МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Северо-Кавказский филиал
ордена Трудового Красного Знамени федерального государственного
бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

КАФЕДРА ОБЩЕНАУЧНОЙ ПОДГОТОВКИ

Бородин А.В.

ТЕОРИЯ ИНФОРМАЦИИ

Методическое пособие
для проведения лабораторных работ

направление подготовки 10.03.01
Информационная безопасность

Ростов-на-Дону
2022 г.

Бородин А.В. «Теория информации». Методическое пособие для проведения лабораторных работ (направление подготовки 10.03.01 - Информационная безопасность); Ростов-на-Дону: Северо-Кавказский филиал МТУСИ. 2022. – 26 с.

Составитель: доцент кафедры ОНП Бородин А.В.

Издание рассмотрено и утверждено
на заседании кафедры ОНП
29.08.2022 года (протокол № 1)

Дисциплина «Теория информации» изучается студентами направления 10.03.01 Информационная безопасность.

Теория информации является одним из важных курсов для подготовки бакалавров, будущая профессиональная деятельность которых связана с процессами обработки и защиты информации. Теория информации связана с изучением систем обработки и передачи информации, измерением количества информации, кодированием. Теория информации решает такие теоретические вопросы как, количественная оценка информации; анализ информационных характеристик источников сообщений и каналов связи и выявление возможности кодирования и декодирования сообщений, обеспечивающих максимально допустимую скорость передачи сообщений по каналу связи с помехами и без помех.

Данные методические указания предназначены для проведения лабораторных работ по курсу «Теория информации» для студентов направления подготовки 10.03.01 Информационная безопасность. Методические указания содержат теоретические сведения, задания и вопросы для самопроверки. Вопросы и задачи, рассматриваемые в данных методических указаниях, являются важными для формирования профессиональных компетенций будущего специалиста в сфере информационной безопасности.

ЛАБОРАТОРНАЯ РАБОТА №1

КОЛИЧЕСТВЕННАЯ ОЦЕНКА ИНФОРМАЦИИ

Цель работы

- Освоение навыков определения количества информации;
- Определение энтропии непрерывных сообщений.

Теоретические сведения

Важной задачей теории информации является количественная оценка передаваемых сообщений, которая называется количеством информации. Количество информации не отображает качественное содержание сообщения, а определяет меру его неопределенности.

Если алфавит некоторого источника сообщений состоит из m знаков, каждый из которых может служить элементом сообщения, то количество N возможных сообщений длины n равно числу перестановок с неограниченными повторениями:

$$N = m^n \tag{1.1}$$

В том случае, если все N сообщений от источника будут равновероятными, получение определенного сообщения равносильно для него случайному выбору одного из N сообщений с вероятностью P = 1/N.

Чем больше N, тем большая степень неопределенности характеризует этот выбор и тем более информативным можно считать сообщение.

Поэтому число N может служить мерой информации. С точки зрения теории информации, мера информации должна быть пропорциональна длине сообщения. В качестве меры неопределенности выбора состояния источника с **равновероятными состояниями** принимают логарифм числа состояний:

$$I = \log_2 N = \log_2 m^n = n \log_2 m \tag{1.2}$$

Эта логарифмическая функция характеризует количество информации.

Количество информации, приходящееся на один элемент сообщения (знак, букву), называется энтропией:

$$H = \frac{I}{n} = \frac{n \cdot \log m}{n} = \log m \tag{1.3}$$

Вычислительные системы основаны на элементах, имеющих два устойчивых состояния «0» и «1», поэтому выбирают основание логарифма равным двум. При этом единицей измерения количества информации, приходящейся на один элемент сообщения, является двоичная единица – **бит**. Двоичная единица (бит) является неопределенностью выбора из двух равновероятных событий.

Так как из $\log_2$ m = 1 следует m = 2, то ясно, что 1 бит – это количество информации, которым характеризуется один двоичный элемент при равновероятных состояниях 0 и 1.

Представленная оценка количества информации базируется на предположении о том, что все знаки алфавита сообщения равновероятны. в общем случае каждый из знаков появляется в сообщении с различной вероятностью. На основании статистического анализа известно, что в сообщении длины n знак x_i появляется n_i раз, т.е. вероятность появления знака:

$$P_i = \frac{n_i}{n},\ (i\ =\ 1, 2, 3, \dots m). \tag{1.4}$$

Все знаки алфавита составляют полную систему случайных событий, поэтому:

$$\sum_{i=1}^{m} P_i = 1 \tag{1.5}$$

Формулы Шеннона для количества информации и энтропии:

$$I = -n\sum_{i=1}^{m} P_i \log P_i$$

$$H = -\sum_{i=1}^{m} P_i \log P_i \tag{1.6}$$

Свойства энтропии.

1) Энтропия H - величина вещественная, неотрицательная и ограниченная, т.е. $H \geq 0$.
2) Энтропия равна нулю, если вероятность одного из элементов множестваравно единице.
3) Энтропия максимальна, если все знаки алфавита равновероятны, т.е.

$$H_{\max} = \log m \tag{1.7}$$

Избыточностью называется

$$r = 1 - \frac{H(X)}{H_{\max}(X)} = 1 - \frac{H(X)}{\log_2 N} \tag{1.8}$$

где X – случайная величина, N – число сообщений.

Пример1. Вычислить количество информации, содержащееся в телевизионном сигнале, соответствующем одному кадру развертки. В кадре 625 строк, а сигнал, соответствующий одной строке, представляет собой последовательность из 600 случайных по амплитуде импульсов, причем амплитуда импульса может принять любое из 8 значений с шагом в 1 В.

Решение. В рассматриваемом случае длина сообщения, соответствующая одной строке, равна числу случайных по амплитуде импульсов в ней: n = 600.

Количество элементов сообщения (знаков) в одной строке равно числу значений, которое может принять амплитуда импульсов в строке m = 8.

Количество информации в одной строке

$$I = n \log 8,$$

а количество информации в кадре

$$I_к = 625 * I = 625*600*\log 8 = 1{,}125*10^6 \text{ бит.}$$

Пример 2. Даны 27 монет равного достоинства, среди которых есть одна фальшивая с меньшим весом. Вычислить сколько раз надо произвести взвешивание на равноплечих весах, чтобы найти фальшивую монету.

Решение. Так как монеты внешне одинаковы, они представляют собой источник с равновероятными состояниями, а общая неопределенность ансамбля, характеризующая его энтропию

$H_1 = \log_2 27$.

Одно взвешивание способно прояснить неопределенность ансамбля, насчитывающего три возможных исхода (левая чаша весов легче, правая чаша весов легче, весы находятся в равновесии). Все исходы являются равновероятными (нельзя заранее отдать предпочтение одному из них), поэтому результат одного взвешивания представляет источник с равновероятными состояниями, а его энтропия

$H_2 = \log_2 3$ бит.

Так как энтропия отвечает требованию аддитивности и при этом

$H_1 = 3*H_2 = 3*\log_2 3$,

то для определения фальшивой монеты достаточно произвести три взвешивания. Алгоритм определения фальшивой монеты следующий. При первом взвешивании на каждую чашку весов кладется по девять монет. Фальшивая монета будет либо среди тех девяти монет, которые оказались легче, либо среди тех, которые не взвешивались, если имело место равновесие. Аналогично, после второго взвешивания число монет, среди которых находится фальшивая монета, сократится до трех. Последнее, третье, взвешивание дает возможность точно указать фальшивую монету.

Задание

Задача 1. Известно, что одно из k возможных сообщений, передаваемых равномерным двоичным кодом, содержит 3 бита информации. Определить, чему равно k.

Задача 2. Сообщения передаются в восьмеричном алфавите $m = 8$, по 4 символа в каждом сообщении. Всего передано 10 сообщений. Найти количество информации в 10 сообщениях.

Задача 3. Символы алфавита обладают двумя качественными признаками.а) Какое количество сообщений можно получить, комбинируя по 3, 4, 5 и 6 элементов в сообщении? б) Найти количество информации, приходящееся на один элемент указанных сообщений.

Задача 4. Некий алфавит состоит из трех букв X, Y, Z. Задание: а) составить максимальное количество сообщений, комбинируя по три буквы; б) какое количество информации приходится на одно такое сообщение; в) определить количество информации на символ первичного алфавита.

Задача 5. Устройство генерирует четыре частоты f1, f2, f3, f4. В шифраторе частоты комбинируются по три частоты в кодовой комбинации. а) Определить максимальное количество комбинаций, составленных их этих частот? б) Определить количество информации на одну кодовую посылку?

Задача 6. Дать описание всех возможных способов определения расположения шахматных фигур на доске. Определить количество информации для каждого способа.

Задача 7. Какое количество информации приходится на одну букву алфавита, состоящего из 16, 25, 32 букв?

Задача 8. Алфавит состоит из букв A, B, C, D. Заданы вероятности встречаемости букв, они равны соответственно PA=PB=0,25; PC=0,34; PD= 0,16. Найти количество информации, приходящееся на один символ сообщения, составленного из такого алфавита.

Задача 9. Задан алфавит, количество символов которого равно 5. Найти количество информации, приходящееся на один символ сообщения, составленногоиз этого алфавита при условии:

а) символы алфавита равновероятны; б) символы алфавита встречаются с вероятностями $P1=0,8$; $P2=0,15$; $P3=0,03$; $P4=0,015$; $P5=0,005$. Определить недогрузку символов во втором случае?

Задача 10. Определить количество информации в каждом сообщении (алфавит русский). а) Ра, ра, ра, ра, ра, ра, ра. б) Соблюдай правила техники безоопасности! Не стой под краном! в) Прощай же, море! Не забуду твоей торжественной красы и долго, долго слышать буду твой гул в вечерние часы.

Задача 11. Чему равна вероятность появления комбинации 10110 при передаче пятизначных двоичных кодов? Чему равно среднее количество информации, приходящейся на одну комбинацию? ($P=1/32=0, 0312$; $I=5$ бит).

Задача 12. Сообщения составлены из равновероятного алфавита, содержащего $m=128$ качественных признаков. Чему равно количество символов в принятом сообщении, если известно, что оно содержит 42 бита информации? Чему равна энтропия этого сообщения? ($n=6$; $H=7$ бит/символ).

Контрольные вопросы

1. Дать определение понятия «количество информации», привести формулу и пояснить все составляющие этой формулы.
2. В чем отличие формулы количества информации для равновероятных событий и разновероятных? Пояснить на примере, привести формулы.
3. Дать определение энтропии. Записать и пояснить формулу Шеннона.
4. Перечислить и доказать основные свойства энтропии.
5. Записать и пояснить формулу Хартли.
6. Что является единицей измерения количества информации, энтропии?Назвать и пояснить все единицы измерения количества информации.
7. Приведите примеры, в которых энтропия сообщения равна нулю, принимает максимальное значение?
8. Дать определение и пояснить правило сложения энтропий для независимых источников?
9. Пояснить как определяется количество информации непрерывных сообщений.
10. Записать и пояснить формулу избыточности кода.

ЛАБОРАТОРНАЯ РАБОТА №2

УСЛОВНАЯ ЭНТРОПИЯ И ЭНТРОПИЯ ОБЪЕДИНЕНИЯ

Цель работы

- Вычисление условной энтропии;
- Вычисление энтропии объединения.

Теоретические сведения

Условная энтропия в теории информации применяется для определения взаимозависимости между символами кодируемого алфавита. Это необходимо с целью определения потерь информации при передаче данных по каналам связи.

Для того, чтобы определить условную энтропию используются условные вероятности.

Пусть при передаче *n* сообщений символ А появился *m* раз, символ В поя- вился *l* раз, а символ А совместно с символом В появился *k* раз, то вероятность появления символа А будет Р(А) = *m/n*, вероятность появления символа В будет Р(В) = *l/n*, вероятность совместного появления символов А и В будет Р(АВ) = *k/n*. Условная вероятность появления символа А относительно В и наоборот будет

Р(А/В) = Р(АВ)/Р(В) = *k/l*,

Р(В/А) = Р(АВ)/Р(А) = *k/m*. (2.1)

Вероятность совместного появления символов А и В

Р(АВ) = Р(В)*Р(А/В) = Р(А)*Р(В/А). (2.2)

Условная энтропия символов А и В определяется выражением

$$H(b_j / a_i) = -\sum_j P(b_j / a_i) \log P(b_j / a_i)$$

$$H(a_i / b_j) = -\sum_j P(a_i / b_j) \log P(a_i / b_j) \qquad (2.3)$$

Индексы *i* и *j* выбраны для характеристики произвольного состояния источника сообщений А и адресата В.

Различают общую условную энтропию и частную. **Общая условная энтропия** сообщения В относительно сообщения А характеризует количество информации, содержащееся в любом символе алфавита, и определяется усреднением по всем символам, т.е. по всем состояниям с учетом вероятности появления каждого из состояний, и равна сумме вероятностей появления символов алфавита, умноженной на неопределенность, которая остается после того как адресат принял сигнал.

$$H(B/A) = -\sum_i P(a_i) H(b_j / a_i) = -\sum_i \sum_j P(a_i, b_j) \log P(b_j / a_i). \quad (2.4)$$

Если передавать m сигналов A и ожидать получить m сигналов B, влияниепомех в канале связи описывается канальной матрицей

	b1	b2	…	bj	…	bm
a1	**P(b1/a1)**	P(b2/a1)	…	P(bj/a1)	…	P(bm/a1)
a2	P(b1/a2)	**P(b2/a2)**	…	P(bj/a2)	…	P(bm/a2)
…	…	…	…	…	…	…
ai	P(b1/ai)	P(b2/ai)	…	**P(bj/ai)**	…	**P(bm/ai)**
…	…	…	…	…	…	…
am	P(b1/am)	P(b2/am)	…	P(bj/am)	…	P(bm/am)

Вероятности, расположенные по диагонали, определяют правильный прием сообщений, а остальные – ложный. Если описывать канал связи со стороны источника сообщений, то прохождение данного сигнала описывается распределением условных вероятностей вида P(bj / ai). Для сигнала a1 это будет распределение вида

$$P(b_1 / a_1) + P(b_2 / a_1) + ... + P(b_j / a_1) + ... + P(b_m / a_1). \quad (2.5)$$

Сумма вероятностей распределения всегда должна равняться единице. Потери информации, которые приходятся на долю сигнала a1, описываются с помощью частной условной энтропии вида

$$H(b_j / a_1) = -\sum_{j=1} P(b_j / a_1) \log P(b_j / a_1) \quad (2.6)$$

Суммирование производится по j, так как i-тое состояние (в данном случае) остается постоянным.

Чтобы учесть потери при передаче всех сигналов по данному каналу связи, надо просуммировать все частные условные энтропии. Для случая равновероятных появлений сигналов на выходе источника

$$H(B/A) = -\frac{1}{m} \sum_j P(b_j / a_i) \log P(b_j / a_i) \quad (2.7)$$

Для случая неравновероятного появления следует учесть вероятность появления каждого символа. Тогда общая условная энтропия будет

$$H(B/A) = -\frac{1}{m}\sum_i P(a_i)\sum_j P(b_j/a_i)\log P(b_j/a_i) \qquad (2.8)$$

Если мы исследуем канал связи со стороны приемника сообщений, то с получением сигнала bj предполагаем, что был послан какой-то из сигналов a1, a2, … ai, … am. При этом канальная матрица будет иметь вид

	b1	b2	…	bj	…	bm
a1	P(a1/b1)	P(a1/b2)	…	P(a1/bj)	…	P(a1/bm)
a2	P(a2/b1)	P(a2/b2)	…	P(a2/bj)	…	P(a2/bm)
…	…	…	…	…	…	…
ai	P(ai/b1)	P(ai/b2)	…	P(ai/bj)	…	P(ai/bm)
…	…	…	…	…	…	…
am	P(am/b1)	P(am/b2)	…	P(am/bj)	…	P(am/bm)

В этом случае единице должны равняться суммы условных вероятностей по столбцам канальной матрицы

$$P(a_1/b_j) + P(a_2/b_j) + ... + P(a_i/b_j) + ... + P(a_m/b_j) = 1 \qquad (2.9)$$

Частная условная энтропия

$$H(a_i/b_j) = -\sum_{i=1} P(a_i/b_j)\log P(a_i/b_j) \qquad (2.10)$$

Общая условная энтропия

$$H(A/B) = -\sum_J P(b_j)\sum_i P(a_i/b_j)\log P(a_i/b_j) \qquad (2.11)$$

Наравне с выражением (2.8) для вычисления общей условной энтропии может быть использовано выражение

$$H(B/A) = -\sum_i\sum_j P(a_i, b_j)\log P(b_j/a_i) \qquad (2.12)$$

Если заданы безусловные вероятности источника и канальная матрица, то можно вычислить энтропию приемника

$$H(B) = -\sum_J P(b_j)\log P(b_j) \qquad (2.13)$$

Энтропия объединения используется для вычисления энтропии совместного появления статистически зависимых сообщений. Например, передав сто раз цифру 5 по каналу связи с помехами, эта цифра была принята 90 раз, цифра 6 была принята 8 раз, цифра 4 – 2 раза. Неопределенность возникновения комбинаций может быть описана с помощью энтропии объединения. H(A, B) - неопределенность того, что будет послано

A, а принято B. Для ансамблей переданных сообщений A и принятых сообщений B энтропия объединения представляет собой сумму вида

$$H(A,B) = -\sum_i \sum_j P(a_i, b_j) \log P(a_i, b_j) \text{ бит/два символа} \qquad (2.14)$$

Энтропия объединения и условная энтропия связаны соотношениями

$$H(A,B) = H(A) + H(B/A) = H(B) + H(A/B)$$

$$H(B/A) = H(A,B) - H(A); H(A/B) = H(A,B) - H(B) \qquad (2.15)$$

Количество информации на символ сообщения, переданного по каналу связи, в котором влияние помех описывается при помощи энтропии объединения, вычисляется так

$$I(A,B) = H(A) + H(B) - H(B/A). \qquad (2.16)$$

Задание

Задача 1. При передаче каждых 100 сообщений длиной по 5 символов в сообщении символ К встречается 50 раз, символ Т – 30 раз. Совместно К и Т встречаются 10 раз. Определить условные энтропии Н(К/Т) и Н(Т/К).

Задача 2. При передаче текстовых сообщений наблюдения показали, что для слов со средней длиной в 6 букв на каждые 100 сообщений буква А встречается 80 раз, буква В встречается 50 раз, буквы А и В вместе встречаются 10 раз. Определить условную энтропию появления А, если в слове присутствует В, и условную энтропию появления В, если в слове присутствует А.

Задача 3. Определить общую условную энтропию сообщений, составленных из алфавита А, В, если вероятности появления символов в сообщении равны PA=0,6; PB=0,4. Условные вероятности переходов одного символа в другой равны P(B/A)=0,15; P(A/B)= 0,1.

Задача 4. В одной корзине два яблока и одна груша, в другой три яблока и одна груша, в третьей – два яблока и две груши. Определить полную условную энтропию возможности вытащить яблоко из любой корзины.

Задача 5. Влияние помех в канале связи описывается следующим распределением условных вероятностей

$$P(b/a) = \begin{vmatrix} 0,98 & 0,01 & 0,01 \\ 0,15 & 0,75 & 0,1 \\ 0,3 & 0,2 & 0,5 \end{vmatrix}$$

Вычислить полную условную энтропию сообщений, передаваемых по данному каналу связи:

а) при равновероятном появлении символов в сообщении; б) при вероятностях P(a1) = 0,7; P(a2) = 0,2; P(a3) = 0,1.

Задача 6. а) Определить частные условные энтропии для каждого символа алфавита a1, a2, a3, a4, если канал связи для передачи сообщений описывается следующей канальной матрицей

$$P(b/a) = \begin{vmatrix} 0,9 & 0,1 & 0 & 0 \\ 0,05 & 0,94 & 0,01 & 0 \\ 0 & 0,01 & 0,98 & 0,01 \\ 0 & 0 & 0,1 & 0,9 \end{vmatrix}$$

б) Найти общую условную энтропию для сообщений, передаваемых по каналу связи, описанному приведенной выше канальной матрицей, если символы источника равновероятны;

в) Найти общую условную энтропию для сообщений, передаваемых по каналу связи, если распределение вероятностей появления символов на выходе источника сообщений имеет вид P(a1) = 0,15; P(a2) = 0,32; P(a3) = 0,25; P(a4) = 0,28.

Задача 7. Определить общую условную энтропию сообщений, передаваемых по каналу связи, описанному канальной матрицей

$$P(a/b) = \begin{vmatrix} 0,9 & 0,1 & 0 & 0 \\ 0,05 & 0,84 & 0,01 & 0 \\ 0,03 & 0,06 & 0,98 & 0,1 \\ 0,02 & 0 & 0,01 & 0,9 \end{vmatrix}$$

Символы алфавита равновероятны.

Задача 8. Определить энтропию приемника сообщений, если вероятности появления символов на выходе источника сообщений равны P(a1) = 0,5; P(a2) = 0,3; P(a3) = 0,2 и канальная матрица имеет вид

$$P(b/a)=\begin{vmatrix} 0,97 & 0,03 & 0 \\ 0,01 & 0,98 & 0,01 \\ 0 & 0,04 & 0,96 \end{vmatrix}$$

Задача 9. Определить энтропию источника сообщений, если вероятности появления символов на входе приемника сообщений равны P(b1) = 0,1; P(b2) = 0,3; P(b3) = 0,4; P(b4) = 0,2 и канальная матрица имеет вид

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

Задача 10. Задана матрица вероятностей системы, объединенной в однусистему из двух взаимозависимых систем A и B

$$P(A/B)=\begin{vmatrix} 0,3 & 0 & 0 \\ 0,2 & 0,3 & 0,1 \\ 0 & 0,1 & 0 \end{vmatrix}$$

Определить полные условные энтропии H(B/A) и H(A/B).

Контрольные вопросы

1. Дать определение условной энтропии. Пояснить для чего она применяется в теории информации.
2. Что такое общая и частная условная энтропия?
3. Какие формулы используются для расчета условной энтропии?
4. Что такое канальная матрица и как она используется при решении задач в теории информации?
5. Пояснить, что такое энтропия объединения и для чего она используется.
6. Привести определение понятия «полной средней взаимной информация».
7. Пояснить, что подразумевают под дискретными системами передачи информации.
8. Дать определение непрерывных систем передачи информации. Привестиих характеристику.
9. Пояснить способ определения условной энтропии для непрерывной системы передачи сообщений.
10. Какие отличия есть при вычислении условной энтропии при равновероятном и неравновероятном появлении сигналов сообщения?

ЛАБОРАТОРНАЯ РАБОТА №3

ВЫЧИСЛЕНИЕ ИНФОРМАЦИОННЫХ ПОТЕРЬ ПРИ ПЕРЕДАЧЕ СООБЩЕНИЙ ПО КАНАЛАМ СВЯЗИ С ШУМАМИ

Цель работы

Освоение метода вычисления информационных потерь при передаче сообщений по каналам связи

Теоретические сведения

Потери информации в каналах связи с шумами описывают с помощью условной энтропии и энтропии объединения. Если помех нет или их уровень низкий настолько, что они не могут уничтожить сигнал или имитировать сигнал в отсутствие передачи, то при передаче ai будет получен сигнал bj, соответствующий переданному сигналу. События A и B жестко связаны, при этомусловная вероятность максимальна P(bj/ai) = 1, и условная энтропия H(A/B) = 0, так как log P(bj/ai) = 0. Для этого случая количество информации в принятом ансамбле сообщений B, равно энтропии передаваемых сообщений ансамбля A

$$I(B,A) = H(A) \tag{3.1}$$

Если уровень помех высок, то любой из принятых сигналов bj может соответствовать любому переданному сигналу ai, статистическая связь между переданными и принятыми сигналами отсутствует. Поэтому вероятности P(ai) и P(bj) являются вероятностями независимых событий и P(bj/ai) = P(bj); P(ai/bj) = P(ai).

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

$$= -\sum_i \sum_j P(b_j)P(a_i)\log P(a_i) = \sum_j P(b_j)H(A) = H(A) \tag{3.2}$$

Так как $\sum_j P(bj) = 1$, условная энтропия равна безусловной, а количество информации, содержащееся в B относительно A равно нулю

$$I(B,A) = H(A) – H(A/B) = 0 \tag{3.3}$$

Информационные характеристики реальных каналов связи лежат между этими двумя предельными случаями. При этом потери информации при передачеk символов по данному каналу связи

$$\Delta I = kH(A/B) \tag{3.4}$$

Из-за помех часть информации искажается, однако между переданными и принятыми сообщениями существует статистическая взаимосвязь. Это позволяет описывать информационные характеристики реальных каналов связи с помощью энтропии объединения статистически зависимых событий. Так как

$$H(A,B) = H(A) + H(A/B) = H(B) + H(B/A) \tag{3.5}$$

то потери в канале связи могут быть учтены с помощью энтропии объединенияследующим образом

$$I(B,A) = H(A) + H(B) - H(B,A). \tag{3.6}$$

Если использовать условную энтропию, то получим

$$I(B,A) = H(A) - H(A/B) = H(B) - H(B/A). \tag{3.7}$$

Для вычисления среднего количества информации, содержащегося в принятом ансамбле сообщений B относительно переданного ансамбля A в условиях действия помех, пользуются следующими выражениями

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

$$I(A,B) = \sum_i \sum_j P(b_j)P(a_i/b_j)\log\frac{P(a_i/b_j)}{P(a_i)} \tag{3.8}$$

Для вычислений часто применяют выражения

$$I(A,B) = \sum_j P(b_j)\sum_i \left[P(a_i/b_j)\log P(a_i/b_j) - P(a_i/b_j)\log P(a_i)\right] \tag{3.9}$$

$$I(B,A) = \sum_j P(a_i)\sum_i \left[P(b_j/a_i)\log P(b_j/a_i) - P(b_j/a_i)\log P(b_j)\right] \tag{3.10}$$

$$(A,B) = I(B,A) = \sum_i \sum_j P(a_i,b_j)\log P(a_i,b_j) - \sum_i \sum_j P(a_i,b_j)\log P(a_i)P(b_j) \tag{3.11}$$

Для полного описания канала связи необходимо задать: канальную матрицу вида P(ai/bj) и безусловные вероятности вида P(bj) или канальную матрицу вида P(bj/ ai) и безусловные вероятности P(ai), или канальную матрицу вида P(ai, bj). В последнем случае сумма значений матрицы по столбцам дает безусловные вероятности вида P(bj) $\left(\sum_j P(b_j) = 1\right)$, а сумма по строкам дает безусловные вероятности вида P(ai) $\left(\sum_i P(a_i) = 1\right)$.

Условные вероятности могут быть найдены из выражений

$$P(a_i/b_j) = \frac{P(b_j,a_i)}{P(b_j)}; P(b_j/a_i) = \frac{P(a_i,b_j)}{P(a_i)} \tag{3.12}$$

Зная условные и безусловные вероятности, можно найти энтропии H(A), H(B), H(A/B), H(B/A). Если уровень помех настолько высок, что с равной вероятностью можно ожидать переход любого символа источника сообщения в произвольный символ первичного алфавита, то энтропия канала связи будет равна log m, а количество информации I = H(A) – log m < 0, значение I может отрицательной величиной, что означает, что канал связи вносит дезинформацию.

Пример. Канал связи задан следующей канальной матрицей

$$P(b/a) = \begin{vmatrix} 0,98 & 0,01 & 0,01 \\ 0,1 & 0,75 & 0,15 \\ 0,2 & 0,3 & 0,5 \end{vmatrix}$$

Вычислить среднее количество информации, которое переносится одним символом сообщения, если вероятности появления символов источника сообщений равны P(a1) = 0,7; P(a2) = 0,2; P(a3) = 0,1. Определить информационные потери при передаче сообщения из 400 символов алфавита a1, a2, a3. Вычислить количество принятой информации.

Решение. Энтропия источника сообщений

$$H(A) = -\sum_{i=1}^{m} P(a_i) logP(a_i) = -(0,7\log 0,7 + 0,2\log 0,2 + 0,1\log 0,1) = 1,1568 \text{ бит/символ}$$

Общая условная энтропия

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

$$= -[0,7(0,98\log 0,98 + 2\cdot 0,01\log 0,01) + 0,2(0,75\log 0,75 +$$

$$+0,1\log 0,1 + 0,15\log 0,15) + 0,1(0,2\log 0,2 + 0,3\log 0,3 + 0,5\log 0,5)] = 0,473 \text{ (бит.символ)}.$$

Потери в канале связи

$$\Delta I = kH(B/A) = 400 \cdot 0,473 = 189,5 \text{ бит}.$$

Энтропия приемника

$$H(B) = -\sum_{j=1}^{m} P(b_j) logP(b_j);$$

$$P(b_1) = \sum_i P(a_i)P(b_1/a_i) = P(a_1)P(b_1/a_1) + P(a_2)P(b_1/a_2) + P(a_3)P(b_1/a_3) = 0,726;$$

$$P(b_2) = \sum_i P(a_i)P(b_2/a_i) = P(a_1)P(b_2/a_1) + P(a_2)P(b_2/a_2) + P(a_3)P(b_2/a_3) = 0,187;$$

$$P(b_1) + P(b_2) + P(b_3) = 1$$

$$H(B) = -(0,726\log 0,726 + 0,187\log 0,187 + 0,087\log 0,087) = 1,094 \text{ бит/символ.}$$

Среднее количество принятой информации

$$I = k\left[H(B) - H(B/A)\right] = kH(B) - \Delta I = 400 \cdot 1,094 - 189,5 = 248,1 \text{ бит.}$$

Задание

Задача 1. Найти информационные потери в канале связи, заданном канальной матрицей.

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

Задача 2. Определить информационные потери в канале связи. Заданном матрицей, если символы алфавита встречаются в сообщениях с равной вероятностью.

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

Задача 3. Определить среднее количество информации, содержащееся в принятом ансамбле сообщений относительно переданного, если сообщения составлены из алфавита A, B, C. Вероятности появления букв алфавита на выходе источника сообщений P(Ai) = P(Bi) = 0,25; P(Ci) = 0,5. Условные вероятности парвида bi/ai следующие

P(A/A)=0,97; P(A/B)=0,02; P(A/C)=0,01;
P(B/A)=0,015; P(B/B)=0,97; P(B/C)=0,01;
P(C/A)=0,015; P(C/B)=0,01 P(C/C)=0,98.

Проверить правильность результата.

Задача 4. Определить информационные потери в канале связи, заданном следующей канальной матрицей

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

Вероятности появления символов A, B, C, D на выходе источника сообщений соответственно равны PA = 0,4; PB = PC =PD =0,2. Определить среднее количество информации в принятых сообщениях относительно переданных.

Задача 5. Используя энтропию объединения, определить количество информации при передаче сообщений, построенных из алфавита 1, 2, 3, если априорные вероятности появления символов первичного алфавита равны между собой,а в результате действия помех 5% символов передаваемых сообщений могут с равной вероятностью перейти в любой другой символ данного алфавита.

Задача 6. Определить количество информации в принятом ансамбле сообщений, если заданы условные вероятности перехода одного сигнала в другой и вероятности появления сигналов на выходе источника сообщений Pa = 0,2; Pb = 0,3; Pc = 0,5; $P(a^1/a) = P(b^1/b) = P(c^1/c) = 0,97$; $P(b^1/a) = P(c^1/a) = P(a^1/b) = P(c^1/b) = P(a^1/c) = P(b^1/c) = 0,015$.

Контрольные вопросы

1. Чему равна энтропия объединения при независимости входящих в нее систем?
2. Как вычислить среднее количество информации в условиях помех?
3. Чему равна энтропия объединения при функциональной зависимости входящих в нее систем?
4. Чему равна взаимная информация между независимыми системами?
5. Может ли быть взаимная информация между двумя системами больше,чем наименьшая из энтропий этих систем?
6. Как вычислить информационные потери при передаче ее от одной системы к другой?

7. Что необходимо для полного описания канала связи?
8. Какие характеристики канала связи можно определить из канальной матрицы?

ЛАБОРАТОРНАЯ РАБОТА №4

ИНФОРМАЦИОННЫЕ ХАРАКТЕРИСТИКИ КАНАЛОВ СВЯЗИ

Цель работы

Вычисление скорости передачи информации и пропускной способности каналов связи.

Теоретические сведения

Основными характеристиками информационных систем являются такие понятия, как энтропия, скорость передачи информации, избыточность, пропускная способность канала связи. Для организации передачи информации по каналу связи надо учитывать не только количество информации, но и обеспечение передачи его в более короткий срок, не только хранение определенного количества, но и хранение с помощью минимального объема аппаратуры и т. д.

Предположим, что по каналу связи передали за время T количество информации, которое равно

$$I_T = H_T(X) - H_T(X/Y) \tag{4.1}$$

Можно вычислить скорость передачи данных

$$V = \frac{I_T}{T} = \frac{1}{T}\left(H_T(X) - H_T(X/Y) \right) = H(X) - H(X/Y) \tag{4.2}$$

Скорость передачи данных представляет собой количество информации, приходящееся на одно сообщение. Если количество сообщений равно *n*, то скорость передачи *n* сообщений в секунду будет определяться

$$V = n\left(H(X) - H(X/Y) \right) \tag{4.3}$$

В этом случае максимальная пропускная способность данного канала представляет собой *c*

$$c = \max V = n(H(X) - H(X/Y))_{\max} = n \cdot I(X,Y)_{\max} \tag{4.4}$$

Различают техническую скорость передачи и информационную скорость передачи информации.

Технической скоростью передачи информации по каналу связи называется число символов, передаваемых в единицу времени

$$V_T = \frac{1}{\tau} \text{ бод.} \tag{4.5}$$

Информационной скоростью передачи информации по каналу связи называется среднее количество информации, которое передается в единицу времени

$$V = nH \text{ бит/с.} \tag{4.6}$$

Если сообщения являются равновероятными, составленные из равновероятных взаимно независимых символов, то их информационная скорость равна

$$V = \frac{1}{\tau} \log m \tag{4.7}$$

Если символы в сообщении не равновероятны, то скорость определяется

$$V = -\frac{1}{\tau} \sum_i p_i \log p_i \tag{4.8}$$

В случае, если символы имеют разную длительность

$$V = -\frac{\sum_i p_i \log p_i}{\sum_i \tau_i p_i} \tag{4.9}$$

Пропускная способность канала передачи информации характеризуется максимальной энтропией

$$c_{\max} = \frac{H_{\max}}{\tau} \text{ бит/с.} \tag{4.10}$$

Для двоичного кода

$$c_{\max} = \frac{\log 2}{\tau} = \frac{1}{\tau} \text{ бит/с.} \tag{4.11}$$

Первая теорема Шеннона.

Пусть есть источник информации с энтропией H(X) и канал связи с пропускной способностью *c*, то если *c* > H(X), то всегда можно закодировать достаточно длинное сообщение таким образом, что оно будет передано без задержек. Если c < H(X), то передача информации без задержек невозможна.

Для всех практических каналов характерно наличие помех. На есть случаи, когда помехи малы, то вероятность искажения передаваемого сообщения равна нулю и можно считать, что все сигналы передаются верно. В этом случае среднее количество информации, переносимое одним символом

$$I(X,Y) = I(Y,X) = H(X), H_{\max} = \log m. \tag{4.12}$$

Следовательно, пропускная способность канала без помех за единицу времени

$$c = n \log m \tag{4.13}$$

Реальные каналы характеризуются тем, что в них всегда есть помехи. Пропускная способность дискретного канала с помехами вычисляется

$$c = n(H(Y) - H(Y/X))_{\max}, \text{ где } H(Y) = \log m. \tag{4.14}$$

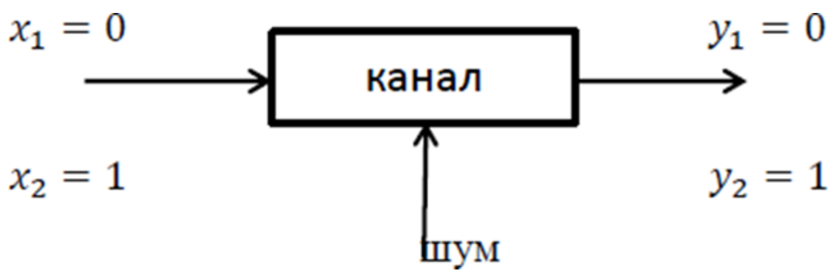
Вторая теорема Шеннона.

Для дан источник информации X, энтропия равна H(X), и пропускная способность равна c. Если H(X) > c , то справедливо, что при любом методе кодировании передача сообщений без задержек и искажений невозможна. Если H(X) < c , то любое достаточно длинное сообщение можно всегда закодировать так, что оно будет предано без задержек и искажений с вероятностью сколь угодно близкой к единице.

Пример 1. Дан дискретный симметричный канал без памяти, на вход которого поступают двоичные символы x1= 0; x2 = 1 с априорными вероятностями P(x1) = 0,85; P(x2) = 0,15. Переходные вероятности задаются соотношением

$$p(y_j / x_i) = \begin{cases} p, j \neq i \\ 1 - p, j = i \end{cases}$$

где p = 0,05 – это вероятность ошибки. Определить апостериорные вероятности.
Решение. Ситуация в канале характеризуется схемой



Так как вероятность ошибки p = 0,05, то вероятность правильного приема q = 1 - 0,05 = 0,95.

В таком канале каждый кодовый символ может быть принят с ошибочной вероятностью

$$p(y_1 / x_2) = p(y_2 / x_1) = p = 0,05.$$

Правильно переданная информация описывается

$$p(y_1 / x_1) = p(y_2 / x_2) = q = 0,95.$$

$$p(x_i / y_j) = \frac{p(x_i)p(y_j / x_i)}{p(y_j)} = \frac{p(x_i)p(y_j / x_i)}{\sum\limits_{i=1} p(x_i)p(y_j / x_i)}.$$

$$p(x_1 / y_1) = \frac{p(x_1)p(y_1 / x_1)}{p(x_1)p(y_1 / x_1) + p(x_2)p(y_1 / x_2)} = \frac{0,85 \cdot 0,95}{0,85 \cdot 0,95 + 0,15 \cdot 0,05} = 0,991$$

$$p(x_1 / y_2) = \frac{p(x_1)p(y_2 / x_1)}{p(x_1)p(y_2 / x_1) + p(x_2)p(y_2 / x_2)} = \frac{0,85 \cdot 0,05}{0,85 \cdot 0,05 + 0,15 \cdot 0,95} = 0,23$$

$$p(x_2 / y_1) = \frac{p(x_2)p(y_1 / x_2)}{p(x_2)p(y_1 / x_2) + p(x_1)p(y_1 / x_1)} = \frac{0,15 \cdot 0,05}{0,15 \cdot 0,05 + 0,85 \cdot 0,95} = 0,009$$

$$p(x_2 / y_2) = \frac{p(x_2)p(y_2 / x_2)}{p(x_2)p(y_2 / x_2) + p(x_1)p(y_2 / x_1)} = \frac{0,15 \cdot 0,95}{0,15 \cdot 0,95 + 0,85 \cdot 0,05} = 0,77.$$

Задание

Задача 1. Задан канал передачи информации без шума, по которому передается сообщение из ансамбля:

$$X = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ 0,34 & 0,46 & 0,16 & 0,04 \end{pmatrix}$$

Средняя длительность передачи одного элемента сообщения в канале τ=0,2 мс.

Найти: пропускную способность канала; скорость передачи информации в канале без шума.

Задача 2. Задан источник с вероятностями появления символов источника алфавита p(x1) = 0,5; p(x2) =0,25; p(x3) = 0,125; p(x4) = 0,125. Между соседними символами имеются корреляционные связи, заданные матрицей вероятностей

$$\begin{pmatrix} \frac{13}{16} & \frac{3}{16} & 0 & 0 \\ \frac{1}{8} & \frac{1}{2} & \frac{3}{8} & 0 \\ 0 & 0 & 0 & 1 \\ \frac{1}{2} & \frac{1}{4} & \frac{1}{4} & 0 \end{pmatrix}$$

Определить избыточность источника при статистической независимости символов и избыточность при зависимости символов.

Задача 3. Задан канал передачи информации, алфавит передаваемых сообщений содержит три символа с вероятностями p1 = 0,2; p2 = 0,7; p3 = 0,1. Чтобы передать информации по каналу без помех был применен равномерный двоичный код. Задана частота тактовых импульсов генератора 500 Гц. Найти пропускную способность канала и скорость передачи информации.

Задача 4. Задан канал связи, по которому передается три символа длительностью τ=0,01 с частотой следования F=1/τ. Матрица безусловных вероятностей источника сигналов

$$\begin{pmatrix} 0,4 \\ 0,3 \\ 0,3 \end{pmatrix}$$

Канал связи характеризуется при p1 = 0,01; p2 = 0,02; p3 = 0,97 матрицей условных вероятностей

$$P(Y/X) = \begin{pmatrix} p_3 & p_2 & p_1 \\ p_1 & p_3 & p_2 \\ p_2 & p_1 & p_3 \end{pmatrix}$$

Определить пропускную способность канала. Сравнить производительность источника и пропускную способность канала.

Задача 5. По двоичному симметричному каналу связи с помехами передаются два символа с вероятностями p(x1) = 0,75 и p(x2) = 0,25. Из-за наличия помех вероятность правильного приема каждого из сигналов уменьшается до 0,875. Длительность одного сигнала τ = 0,1 с.

Необходимо определить: производительность и избыточность источника; скорость передачи информации и пропускную способность канала связи.

Задача 6. Определить скорость передачи информации для сообщений английского алфавита, при этом известно, что буквы e, t, o, n передаются за 10 мс каждая, а остальные за 20 мс каждая. При решении применить данные о распределении вероятностей букв в английском тексте.

Контрольные вопросы

Дать определения и пояснения технической и информационной скорости передачи. Назвать единицы измерения и области применения этих понятий.

Дать определение информационной скорости для равновероятных сообщений. В чем заключается отличие от случая неравновероятных сообщений?

Дать определение пропускной способности канала без помех и с помехами, назвать единицы измерения, привести области применения этого понятия.

Сформулируйте и поясните первую и вторую теоремы Шеннона. В каких задачах нашли применение эти теоремы?

Литература

1. Белов В.М. Теория информации. Курс лекций. Учебное пособие для вузов. Москва: Горячая линия – Телеком, 2012.

2. Андреев А.Н., Краснов Р.П., Чепелев М.Ю. Теория электрической связи. Курс лекций. Учебное пособие для вузов. Москва: Горячая линия – Телеком, 2014.

3. Бурькова Е.В. Теория информации. Методические указания. Оренбургский государственный университет, 2018.