = 4.$$

Пример 7.4. Получить алгоритм кодирования и декодирования кодовых комбинаций в систематическом коде, позволяющим обнаруживать двойные или исправлять одиночные ошибки, если число информационных символов $k = 3$.

Решение. Определим минимальное кодовое расстояние:

$$d_{\min} = 2S + 1 = m + 1 = 2 \cdot 1 + 1 = 2 + 1 = 3.$$

Число контрольных символов

$$r_{d=3} \geq E\log((k+1) + E\log(k+1)) =$$
$$= E\log((3+1) + E\log(3+1)) = E\log(4+2) = 3.$$

Строим образующую матрицу.

$$M = \begin{Vmatrix} 100011 \\ 010101 \\ 001111 \end{Vmatrix}.$$

Из образующей матрицы строим проверочную:

$$N = \begin{array}{c} a_1 a_2 a_3 a_4 a_5 a_6 \\ \begin{Vmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{Vmatrix} \end{array}.$$

Из проверочной матрицы получаем алгоритм образования контрольных символов:

$$a_4 = a_2 \oplus a_3;$$
$$a_5 = a_1 \oplus a_3;$$
$$a_6 = a_1 \oplus a_2 \oplus a_3.$$

На приёмной стороне производятся S_i проверки, которые составляются на основании алгоритма кодирования:

$$S_1 = a_2 \oplus a_3 \oplus a_4;$$
$$S_2 = a_1 \oplus a_3 \oplus a_5;$$
$$S_3 = a_1 \oplus a_2 \oplus a_3 \oplus a_6.$$

Синдром $S_1 S_2 S_3$ однозначно указывает на номер искажёния разряда. Рассмотрим всевозможные состояния $S_1 S_2 S_3$:

S_1	S_2	S_3	
0	0	0	– искажений нет;
0	0	1	– искажён a_6;
0	1	0	– искажён a_5;
1	0	0	– искажён a_4;
1	0	1	– искажён a_3;
1	1	1	– искажён a_2;
0	1	1	– искажён a_1.

Пример 7.5. На основании алгоритма, полученного в примере 7.4, закодировать кодовую комбинацию $G(X) = 111$ в систематическом коде с кодовым расстоянием $d_{\min} = 3$.

Решение. Определим значения контрольных символов. Для чего пронумеруем символы входной комбинации:

$$\begin{array}{c} \phantom{G(X) = {}} a_1 a_2 a_3 \\ G(X) = 1\ 1\ 1. \end{array}$$

Тогда

$$a_4 = 1 \oplus 1 = 0;$$
$$a_5 = 1 \oplus 1 = 0;$$
$$a_6 = 1 \oplus 1 \oplus 1 = 1.$$

В результате получим кодовую комбинацию

$$F(X) = 111001.$$

Ответ: $F(X) = 111001$.

Пример 7.6. На основании алгоритма для S_i проверок, полученных в примере 7.4, декодировать комбинацию $F'(X) = 110001 \rightarrow a_1a_2a_3a_4a_5a_6$.

Решение. Определим значения S_i проверок:

$$S_1 = 1 \oplus 0 \oplus 0 = 1;$$
$$S_2 = 1 \oplus 0 \oplus 0 = 1;$$
$$S_3 = 1 \oplus 1 \oplus 0 \oplus 1 = 1.$$

Синдром $S_1S_2S_3 = 111$ указывает, что искажён символ a_3. Изменяем значение этого символа на противоположный и получаем исправленную кодовую комбинацию

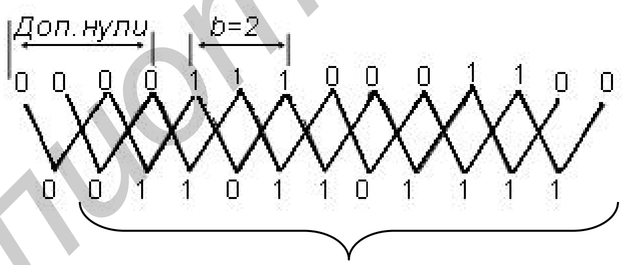
$$F(X) = 111001,$$

что совпадает с кодовой комбинацией примера 7.5.

Ответ: искажён a_3, $F(X) = 111001$.

Пример 7.7. Закодировать в рекуррентном коде последовательность информационных символов $G(X) = 1110001100$ с шагом сложения $b = 2$.

Решение. Кодирование произведём с помощью кодера, структурная схема которого представлена в [4]. Из схемы следует, что контрольные символы формируются с задержкой на b тактов. Поэтому перед информационной последовательностью, подлежащей кодированию, необходимо приписать $2b$ нулей, т. е. четыре. Контрольные символы образуются путём сложения по модулю два двух информационных символов, расположенных на расстоянии b друг от друга. Процесс образования контрольных символов показан на рис. 7.1.



Контрольные символы

Рис. 7.1. Схема построения рекуррентного кода с b = 2

В данном коде после каждого информационного символа следует проверочный символ. Таким образом, на выходе получим последовательность символов $F(X) = 10101101000111100101$.

Ответ: закодированная последовательность $F(X) = 1010110100\ 0111100101$.

Пример 7.8. Записать порождающий полином для импульсной переходной характеристики H = (11.00.10.11.00.00….).

Решение. $H(x) = 1 + x + x^4 + x^6 + x^7$.

7.3. Задачи и упражнения

7.3.1. По каналу связи передаются кодовые комбинации

$$x_1 = 1001001,\ x_2 = 1011011,\ x_3 = 0110101.$$

Определить минимальное кодовое расстояние.

Ответ: $d_{\min} = 2$.

7.3.2. В качестве информационных последовательностей используется двоичный $k = 2$ разрядный код. В канал связи передаются последовательности длиной $n = 9$. Определить число разрешённых кодовых комбинаций; общее число n-разрядных кодовых комбинаций; число случаев появления необнаруживаемых, обнаруживаемых и исправляемых ошибок; общее число возможных случаев передачи.

Ответ: $N_1 = 32$, $N_2 = 512$, $N_3 = 480$, $N_4 = 992$, $N_5 = 15360$, $N_6 = 16384$.

7.3.3. Определить число контрольных символов (r) в коде, позволяющем исправлять одинарную ошибку или обнаруживать двукратные искажения, если число информационных символов $k = 5$.

Ответ: $r = 4$.

7.3.4. Определить число контрольных символов в коде, позволяющем обнаруживать двойные и исправлять единичные ошибки в кодовых комбинациях длиной $n = 9$.

Ответ: $r = 5$.

7.3.5. По условиям задачи 7.3.2 определить процент обнаруживаемых ошибочных кодовых комбинаций по отношению к общему числу возможных случаев передачи; процент исправления ошибочных кодовых комбинаций по отношению к числу обнаруживаемых ошибочных комбинаций, а также избыточность кода.

Ответ: процент обнаружения составляет 93,75, процент исправления – 3,1, избыточность – 44 %.

7.3.6. Получить алгоритм кодирования и декодирования кодовых комбинаций в систематическом коде, позволяющем обнаруживать двойные или исправлять единичные ошибки, если число информационных символов $k = 5$.

7.3.7. На основании алгоритма, полученного в задаче 7.3.6, закодировать кодовую комбинацию $G(X) = 11101$ в систематическом коде с кодовым расстоянием $d_{\min} = 3$.

7.3.8. На основании алгоритма для S_i проверок, полученных в задаче 7.3.6, декодировать кодовую комбинацию $F'(X) = 111000011$.

7.3.9. Закодировать в рекуррентном коде последовательность информационных символов 1111000011111100 с шагом сложения $b = 3$. Привести функциональную электрическую схему кодирующего устройства и с её помощью пояснить процесс образования контрольных символов.

Ответ: $F(X) = 10101011010100011111101111110000$.

7.3.10. Из канала связи с помехами поступила последовательность $F'(X) = 10010111010100011111101111111000$, закодированная в рекуррентном коде с шагом сложения $b = 3$. Декодировать данную последовательность. Привести функциональную электрическую схему декодера и с её помощью пояснить процесс декодирования.

Ответ: $G(X) = 111100000111111 00$.

7.3.11. Из канала связи с помехами поступила последовательность 100101110101000111111011111110000, закодированная в рекуррентном коде с шагом сложения $b = 3$. Декодировать данную последовательность. Привести функциональную электрическую схему декодера и дать описание её работы.

7.3.12. Привести функциональную схему кодирующего устройства несистематического свёрточного кода, если частичные порождающие полиномы имеют вид $P_1(x) = x^4 + x^3 + x + 1$; $P_2(x) = x^4 + x^2 + 1$.

Закодировать с помощью данного устройства кодовую комбинацию $G(x)$, соответствующую числу 22, записанному в двоичном коде. Записать импульсную переходную характеристику кодера.

7.3.13. Привести функциональную схему кодирующего устройства систематического свёрточного кода для порождающего полинома $P(x) = x^4 + x^2 + x + 1$.

Закодировать с помощью данного устройства кодовую комбинацию $G(x)$, соответствующую числу 26, записанному в двоичном коде. Записать импульсную переходную характеристику кодера.

7.3.14. Привести функциональную схему кодирующего устройства несистематического свёрточного кода (8,4) для частичных порождающих полиномов $P_1(x) = x^3 + x^2 + x + 1$ и $P_2(x) = x^3 + x^2 + 1$. Проиллюстрировать работу кодера с помощью кодового дерева, если входная последовательность $G(x)$ представляет число 21, записанное в двоичном коде.

7.3.15. Привести функциональную схему кодирующего устройства систематического свёрточного кода (8,4) для порождающего полинома $P(x) = x^3 + x + 1$. Проиллюстрировать работу кодера с помощью кодового дерева, если входная последовательность $G(x)$ представляет число 27, записанное в двоичном коде.

7.3.16. Привести функциональную схему кодирующего устройства несистематического свёрточного кода (8,4) для частичных порождающих полиномов $P_1(x) = x^3 + x^2 + x + 1$ и $P_2(x) = x^3 + x^2 + 1$. Построить решётчатую диаграмму и с её помощью произвести кодирование информационной последовательности $G(x)$, соответствующей числу 19, записанному в двоичном коде.

7.3.17. Привести функциональную схему кодирующего устройства систематического свёрточного кода (8,4) для порождающего полинома $P(x) = x^3 + x + 1$. Построить решётчатую диаграмму и с её помощью произвести кодирование информационной последовательности $G(x)$, соответствующей числу 21, записанному в двоичном коде.

8. КОДИРОВАНИЕ КАК СРЕДСТВО КРИПТОГРАФИЧЕСКОГО ЗАКРЫТИЯ ИНФОРМАЦИИ

8.1. Правила шифрования

8.1.1. При шифровании методом простой подстановки буквы кодируемого сообщения прямо заменяются другими буквами того же или другого алфавита.

8.1.2. В методе Вижинера каждая буква используемого алфавита нумеруется. Затем под сообщением подписывается с повторением ключ, который представляет собой некоторое слово или просто последовательность букв. Цифровой эквивалент каждой буквы криптограммы определяется в результате сложения цифровых эквивалентов буквы сообщения и подписанной под ней буквы ключа с приведением по модулю, равным старшей цифре используемого алфавита. Полученная последовательность цифр заменяется буквами используемого алфавита.

8.1.3. При шифровании шифром с автоключом шифрование начинается с ключа, называемого первичным, и продолжается с помощью открытого текста или криптограммы, смещённой на длину первичного ключа.

8.1.4. При гомофонической замене одному символу открытого текста ставят в соответствие несколько символов шифртекста.

8.1.5. Полиалфавитная подстановка использует несколько алфавитов шифртекста.

8.1.6. Полиграммная замена формируется из одного алфавита с помощью специальных правил. При использовании шифра Плейфера алфавит располагается в матрице. Открытый текст разбивается на пары символов. Каждая пара символов открытого текста заменяется на пару символов и символов по определённым правилам.

8.1.7. При шифровании перестановкой открытый текст разбивается на группы определённой длины, а ключом задаётся порядок перестановки букв в группе. Наиболее сложные перестановки осуществляются по гамильтоновым путям.

8.1.8. В процессе шифрования по методу гаммирования цифровые эквиваленты знаков закрываемого сообщения складываются с псевдослучайной последовательностью чисел, именуемой гаммой, и приводятся по модулю k, где k – объём алфавита знаков. Таким образом, псевдослучайная последовательность выполняет здесь роль ключа. Данный метод используется для криптографического закрытия сообщений, уже выраженных в двоичном коде.

8.1.9. В стандарте DES используется произведение простых шифров, основанных на подстановках и перестановках.

8.1.10. Стандарт на шифрование данных (ГОСТ 28147–89) предусматривает использование режимов замены и гаммирования.

8.1.11. В криптографических системах с открытым ключом один ключ используется для шифрования, а другой – для расшифрования.

Пример 8.1. Зашифровать фразу «ОТКРЫТЫЙ ТЕКСТ» шифром Плейфера.

Решение. Воспользовавшись матрицей алфавита шифра Плейфера (табл. П.5.1), получим криптограмму

«ЛДЭЪРФР-ЛФС,ЬЛ».

Пример 8.2. Открытый текст «Я СТУДЕНТ ТРЕТЬЕГО КУРСА БГУИР.» зашифровать методом перестановки. Правила перестановки (ключ) группы из восьми букв с порядковыми номерами 1–2–3–4–5–6–7–8 переставить в порядок 5–6–2–1–3–7–4–8.

Решение. Разбиваем открытый текст на группы длиной по восемь элементов. В результате чего получим четыре группы:

Я СТУДЕНТ ТРЕТЬЕГО КУРСА БГУИР.

1234567812345678123456781234567

Осуществляя перестановки по заданному ключу, получим

«УД□ЯСЕТНЕТ□ТТЬРЕУРОГ□СКАИРБ□Г.У»

Пример 8.3. Зашифровать сообщение «МОЗГ» алгоритмом RSA, если открытый ключ (e,n) = (7.33), а секретный ключ (d,n) = (3.33).

Решение. Представим шифруемое сообщение как последовательность целых чисел, взятых из табл. П.6.1, «13–15–08–04» . Зашифруем эту последовательность, используя открытый ключ (7.33):

$$C_1 = 13^7(\mathrm{mod}\,33) = 62748517(\mathrm{mod}\,33) = 7,$$

$$C_2 = 15^7(\mathrm{mod}\,33) = 170859375(\mathrm{mod}\,33) = 27,$$

$$C_3 = 8^7(\mathrm{mod}\,33) = 2097152(\mathrm{mod}\,33) = 2,$$

$$C_4 = 4^7(\mathrm{mod}\,33) = 16384(\mathrm{mod}\,33) = 16.$$

В канал связи поступит криптограмма «07–27–02–16». Расшифруем это сообщение с помощью секретного ключа (3.33).

Получим:

$$M_1 = 7^3(\mathrm{mod}\,33) = 343(\mathrm{mod}\,33) = 13,$$

$$M_2 = 27^3(\mathrm{mod}\,33) = 19683(\mathrm{mod}\,33) = 15,$$

$$M_3 = 2^3(\mathrm{mod}\,33) = 8,$$

$$M_4 = 16^3(\mathrm{mod}\,33) = 4096(\mathrm{mod}\,33) = 4.$$

Таким образом, в результате дешифрации криптограммы получено исходное сообщение «13–15–08–04», что согласно табл. П.6.1 соответствует исходному тексту «МОЗГ». А теперь удостоверимся, что открытым ключом (7.33) невозможно правильно дешифровать криптограмму «07–27–02–16». Результат дешифровки:

$$M_1^* = 7^7(\mathrm{mod}\,33) = 823543(\mathrm{mod}\,33) = 28,$$
$$M_2^* = 27^7(\mathrm{mod}\,33) = 10460353203\ (\mathrm{mod}\ 33) = 3,$$
$$M_3^* = 2^7(\mathrm{mod}\,33) = 127(\mathrm{mod}\,33) = 28,$$
$$M_4^* = 16^7(\mathrm{mod}\,33) = 268435456(\mathrm{mod}\,33) = 25.$$

Таким образом, в результате дешифровки открытым ключом получим сообщение в цифровом эквиваленте «28–03–28–25», что не соответствует исходному «13–15–08–04».

8.2. Задачи и упражнения

8.2.1. Закодировать сообщение «КРИПТОГРАММА» методом простой подстановки, используя в качестве ключа буквы английского алфавита в соответствии с табл. 8.1.

Таблица 8.1

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Ю	Я
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Ответ: JPIORNDPALLA.

8.2.2. Зашифровать сообщение «ТЕЛЕМЕХАНИКА» кодом Вижинера ключом «ЭКЗАМЕН» .

Ответ: РРУЖШМДЮЧСЛН.

8.2.3. Произвести шифрование фамилии, имени и отчества студента, выполняющего контрольное задание, методом моноалфавитной простой подстановки. В качестве ключа взять буквы русского алфавита, сдвинутые на пять значений. Указать недостатки данного метода.

8.2.4. Зашифровать фамилию студента, выполняющего контрольное задание, с помощью квадрата Полибиуса, предварительно исходное сообщение представить буквами английского алфавита.

8.2.5. Зашифровать имя и отчество студента, выполняющего контрольное задание, кодом Виженера, в качестве ключа использовать фамилию. Указать достоинства данного метода.

8.2.6. Зашифровать фамилию студента, выполняющего контрольное задание, кодом Бофора $y_i = k_i - x_i$ (mod 33). Указать достоинства данного кода.

8.2.7. Зашифровать фамилию и отчество студента, выполняющего контрольное задание, с автоключом при использовании открытого текста. В качестве первичного ключа использовать своё имя.

8.2.8. Зашифровать фамилию и отчество студента, выполняющего контрольное задание, с автоключом при использовании криптограммы. В качестве первичного ключа использовать своё имя.

8.2.9. Зашифровать фамилию и имя студента, выполняющего контрольное задание, шифром Плэйфера.

8.2.10. Зашифровать фамилию, имя и отчество студента, выполняющего контрольное задание, методом усложнённой перестановки, если запись по строкам производится ключом К1: 4–1–5–3–6–2, а чтение по столбцам в соответствии с ключом К2: 2–4–1–3.

8.2.11. Зашифровать и дешифровать фамилию студента, выполняющего контрольное задание, методом гаммирования в двоичном коде, если псевдослучайная последовательность чисел (гамма) имеет вид 10–2–16–29–11–17–1––21–25–3–18–5–23.

8.2.12. Рассчитать и выбрать секретные ключи для тайной переписки между двумя абонентами без передачи ключей. Зашифровать и дешифровать число 17. Привести схему алгоритма шифровки и дешифровки.

8.2.13. Рассчитать и выбрать ключи для тайной переписки между двумя абонентами в системе RSA (криптосистема с открытым ключом). Зашифровать и дешифровать число 23. Привести схему алгоритма выбора ключей и процесса шифровки и дешифровки.

8.2.14. Рассчитать и выбрать ключи для системы с электронной подписью. Зашифровать и дешифровать сообщение, соответствующее числу 13. Привести схему алгоритма выбора ключей и процесса обмена информацией между двумя абонентами.

8.2.15. Получить хеш-код для сообщения, представляющего имя студента, выполняющего контрольное задание, при помощи хеш-функции с параметрами $p = 11$ и $q = 17$. Вектор инициализации H_0 выбирается студентом самостоятельно.

9. СЖАТИЕ ДАННЫХ

9.1. Основные понятия

Рассмотрим основные методы сжатия данных.

Вероятностные методы сжатия используют кодовые слова переменной длины. В основе вероятностных методов сжатия (алгоритмов Шеннона – Фано и Хаффмена) лежит идея построения «дерева», на «ветвях» которого положение символа определяется частотой его появления. Каждому символу присваивается код, длина которого обратно пропорциональна частоте появления этого символа.

При **арифметическом кодировании** строка символов заменяется действительным числом больше нуля и меньше единицы. Арифметическое кодирование позволяет обеспечить высокую степень сжатия, особенно в случаях, когда сжимаются данные, где частота появления различных символов сильно варьируется. Однако сама процедура арифметического кодирования требует мощных вычислительных ресурсов, т. к. активно использует нецелочисленную арифметику, и до недавнего времени этот метод мало применялся при сжатии передаваемых данных.

В основе **алгоритма словарей** лежит идея замены наиболее часто встречающихся последовательностей символов (строк) в передаваемом потоке ссылками на «образцы», хранящиеся в специально создаваемой таблице (словаре).

Кодирование повторов применяется в основном для сжатия растровых изображений (графических файлов). Один из вариантов метода RLE предусматривает замену последовательности повторяющихся символов на строку, содержащую этот символ, и число, соответствующее количеству его повторений. Применение метода кодирования повторов для сжатия текстовых файлов оказывается неэффективным. Поэтому в современных системах передачи кодированной цифробуквенной информации алгоритм RLE используется редко.

Пример 9.1. По методу Шеннона – Фано произвести сжатие символьной строки *aaaaaaaaaabbbbbbbbccccccdddddeeeefff*.

Решение. Первые биты кодов всех символов одной половины устанавливаются в 0, а второй – в 1. После этого каждую группу делят еще раз пополам и так до тех пор, пока в каждой группе не останется по одному символу.

Каждый символ исходной строки можно закодировать так, как показано в табл. 9.1.

Таблица 9.1

Символ	Частота появления	Код
a	10	11
b	8	10
c	6	011
d	5	010
e	4	001
f	3	000

Можно видеть, что если раньше каждый символ кодировался 8 битами, то теперь требуется максимум три бита.

Пример 9.2. Произвести сжатие символьной строки по методу Хаффмена. Исходные данные и результат сжатия приведены в табл. 9.2.

Пример 9.3. Закодировать арифметическим методом слово РАДИОВИЗИР.

Решение. Перед началом работы кодера соответствующий кодируемому тексту исходный интервал составляет [0–1).

Алфавит кодируемого сообщения содержит следующие символы (буквы): **{ Р, А, Д, И, О, В, З }**.

Определим количество (встречаемость, вероятность) каждого из символов алфавита в сообщении и назначим каждому из них интервал, пропорциональный его вероятности. С учётом того, что в кодируемом слове всего 10 букв, получим соответствующие интервалы (табл. 9.3).

Таблица 9.2

Символ	Частота появления	Порядок кодирования						Кодовое слово
c	22	22	22	26	32	42	58	01
e	20	20	20	22	26	32	42	00
h	16	16	16	20	22	26		111
i	16	16	16	16	20			110
a	10	10	16	16				100
k	10	10	10					1011
m	4	6						10101
b	2							10100

Таблица 9.3

Символ	Вероятность	Интервал
А	0,1	0–0,1
Д	0,1	0,1–0,2
В	0,1	0,2–0,3
И	0,3	0,3–0,6
З	0,1	0,6–0,7
О	0,1	0,7–0,8
Р	0,2	0,8–1

Располагать символы в таблице можно в любом порядке: по мере их появления в тексте, в алфавитном или по возрастанию вероятностей – это совершенно не принципиально. Результат кодирования при этом будет разным, но эффект – одинаковым.

Итак, перед началом кодирования исходный интервал составляет [0–1).

После просмотра первого символа сообщения **Р** кодер сужает исходный интервал до нового [0,8–1), который модель выделяет этому символу. Таким образом, после кодирования первой буквы результат кодирования будет находиться в интервале чисел [0,8–1).

Следующим символом сообщения, поступающим в кодер, будет буква **А**. Если бы эта буква была первой в кодируемом сообщении, ей был бы отведён интервал [0–0,1), но она следует за **Р** и поэтому кодируется новым *подынтервалом внутри уже выделенного для первой буквы*, сужая его до величины [0,80–0,82). Другими словами, интервал [0–0,1), выделенный для буквы **А**, располагается теперь внутри интервала, занимаемого предыдущим символом (начало и конец нового интервала определяются путём прибавления к началу предыдущего интервала произведения ширины предыдущего интервала на значения интервала, отведённые текущему символу). В результате получим новый рабочий интервал [0,80–0,82), т. к. предыдущий интервал имел ширину в 0,2 единицы и одна десятая от него есть 0,02.

Следующему символу **Д** соответствует выделенный интервал [0,1–0,2), что применительно к уже имеющемуся рабочему интервалу [0,80–0,82) сужает его до величины [0,802–0,804).

Следующим символом, поступающим на вход кодера, будет буква **И** с выделенным для неё фиксированным интервалом [0,3–0,6). Применительно к уже имеющемуся рабочему интервалу получим [0,8026–0,8032).

Продолжая в том же духе, имеем:

вначале		[0,0–1,0)
после просмотра	Р	[0,8–1,0)
	А	[0,80–0,82)
	Д	[0,802–0,804)
	И	[0,8026–0,8032)
	О	[0,80302–0,80308)
	В	[0,803032–0,803038)
	И	[0,8030338–0,8030356)
	З	[0,80303488–0,80303506)
	И	[0,803034934–0,803034988)
	Р	[0,8030349772–0,8030349880)

Результат кодирования: интервал [0,8030349772–0,8030349880].

Пример 9.4. Рассмотрим сжатие последовательности символов *ACCOUNTbbbbbbbMOUNT*, в которой *b* означает символ пробела.

Если для обозначения выполненного сжатия символов пробела модем использует специальный символ *Sc*, то между модемами будет передана последовательность символов *ACCONTSc7MOUNT*. Символ *Sc* в этой последовательности означает, что было произведено сжатие символов пробела, а число 7 указывает, сколько именно символов пробела заменено символом *Sc*. С помощью этой информации принимающий модем может восстановить данные.

Однако в последовательности передаваемых символов может встретиться пара символов *S* и *c*, которые являются частью данных, а не специальным символом *Sc*, обозначающим сжатие. Чтобы принимающий модем воспринимал эти символы как данные, передающий модем при обнаружении пары символов *Sc* добавляет в передаваемую последовательность ещё одну такую пару. Таким образом, если модем принял от терминала поток данных *XYZScABC*, то по телефонному каналу он передаст следующую последовательность символов: *XYZScScABC*. На принимающем модеме при обнаружении первого специального символа *Sc* проверяется следующий символ. Если им окажется не число, а ещё один такой символ, модем отбросит второй символ и восстановит первоначальный поток данных.

9.2. Задачи и упражнения

9.2.1. Произвести сжатие символьной строки *fggfsdrdrrsdfgsrgdsrgghhhrfr* по методу Шеннона – Фано и определить коэффициент сжатия.

9.2.2. Произвести сжатие символьной строки *fggfsdrdrrsdfgsrgdsrgghhhrfr* по методу Хаффмена и определить коэффициент сжатия.

9.2.3. Произвести сжатие строки *babbaabb* по методу сжатия данных LZW.

9.2.4. Произвести сжатие строки *aaaabbcccccdddddeeeefgggg* методом кодирования повторов.

9.2.5. Произвести арифметическое сжатие слова ТЕЛЕМЕХАНИКА. Проверить правильность полученного результата путём декодирования результирующего интервала.

10. ПРЕОБРАЗОВАНИЕ НЕПРЕРЫВНЫХ СООБЩЕНИЙ В ДИСКРЕТНЫЕ СИГНАЛЫ

10.1. Основные формулы

Функции $f(t)$, не содержащие частот F_{max}, полностью определяются своими мгновенными значениями в моменты времени, отстоящие друг от друга на $1/2F_{max}$, т. е.

$$\Delta t \le 1/(2F_{max})\,. \qquad (10.1)$$

Периодическая последовательность прямоугольных импульсов представляется рядом Фурье:

$$U(t) = U\left(\frac{1}{Q} + \sum_{k=1}^{\infty}\frac{2}{k\cdot\pi}\sin\frac{k\pi}{Q}\cos k\omega_1 t\right) = A_0 + \sum_{k=1}^{\infty} A_k \cos k\omega_1 t. \qquad (10.2)$$

Средняя мощность, выделяемая сигналом на активном сопротивлении, равном 1 Ом:

$$\bar{P} = A_0^2 + \sum_{k=1}^{\infty}\frac{A_k^2}{2}\,. \qquad (10.3)$$

Практическая полоса частот:

$$\Delta F = \mu/\tau, \qquad (10.4)$$

где $\mu = 0{,}5\ldots2$.

Пример 10.1. Рассчитать и построить спектр периодической последовательности прямоугольных импульсов амплитудой $U = 10$ В, периодом $T = 20$ мс и длительностью $\tau = 5$ мс. Определить практическую ширину спектра и среднюю мощность сигнала в этой полосе частот.

Решение. Определим скважность импульсов:

$$\mathrm{Q} = T/\tau = 20/5 = 4.$$

Частоту следования импульсов находим из выражения

$$F_1 = 1/T = 1000/20 = 50 \text{ Гц}.$$

Расчёт амплитуд составляющих спектр произведём по выражению (10.2):

– амплитуда постоянной составляющей

$$A_0 = U/Q = 10/4 = 2{,}5 \text{ В, частота } F_0 = 0 \text{ Гц;}$$

– амплитуда гармонической составляющей на частоте F_1, т. е. $k = 1$:

$$A_1 = \frac{2U}{\pi}\sin\frac{\pi}{Q} = \frac{2\cdot 10}{3{,}14}\sin\frac{180^\circ}{4} = 6{,}37\sin 45^\circ = 6{,}37\cdot 0{,}70 = 4{,}5 \text{ В, частота } F_1\text{=50 Гц;}$$

– амплитуда гармонической составляющей на частоте $2F_1$, т. е. $k = 2$:

$$A_2 = \frac{2U}{2\pi}\sin\frac{2\pi}{Q} = \frac{2\cdot 10}{2\cdot 3{,}14}\sin 90^\circ = 3{,}18 \text{ В, частота } 2F_1 = 100 \text{ Гц;}$$

– амплитуда гармонической составляющей на частоте $3F_1$, т. е. $k = 3$:

$$A_3 = \frac{2U}{3\pi}\sin\frac{3\pi}{Q} = \frac{2\cdot 10}{3\cdot 3{,}14}\sin 135^\circ = 1{,}49 \text{ В, частота } 3F_1 = 150 \text{ Гц;}$$

– амплитуда гармонической составляющей на частоте $4F_1$, т. е. $k = 4$:

$$A_4 = \frac{2U}{4\pi}\sin\frac{4\pi}{Q} = \frac{2\cdot 10}{4\cdot 3{,}14}\sin\pi = 0 \text{ В, частота } 4F_1 = 200 \text{ Гц.}$$

На этом расчёт закончим, т. к. в условии задачи требуется определить практическую полосу частот, которая определяется первым лепестком спектра.

По полученным данным построим спектр частот (рис. 10.1).

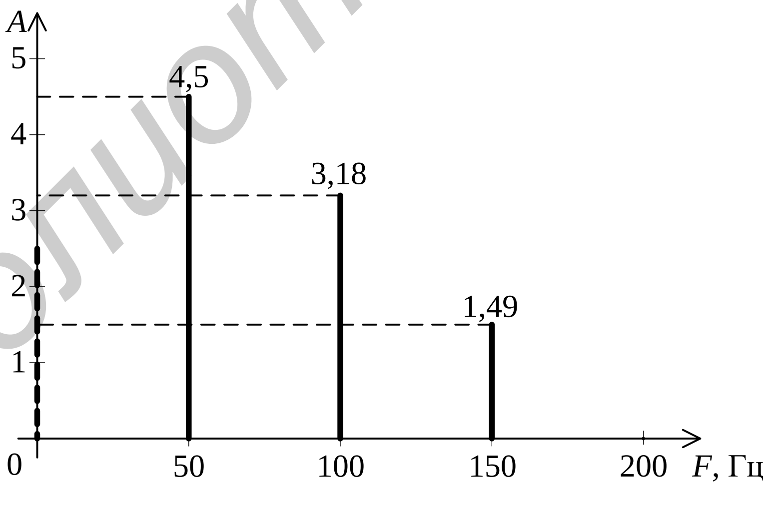


Рис. 10.1. Спектр периодической последовательности импульсов при $Q = 4$

Практическую полосу частот найдём из выражения (10.4) при $\mu = 1$:

$$\Delta F = 1/\tau = 1000/5 = 200 \text{ Гц.}$$

Средняя мощность составляющих, входящих в первый лепесток (ΔF = 200 Гц),

$$\overline{P} = A_0^2 + A_1^2/2 + A_2^2/2 + A_3^2/2 = (2,5)^2 + (4,5)^2/2 + (3,18)^2/2 + (1,49)^2/2 =$$
$$= 6,25 + 10,125 + 5,06 + 1,11 = 22,55 \text{ Вт.}$$

Ответ: $\Delta F = 200$ Гц; $\overline{P} = 22,55$ Вт.

Пример 10.2. По данным примера 10.1 определить импульсную и полную среднюю мощность сигнала, а также процент мощности, приходящийся на составляющие в практической полосе частот.

Решение. Импульсная мощность:

$$\overline{P}_{\text{имп}} = U^2 = 10^2 = 100 \text{ Вт.}$$

Полная средняя мощность:

$$\overline{P}_{\Sigma} = P_{\text{имп}} / Q = 100 / 4 = 25 \text{ Вт.}$$

Отношение средней мощности спектральных составляющих первого лепестка к полной средней мощности составляет

$$\overline{P} / \overline{P}_{\Sigma} = 22,25 / 25 = 0,902 = 90,2\ \%.$$

Ответ: $P_{\text{имп}} = 100$ Вт; $\overline{P}_{\Sigma} = 25$ Вт; $\overline{P} / \overline{P}_{\Sigma} = 90,2$ %.

Пример 10.3. Определить практическую ширину спектра периодической последовательности прямоугольных импульсов амплитудой U = 50 В и скважностью Q = 2, если требуется учесть все гармонические составляющие сигнала, амплитуды которых более 0,25 от амплитуды первой гармоники.

Решение. Число подлежащих учёту гармоник k может быть получено из выражения (10.2):

$$\frac{A_k}{A_1} = \frac{2U}{k\pi} \cdot \frac{\pi}{2U} = \frac{1}{k} = 0,25,$$

откуда k = 4.

Таким образом, практическая ширина спектра в рассмотренном примере оказывается равной $4F_1$, в ней размещается всего две гармоники (первая и третья) и постоянная составляющая.

Средняя мощность $\overline{P}_{k4}$, выделяемая в активном сопротивлении, равном 1 Ом, перечисленными составляющими, будет равна

$$\overline{P}_{k4} = \frac{U^2}{4} + \frac{1}{2}\left(\frac{2U}{\pi}\right)^2 + \frac{1}{2}\left(\frac{2U}{3\pi}\right)^2 = \frac{50^2}{4} + \frac{1}{2}\left(\frac{100}{3,14}\right)^2 + \frac{1}{2}\left(\frac{100}{9,42}\right)^2 \cong$$
$$\cong 625 + 507 + 56 = 1188 \text{ Вт.}$$

Средняя мощность, выделяемая на единичном сопротивлении всеми составляющими сигнала, будет равна

$$\overline{P}_{k\Sigma} = P_{\text{имп}} / Q = 50^2 / 2 = 1250 \text{ Вт.}$$

Таким образом, $\left(\bar{P}_{k4}/\bar{P}_{k\Sigma}\right)100 \cong 95\,\%$, т. е. составляющие, входящие в практическую полосу частот, выделяют в активном сопротивлении 95 % всей мощности сигнала.

Ответ: $\Delta F = 4F_1$; $\left(\bar{P}_{k4}/\bar{P}_{k\Sigma}\right) = 95\%$.

10.2. Задачи и упражнения

10.2.1. Рассчитать и построить спектр периодической последовательности прямоугольных импульсов со следующими параметрами: B = 15 В, $T = 30$ мс, $\tau = 10$ мс. Определить необходимую ширину спектра сигнала, если требуется учесть спектральные составляющие сигнала с амплитудой, равной 0,1 от амплитуды первой гармоники.

Ответ: 333 Гц.

10.2.2. Рассчитать и построить спектр сигнала, образованного суммой последовательностей прямоугольных импульсов со следующими параметрами: B_1 = 5 В; $\tau_1 = 10$ мс; T_1 = 40 мс; B_2 = 10 В; $\tau_2 = 5$ мс; T_2 = 40 мс; B_3 = 2,5 В; $\tau_3 = 5$ мс; T_3 = 40 мс. Определить ширину спектра сигнала.

Ответ: 200 Гц.

10.2.3. Определить среднюю мощность, выделяемую всеми составляющими периодической последовательности прямоугольных импульсов со скважностью, равной 5, и амплитудой, равной 15 В.

Ответ: $\bar{P}_{k\Sigma} = 45$ Вт.

10.2.4. По спектру, изображенному на рис. 10.2, найти временную функцию периодического сигнала. Определить период, среднюю и импульсную мощности сигнала, а также амплитуду постоянной составляющей.

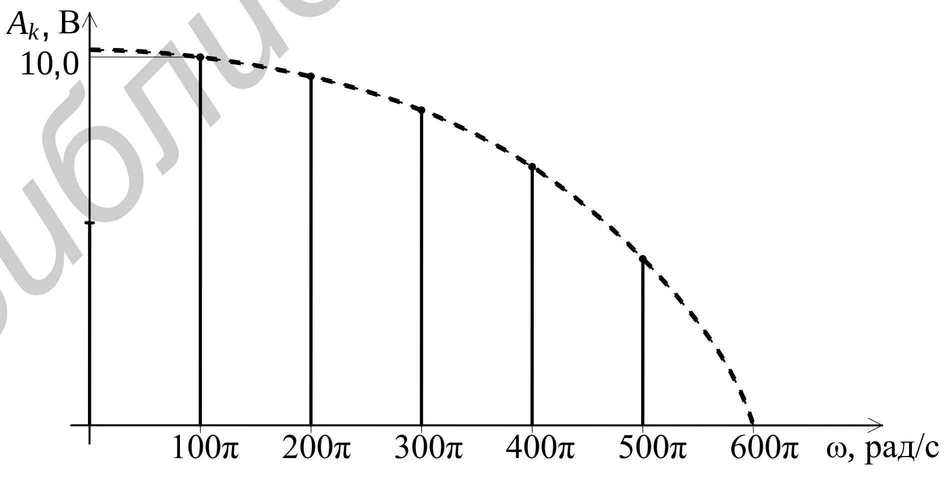


Рис. 10.2. Спектр сигнала

Ответ: T = 20 мс; $P_{имп} \cong 986$ Вт; $\bar{P}_{k\Sigma} \cong 164$ Вт; A_0 = 5,23 В.

10.2.5. Определить практическую ширину спектра периодической последовательности прямоугольных импульсов с амплитудой $B = 10$ В и периодом T, равным 2τ, если требуется учесть все гармонические составляющие сигнала, амплитуды которых более 0,333 амплитуды первой гармоники. Какая часть мощности выделяется в активном сопротивлении, если средняя мощность сигнала равна 50 Вт.

Ответ: $\Delta F = \dfrac{3}{2\tau}$; 94 %.

10.2.6. Определить практическую ширину спектра периодической последовательности прямоугольных импульсов с периодом T, равным 4τ, если требуется учесть все гармонические составляющие сигнала, амплитуды которых более 0,17 амплитуды первой гармоники.

Ответ: $\Delta F = \dfrac{2}{\tau}$.

10.2.7. Определить среднюю мощность, выделяемую в активном сопротивлении всеми составляющими периодической последовательности прямоугольных импульсов с амплитудой $B = 6$ В, периодом $T = 30$ мс и длительностью $\tau = 5$ мс.

Ответ: $\bar{P} = 6$ Вт.

10.2.8. Определить импульсную и среднюю мощность, выделяемую всеми составляющими периодической последовательности прямоугольных импульсов со скважностью, равной 3,5, и амплитудой, равной 7 В.

Ответ: $P_{\text{имп}} = 49$ Вт; $\bar{P} = 14$ Вт.

10.2.9. Определить период дискретизации непрерывной функции, ограниченной максимальной частотой $F_{\max} = 50$ Гц.

Ответ: $\Delta t \le 20$ мс.

10.2.10. Определить период опроса датчиков и скважность импульсов в каждом канале, если число каналов $n = 5$, максимальная частота спектра передаваемого сообщения $F_{\max} = 10$ Гц, а скважность суммарной последовательности импульсов равна двум.

Ответ: $\Delta t \le 100$ мс; $Q = 10$.

10.2.11. По условию задачи 10.2.10 рассчитать и построить спектр сигнала для одного канала, определить полные импульсную и среднюю мощности сигнала, а также среднюю мощность сигнала в полосе частот, равной $0{,}5/\tau$, если амплитуда импульсов в каждом канале равна 10 В.

Ответ: $P_{\text{имп}} = 100$ Вт; $\bar{P} = 10$ Вт.

ПРИЛОЖЕНИЕ 1

ЗНАЧЕНИЯ ДВОИЧНЫХ ЛОГАРИФМОВ ЦЕЛЫХ ЧИСЕЛ ОТ 1 ДО 194

Таблица П.1.1

x	$\log_2 x$	x	$\log_2 x$	x	$\log_2 x$
		30	4,907	60	5,907
1	0,000	31	4,954	61	5,931
2	1,000	32	5,000	62	5,951
3	1,585	33	5,044	63	5,977
4	2,000	34	5,087	64	6,000
5	2,322	35	5,129	65	6,022
6	2,585	36	5,170	66	6,044
7	2,807	37	5,209	67	6,066
8	3,000	38	5,248	68	6,087
9	3,170	39	5,285	69	6,109
10	3,332	40	5,322	70	6,129
11	3,459	41	5,358	71	6,150
12	3,585	42	5,392	72	6,170
13	3,700	43	5,426	73	6,190
14	3,807	44	5,459	74	6,209
15	3,907	45	5,492	75	6,229
16	4,000	46	5,524	76	6,248
17	4,087	47	5,555	77	6,267
18	4,170	48	5,585	78	6,285
19	4,248	49	5,615	79	6,304
20	4,322	50	5,644	80	6,322
21	4,392	51	5,672	81	6,340
22	4,459	52	5,700	82	6,358
23	4,524	53	5,728	83	6,375
24	4,585	54	5,755	84	6,392
25	4,644	55	5,781	85	6,409
26	4,700	56	5,807	86	6,426
27	4,755	57	5,833	87	6,443
28	4,807	58	5,858	88	6,459
29	4,858	59	5,883	89	6,470

Окончание табл. П.1.1

x	$\log_2 x$	x	$\log_2 x$	x	$\log_2 x$
90	6,492	125	6,966	160	7,322
91	6,508	126	6,977	161	7,331
92	6,524	127	6,989	162	7,340
93	6,539	128	7,000	163	7,349
94	6,555	129	7,011	164	7,358
95	6,570	130	7,022	165	7,366
96	6,585	131	7,033	166	7,375
97	6,600	132	7,044	167	7,384
98	6,615	133	7,055	168	7,392
99	6,629	134	7,066	169	7,401
100	6,644	135	7,077	170	7,409
101	6,658	136	7,087	171	7,418
102	6,672	137	7,098	172	7,426
103	6,687	138	7,109	173	7,435
104	6,700	139	7,119	174	7,443
105	6,714	140	7,129	175	7,451
106	6,728	141	7,140	176	7,459
107	6,741	142	7,150	177	7,468
108	6,755	143	7,160	178	7,476
109	6,768	144	7,170	179	7,484
110	6,781	145	7,180	180	7,492
111	6,794	146	7,190	181	7,500
112	6,807	147	7,200	182	7,508
113	6,820	148	7,209	183	7,516
114	6,833	149	7,219	184	7,524
115	6,845	150	7,229	185	7,531
116	6,858	151	7,238	186	7,539
117	6,870	152	7,248	187	7,547
118	6,883	153	7,257	188	7,555
119	6,895	154	7,267	189	7,562
120	6,907	155	7,276	190	7,570
121	6,919	156	7,285	191	7,577
122	6,931	157	7,295	192	7,585
123	6,943	158	7,304	193	7,592
124	6,954	159	7,313	194	7,600

ПРИЛОЖЕНИЕ 2

ЗНАЧЕНИЕ ФУНКЦИЙ $-p \cdot \log_2 p$ И $-\log_2 p$

Таблица П.2.1

p	$-\log_2 p$	$-p \cdot \log_2 p$	p	$-\log_2 p$	$-p \cdot \log_2 p$	p	$-\log_2 p$	$-p \cdot \log_2 p$
0,00		0,0000	0,35	1,5146	0,5301	0,70	0,5146	0,3602
0,01	6,6439	0,0664	0,36	1,4739	0,5306	0,71	0,4941	0,3508
0,02	5,6439	0,1129	0,37	1,4344	0,5307	0,72	0,4739	0,3412
0,03	5,0589	0,1518	0,38	1,3959	0,5304	0,73	0,4540	0,3314
0,04	4,6439	0,1858	0,39	1,3585	0,5298	0,74	0,4344	0,3215
0,05	4,3219	0,2161	0,40	1,3219	0,5288	0,75	0,4150	0,3113
0,06	4,0589	0,2435	0,41	1,2863	0,5274	0,76	0,3959	0,3009
0,07	3,9365	0,2686	0,42	1,2515	0,5256	0,77	0,3771	0,2903
0,08	3,6439	0,2915	0,43	1,2176	0,5236	0,78	0,3585	0,2796
0,09	3,4739	0,3127	0,44	1,1844	0,5211	0,79	0,3401	0,2687
0,10	3,3219	0,3322	0,45	1,1520	0,5184	0,80	0,3220	0,2575
0,11	3,1844	0,3503	0,46	1,1202	0,5153	0,81	0,3040	0,2462
0,12	3,0589	0,3671	0,47	1,0893	0,5120	0,82	0,2863	0,2348
0,13	2,9434	0,3826	0,48	1,0589	0,5083	0,83	0,2688	0,2231
0,14	2,8365	0,3971	0,49	1,0292	0,5043	0,84	0,2515	0,2113
0,15	2,7370	0,4105	0,50	1,0000	0,5000	0,85	0,2345	0,1993
0,16	2,6439	0,4230	0,51	0,9714	0,4954	0,86	0,2176	0,1871
0,17	2,5564	0,4346	0,52	0,9434	0,4906	0,87	0,2009	0,1784
0,18	2,4739	0,4453	0,53	0,9159	0,4854	0,88	0,1844	0,1623
0,19	2,3959	0,4552	0,54	0,8890	0,4800	0,89	0,1681	0,1496
0,20	2,3219	0,4644	0,55	0,8625	0,4744	0,90	0,1520	0,1368
0,21	2,2515	0,4728	0,56	0,8365	0,4684	0,91	0,1361	0,1238
0,22	2,1844	0,4806	0,57	0,8110	0,4623	0,92	0,1203	0,1107
0,23	2,1203	0,4877	0,58	0,7859	0,4558	0,93	0,1047	0,0974
0,24	2,0589	0,4941	0,59	0,7612	0,4491	0,94	0,0893	0,0839
0,25	2,0000	0,5060	0,60	0,7370	0,4422	0,95	0,0740	0,0703
0,26	1,9434	0,5053	0,61	0,7331	0,4350	0,96	0,0589	0,0565
0,27	1,8890	0,5100	0,62	0,6897	0,4276	0,97	0,0439	0,0426
0,28	1,8365	0,5142	0,63	0,6666	0,4199	0,98	0,0291	0,0286
0,29	1,7859	0,5179	0,64	0,6439	0,4121	0,99	0,0145	0,0143
0,30	1,7370	0,5211	0,65	0,6215	0,4040	1,00	0,0000	0,0014
0,31	1,6897	0,5238	0,66	0,5995	0,3957			
0,32	1,6439	0,5260	0,67	0,5778	0,3871			
0,33	1,5994	0,5278	0,68	0,5564	0,3784			
0,34	1,5564	0,5292	0,69	0,5353	0,3694			

ПРИЛОЖЕНИЕ 3

ОБЩИЙ ПОРЯДОК ПОДГОТОВКИ И ЗАЩИТЫ КОНТРОЛЬНОЙ РАБОТЫ

При выполнении контрольной работы необходимо соблюдать следующий порядок:

1) выполнить вариант, номер которого указывает преподаватель;

2) перед решением каждой задачи должно быть полностью приведено её условие;

3) решение задач должно сопровождаться пояснениями, ссылками на источники и выводами;

4) работа выполняется с помощью средств вычислительной техники на отдельных листах формата А4, которые должны быть сброшюрованы и снабжены титульным листом (рис. П.3.1).

5) текстовая часть и рисунки выполняются в соответствии с требованиями Стандарта предприятия «Дипломные проекты (работы) СТП 01-2013»;

6) в конце контрольной работы следует привести список использованной литературы;

7) работа на последней странице должна быть подписана студентом с указанием даты её выполнения;

8) законченная работа должна быть представлена преподавателю для проверки не позже десяти дней до начала экзаменационной сессии;

9) проверенная и получившая положительную оценку работа защищается студентом перед преподавателем;

10) в случае незачёта по расчётной работе студент обязан выполнить работу над ошибками и повторно предъявить её для проверки преподавателю;

11) студенты, не получившие зачёта по расчётной работе, к экзамену не допускаются.

Примечание. В задачах и упражнениях приняты обозначения буквами Z, K и L, где Z – последняя цифра номера группы, K – первая цифра индивидуального номера студента, L – вторая цифра индивидуального номера студента. Например, для студента группы 902402 с индивидуальным номером по зачётной книжке 25 (902402–25) Z = 2, K = 2 и L = 5.

Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Факультет заочного обучения

Кафедра систем управления

КОНТРОЛЬНАЯ РАБОТА

по дисциплине «Теория передачи информации»
для студентов специальности 1-53 01 07
«Информационные технологии и управление
в технических системах»

Выполнил студент группы 002402 В. М. Семёнов

Руководитель (должность) М. В. Танк

Минск 20XX

Рис. П.3.1. Пример оформления титульного листа

ПРИЛОЖЕНИЕ 4

ЗАДАЧИ И УПРАЖНЕНИЯ К КОНТРОЛЬНОЙ РАБОТЕ

1. Вероятности совместного появления $P(x_i, y_j)$ объединения двух ансамблей заданы в виде табл. П.4.1 (X и Y – две последние цифры номера зачётной книжки). Определить точные и средние количества неопределенности в совместном наступлении событий x_i и y_j, а также точные и средние количества неопределенности в y_j при известном исходе x_i.

Таблица П.4.1

y_j	x_i		
	x_1	x_2	x_3
y_1	0,1	0,11 + 0,0k	0,09
y_2	0,09	0,03	0,02
y_3	0,3 – 0,0k	0,16 + 0,0L	0,1 – 0,0L

2. По линии связи с помехами передаётся одно из двух сообщений x_1 или x_2 с вероятностями p и q соответственно, причём $p + q = 1$. На приёмном конце канала сигналу x_1 соответствует y_1, а сигналу x_2 соответствует y_2. Заданы условные вероятности правильного приёма $P(y_1/x_1) = \Delta$ и $P(y_2/x_2) = \delta$. Определить количество информации $I(Y,X)$.

3. По каналу связи передаётся один из двух сигналов x_1 или x_2 с одинаковыми вероятностями. На выходе сигналы x_1 и x_2 преобразуются в сигналы y_1 и y_2, причём из-за помех, которым одинаково подвержены сигналы x_1 и x_2, в передачу вносится ошибка так, что в среднем Z сигналов из 100 принимается неверно. Определить среднее количество информации на один сигнал. Сравнить её с количеством информации при отсутствии помех.

4. На вход линии связи, в которой действует помеха, поступает сообщение X в восьмиразрядном двоичном коде. На выходе линии связи зафиксирована искажённая последовательность Y. Определить точные и средние количества информации, содержащиеся в Y о X.

В качестве X принять число zkL, переведённое в двоичный эквивалент (при необходимости дополнить до восьмиразрядного дописыванием нуля), в качестве Y принять двоичное число X, циклически сдвинутое влево на z разрядов.

5. Определить энтропии $H(X)$, $H(Y)$, $H(X/Y)$, $H(X,Y)$, если задана матрица вероятностей состояний системы, объединяющей источники X и Y:

$$P(x_i, y_j) = \begin{vmatrix} 0{,}4+0{,}01\times k & 0{,}1-0{,}01\times k & 0 \\ 0 & 0{,}2 & 0{,}1-0{,}01\times L \\ 0 & 0 & 0{,}2+0{,}01\times L \end{vmatrix}.$$

6. Ансамбли событий X и Y объединены. Вероятности совместных событий (x_i, y_j) приведены в табл. П.4.2.

Таблица П.4.2

y_j	x_i		
	x_1	x_2	x_3
y_1	0,1 + 0,0k	0,2 – 0,0k	0,3 – 0,0L
y_2	0,25	0	0,15 + 0,0L

Определить:

1) энтропию ансамблей X и Y;

2) энтропию объединённого ансамбля (X,Y);

3) условные энтропии ансамблей;

4) количество информации, содержащейся в событиях Y относительно событий X.

7. Источник, используя алфавит из двух символов x_1 и x_2, вырабатывает последовательность, состоящую из этих символов. Вероятностные связи в данной последовательности имеют место между четырьмя символами. Определить все возможные состояния источника и порядок их следования в данной последовательности.

Исходную последовательность записать, представив число zkL в виде двоичного числа и поставив каждой его цифре в соответствие символ последовательности по следующему правилу: нулю – символ x_1, единице – символ x_2.

8. Источник сообщений вырабатывает три различных символа x_1, x_2, x_3 с соответствующими вероятностями 0,4; 0,5; 0,1.

Вероятности появления пар заданы в табл. П.4.3.

Определить энтропию и сравнить её с энтропией источника, у которого отсутствуют коррелятивные связи.

Таблица П.4.3

$x_i\,x_j$	x_1x_1	x_1x_2	x_1x_3	x_2x_1	x_2x_2	$x_2\,x_3$	x_3x_1	x_3x_2	x_3x_3
$P(x_i,x_j)$	0,1	0,2 + 0,0L	0,1	0,2 + 0,0k	0,3 – 0,0L	0	0,1 – 0,0k	0	0

9. Источник сообщений вырабатывает символы a и b. Условные вероятности имеют следующие значения: $P(a/b)$ = 0,1 + 0,0k; $P(b/b)$ = 0,9 – 0,0k; $P(b/a)$ = 0,7 + 0,0L; $P(a/a)$ = 0,3 – 0,0L. Определить энтропию источника.

10. Эргодический источник с энтропией $H(X)$ бит вырабатывает четыре различных символа. Найти отношение числа типичных к общему числу всевозможных последовательностей длиной M = 100 символов. Принять $H(X)$ равным десятичному числу Z, K, где Z – целая часть, а K – десятичная часть.

11. Источник вырабатывает два символа A и B с вероятностями $P(A)$ = 0,5 + 0,kL и $P(B)$ = 0,5 – 0,kL соответственно. Определить количество возможных последовательностей, содержащих n_A символов A, причём $n_A + n_B = 4$. Определить вероятность события, которое заключается в том, что в выработанной источником последовательности длиной M содержится n_A символов A.

12. Оценить, какую долю общего числа возможных последовательностей следует учитывать в практических расчётах, если эргодический источник, имеющий энтропию $H(X)$, вырабатывает 2^{z+3} различных символов, а длина последовательностей $M = 50$. Принять $H(X) = Z$, K – десятичное число.

13. Определить выигрыш в мощности при использовании источника с гауссовской плотностью распределения по сравнению с источником, имеющим в интервале (α, β) равномерную плотность распределения.

14. Вычислить относительную энтропию случайной величины X, распределённой по гауссовскому закону. Принять δ_x равным kL.

Примечание. Плотность вероятности случайной величины X, распределённой по гауссовскому закону, определяется выражением

$$W(x) = \frac{1}{\delta_x\sqrt{2\pi}} \exp\left(-\frac{x^2}{2\delta_x{}^2}\right).$$

15. Определить энтропию случайной величины, распределённой по экспоненциальному закону (принять $c = zL + k$):

$$W(X) = \begin{cases} ce^{-cx}, x \geq 0; \\ 0, x \leq 0; c > 0. \end{cases}$$

16. Произвести сжатие символьной строки, содержащей фамилию, имя и отчество студента, выполняющего контрольное задание, по методу Шеннона – Фано и определить коэффициент сжатия.

17. Произвести сжатие символьной строки, содержащей фамилию, имя и отчество студента, выполняющего контрольное задание, по методу Хаффмена и определить коэффициент сжатия.

18. Произвести сжатие и восстановление текстовой строки, содержащей отчество студента, выполняющего контрольное задание, методом арифметического кодирования.

19. Произвести сжатие текстовой строки, содержащей фамилию студента, выполняющего контрольное задание, по методу сжатия данных LZW.

20. Произвести сжатие текстовой строки *XXXXXYYYZZYYYYYXXXZZZZZ* по методу кодирования повторов, где *X*, *Y* и *Z* начальные буквы фамилии, имени и отчества студента, выполняющего контрольное задание, соответственно. Указать недостатки данного метода.

21. Произвести шифрование фамилии, имени и отчества студента, выполняющего контрольное задание, методом моноалфавитной простой подстановки. В качестве ключа взять буквы русского алфавита, сдвинутые на $k + L$. Указать недостатки данного метода.

22. Зашифровать фамилию студента, выполняющего контрольное задание, с помощью квадрата Полибиуса. Предварительно исходное сообщение представить буквами английского алфавита.

23. Зашифровать имя и отчество студента, выполняющего контрольное задание, кодом Виженера, в качестве ключа использовать фамилию. Указать достоинства данного метода.

24. Зашифровать фамилию студента, выполняющего контрольное задание, кодом Бофора $y_i = k_i - x_i \pmod{33}$. Указать достоинства данного кода.

25. Зашифровать фамилию и отчество студента, выполняющего контрольное задание, с автоключом при использовании открытого текста. В качестве первичного ключа использовать своё имя.

26. Зашифровать фамилию и отчество студента, выполняющего контрольное задание, с автоключом при использовании криптограммы. В качестве первичного ключа использовать своё имя.

27. Зашифровать фамилию и имя студента, выполняющего контрольное задание, шифром Плэйфера.

28. Зашифровать фамилию, имя и отчество студента, выполняющего контрольное задание, методом усложненной перестановки, если запись по строкам производится ключом *К*1: 4–1–5–3–6–2, а чтение по столбцам в соответствии с ключом *К*2: 2–4–1–3.

29. Зашифровать и дешифровать фамилию студента, выполняющего контрольное задание, методом гаммирования в двоичном коде, если псевдослучайная последовательность чисел (гамма) имеет следующий вид: 10–2–16–29–11–17–1–21–25–3–18–5–23.

30. Рассчитать и выбрать секретные ключи для тайной переписки между двумя абонентами без передачи ключей. Зашифровать и дешифровать число kL. Привести схему алгоритма шифровки и дешифровки.

31. Рассчитать и выбрать ключи для тайной переписки между двумя абонентами в системе RSA (криптосистема с открытым ключом). Зашифровать и дешифровать число kL. Привести схему алгоритма выбора ключей и процесса шифровки и дешифровки.

32. Рассчитать и выбрать ключи для системы с электронной подписью. Зашифровать и дешифровать сообщение, соответствующее числу kL. Привести схему алгоритма выбора ключей и процесса обмена информацией между двумя абонентами.

33. Получить хеш-код для сообщения, представляющего имя студента, выполняющего контрольное задание, при помощи хеш-функции с параметрами $p = 11$ и $q = 17$. Вектор инициализации H_0 выбирается студентом самостоятельно.

34. По непрерывному каналу передаётся сигнал, спектр которого ограничен полосой частот F Гц. Определить пропускную способность канала таким образом, чтобы погрешность передаваемого сигнала не превышала z процентов. Принять $F = zL + k$.

35. Непрерывный канал связи с пропускной способностью $C\ \frac{\text{дв.ед.}}{\text{с}}$ предназначен для передачи квантованного сигнала с полосой частот F Гц. Определить число различных уровней измеряемого сигнала и погрешность измерений. В качестве F взять kL, C принять равным $5 \times Z$, если амплитуда полезного сигнала равна Z вольт.

36. По радиолинии, на входе которой действует гауссовский шум с удельной мощностью 10^{-L} Вт/Гц, передаётся 2^{L} сообщения в течение 10^{-k} с. Определить минимальную мощность полезного сигнала на входе приёмника, если полоса пропускания приёмника равна 100 Гц.

37. В информационном канале используется сменно-качественный код, при котором запрещается передача подряд двух одинаковых символов. Алфавит кода состоит из n различных символов. Вероятности передачи всех разрешённых пар символов одинаковы. Длительности всех символов также одинаковы и равны $\tau = L$ мс. Определить скорость передачи информации. В качестве n взять $E[(z + L + k)/3]$, где E – знак округления в большую сторону.

38. В дискретном канале для передачи сообщений используются три различных символа с длительностями $\tau_1 = \tau_2 = 10(k + 1)$ мс и $\tau_3 = 20 - L$ мс. Определить пропускную способность канала.

39. В канал связи передаются сообщения длиной $n = 10$ элементов, каждый из которых может принимать $m = 4$ состояния с вероятностями $P_1 = 0{,}2 + 0{,}0k$, $P_2 = 0{,}3 - 0{,}0k$, $P_3 = 0{,}1 + 0{,}0L$, $P_4 = 0{,}4 - 0{,}0L$. Время передачи одного сообщения $\tau = 0{,}1\,z$. Определить скорость передачи информации и пропускную способность канала связи.

40. По бинарному каналу передаются два сообщения. В качестве сообщений принять числа zkL и zLk, представленные в двоичном эквиваленте (оба двоичных сообщения дополнить до 10-разрядных). Длительность каждого элемента сообщения $\tau = 10$ мс. Определить скорость передачи каждого сообщения и пропускную способность двоичного канала.

41. По каналу связи без помех передаются пять сообщений с вероятностью $P(x_1) = 1/2$, $P(x_2) = 1/4$, $P(x_3) = 1/8$, $P(x_4) = 1/16$, $P(x_5) = 1/32$ в двоичном коде. Определить нижнюю границу средней длины кодового слова.

42. Построить код Шеннона – Фано для восьми сообщений, имеющих следующие вероятности: $P(x_1) = 0{,}2 + 0{,}0k$, $P(x_2) = 0{,}2 + 0{,}0L$, $P(x_3) = 0{,}15 - 0{,}0k$, $P(x_4) = 0{,}13 - 0{,}0L$, $P(x_5) = 0{,}12 + 0{,}0z$, $P(x_6) = 0{,}10 - 0{,}0z$, $P(x_7) = 0{,}07$, $P(x_8) = 0{,}03$. Определить среднее число нулей и единиц, приходящихся на одно сообщение.

43. Для передачи по каналу связи без шумов используется код, состоящий из двух букв a_1 и a_2, появляющихся с вероятностями $P(a_1) = 0{,}K \times 0{,}L$ и $P(a_2) = 1 - P(a_1)$ соответственно. Применить метод Шеннона – Фано к кодированию всевозможных однобуквенных, двухбуквенных и трёхбуквенных сообщений. Определить среднюю длину в каждом случае и результаты сравнить между собой.

44. Построить код Хаффмена для восьми сообщений, имеющих следующие вероятности: $P(x_1) = 0{,}2 + 0{,}0k$, $P(x_2) = 0{,}2 + 0{,}0L$, $P(x_3) = 0{,}15 - 0{,}0k$, $P(x_4) = 0{,}13 - 0{,}0L$, $P(x_5) = 0{,}12 + z$, $P(x_6) = 0{,}10 - 0{,}0z$, $P(x_7) = 0{,}07$, $P(x_8) = 0{,}03$. Определить среднее число нулей и единиц, приходящихся на одно сообщение.

45. Получить алгоритм кодирования и декодирования кодовых комбинаций в систематическом коде, позволяющем обнаруживать двойные или исправлять одиночные ошибки, если число информационных символов $K = 5$. Закодировать по полученному алгоритму число kL.

46. Закодировать в рекуррентном коде последовательность информационных символов с шагом сложения $b = 3$. Процесс образования контрольных символов пояснить с помощью функциональной электрической схемы. В качестве последовательности принять число zkL, представленное в двоичном коде, с повторением дважды. Привести описание работы кодера.

47. Из канала связи с помехами поступила последовательность, закодированная в рекуррентном коде (последовательность записать, как в задании 46) с шагом сложения $b = 3$. Декодировать данную последовательность. Привести функциональную электрическую схему декодера и дать описание её работы.

48. Привести функциональную схему кодирующего устройства несистематического свёрточного кода, если частичные порождающие полиномы имеют следующий вид: $P_1(x) = x^4 + x^3 + x + 1$; $P_2(x) = x^4 + x^2 + 1$.

Закодировать с помощью данного устройства кодовую комбинацию $G(x)$, соответствующую числу kL, записанному в двоичном коде. Записать импульсную переходную характеристику кодера.

49. Привести функциональную схему кодирующего устройства систематического свёрточного кода для порождающего полинома $P(x) = x^4 + x^2 + x + 1$.

Закодировать с помощью данного устройства кодовую комбинацию $G(x)$, соответствующую числу kL, записанному в двоичном коде. Записать импульсную переходную характеристику кодера.

50. Привести функциональную схему кодирующего устройства несистематического свёрточного кода (8,4) для частичных порождающих полиномов $P_1(x) = x^3 + x^2 + x + 1$ и $P_2(x) = x^3 + x^2 + 1$. Проиллюстрировать работу кодера с помощью кодового дерева, если входная последовательность $G(x)$ представляет число kL, записанное в двоичном коде.

51. Привести функциональную схему кодирующего устройства систематического свёрточного кода (8,4) для порождающего полинома $P(x) = x^3 + x + 1$. Проиллюстрировать работу кодера с помощью кодового дерева, если входная последовательность $G(x)$ представляет число kL, записанное в двоичном коде.

52. Привести функциональную схему кодирующего устройства несистематического свёрточного кода (8,4) для частичных порождающих полиномов $P_1(x) = x^3 + x^2 + x + 1$ и $P_2(x) = x^3 + x^2 + 1$. Построить решетчатую диаграмму и произвести кодирование с ее помощью информационной последовательности $G(x)$, соответствующей числу kL, записанному в двоичном коде.

53. Привести функциональную схему кодирующего устройства систематического свёрточного кода (8,4) для порождающего полинома $P(x) = x^3 + x + 1$. Построить решетчатую диаграмму и с её помощью произвести кодирование информационной последовательности $G(x)$, соответствующей числу kL, записанному в двоичном коде.

ПРИЛОЖЕНИЕ 5

МАТРИЦА АЛФАВИТА ШИФРА ПЛЭЙФЕРА

Таблица П.5.1

А	Ж	Б	М	Ц	В
Ч	Г	Н	Ш	Д	0
Е	Щ	,	Х	У	П
·	З	Ъ	Р	И	Й
С	Ь	К	Э	Т	Л
Ю	Я	□	Ы	Ф	–

ПРИЛОЖЕНИЕ 6

ТАБЛИЦА КОДИРОВАНИЯ БУКВ РУССКОГО АЛФАВИТА

Таблица П.6.1

Буква	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л
Цифра	01	02	03	04	05	06	07	08	09	10	11	12

Буква	М	Н	О	П	Р	С	Т	У	Ф	К	Ц	Ч
Цифра	13	14	15	16	17	18	19	20	21	22	23	24

Буква	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	□ (пробел)
Цифра	25	26	27	28	29	30	31	32	33

ЛИТЕРАТУРА

1. Шулигин, В. И. Основы теории передачи информации. В 2 ч. Ч. 1 : Экономное кодирование : учеб. пособие / В. И. Шулигин. – Харьков : Харьковский авиационный институт, 2013. – 102 с.

2. Лидовский, В. В. Теория информации : учеб. пособие / В. В. Лидовский. – М. : Компания Спутник+, 2013. – 111 с.

3. Дмитриев, В. И. Прикладная теория информации / В. И. Дмитриев. – М. : Высш. шк., 1989. – 320 с.

4. Сорока, Н. И. Методический комплекс по теории передачи информации. Электронное издание / Н. И. Сорока, Г. А. Кривинченко. – Минск : БГУИР, 2009. – 210 с.

5. Игнатов, В. А. Теория информации и передачи сигналов / В. А. Игнатов. – М. : Радио и связь, 1991.– 280 с.

6. Шнайер, Брюс. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Брюс Шнайер. – М. : ТРИУМФ, 2002. – 816 с.

Св. план 2014, поз. 26

Учебное издание

Сорока Николай Ильич
Кривинченко Георгий Александрович

ТЕОРИЯ ПЕРЕДАЧИ ИНФОРМАЦИИ. СБОРНИК ЗАДАЧ

ПОСОБИЕ

Редактор *Е. С. Чайковская*
Корректор *Е. Н. Батурчик*
Компьютерная правка, оригинал-макет *Е. Д. Степусь*

Подписано в печать 02.06.2015. Формат 60×84 $^{1}/_{16}$. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. . Уч.-изд. л. 4,0. Тираж 150 экз. Заказ 219.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники».
Свидетельство о государственной регистрации издателя,
изготовителя, распространителя печатных изданий №1/238 от 24.03.2014,
№2/113 от 07.04.2014, №3/615 от 07.04.2014.
ЛП №02330/264 от 14.04.2014.
220013, Минск, П. Бровки, 6