

ОСНОВНЫЕ ПОНЯТИЯ ТЕОРИИ ИНФОРМАЦИИ

Теорией информации называется наука, изучающая количественные закономерности, связанные с получением, передачей, обработкой и хранением информации. Возникнув в 40-х годах нашего века из практических задач теории связи, теория информации в настоящее время становится необходимым математическим аппаратом при изучении всевозможных процессов управления.

Черты случайности, присущие процессам передачи информации, заставляют обратиться при изучении этих процессов к вероятностным методам. При этом не удастся ограничиться классическими методами теории вероятностей, и возникает необходимость в создании новых вероятностных категорий. Поэтому теория информации представляет собой не просто прикладную науку, в которой применяются вероятностные методы исследования, а должна рассматриваться как раздел теории вероятностей.

Получение, обработка, передача и хранение, различного рода информации - неременное условие работы любой управляющей системы. В этом процессе всегда происходит обмен информацией между различными звеньями системы. Простейший случай - передача информации от управляющего устройства к исполнительному органу (передача команд). Более сложный случай - замкнутый контур управления, в котором информация о результатах выполнения команд передается управляющему устройству с тем же самым обратным обменом.

Любая информация для того чтобы быть переданной, должна быть соответственным образом «закодирована», т. е. переведена на язык специальных символов или сигналов. Сигналами, передающими информацию, могут быть электрические импульсы, световые или звуковые колебания, механические перемещения и т. д.

Одной из задач теории информации является **отыскание наиболее экономных методов кодирования**, позволяющих передать заданную информацию с помощью минимального количества символов. Эта задача решается как при отсутствии, так и при наличии искажений (помех) в канале связи.

Другая типичная задача теории информации ставится следующим образом: имеется **источник информации** (передатчик), непрерывно вырабатывающий информацию, и **канал связи**, по которому эта информация передается в другую инстанцию (**приемник**). Какова должна быть пропускная способность канала связи для того, чтобы канал справлялся со своей задачей, т. е. передавал всю поступающую информацию без задержек и искажений?

Ряд задач теории информации относится к определению объема запоминающих устройств, предназначенных для хранения информации, к способам ввода информации в эти запоминающие устройства и вывода ее для непосредственного использования.

Чтобы решать подобные задачи, нужно прежде всего научиться измерять количественно объем передаваемой или хранимой информации, пропускную способность каналов связи и их чувствительность к помехам (искажениям). Основные понятия теории информации позволяют дать количественное описание процессов передачи информации и наметить некоторые математические закономерности, относящиеся к этим процессам.

Энтропия как мера степени неопределенности состояния физической системы

Любое сообщение, с которым мы имеем дело в теории информации, представляет собой **совокупность сведений о некоторой физической системе**. Например, на вход автоматизированной системы управления производственным цехом может быть передано сообщение о нормальном или повышенном проценте брака, о химическом составе сырья или температуре в печи. На вход системы управления средствами противовоздушной обороны может быть передано сообщение о том, что в воздухе находятся две цели, летящие на определенной высоте, с определенной скоростью. На тот же вход может быть передано сообщение о том, что на определенном аэродроме в данный момент находится такое-то количество истребителей в боевой готовности, или что аэродром выведен из строя огневым воздействием противника, или что первая цель сбита, а вторая продолжает полет с изменённым курсом. Любое из этих сообщений описывает состояние какой-то физической системы.

Очевидно, если бы состояние физической системы было известно заранее, не было бы смысла передавать сообщение. **Сообщение приобретает смысл только тогда, когда состояние системы заранее не известно, случайно.**

ОСНОВНЫЕ ПОНЯТИЯ ТЕОРИИ ИНФОРМАЦИИ

В качестве объекта, о котором передается информация, мы будем рассматривать некоторую физическую систему X , которая случайным образом может оказаться в том или ином состоянии, т. е. систему, которой заведомо присуща какая-то степень

неопределенности.

Очевидно, сведения, полученные о системе, будут, вообще говоря, тем ценнее и содержательнее, чем больше была неопределенность системы до получения этих сведений («априори»). Возникает естественный вопрос: что значит «большая» или «меньшая» степень неопределенности и чем можно ее измерить?

Чтобы ответить на этот вопрос, сравним между собой две системы, каждой из которых присуща некоторая неопределенность.

В качестве первой системы возьмем монету, которая в результате бросания может оказаться в одном из двух состояний:

1) выпал герб и 2) выпала цифра. В качестве второй — игральную

кость, у которой шесть возможных состояний: 1, 2, 3, 4, 5 и 6.

Спрашивается, не определенность какой системы больше?

Очевидно, второй, так как у нее больше возможных состояний, в каждом из которых она может оказаться с одинаковой вероятностью. При бросании монеты тоже имеется два возможных состояния, но степень неопределенности гораздо

больше. Очевидно что степень неопределенности физической системы определяется не только числом её **ВОЗМОЖНЫХ СОСТОЯНИЙ**, но и **вероятностями** состояний.

Энтропия

Перейдем к общему случаю. Рассмотрим некоторую систему X , которая может принимать конечное множество состояний: x_1, x_2, \dots, x_n с вероятностями p_1, p_2, \dots, p_n , где $p_i = P(X \sim x_i)$

x_1	x_1	x_2	\dots	x_n
p_1	p_1	p_2	\dots	p_n

$$\sum_{i=1}^n p_i = 1.$$

$$H(X) = - \sum_{i=1}^n p_i \log p_i.$$

Энтропия

Эта табличка по написанию сходна с рядом распределения прерывной случайной величины X с возможными значениями x_1, x_2, \dots, x_n , имеющими вероятности p_1, p_2, \dots, p_n

И действительно, между физической системой X с конечным множеством состояний и прерывной случайной величиной много общего; для того чтобы свести первую ко второй, достаточно приписать каждому состоянию какое-то числовое значение (скажем, номер состояния). Подчеркнем, что для описания степени неопределенности системы совершенно неважно, как и именно значения x_1, x_2, \dots, x_n записаны в верхней строке таблицы; важны только количество этих значений и их вероятности.

В качестве меры априорной неопределенности системы (или прерывной случайной величины X) в теории информации применяется специальная характеристика, называемая

энтропией. Понятие энтропии является в теории информации основным.

Энтропией, системы состояний системы

$$H(X) = - \sum_{i=1}^n p_i \log p_i$$

ий вероятностей различных состояний, взятая с обратным знаком:

Свойства энтропии

Энтропия $H\{X\}$, как мы увидим в дальнейшем, обладает рядом свойств, оправдывающих ее выбор в качестве характеристики степени неопределенности. Во-первых, она обращается в нуль, когда одно из состояний системы достоверно, а другие — невозможны.

Во-вторых, при заданном числе состояний она обращается в максимум, когда эти состояния равновероятны, а при увеличении числа состояний — увеличивается. Наконец, и это самое главное, она **обладает свойством аддитивности**, т. е. **когда несколько независимых систем объединяются в одну, их энтропии складываются**.

Логарифм в формуле может быть взят при любом основании $a > 1$. Перемена основания равносильна простому умножению энтропии на постоянное число, а выбор основания равносильно выбору определенной единицы измерения энтропии. Если за основание выбрано число 10, то говорят о «десятичных единицах» энтропии, если 2 — о «двоичных единицах». На практике удобнее всего пользоваться логарифмами при основании 2 и измерять энтропию в двоичных единицах; это хорошо согласуется с применяемой в электронных цифровых вычислительных машинах двоичной системой счисления.

В дальнейшем мы будем везде, если не оговорено противное, под символом \log понимать двоичный логарифм.

Двоичная единица

Легко убедиться, что при выборе 2 в качестве основания логарифмов за единицу измерения энтропии принимается энтропия простейшей системы X , которая имеет два равновозможных состояния:

x_1	x_1	x_2
p_1	$\frac{1}{2}$	$\frac{1}{2}$

$$H(X) = -\left(\frac{1}{2} \log \frac{1}{2} + \frac{1}{2} \log \frac{1}{2}\right) = 1.$$

Определенная таким образом единица энтропии называется «двоичной единицей» и иногда обозначается bit (от английского «binary digit» — двоичный знак). Это энтропия одного разряда двоичного числа, если он с одинаковой вероятностью может быть нулем или единицей.

Энтропия системы с равновероятными состояниями

Измерим в двоичных единицах энтропию системы X , которая имеет n равновероятных состояний:

x_1	x_1	x_2	\dots	x_n
p_i	$\frac{1}{n}$	$\frac{1}{n}$	\dots	$\frac{1}{n}$

Имеем:
$$H(X) = -n \frac{1}{n} \log \frac{1}{n} = -\log 1 + \log n$$

или
$$H(X) = \log n,$$

т. е. **энтропия системы с равновероятными состояниями равна л о г а р и ф м у числа состояний.**

Например, для системы с восемью состояниями $H(X) = \log 8 = 3$. Докажем, что в случае, когда состояние системы в точности известно заранее, ее энтропия равна нулю. Действительно, в этом случае все вероятности p_1, p_2, \dots, p_n в формуле (18.2.2) обращаются в нуль, кроме одной —

например p_k , которая равна единице. Член $p_k \log p_k$ обращается в нуль, так как $\log 1 = 0$. Остальные члены то: $\lim_{p \rightarrow 0} p \log p = 0$. нуль, так как

Энтропия системы с **конечным множеством состояний** достигает максимума, когда все состояния **равновероятны**.

$$H_{\max}(X) = \log n,$$

максимальная энтропия системы равна:

т. е. максимальное значение энтропии системы числом состояний равно логарифму числа состояний и достигается, когда все состояния равновероятны.

Вычисление энтропии по формуле можно несколько упростить, если ввести специальную функцию:

Где логарифм берет вид: $H(X) = \sum_{i=1}^n \eta(p_i)$. Формула принимает

Определить энтропию физической системы, которая может оказаться в одном из четырех возможных состояний. Вероятности этих состояний равны соответственно 0,2; 0,3; 0,4; 0,1. Записываем условия в виде таблицы

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

По формуле имеем: $H(X) = \eta(0,2) + \eta(0,3) + \eta(0,4) + \eta(0,1)$.

$$H(X) = 0,4644 + 0,5211 + 0,5288 + 0,3322 \approx 1,85 \text{ (дв. ед.)}$$

Определить энтропию системы, состояние которой описывается прерывной случайной величиной X с рядом распределения

x_i	x_1	x_2	x_3	x_4	x_5
p_i	0,01	0,01	0,01	0,01	0,96

Решение. $H(X) = 4\eta(0,01) + \eta(0,96) \approx 0,322 \text{ (дв. ед.)}$.

Примеры

Пример 3. Определить максимально возможную энтропию системы, состоящей из трех элементов, каждый из которых может быть в четырех возможных состояниях.

Решение. Общее число возможных состояний системы равно

$$n = 4 \cdot 4 \cdot 4 = 64.$$

Максимально возможная энтропия системы равна $\log 64 = 6$ (дв. ед.).

Пример 4. Определить максимально возможную энтропию сообщения, состоящего из пяти букв, причем общее число букв в алфавите равно 32.

Решение.

Число возможных состояний системы $n = 32^5$.

Максимально возможная энтропия равна $5 \log 32 = 25$ (дв. ед.).

Энтропия сложной системы.

На практике часто приходится определять энтропию для сложной системы, полученной объединением двух или более простых систем.

Под объединением двух систем X и Y с возможными состояниями $\{x_1, \dots, x_p\}$ и $\{y_1, \dots, y_t\}$ понимается сложная система (X, Y) , состоящая из состояний (x_i, y_j) представляющих собой все возможные комбинации состояний $\{x_i\}$ и $\{y_j\}$ систем X и Y .

Очевидно, число возможных состояний системы (X, Y) равно $p \cdot t$. Обозначим P_{ij} в $P((X \sim x_i)(Y \sim y_j))$ то система (X, Y) будет в состоянии (x_i, y_j) :

Вероятности P_{ij}

$y_j \backslash x_i$	x_1	x_2	\dots	x_n
y_1	P_{11}	P_{21}	\dots	P_{n1}
y_2	P_{12}	P_{22}	\dots	P_{n2}
\vdots	\vdots	\vdots	\dots	\vdots
y_m	P_{1m}	P_{2m}	\dots	P_{nm}

таблицы (матрицы)

Теорема сложения энтропий

Найдем энтропию сложной системы. По определению она равна сумме произведений вероятностей всех возможных ее состояний на их логарифмы с обратным знаком:

$$H(X, Y) = - \sum_{i=1}^n \sum_{j=1}^m P_{ij} \log P_{ij} \quad \text{или, в других обозначениях} \quad H(X, Y) = \sum_{i=1}^n \sum_{j=1}^m \eta(P_{ij}).$$

Энтропию сложной системы, как и энтропии простой, тоже можно записать в форме математического ожидания $H(X, Y) = M[-\log P(X, Y)]$. Подставляя в (), получим $H(X, Y) = M[-\log P(X) - \log P(Y)]$, или

$$H(X, Y) = H(X) + H(Y),$$

т. е. при объединении независимых систем их энтропии складываются

Доказанное положение называется теоремой сложения энтропий.

Теорема сложения энтропий может быть легко обобщена на произвольное число

$$H(X_1, X_2, \dots, X_s) = \sum_{k=1}^s H(X_k).$$

Условная энтропия. Объединение зависимых систем

Если две системы X и Y объединяются в одну, то энтропия объединенной системы равна энтропии одной из ее составных частей плюс условная энтропия второй части относительно первой:

$$H(X, Y) = H(X) + H(Y|X),$$

Полная условная энтропия не может превосходить безусловную:

$$H(Y|X) \leq H(Y).$$

Степень неопределенности системы не может увеличиться оттого, что состояние какой-то другой системы стало известным.

Теорему об энтропии сложной системы легко можно распространить на любое число объединяемых систем:

$$H(X_1, X_2, \dots, X_s) = H(X_1) + H(X_2|X_1) + H(X_3|X_1, X_2) + \dots + H(X_s|X_1, X_2, \dots, X_{s-1}),$$

где энтропия каждой последующей системы вычисляется при условии, что состояние всех предыдущих известно.

Энтропия и информация

Энтропия была определена как мера неопределенности состояния некоторой физической системы. Очевидно, что в результате получения сведений неопределенность системы может быть уменьшена. Чем больше объем полученных сведений, чем они более содержательны, тем больше будет информация о системе, тем менее неопределенным будет ее состояние. **Естественно поэтому количество информации измерять уменьшением энтропии той системы, для уточнения состояния которой предназначены сведения.** Рассмотрим некоторую систему X , над которой производится наблюдение, и оценим информацию, получаемую в результате того, что состояние системы X становится полностью известным. До получения сведений (априори) энтропия системы была $H(X)$; после получения сведений состояние системы полностью определилось, т. е. энтропия стала равной нулю. Обозначим I_x информацию, получаемую в результате выяснения системы $I_x = H(X) - 0$, а также уменьшению энтропии: $I_x = H(X)$, или **количество информации, приобретаемое при полном выяснении состояния некоторой физической системы, равно энтропии этой системы.**

Кодирование сообщений.

При передаче сообщения по линиям связи всегда приходится пользоваться тем или иным кодом, т. е. представлением сообщения в виде ряда сигналов. Общеизвестным примером кода может служить принятая в телеграфии для передачи словесных сообщений азбука Морзе. С помощью этой азбуки любое сообщение представляется в виде комбинации элементарных сигналов: точка, тире, пауза (пробел между буквами), длинная пауза (пробел между словами).

Вообще **кодированием называется отображение состояния одной физической системы с помощью состояния некоторой другой**. Например, при телефонном разговоре звуковые сигналы кодируются в виде электромагнитных колебаний, а затем снова декодируются, превращаясь в звуковые сигналы на другом конце линии. **Наиболее простым случаем кодирования является случай, когда обе системы X и Y (отображаемая и отображающая) имеют конечное число возможных состояний**. Так обстоит дело при передаче записанных буквами сообщений, например, при телеграфировании. Мы ограничимся рассмотрением этого простейшего случая кодирования.

Кодирование

Пусть имеется некоторая система X (например, буква русского алфавита), которая может случайным образом принять одно из состояний x_1, x_2, \dots, x_n . Мы хотим отобразить ее (закодировать) с помощью другой системы Y , возможные состояния которой y_1, y_2, \dots, y_m . Если $m < n$, (число состояний системы Y меньше числа состояний системы X), то нельзя каждое состояние системы X закодировать с помощью одного-единственного состояния системы Y . В таких случаях одно состояние системы X приходится отображать с помощью определенной комбинации (последовательности) состояний системы Y . Так, в азбуке Морзе буквы отображаются различными комбинациями 'элементарных символов (точка, тире). **Выбор таких комбинаций и установление соответствия между передаваемым сообщением и этими комбинациями и называется «кодированием» в узком смысле слова.**

Понятие оптимального кода

Коды различаются по числу элементарных символов (сигналов), из которых формируются комбинации, иными словами — по числу возможных состояний системы K . В азбуке Морзе таких элементарных символов четыре (точка, тире, короткая пауза, длинная пауза). Передача сигналов может осуществляться в различной форме: световые вспышки, посылки электрического тока различной длительности, звуковые сигналы и т. п. Код с двумя элементарными символами (0 и 1) называется двоичным. Двоичные коды широко применяются на практике, особенно при вводе информации в электронные цифровые вычислительные машины, работающие по двоичной системе счисления. Одно и то же сообщение можно закодировать различными способами. Возникает вопрос об оптимальных (наивыгоднейших) способах кодирования. Естественно считать наивыгоднейшим такой код, при котором на передачу сообщений затрачивается минимальное время. Если на передачу каждого элементарного символа (например 0 или 1) тратится одно и то же время, то **оптимальным будет такой код, при котором на передачу сообщения заданной длины будет затрачено минимальное количество элементарных символов.**

Двоичным код букв русской азбуки

Предположим, что перед нами поставлена задача: закодировать двоичным кодом буквы русской азбуки так, чтобы каждой букве соответствовала определенная комбинация элементарных символов 0 и 1 и чтобы среднее число этих символов на букву текста было минимальным.

Рассмотрим 32 буквы русской азбуки: а, б, в, г, д, е, ж, з, и, й, к, л, м, н, о, п, р, с, т, у, ф, х, ц, ч, ш, щ, т>, ы, ь, э, ю, я плюс промежуток между словами, который мы будем обозначать «—». Если, как принято в телеграфии, не различать букв ъ и ь (это не приводит к разночтениям), то получится 32 буквы: а, б, в, г, д, е, ж, з, и, й, к, л, м, н, о, п, р, с, т, у, ф, х, ц, ч, ш, щ, (ъ, ь), ы, э, ю, я, «—».

Первое, что приходит в голову — это, не меняя порядка букв, занумеровать их подряд, приписав им номера от 0 до 31, и затем перевести нумерацию в двоичную систему счисления. **Двоичная система — это такая** $12 = 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0$ **цифр представляют собой разные степени двух.** Например, десятичное число 12 изобразится в виде

Простейший код

Каждое из чисел 0. 1 . 2 31 может быть изображено пятизначным двоичным числом.

Тогда получим следующий код:

а — 00000

б — 00001

в — 00010

г — 00011

.....

я — 11110

«—» — 11111

В этом коде на изображение каждой буквы тратится ровно 5 элементарных символов. **Возникает вопрос, является ли этот простейший код оптимальным** и нельзя ли составить другой код, в котором у букву будет в среднем приходиться меньше элементарных символов?

Частоты букв в русском тексте.

Действительно, в нашем коде на изображение каждой буквы — час о встречающихся «а», «е», «о» или редко встречающихся «щ», «э», «ф» — тратится одно и то же число элементарных символов.

Очевидно, разумнее было бы, чтобы часто встречающиеся буквы были закодированы меньшим числом символов, а реже встречающиеся — большим.

Чтобы составить такой код, очевидно, нужно знать частоты букв в русском тексте. Эти частоты приведены в таблице () Буквы

Буква	Частота	Буква	Частота	Буква	Частота	Буква	Частота
«—»	0,145	р	0,041	я	0,019	х	0,009
о	0,095	в	0,039	ы	0,016	ж	0,008
е	0,074	л	0,036	з	0,015	ю	0,007
а	0,064	к	0,029	ъ, ь	0,015	ш	0,006
и	0,064	м	0,026	б	0,015	ц	0,004
т	0,056	д	0,026	г	0,014	щ	0,003
н	0,056	п	0,024	ч	0,013	э	0,003
с	0,047	у	0,021	й	0,010	ф	0,002

Код Шеннона — Фэно

Пользуясь такой таблицей, можно составить наиболее экономичный код на основе соображений, связанных с количеством информации. Очевидно, код будет самым экономичным, когда каждый элементарный символ будет передавать максимальную информацию.

Рассмотрим элементарный символ (т. е. изображающий его сигнал) как физическую систему с двумя возможными состояниями: 0 и 1.

Информация, которую дает этот символ, равна энтропии системы и максимальна в случае, когда оба состояния равновероятны; в этом случае элементарный символ передает информацию 1 (дв. ед.).

Поэтому основой оптимального кодирования будет требование, чтобы элементарные символ

в закодированном тексте встречались в среднем одинаково часто.

Способ построения кода, удовлетворяющего поставленному условию; этот способ известен под названием «кода Шеннона — Фэно». Идея его состоит в том, что кодируемые символы (буквы или комбинации букв) разделяются на две приблизительно равновероятные группы: для первой группы символов на первом месте комбинации ставится 0 (первый знак двоичного числа, изображающего символ); для второй группы — 1.

Кода Шеннона — Фэно на материале русского алфавита

Буква	Двоичное число	Буква	Двоичное число	Буква	Двоичное число
←→	000	к	10111	ч	111100
о	001	м	11000	й	1111010
е	0100	д	110010	х	1111011
а	0101	п	110011	ж	1111100
и	0110	у	110100	ю	1111101
т	0111	я	110110	ш	11111100
н	1000	ы	110111	щ	11111101
с	1001	з	111000	ц	11111110
р	10100	ъ, ь	111001	в	111111110
р	10101	б	111010	ф	111111111
в	10110	г	111011		
л					

С помощью приведённой таблицы можно закодировать и декодировать любое сообщение.

Способ кодирования

В виде примера запишем двоичным кодом фразу: «теория информации»

```
01110100001101000110110110000  
011010001111111100110100  
110000101111110101100110
```

Заметим, что здесь нет необходимости отделять друг от друга буквы специальным знаком, так как и без этого декодирование выполняется однозначно. В этом можно убедиться, декодируя с помощью таблицы 18.8.2 следующую фразу:

```
10011100110011001001111010000  
1011100111001001101010000110101  
010110000110110110
```

(«способ кодирования»).

Ошибки при кодировании и передаче сообщения практически исключены

Однако необходимо отметить, что любая ошибка при кодировании (случайное перепутывание знаков 0 и 1) при таком коде губительна, так как декодирование всего следующего за ошибкой текста становится невозможным. Поэтому данный принцип кодирования может быть рекомендован только в случае, когда ошибки при кодировании и передаче сообщения практически исключены.

Возникает естественный вопрос: а является ли составленный нами код при отсутствии ошибок действительно оптимальным? Для того чтобы ответить на этот вопрос, найдем среднюю информацию, приходящуюся на один элементарный символ (0 или 1), и сравним ее с максимально возможной информацией, которая равна одной двоичной единице. Для этого найдем сначала среднюю информацию, содержащуюся в одной букве передаваемой а одну букву:

$$H(b) = - \sum_{i=1}^{32} p_i \log p_i = \sum_{i=1}^{32} \eta(p_i).$$

где p_i — вероятность того, что буква примет определенное состояние («—», о, е, а, …, ф).

Информация на один символ

Из табл. () имеем

$$H(\beta) = \eta(0,145) + \eta(0,095) + \dots + \eta(0,003) + \eta(0,002) \approx 4,42$$

(дв. единиц на букву текста).

По таблице 18.8.2 определяем среднее число элементарных символов на букву

$$n_{cp} = 3 \cdot 0,145 + 3 \cdot 0,095 + 4 \cdot 0,074 + \dots \\ \dots + 9 \cdot 0,003 + 9 \cdot 0,002 = 4,45.$$

Деля энтропию $H(\beta)$ на среднее число элементарных символов на букву, получаем информацию на один элементарный символ

Таким образом, информация на один символ весьма близка к своему верхнему пределу 1, а выбранный нами код весьма близок к оптимальному. Оставаясь в пределах задачи кодирования по буквам, мы ничего лучшего получить не сможем. Заметим, что в случае кодирования просто каждой буквой пятью битами (дв. ед.), информация на один символ была бы

$$I_{1c} = \frac{4,42}{5,00} = 0,884 \text{ (дв. ед.)}$$