ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

УПРАВЛЕНИЕ ДИСТАНЦИОННОГО ОБУЧЕНИЯ И ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

Кафедра «Вычислительные системы и информационная безопасность»

Курс лекций

по дисциплине

«Теория информации»

Авторы
Ганжур М.А.,
Ганжур А.Г.

Ростов-на-Дону, 2018

Аннотация

«Курс лекций» предназначен для студентов очной формы обучения направлений «10.03.01 Информационная безопасность»; «10.05.02 Информационная безопасность телекоммуникационных систем».

Авторы

Старший преподаватель кафедры
«Вычислительные системы и информационная безопасность»
Ганжур М.А.

Старший преподаватель кафедры
«Вычислительные системы и информационная безопасность»
Ганжур А.Г.

Оглавление

1. Математические модели сигналов и помех 4

2. Спектральный подход к составлению моделей сигналов 9

3. Определение энтропии сложного сигнала.....14

4. Расчет энтропии зависимых и независимых сообщений 17

5. Расчет энтропии сложных сообщений 22

6. Кодирование Хаффмана.....24

7. Кодирование Шеннона – Фено.....29

8. Обыкновенное кодирование 31

1. Кодовые расстояния 31

9. ОПРЕДЕЛЕНИЕ ЭНТРОПИИ ДИСКРЕТНОГО СИГНАЛА.....37

1. Случайные величины и процессы 37
2. Энтропия дискретных сообщений 40

Список литературы .....Ошибка! Закладка не определена.

1. МАТЕМАТИЧЕСКИЕ МОДЕЛИ СИГНАЛОВ И ПОМЕХ

Функциональный подход к составлению математических моделей сигналов

Математической моделью сигнала называется приближенное математическое описание физического процесса, используемого для передачи информации.

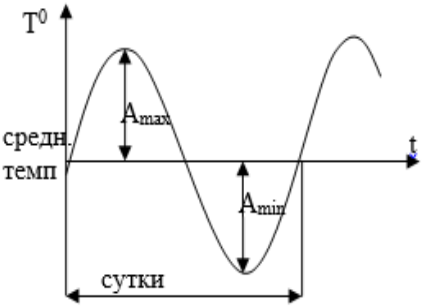
Все **параметры сигналов** можно разделить на:

- структурные;
- идентифицирующие;
- информативные.

Структурные параметры определяют *число степеней свободы сигнала.* Число степеней свободы сигнала – это число способов, которыми каждое возможное сообщение может быть представлено в виде сигнала. Например:

Пусть необходимо получить информацию о каком-то переодическом процессе, изменяющемся по гармоническому закону (допустим суточные колебания температуры). Сигнал будет иметь вид:

$T^0(t) = A^0\sin(2\pi ft + \varphi)$ (3.1)



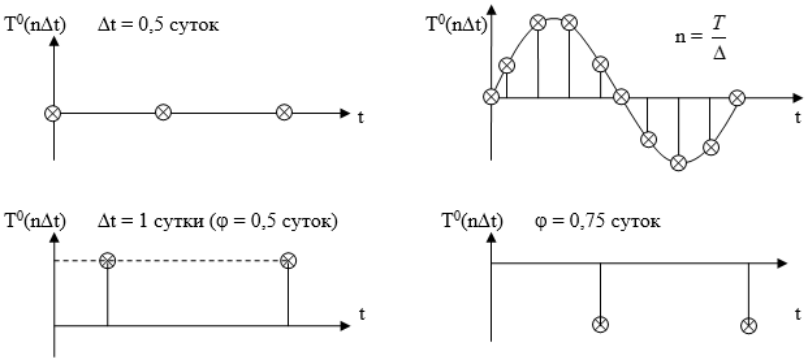
где A – амплитуда отклонения от среднего значения;

$f = \frac{1}{24}$ 1/час

φ - фазовый сдвиг – когда начинаем отчет (утро, день вечер, ночь и опять утро…)

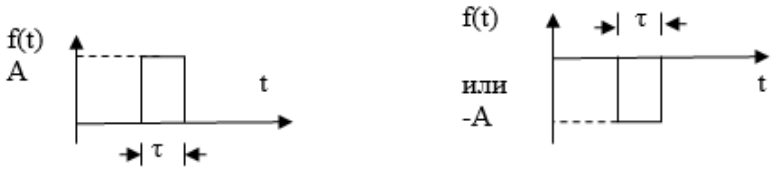
При таком способе передачи сообщения о среднесуточном колебании температуры изменению подлежит только один параметр (A – амплитуда).

Теперь представим, что сведения о температуре передаются дискретно, через промежутки Δt. Здесь возможны разные варианты, даже курьезные. Например:



В приведенном примере Δt можно изменять как угодно, а значит, вариантов сигналов о сообщении может быть как угодно много. Т.е. в примере рассмотрен случай, когда сигнал $T^0(t)$ в случае квантования по времени может иметь *бесчисленное* число степеней свободы.

Если же сообщение о, например, прохождении детали на конвейере поступает на счетчик и передается сигналом в виде прямоугольного импульса определенной амплитуды, то степеней свободы сигнала только две:



Идентифицирующие параметры служат для выделения полезного сигнала среди других сигналов, не предназначенных для данного адресата. Самый простой пример – это назвать адреса в цифровом сигнале. Или несущая частота в радиосвязи (сигнал предназначен только для настроенных на эту частоту). В TV уровне импульсов и их длительности несут информацию о строках, кадрах, цветах, …)

Информационные параметры служат для *кодирования* передаваемой информации. Например, если вы передаете информацию о количестве денег, то длина кодовой посылки определяет точность передачи сообщения. Пусть денег 1200р 50к

N=1 – точность единицы тысяч

N=2 – точность единицы сотен

…… и т.д.

N=6 – точность десятые доли копейки или копейка, но возможности –

десятки тысяч.

В выражении (3.1) в качестве информативных могут использоваться только значения А, но если гармонический сигнал не привязать к конкретному времени, то информативными могут быть и А и $\omega = 2\pi f$ и даже фаза φ. Пример – информация у летчика о приближении и напряжении ЗУР.

При передаче сообщения происходят следующие процессы:

а) сообщение (какое-то из многих генерируемых источником) трансформируется (превращается) в состояние сигнала. Между сообщением и состоянием сигнала существует соответствие;

б) сигнал в канале искажается помехой, что непредсказуемо (случайно) изменяет состояние сигнала;

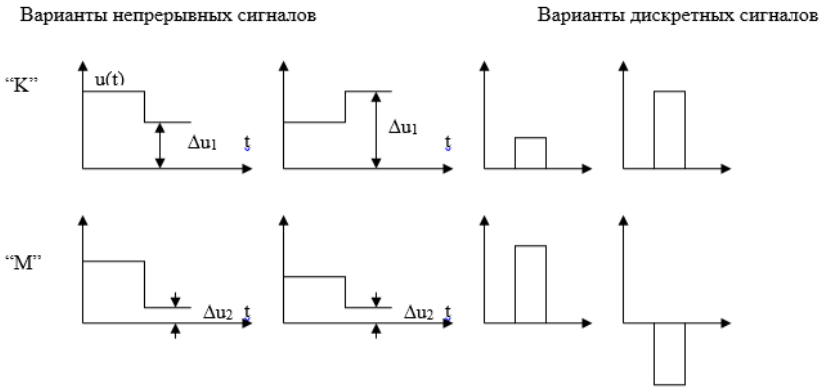
в) на приемном конце линии связи по измененному состоянию сигнала принимается решение относительно переданного сообщения.

Очевидно, что при восстановлении сообщения возможны ошибки. Вероятность возникновения ошибок ведет тем меньше, чем существенней в некотором смысле различаются между собой состояния сигнала, соответствующие различным сообщениям.

Следовательно, возникает необходимость определения *степени различия* между возможными состояниями сигнала. Для этого существуют различные приемы, которые будут рассмотрены отдельно.

Рассмотрим примеры содержательного порядка. Пусть посылаются сигналы о двух сообщениях. Условно их назовем “0” или “1”. Например, прохождение через остановку коммерческого (“К”) или муниципального (“М”) автобусов.

Сигналы

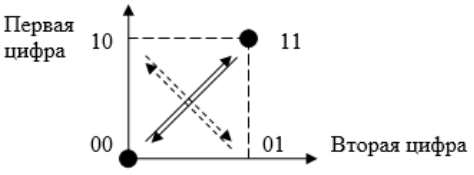


Варианты цифровых двухразрядных кодов:

"0"	00	00	11	01	10	00	01	10
"1"	10	01	00	10	01	11	11	11

Вторые варианты для непрерывных и дискретных сигналов и выделенные варианты цифровых кодов будут более устойчивыми к действию помех, т.к. разница между значениями для непересекающихся сообщений здесь больше, а значит перевести состояния сигналов из соответствия одному сообщению в соответствие другому – труднее.

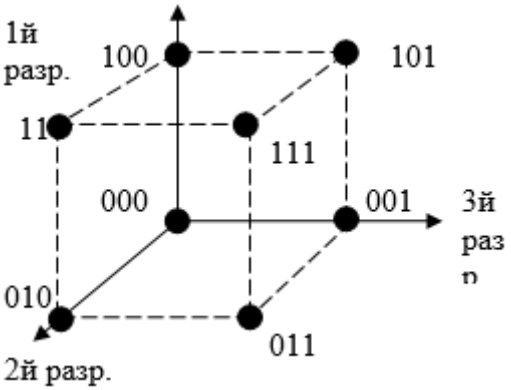
Для решения задач определения различий между возможными состояниями сигналов используются некоторые абстрактные пространства, в которых сигналы представляются в виде *векторов,* а соответствия в виде точек в этом пространстве. Например, для варианта цифровых двухразрядных кодов используется двухмерное пространство (обозначается R^2), т.е. плоскость.



Геометрически видно, что гипотенузы больше катетов и что все гипотенузы равны. Для этого случая могут быть определены *четыре сообщения:*

00, 01, 10 и 11. Им можно поставить в соответствие четыре кода с одинаковой разностью.

Рассуждая аналитически, можно перейти к трехмерному пространству.



Пространство R^3 (евкандово, трехмерное) Некоторые обозначения:

Нулевой вектор – это вектор все координаты которого равны нулю.

2. СПЕКТРАЛЬНЫЙ ПОДХОД К СОСТАВЛЕНИЮ МОДЕЛЕЙ СИГНАЛОВ

В теории информации наиболее распространена аппроксимация (представление, в форме) сигнала u(t) суммой гармонических колебаний. Это производится на основании разложения функции описывающей сигнал, в ряд Фурье и называется спектральным разложением.

$$u(t) = \sum_{k=-\infty}^{+\infty} C_k e^{j2\pi\frac{t}{T}k}$$

→ обратное преобразованиеие Фурье

$$C_k = \frac{2}{T}\int_{-\frac{t}{2}}^{\frac{t}{2}} u(t)e^{j2\pi\frac{t}{T}k}\,dt$$

Как видно из этих выражений спектр периодического сигнала существует только при дискретных значениях частоты.

$$0;\ \pm\omega_1 = \frac{\pm 2\pi}{T};\ \pm\omega_2 = \frac{\pm 4\pi}{T};\ \dots$$

Такой спектр называют дискретным (или линейчатым).

Было также показано, что и непериодический сигнал может быть представлен в виде неправильной суммы периодических гармонических сигналов различной амплитуды и частоты (2.8), (2.9), (2.10).

И в этом случае работают формулы прямого и обратного преобразований Фурье. Напомним их:

$$y(t) = \frac{1}{2\pi}\int_{-\infty}^{+\infty} Y(j\omega)e^{j2\omega t}\,d\omega$$

→ обратное преобразованиеие Фурье

$$Y(j\omega) = \int_{-\infty}^{+\infty} y(t)\,e^{-j2\omega t}\,dt$$

→ прямое преобразованиеие Фурье

С точки зрения передачи сигналов в качестве в качестве связи этот факт играет очень важную роль. Дело в том, что каналы связи по разному ведут себя, когда по ним передается сигнал

различной частоты.

Простые примеры: телефонный провод, коаксиальный кабель, волновод, оптоволоконный кабель.

Звуковые частоты → инфранизкие частоты → низкие частоты → высокие частоты → СВЧ → оптические и т.д

В тоже время разложения Фурье предполагают бесконечные пределы изменения частоты (увеличения в сторону от + ω до + ∞ и уменьшения в сторону от - ω до - ∞), кроме этого происходит уменьшение амплитуды колебаний с увеличением частоты

$$C_k = \int (e^{-\frac{j2\pi tk}{T}})dt = f\left(\frac{1}{e^{j\omega tk}}\right)\ \omega \to \pm\infty;\ C_k \to 0$$

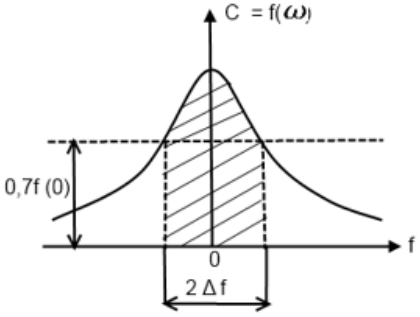
Таким образом, при спектральном подходе каждый сигнал (периодический или непериодический) может быть представлен спектром частотой, а спектром амплитуд.

В свою очередь линии связи имеют ограничения по пропускаемому спектру частот и амплитуд.

В связи с этим реально существуют ограничения в передаче спектром сигналов той или иной линией связи, что приводит к искажению сигнала, т.е. несоответствию формы сигналов на входе и выходе линии связи.

Замечание.

1) Спектральные возможности линии связи по частоте определяются показателем, называемым полосой пропускания или частотной полосой пропускания.



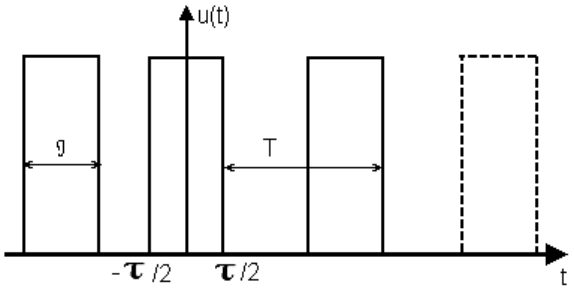
0-полосы пропускания на максимальном значении усилительных свойств в функции частоты это основная частота (*). 2Δf – определяется на уровне 0,7f(0) = f_{max}.

2) Чем больше разлагаемая в спектр функция сигнала отличается от гармонической, тем шире её спектр, который необходимо передавать по линии связи для восстановления формы сигнала на определенном конце.

3) Убывание амплитуд составляющих спектра с удалением от основной частоты происходит достаточно быстро, что дает возможность ограничивать спектр сигнала без существенных потерь и искажений.

Пример. Рассмотрим случай, когда по линии связи передаются периодические прямоугольные импульсы, имеющие длительность τ, амплитуду u и частоту повторения $f_1 = \frac{U}{T}$ (T – период следования импульсов).

Необходимо найти спектр сигнала.



$$C_k = \frac{2}{T}\int_{-\tau/2}^{\tau/2} Ue^{-j\omega tk}\,dt = (\text{т.к. импульс симметричен}) = \frac{C_k}{2}$$

$$= \frac{1}{T}\int_{0}^{\tau} Ue^{-j\omega tk}\,dt = = -\frac{U}{j\omega tk}e^{-j\omega tk}\Big|_{-\tau/2}^{\tau/2}$$

$$= \frac{U\tau}{T\frac{\omega k\tau}{2}}\cdot\frac{e^{j\frac{\omega k\tau}{2}} - e^{-j\frac{\omega k\tau}{2}}}{2j} =$$

$$= \frac{U\tau}{T\frac{\omega k\tau}{2}}$$

$$\cdot\frac{\cos\left(\frac{\omega k\tau}{2}\right) + jsin\left(\frac{\omega k\tau}{2}\right) - \cos\left(\frac{\omega k\tau}{2}\right) + jsin\left(\frac{\omega k\tau}{2}\right)}{2j}$$

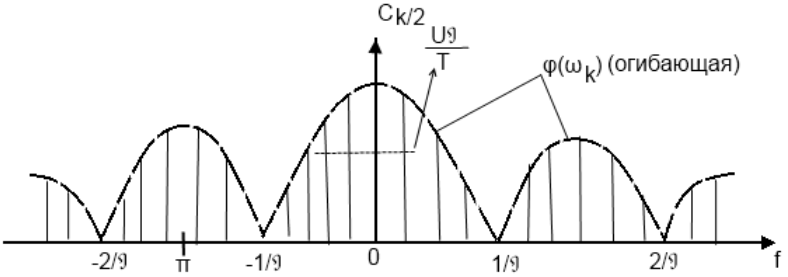
$$= \frac{U\tau\cdot \cancel{j2}sin\left(\frac{\omega k\tau}{2}\right)}{T\frac{\omega k\tau}{2}\cancel{2j}} == \frac{U\tau}{T}\cdot\frac{sin\left(\frac{\omega k\tau}{2}\right)}{\frac{\omega k\tau}{2}}$$

Т.к. спектр амплитуд $C_k\,|_{-\infty\ll+\infty}$ должен состоять из дей-

ствительных и положительных компонентов, а функция $\frac{sin\alpha}{\alpha}$ меняет знак через каждое значение кратное π, то полученный результат можно записать как

$$\frac{C_k}{2} = \frac{U\tau}{T}\left|\frac{sin\left(\frac{\omega k\tau}{2}\right)}{\frac{\omega k\tau}{2}}\right| e^{-jn\pi}$$

Последний множитель – индикатор знака, который можно рассматривать, как некоторую функцию $\varphi(\omega_k) = n\pi$ огибающую спектра импульсной последовательности. Это можно изобразить следующим образом



Спектр фаз и спектр амплитуд пропорционален значениям модуля функции $\frac{sin\alpha}{\alpha}$. Спектр амплитуд → вертикальная штриховка.

Постоянная составляющая $C_0 = \frac{U\tau}{T}$ равна среднему значению сигнала за период. Огибающая спектра амплитуд пересекается с осью абсцисс в точках α=nπ (n=±1,±2,±3,…). Они соответствуют частотам:

$$\frac{\omega k\tau}{2} = n\pi \Rightarrow \frac{f_n \cancel{2\pi}\tau}{\cancel{2}} = n\cancel{\pi} \Rightarrow f_n = \frac{n}{\tau}$$

Просматривается вывод: ширина спектра периодической последовательности импульсов $\Delta f \approx f_n \approx \frac{n}{\tau}$, обратнопропорциональна длительности импульсов τ и не зависит от периода Т.

Вопрос о том, какую часть спектра необходимо сохранить при передаче сигнала по каналу связи (какое значение n нужно выбрать в выражении для Δf), зависит от конкретных обстоятельств:

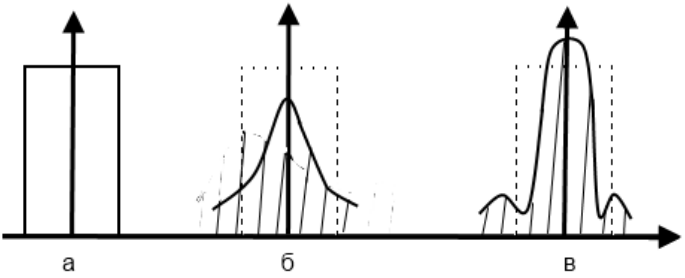
- информативности тех или иных параметров сигнала (ам-

плитуды, формы, крутизны фронтов);

- уровня помех;

-интенсивности потока информации в канале и т.д.

Если вводятся ограничения на спектр, то результаты можно продемонстрировать следующими рисунками:



а – передаваемый импульс; б – $\Delta f = 1/2\tau$; в - $\Delta f = 1/\tau$

Как правило выбирается n≈1. Поэтому Δf* т ≈ 1, т.е. произведение ширины спектра периодической последовательности импульсов на длительность импульса есть величина близкая к единице.

Это справедливо и для одиночных импульсов. Однако в радиотехнике (например TV), где сохранение формы играет важную роль значения Δf должна быть 1/т.

3. ОПРЕДЕЛЕНИЕ ЭНТРОПИИ СЛОЖНОГО СИГНАЛА

Определение условий энтропии сложной системы

Задача: определить условие энтропии h (b/a) и h(a/b) сложной системы, вероятность состояний которой $p(a_k,b_i)$ заданы.

[a] = [кросс; плавание; гимнастика]

[b] = [3,4,5]

Вариант 1

Задача: Известно только [a] и $p(a_i)$: a_1 = 0,25; a_2 = 0,55; a_3 = 0,20;

$$h(a) = -\sum_{i=1}^{m} p(a_i) \cdot \log_2 p(a_i) = -(0.25 \cdot \log_2 0.25 + 0.55 \cdot \log_2 0.55 + 0.20 \cdot \log_2 0.20) \approx 1.43 \frac{бит}{сообщение}$$

Расшифровка условия задачи: статистика показывает, что при сдаче дисциплины тремя способами оценки дают следующие вероятности (таблица $p(a_k,b_i)$)

Вариант 2

Задача:

b\a	a_1	a_2	a_3
b_1	0.15	0.25	0.05
b_2	0.10	0.20	0.05
b_3	0	0.10	0.10

Решение:

$p(a_1)$ = 0,25 ; $p(a_2)$ = 0,55 ; $p(a_3)$ = 0,20 –> $p(a_k)$;

$p(b_1)$ = 0,25 ; $p(b_2)$ = 0,55 ; $p(b_3)$ = 0,20 –> $p(b_i)$;

Делим $p(a_k,b_i)$ на $p(b_i)$ и получим $p(b_i / a_k)$

b\a	a_1	a_2	a_3
b_1	0.6	0.45	0.25
b_2	0.4	0.36	0.25
b_3	0	0.19	0.5

Делим $p(a_k,b_i)$ на $p(a_k)$ и получим $p(a_k/b_i)$

b\a	a_1	a_2	a_3
b_1	0.33	0.56	0.11
b_2	0.29	0.57	0.14
b_3	0	0.5	0.5

Какова неопределенность системы в двух случаях

h(b/a) – с точки зрения названия оценки (3,4,5), если $a_к$ принимает различные значения;

h(a/b) – с точки зрения вида сдачи экзамена, если установить различные значения оценок.

Формула для этого случая m=3

$$h(\mathrm{b/a}) = -\sum_{\mathrm{k}=1}^{\mathrm{m}}\sum_{i=1}^{l} p(a_k)\cdot p(b_i/a_k)\log p(bi/a_k) \qquad \mathrm{l}=3$$

Или $$h(\mathrm{b/a}) = -\sum_{\mathrm{k}=1}^{\mathrm{m}} p(a_k)\sum_{i=1}^{l} p(b_i/a_k)\log p(bi/a_k)$$

Тогда:

$$\mathrm{h(b/a)} = -0.25\cdot(0.6\cdot\log 0.6 + 0.4\cdot\log 0.4) - 0.55\cdot(0.45\cdot\log 0.45 + 0.36\cdot\log 0.36 + 0.19\cdot\log 0.19) -$$

$$-0.20\cdot(0.25\cdot\log 0.25 + 0.5\cdot\log 0.5) \approx 1.37\ \frac{\text{бит}}{\text{сообщение}}$$

$$\mathrm{h(a/b)} = -0.45\cdot(0.33\cdot\log 0.33 + 0.56\cdot\log 0.56 + 0.11\cdot\log 0.11) -$$

$$-0.35\cdot(0.29\cdot\log 0.29 + 0.57\cdot\log 0.57 + 0.14\cdot\log 0.14) - 0.20\cdot(0.5\cdot\log 0.5 + 0.5\cdot\log 0.5) \approx 1.29\ \frac{\text{бит}}{\text{сообщение}}$$

То есть сравнение дает большую неопределенность для случая, когда нас интересует оценка при задаваемых видах сдачи, чем случая, когда мы фиксируем оценки, а неопределенность составляет виды сдачи. Действительно, при получении «5» неопределенность остается только по 2-м видам сдачи (плавание и гимнастика). Получение «3» с большей вероятностью можно указывать, что сдавалось плавание (a_2).

Вариант 3

Пусть пришло сообщение, что плавание сдаваться не будет. Исходная таблица уже не подходит, так как она составлена для случая 3-х видов сдачи, а теперь будет только 2. Поэтому нужны новые данные:

b\a	a_1	a_3
$b_1=3$	0.30	0.20
$b_2=4$	0.20	0.20
$b_3=5$	0	0.10

Это уже другая система, поэтому постановка задачи – сколько информации содержится в сообщении снятии плавания (как вида сдачи) – некорректна. В данном случае информация рассматривается, как разница энтропий системы до получения информации и после получения информации.

$J = H_a - H_b$

4. РАСЧЕТ ЭНТРОПИИ ЗАВИСИМЫХ И НЕЗАВИСИМЫХ СООБЩЕНИЙ

Энтропия сложного сообщения

Сложная система получается объединением двух и более простых систем. При этом состояние сложной системы (a,b) представляет собой все возможные комбинации состояний a_k и b_j составляющих систем. Сообщениями о состоянии сложной системы называются сложными сообщениями.

Например – две одновременно подбрасываемые монеты, амплитуда и длительность импульса, амплитуда и частота гармонического сигнала.

Если a и b независимы, то

$$P(a_k, b_j) = P(a_k)P(b_j)$$

$$\log P(a_k, b_j) = \log P(a_k) + \log P(b_j)$$

$$h(a,b) = -P(a_1)P(b_1)[\log P(a_1) + \log P(b_1)] - P(a_1)P(b_2)[\log P(a_1) + \log P(b_2)] - \dots - P(a_m)P(b_j)[\log P(a_m) + \log P(b_j)] = \cdots$$

$$= \left| \sum_{k=1}^{m} P(a_k) = 1 \text{ и } \sum_{k=1}^{m} P(b_j) = 1 \right| = h(a) + h(b)$$

Т.е. при объединении независимых систем энтропии этих систем складываются.

Условная энтропия. Объединение зависимых систем.

Пусть имеются две системы X и Y в общем случае зависимые. Предположим, что система X приняла состояние x_i . Обозначим условную вероятность того, что система Y примет состояние y_i при условии, что X находится в x_i через $P(y_i/ x_i)$.

Определим условную энтропию систем Y при условии, что система X находится в состоянии X_i . Обозначим её через $H(Y/ x_i)$. По общему определению энтропии:

$$H(Y/x_i) = -\sum_{i=1}^{m} P(y_i/x_i) \log P(y_i/x_i)$$

Функцию - p(a)*log p(a) часть обозначим через n(a). Она табулирована и есть во всех справочниках. Тогда:

$$H(Y/x_i) = -\sum_{i=1}^{m} \eta[P(y_i/x_i)]$$

или $H(Y/ x_i) = M[-\log P(Y/ x_i)]$

Условная энтропия в общем случае различна для различных x_i . Поэтому необходимо опре- делить среднее значение (оно

называется еще полным) энтропии системы Y с учетом того, что система X может принимать различные состояния (сложить с умножением индекса x_i)

Условная энтропия

$$H(Y/X) = -\sum_{i=1}^{n} P_i \, H(Y/x_i) = -\sum_{i=1}^{n} P(x_i) \, H(Y/x_i)$$

где p_i – вероятность $p(x_i)$

Теперь :

$$H(Y/X) = \sum_{i=1}^{n} P(x_i) \sum_{j=1}^{m} \eta \, P\left(y_j/x_i\right)$$

Внеся $p(x_i)$ под знак второй суммы:

Расчетные формулы:

$$H(Y/X) = \sum_{i=1}^{n}\sum_{j=1}^{m} P(x_i)\,\eta\, P\left(y_j/x_i\right)$$

$$= -\sum_{i=1}^{n}\sum_{j=1}^{m} P(x_i)\, P\left(y_j/x_i\right) log P(y_0/x_i)$$

Но есть теорема умножения вероятностей p(AB) = p(A) * p(B/A), по которой $p(x_i)*p(y_i/ x_i) = P(x_i y_j)$

Следовательно:

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

Через М. О.: H(Y/X) = M[-log P(Y/X)]

Величина H(Y/X) характеризует степень неопределенности системы Y, остающейся после того, как состояние системы X полностью определилось. Она называется полной условной энтропией системы Y относительно X.

Пример. Имеются две объединенные системы X и Y. Вероятности их совместных состояний заданы таблицей. Определить H(Y/X) и H(X/Y)

x_i / y_j	x_1	x_2	x_3	r_j
y_1	0.1	0.2	0	0.3
y_2	0	0.3	0	0.3
y_3	0	0.2	0.2	0.4
p_j	0.1	0.7	0.2	-

Вводим добавочную строку а столбец для определения $p(x_i)$ и $p(y_i)$. Они определения сложение его столбцам и строкам.

Разделив табличные значения на полученные вероятности p_j и r_j получим еще две таблицы:

1	0,2/0,7	0
0	0,3/0,7	0
0	0,2/0,7	1

0,1/0,3	0,2/0,3	0
0	1	0
0	0,2/0,4	0,2/0,4

Теперь:

$$H(Y/X) = 0.7\,[\eta(0.2/0.7) + \eta(0.3/0.7) + \eta(0.2/0.7)]$$

Остальные условные энтропии равны нулю: n(1) = n(0) = 0!

Используя таблицы n, получаем H(Y/X) = 1.09 $\frac{\text{дв.ед}}{\text{сообщ}}$

Поступая аналогично со второй таблицей, получаем

$$H(X/Y) = 0.3[\eta(0.1/0.3) + \eta(0.2/0.3)] + 0.4[\eta(0,2/0,4) + \eta(0.2/0.4)] = 0.68\ \frac{\text{дв.ед}}{\text{сообщ}}$$

Энтропия объединенной системы

Если две системы объединяются в одну, то энтропия объединенной системы равна энтропии одной из её составных частей плюс условия энтропия второй части относительно первой : H(X,Y) = H(X) + H (Y/X)

Доказательство: P(X,Y) = P(X) P(Y/X) – по теореме умножения вероятностей

Следовательно: log P(X,Y) = log P(X) + log P(Y/X)

Откуда: H(X,Y) = M [-log P(X) + M [-log P(Y/X)]

Или: H(X,Y) = H(X) + H(Y/X) что и доказывалось.

$H(x_1,x_2,\ldots,x_s) = H(x_1) + H(x_2/x_1) + H(x_3/x_1, x_2) + \ldots + H(x_s/x_1, x_2,\ldots, x_{s-1})$

Предшествующую задачу можно формулировать следующим образом:

Ансамбли событий $X(x_1, x_2, x_3)$ и $Y(y_1, y_2)$ объединены. Вероятности совместных событий приведены в таблице.

y_i \ x_i	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 объединенных ансамблей X и Y

3) Условную энтропию ансамблей X и Y

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

$$P(x_1) = P(x_1, y_1) + P(x_1, y_2) = 0{,}1 + 0{,}25 = 0{,}35$$

$$P(x_2) = P(x_2, y_1) + P(x_2, y_2) = 0{,}2 + 0 = 0{,}2$$

$$P(x_3) = P(x_3, y_1) + P(x_3, y_2) = 0{,}3 + 0{,}15 = 0{,}45$$

$$P(y_1) = P(x_1, y_1) + P(x_2, y_1) + P(x_3, y_1) = 0{,}1 + 0{,}2 + 0{,}3 = 0{,}6$$

$$P(y_2) = P(x_1, y_2) + P(x_2, y_2) + P(x_3, y_2) = 0{,}25 + 0 + 0{,}15 = 0{,}4$$

Тогда энтропия событий будет равна:

$$h(X) = -\sum_{i=1}^{3} P(x_i)\ \log_2 P(x_i);$$

$$-0{,}35 \log_2 0{,}35 - 0{,}2 \log_2 0{,}2 - 0{,}45 \log_2 0{,}45 = 1{,}512 \frac{\text{бит}}{\text{сообщ}}$$

$$h(Y) = -\sum_{i=1}^{2} P(y_i)\ \log_2 P(y_i); -0{,}6 \log_2 0{,}6 - 0{,}4 \log_2 0{,}4 = 0{,}971 \frac{\text{бит}}{\text{сообщ}}$$

2) Энтропию объединенных ансамблей X и Y находим, используя

$$h(X,Y) = -\sum_{i=1}^{n}\sum_{j=1}^{m} P(x_i, y_j) \log_2 P(x_i, y_j)$$

$$h(X,Y) = -\sum_{i=1}^{3}\sum_{j=1}^{2} P(x_i, y_j) \log_2 P(x_i, y_j) =$$

$$= -0{,}1 \log_2 0{,}1 - 0{,}25 \log_2 0{,}25 - 0{,}2 \log_2 0{,}2 - 0{,}3 \log_2 0{,}3 - 0{,}15 \log_2 0{,}15 = 2{,}228 \frac{\text{бит}}{\text{сообщ}}$$

3) Условную энтропию ансамблей X и Y удобно определить, используя свойство

$$h(X,Y) = h(X) + h\left({}^{Y}/_{x_i}\right); \text{или:}$$

$$h(Y/X) = h(X,Y) - h(X) = 2{,}228 - 1{,}512 = 0{,}716 \frac{\text{бит}}{\text{сообщ}}$$
$$h(X/Y) = h(X,Y) - h(Y) = 2{,}228 - 0{,}971 = 1{,}257 \frac{\text{бит}}{\text{сообщ}}$$

5. РАСЧЕТ ЭНТРОПИИ СЛОЖНЫХ СООБЩЕНИЙ

Энтропия сложного опыта. Условная энтропия

Постановка задачи.

А) Пусть имеем 2 независимых опыта X и Y с конечным числом исходов n и m и дискретным распределениями:

Опыт X→ $p(x_i)$; i = 1, n

Опыт Y→ $p(y_i)$; j = 1, m

$$h(X) = -\sum_{i=1}^{n} p(x_i) \cdot \log_2 p(x_i)$$

$$h(Y) = -\sum_{j=1}^{m} p(y_j) \cdot \log_2 p(y_j)$$

Поскольку опыт сложный, независимые опыта X и Y осуществляются одновременно. Каждому исходу такого сложного опыта соответствует наступление пары исходов x_i и y_i в соответствующие моменты времени. Всего исходов таких опытов будет $n \cdot m$.

$x_1\ y_1$	…	$x_n\ y_1$
…	…	…
$x_1\ y_m$	…	$x_n\ y_m$

Для сложного опыта выражение $h(X) = -\sum_{i=1}^{n} p(x_i) \cdot \log_2 p(x_i)$ записывается в виде

$$h(X,Y) = -\sum_{i=1}^{n}\sum_{j=1}^{m} p(x_i,y_j) \cdot \log_2 p(x_i,y_j) \quad (4.9)$$

Так как X и Y независимы , то

$$p(x_i,y_j) = p(x_i) \cdot p(y_j) \quad (4.10)$$

После подстановки (4.10) в (4.9),преобразований и применения нормирования $\sum_{i=1}^{n} p(x_i) = 1$ и $\sum_{j=1}^{m} p(y_j) = 1$ получим конечный результат:

$$h(x,y) = h(x) + h(y)$$

То есть энтропия сложного опыта X и Y равна суме энтропий независимых опытов (при независимых опытах).

Условие сохраняется для любого количества независимых опытов.

Б) Пусть опыты X и Y – зависимы. Это значит, что $p(x_i, y_j) = p(x_i) \cdot p\left(y_j/x_i\right)$, где $p\left(y_j/x_i\right)$ – условная вероятность исхода y_j в опыте Y при условии, что в опыте X наступил исход x_i.

Из выражения (4.9) найдем энтропию:

$$h(x,y) = -\sum_{i=1}^{n}\sum_{j=1}^{m} p(x_i) \cdot p\left(y_j/x_i\right) \cdot \log_2\left[p(x_i) \cdot p\left(y_j/x_i\right)\right]$$

$$=$$

$$= -\sum_{i=1}^{n} p(x_i) \cdot \log_2 p(x_i) \cdot \sum_{j=1}^{m} p\left(y_j/x_i\right) - \sum_{i=1}^{n} p(x_i) \cdot \sum_{j=1}^{m} p\left(y_j/x_i\right) \cdot \log_2 p\left(y_j/x_i\right)$$

однако

$$\sum_{j=1}^{m} p\left(y_j/x_i\right) = p\left(y_1/x_i\right) + p\left(y_2/x_i\right) + \cdots + p\left(y_m/x_i\right) = 1$$

Последнее означает, что при наступлении в опыте X результата в опыте Y обязательно наступает один из исходов ,,..,, т.к. они образуют полную группу несовместимых событий.

Поэтому $h(X,Y) = h(X) + h_X(Y)$ (4.12), где $h_x(Y)$ средняя условная энтропия опыта Y

$$h_X(Y) = \sum_{i=1}^{n} p(x_i) \sum_{j=1}^{m} \log_2 p\left(y_j/x_i\right)$$

Т.е. энтропия сложного опыта X, Y равна сумме безусловной энтропии опыта X и средняя условной энтропии опыта Y при условии наступления исхода опыта X.

То же относится и к опыту Y, X, т.к $h(X) + h_X(Y) = hY + h_Y(X)$ (4.13).

6. КОДИРОВАНИЕ ХАФФМАНА

Эффективное кодирование (статическое кодирование)

Исходящая позиция. Источник информации выдает сообщения, которые нужно закодировать. Источник избыточен, т.е. его энтропия меньше максимальной! (Уменьшение энтропии источника обуславливается двумя факторами: отличием закона распределения вероятностей букв a_j от равномерного и наличием корреляционных связей между буквами)

Кодирование тем эффективнее, чем меньше средняя длина $\bar{n}$ кодограмм z_j, отображающих буквы a_i источника. Другими словами, эффективность достигается максимальной информационной нагрузкой на каждый символ кода z_j, несущий информацию. Теория информации определяет предел-полная независимость и равновероятность букв кодового алфавита.

Сущностью эффективного кодирования и является переход от алфавита источника $\{a_i\}$ $(i = \overline{1, m_a})$, составляемого из зависимых и неравновероятных букв, к алфавиту кода $\{z_j\}$ $(j = \overline{1, m_z})$, символы которого независимы и равновероятны, т.е. описание сообщений другим безызбыточным «языком».

Теоретической базой эффективного кодирования служит теорема К. Шеннона для дискретного двоичного канала без помех.

Сущность этой теоремы:

Если производительность источника информации

$$v_a \cdot h(a)$$

не превышает пропускную способность С канала связи, то существует такой способ кодирования, при котором среднее число двоичных сигналов $\bar{n}$ кода, приходящихся на один элемент сообщения, будет минимальным и равным энтропии источника

$$\overline{n_{min}} = h(a)$$

Для выполнения алгоритма эффективного кодирования рассмотрим вначале безызбыточный источник, обладающий максимальной энтропией.

В этом случае эффективным кодом является равномерный код на все сочетания – простая двоичная нумерация возможных сообщений. Это можно показать следующим образом

$$h(a) = \log m_a$$

Количество комбинаций равномерного кода на все сочета-

ния

$$N = 2^n.$$

Эти комбинации имеют постоянную длину

$$n = \log N$$

Если использовать все N комбинаций (полное их использование), то

$$N = \overline{m_a}$$

и тогда

$$n = \log_a m_a = h(a)$$

Т.е. длина кодограмм в данном случае совпадает с теоретическим пределом Шеннона

$$n = \bar{n}_{min}$$

Если источник обладает избыточностью, то его состояния неравновероятны или коррелированны или неравновероятны и коррелированны одновременно. В этом случае эффективное кодирование напрямую невозможно. Необходимо провести (осуществить) декорреляцию букв первичного алфавита источника, а затем устранить избыточность, обусловленную неравными вероятностями появления новых букв. Эти две операции объединяются в одну единую, получившую название статистического кодирования.

Статистическое кодирование использует неравномерные коды, в которых более вероятным буквам источника соответствуют короткие кодовые комбинации, а менее вероятным – длинные. При этом удается значительно уменьшить среднюю длину кодограмм.

Первый этап.

Декорреляция. Сущность деккоряляции состоит в рассмотрении коррелированных сообщений источника как независимых, т.е. в расширении алфавита источника.

Например, для алфавита, состоящего из двух букв в случае наличия корреляции должны быть известны вероятности

$$p(a_1) = P_1;\ p(a_2) = P_2;\ p\left(a_1/a_1\right) = P_3;\ p\left(a_2/a_1\right) = P_4;\ p\left(a_1/a_2\right) = P_5;\ p\left(a_2/a_2\right) = P_6$$

Все состояния источника объединены в две группы:

$$p(a_1);\ p\left(a_1/a_1\right);\ p\left(a_2/a_1\right) \text{ и } p(a_2);\ p\left(a_1/a_2\right);\ p\left(a_2/a_2\right)$$

Получив «информацию» об источнике мы как бы её увеличиваем, т.к. нам эта информация придет не только о состоянии источника (a_1 или a_2), но и о том, каким образом осуществлен

переход в каждое из этих состояний

Второй этап.

Второй этап статистического кодирования связан с получением возможностей как можно быстрее передавать информацию, т.е. уменьшением до минимума средних длин кодограмм.

Теоретически доказано, что оптимальное статистическое кодирование будет в том случае, если длина кодограммы (кода, соответствующего сообщению) будет определяться частной энтропией сообщения

$$n_j = -\log p(A_j)$$

где n_j — длина кодограммы (количество канальных символов в ней)

A_j — j -ое сообщение источника А

$p(A_j)$ — вероятность сообщения A_j

Если это условие выполнить, то среднюю длину кодограмм можно уменьшить до теоретического предела Шеннона:

$$\bar{n} = \sum_{j=1}^{m} n_j p(A_j) = -\sum_{j=1}^{m} p(A_j) \cdot \log p(A_j) = H(A)$$

Используемые при этом неравномерные коды получили название статистических кодов.

При построении неравномерных статистических кодов необходимо (следует) стремиться к оптимальности, сводимой к минимизации средней длины.

Рассмотрим процедуру построения такого кода, предложенную английским ученым Д. А. Хаффманом.

Пусть необходимо построить оптимальный код для отображения М сообщений, если известны основание кода и вероятности возникновения каждого из сообщений $p(x_{01}),\ p(x_{02}), \ldots, p(x_{0j}), \ldots, p(x_{0M})$. Процедура построения сводится к построению кодового дерева.

1) Исходные события К (отсчеты, сообщения) располагаются в порядке убывания вероятности их возникновения;
2) События разбиваются на группы, в каждой из которых объединятся N событий, где 2 ≤ N ≤ K. Первая группа включает в себя наименее вероятные события;
3) Каждая получаемая группа событий рассматривается, как новое событие с вероятностью появления, равной сумме вероятностей возникновения событий, входя-

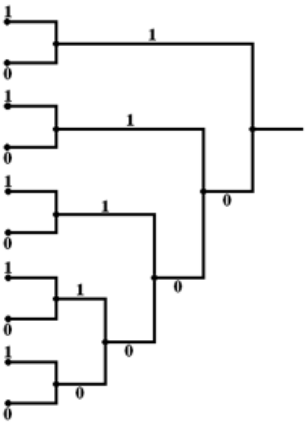
щих в эту группу;

4) Полученное новое событие располагается в соответствии с принципом убывания вероятностей
5) Ветви кодового дерева обозначаются индексами от 0 до K-1.

Пример. Посторожить двоичный оптимальный код, отображающий десять отсчетов (т.е. один разряд десятичной системы счисления), если отсчеты (события) возникают с вероятностями $1/4, 1/4, 1/8, 1/8, 1/16, 1/16, 1/32, 1/32, 1/32, 1/32$.

Решение. Расположим события в порядке убывания вероятностей и обозначим каждое, как x_{0j}

Номер	Отсчет	Вероятность	Кодовое дерево
1	x_{01}	1/4	11
2	x_{02}	1/4	10
3	x_{03}	1/8	011
4	x_{04}	1/8	010
5	x_{05}	1/16	0011
6	x_{06}	1/16	0010
7	x_{07}	1/32	00011
8	x_{08}	1/32	00010
9	x_{09}	1/32	00001
10	x_{10}	1/32	00000



Каждое событие должно соответствовать концевой вершине кодового дерева. При K = 2 каждая группа содержит два события. Построение кодового дерева начнем с концевых узлов, соответствующих наименее вероятным событиям x_{09} , x_{10} ; x_{07} , x_{08}.получим новые события с вероятностью возникновения 1/16. Далее переходим к группе событий обладающих вероятностью возникновения 1/16 и в соответствии с этой процедурой последовательно строим кодовое дерево. Каждую ветвь такого дерева обозначим индексами «0» и «1» и двигаясь от вершины кодового дерева к концевому узлу, находим значение кодовой комбинации, как последовательность обозначений пройденных ветвей кодового дерева.

Для оценки оптимальности кода найдем среднее и оптимальное значение длины кода и сравним их:

$$n_{ср} = \sum_{j=1}^{j=M} P(x_j) n_j = 2 \cdot 2\frac{1}{4} + 2 \cdot 3\frac{1}{8} + 2 \cdot 4\frac{1}{16} + 4 \cdot 5\frac{1}{32} = 2\frac{7}{8}$$

$$n_{опт} = \frac{\left(-2\frac{1}{4}\log_2\frac{1}{4} - 2\frac{1}{8}\log_2\frac{1}{8} - 2\frac{1}{16}\log_2\frac{1}{16} - 4\frac{1}{32}\log_2\frac{1}{32} -\right)}{\log_2 2} = 2\frac{7}{8}$$

Так как $n_{ср} = n_{опт}$, то полученный код является максимальным.

7. КОДИРОВАНИЕ ШЕННОНА – ФЕНО

Идея кода состоит в том, что кодируемые символы (буквы или комбинация букв) разделяются на две приблизительно равновероятные группы. Для первой группы символьное на первом месте ставиться комбинация «0», для второй «1». Далее каждая группа снова делится на две приблизительно равновероятные подгруппы. Для символов первой подгруппы на втором месте ставиться ноль, для второй подгруппы – единица и т.д.

Рассмотрим построение кода Шеннона – Фено для восьми независимых сообщений. Кодирование этих сообщений обыкновенным равномерным кодом потребовало бы трех кодовых символов на сообщение. Статистическое кодирование позволяет значительно уменьшить эту цифру.

Сообщение	Вероятность	Ступени разбиения							Кодограммы
		1	2	3	4	5	6	7	
A_1	½	1	0	0	0	0	0	0	1
A_2	¼	0	1	0	0	0	0	0	01
A_3	1/8	0	0	1	0	0	0	0	001
A_4	1/16	0	0	0	1	0	0	0	0001
A_5	1/32	0	0	0	0	1	0	0	00001
A_6	1/64	0	0	0	0	0	1	0	000001
A_7	1/128	0	0	0	0	0	0	1	0000001
A_8	1/128	0	0	0	0	0	0	0	0000000

Для рассматриваемого примера энтропия сообщений

$$\mathrm{H(A)} = -\sum_{i=1}^{8} p(A_i)\log p(A_i) = 1\frac{63}{64}$$

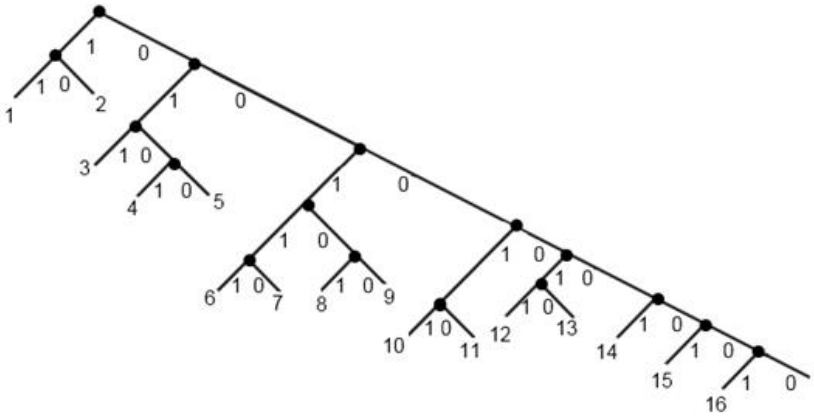
Средняя длина кодограмм

$$n = \sum_{i=1}^{8} p(Z_i)n_i = 1\frac{63}{64}$$

Условие оптимального кодирования выполнено: средняя длина кодограмм равна энтропии сообщений.

Пусть задано некоторое гипотетическое сообщение, включающее 16 элементов, вероятности появления которых заданы таблицей

Элемент	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Вероятность	0.3	0.2	0.1	0.1	0.05	0.05	0.03	0.03	0.03	0.02	0.02	0.02	0.02	0.01	0.01	0.01
Код	11	10	011	0101	0100	00111	00110	00101	00100	00011	000101	000100	00001	000001	0000010	0000000
Инв. код	00	01	100	1010	1011	11000	11001	11010	11011	11100	111010	111011	11110	111110	1111101	1111111



Комбинация построенного оптимального кода разделяется без специальных знаков

читается только однозначно:

11 – 011 – 0100 – 011 – 5

1 3 5 3 5

Алгоритм:

1) Все возможные элементы сообщения записываются в порядке убывания вероятности их появления;
2) Записанная последовательность разбивается на две группы так, чтобы суммы вероятностей элементов в каждой группе были по возможности равными;
3) Первым кодовым знаком в первой группе назначают «0», а во второй «1»;
4) Разбиение продолжается по этому же принципу;
5) Процесс разбиения продолжается до выделения каждого элемента.

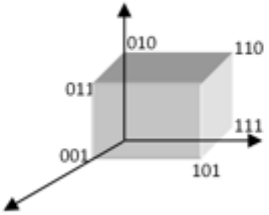
8. ОБЫКНОВЕННОЕ КОДИРОВАНИЕ

1. Кодовые расстояния

Одной из важнейших характеристик кода является расстояние между двумя ближайшими точками кодового пространства. Оно называется кодовым расстоянием (или хеммингловым расстоянием).

Здесь два понятия: кодовое пространство и кодовое расстояние.

Кодовое пространство – это векторнгое пространство, дискретное, целых вещественных чисел с метрикой Хэмминга. Точки ∟ (так оно обозначается) пространства расположены в вершинах n-мерного «куба» с единичными ребрами.

Для n=2	Для n=3	Для n=4
00		0001
01		0011
10		0100
11		…

Кодовые расстояния определяются, как различие между двумя ближайшими разрешенными кодограммами. Оно определяется как:

$$d = \sum_{i=1}^{n} z_{ij} \oplus z_{il}$$

где z_{ij} и z_{il} – кодовые комбинации (или коды) между которыми определяется кодовое расстояние.

$\oplus$ – знак сложения по mod2

Правила сложения по mod2: 0+0=0; 0+1=1; 1+0=1; 1+1=0 без переноса!

Задание. Определить кодовое расстояние между кодами 010 и 101

$$\begin{array}{r} \oplus \begin{array}{r} 010 \\ 101 \end{array} \\ \hline 111 \end{array}$$

Чтобы определить кодовые расстояния, необходимо под-

считать число разрядов, в которых ближайшие разрешенные кодограммы имеют разные символы.

Задание. Определить кодовое расстояние между:

Двоичными кодами с десятичными эквивалентами d_{12} , d_{78}

0001 0100

1000 0011

1010 0000

Разрешенными кодовыми комбинациями являются 1, 8, 10 и 4, 3, 0. d_1

Классификация обыкновенных кодов

<table>
<tr><td colspan="6">Обыкновенные коды</td></tr>
<tr><td colspan="4">цифровые</td><td colspan="2">Нецифровые</td></tr>
<tr><td colspan="2">взвешенные</td><td colspan="2">невзвешенные</td><td colspan="2">комбинаторные</td><td>некомбинаторные</td></tr>
<tr><td>двоичные</td><td>недвоичные</td><td>отраженные</td><td>сдвинутые</td><td>На основе</td><td>–сочетаний
–размещений
–перестановок</td><td>- буквенно-цифровые
- азбука Морзе
- Щ–код</td></tr>
</table>

Цифровые коды связаны с переводом сообщений в цифровую форму с учетом количественных характеристик.

Нецифровые коды – предназначены для кодирования качественных сообщений.

Взвешенные коды – это коды, у которых «вес» единицы каждого разряда различен.

Невзвешенные коды – это коды, у которых «вес» единицы каждого разряда имеет одинаковый вес, а числа различаются только по их расположению. Например, код с одинаковым числом единиц (2 единицы, 4 разряда). 0011, 0101, 0110, 1001, 1100. Будут и другие коды.

Из взвешенных кодов наиболее распространен двоичный код с весами 2^{n-1}..8–4–2–1 т.е. представленные числа в обычной двоичной системе счисления. Заметим, что каждому числу от 0 до ∞ соответствует единственная комбинация этих весов, в соответствии с которой располагаются единицы в позициях кода. Однако, для представления цифр от 0 до 9 могут быть применены разновидности кода с весами:2–4–2–1 или 7–4–2–1 и др.

Рассмотрим эти исходы.

Задание. Нарисовать таблицу, оставив две колонки пустыми

Недостатком двоичных кодов является их громоздкость при записи, хотя они в силу простой реализации в технических устройствах наиболее распространены. Часто двоичные коды при записи представляют эквивалентными (десятичными, восьмеричными и др.). Например, $8_{10}=1000_2=10_8$.

Заполним таблицу восьмеричным кодом.

Десятичный код	Двоичный код 8–4–2–1	Двоичный код 2–4–2–1	Двоичный код 7–4–2–1	Код Грея	Восьмеричный код
0	0000	0000	0000	0000	0
1	0001	0001	0001	0001	1
2	0010	0010	0010	0011	2
3	0011	0011	0011	0010	3
4	0100	0100	0100	0110	4
5	0101	1011	0101	0111	5
6	0110	1100	0110	0101	6
7	0111	1101	1000	0100	7
8	1000	1110	1100	1100	10
9	1001	1111	1010	1101	11

Свойства:

Двоичный код 2–4–2–1 удобен тем, что инвертированная кодограмма каждой цифры дополняет основную кодограмму этой цифры до 9 после сложения по mod2. Например, 1 и 8; 2 и 7; 3 и 6; 4 и 5.

Двоичный код 7–4–2–1 отличается тем, что число единиц в каждой комбинации не превышает двух, что в ряде случаев используется для повышения помехоустойчивости передачи.

В двоично-десятичном коде, который объединяет преимущества двоичной и удобство десятичной систем, каждая цифра записывается в виде четырехразрядного числа.

Взвешенные двоичные коды имеют существенный недостаток – они неудобны для применения в АЦП (угол – код; температура – код; скорость – код; и т.д.). Это связано с тем, что соседние комбинации этих кодов могут значительно отличаться друг от друга. Например, 7_2 и 8_2 (0111 и 1000) не совпадают ни в одном разряде. Элементы преобразователя, фиксирующие значение каждого разряда, имеют различную инерционность. Например, счетчик: 0111 +1 => 1000. В промежутке могут быть любые другие значения (от 0 до 15).

От этого недостатка свободны коды, образованные из взвешенных двоичных кодов путем изменения последовательности кодовых комбинаций. Т.к. веса единиц при этом теряют свой смысл, подобные коды не являются взвешенными.

Наиболее распространенным невзвешенным цифровым двоичным кодом является код Грея, называемый отраженным (рефлексным) кодом или еще называют единошаговым кодом. У кода значительное свойство – соседние комбинации в нем отличаются друг от друга только в одном разряде. Следовательно,

ошибки из-за инерционности здесь не превышает единицы младшего разряда. 0001→0011 (успел перейти второе значение, не успел первое значение!).

Важно! Т.к. машинные скорости обработки информации и скорости её изменения в инерциальных системах – несовместимы.

Чтобы из обычного двоичного числа получить код Грея, необходимо сложить по mod2 исходную комбинацию с такой же комбинацией, сдвинутый вправо на один разряд. Младший разряд второго слагаемого при этом отбрасывается.

$0_{10} = 0000$ 2_{10} 0010 3_{10} 0011 И т.д.

$1_{10} = 0001$ 0010 0011

$2_{10} = 0010$ 0011 0010

Сдвинутые коды также строятся по таким принципам, но за счет изменений процедуры формирования они приобретают другие свойства.

Инверсный код – это код, который в сумме по mod2 с исходным дает значение единицу во всех разрядах. Он получается инвертированием всех разрядов прямого (исходного) кода.

Цифровые недвоичные коды

Например, двоичные коды одинакового суммарного веса третьего разряда ∑вес = 5:

I разряд	II разряд	III разряд
0	0	5
0	1	4
0	2	3
0	3	2
0	4	1
0	5	0
…	…	…
5	0	0

Или: десятичные коды одинакового суммарного веса с ограничением в разрядах третьего разряда ∑вес = 5:

I разряд	II разряд	III разряд
3	**3**	**1**
1	3	1
2	3	0
3	2	0
3	1	1

Свойства:

1) Сумма цифр кода не должна превосходить сумму ограничений по разрядам
2) Если суммы цифр кода и ограничений совпадают, то у кода всего одно значение
3) Если сумма цифр кода равна единице, то число значений кода равно числу разрядов, в которых ограничение не равно 0

Нецифровые коды

Ранее было определено, что нецифровые коды служат для передачи команд телеуправления, создания систем данных, передачи стандартных сообщений и других целей, связанных с качественным характером информации.

Здесь есть несколько критериев целесообразности использования таких кодов. Вот некоторые из них:

1) Возрастание числа комбинаций на ограниченное число разрядов;
2) Использование акцентов восприятия с выделением приоритета одного из них;
3) Повышение защищенности от помех и др. аналогичных факторов.

Примеры:

1) Один разряд Двоичный код – 2 комбинаций 0,1
Десятичный код – 10 комбинаций 0,1,2,3,4,5,6,7,8,9
Буквенный код – 30 комбинаций

Несколько разрядов (n) – размещения $A_m^n = \frac{m!}{(n-m)!}$

m – число размещаемых элементов в n разрядах/

Размещения – это когда создаются такие n-разрядные соединения, в которых отличия, как самими элементами, так и порядком их построения (abc) A_3^2 будет: ab, ba, ac, ca, bc, cb.

Сочетания – это соединения в n разрядов, отличающиеся друг от друга только самими элементами, т.е. количество сочетаний в n! раз меньше количества размещений.

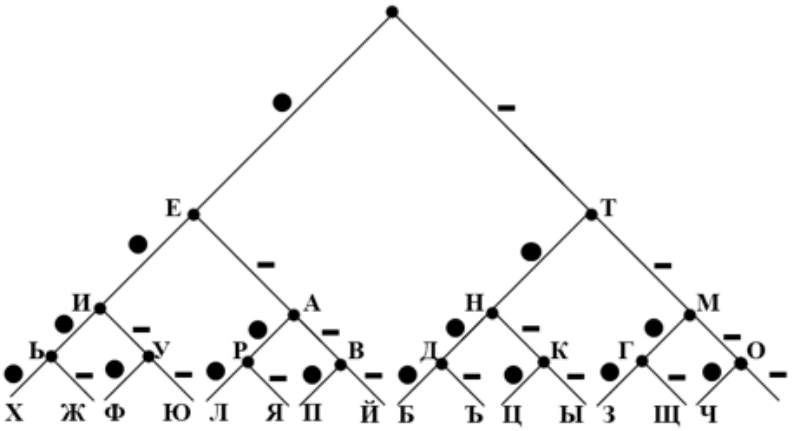
$$C_m^n = \frac{m!}{n!\,(m-n)!}$$

Существует такие перестановки, когда отличие только в порядке расположения элементов.

Примеры: номера машин (комбинация сочетаний и размещений)

номера авиарейсов, маршрутов дорог и т.п.

2) Коды применяемые для слепых (Брайлера), морских (флаги), Морзе и др.



3) Сокращения, имеющие определенный смысл: SOS ; 73! ; 88! ; OK! ; 99! ; три звонка в театре и т.п.

Задание. Записать число в двоичном, двоично-десятичном, восьмеричном, отраженном и инверсном коде.

Отраженный код: исходная двоичная комбинация складывается по mod2 с такой же комбинацией, сдвинутой вправо на один разряд (код Грея). Младший разряд сдвинутого кода при этом не учитывается.

Невзвешенный код: записать цифровые десятичные трехразрядные коды, сумма которых равна S, а значения ограничений по разрядам A_i (i = 1, 2, 3).

9. ОПРЕДЕЛЕНИЕ ЭНТРОПИИ ДИСКРЕТНОГО СИГНАЛА

1. Случайные величины и процессы

Случайные события

В основе ТИ несколько обеспечивающих теоретических направлений. Часть из них изучается на кафедре высшей математики, часть на кафедре ИУС (Тищенко). В большей мере необходимы знания по теории вероятностей, а также по другим направлениям (математическая логика, теория множеств, теория графов и т.д.).

Сегодняшняя задача – остановиться на основополагающих положениях теории вероятности. При этом подход будет менее строгий, чем аксиоматический, который применяется у математиков. Нас больше будет интересовать статистический смысл основных понятий и закономерностей теории вероятности. Такой подход имеет не только абстрактный (математический) смысл, но и физическую (реалистическую) интерпретацию. Но, как и при изучении любой теории (или «точкой» дисциплины) важную роль играют условия, под которыми подразумевается понятие, определение, математическое соотношения и т. д.

Случайное события – это событие, которое может произойти, а может и не произойти. Мы как бы будем наблюдать со стороны, т.е. предполагать существование некого «экспериментатора», который наблюдает за ходом эксперимента (опыта).

Мера случайности события – вероятность. Это численная величина (характеристика случайного события), принимающая значения от 0 до 1. Если вероятность равна 0, то событие невозможно, если 1 – то достоверное (т.е. всегда появлялось в результате эксперимента).

События с большой вероятностью при наблюдении появляются чаще, чем с меньшей. Вероятность случайного события можно оценить приближенно, как отношение числа опытов, в которых событие произошло к числу опытов, которые наблюдались. Чем больше наблюдений, тем выше достоверность оценки вероятности

Если исход опыта случаен, то результат всегда можно разделить на А и $\overline{A}$. Это противоположные события. Они несовместимые, т.е. не могут произойти одновременно.

В процессе эксперимента можно вести наблюдение за

несколькими событиями одновременно. Например – бросание игральной кости: A, B, C, D (четное, нечетное, кратное трем, простое число очков).

Суммой событий называется появление в результате опыта, по крайней мере, одного из событий – слагаемых. Например, если через E_i обозначить событие, заключающееся в выпадении i очков при бросании кости, то событие A (частный результат) равно сумме

$$E_2 + E_4 + E_6$$

Произведением событий называется их совместное появление в опыте. Например, в том же опыте с игральной костью выпадение трех очков знаменует появление трех событий B, C, и D. Очевидно, что вероятность произведения несовместимых событий равна нулю. Запись $P(A, \overline{A}) = 0$

Необходимо различать отношение зависимости событий. Два случайных события называются независимыми, если вероятность одного из них не зависит от того, появилось другое событие или нет. В противном случае события зависимые.

Зависимые события характеризуются условной вероятностью. Для A и B записываются как P(A/B), что означает вероятность событии A при условии, что событие B произошло. В общем случае $P(A) \neq P(A/B)$. Если события A и B несовместимы, то они всегда зависимы, т.к. при $P(A) \neq 0$, вероятность $P(A/B) \equiv 0$.

В теории вероятности большую роль играют теоремы сложения и умножения вероятностей.

Теорема сложения для двух случайных совместных событий A и B выражается так

$$P(A+B) = P(A) + P(B) - P(AB)$$

Формула справедлива для совместных событий, т.е. которые могут произойти, как раздельно, так и вместе. Например, прибытие автобусов на остановку (N_i и N_j) два варианта прибытия + неприбытие ни одного. Если событие A и B несовместимы (однопутная Ж/Д станция, два поезда), то $P(A/B) = 0$ и выражение упрощается $P(A+B)=P(A) + P(B)$. Для любого числа несовместимых событий $P(\sum A_i) = \sum P(A_i)$

Несовместимые события образуют полную группу, если сумма вероятностей этих событий равна единицы.

Теорема умножения вероятностей для двух случайных событий A и B может быть записана в виде

$P(AB) = P(A)\ P(B/A)$ или

$P(AB) = P(B)\ P(A/B)$

С теоремами сложения и умножения тесно связана формула

полной вероятности. Эту формулу просто вывести из решения следующей задачи: событие А может произойти лишь совместно с одним из событий $H_1,\ldots,H_n$, образуют полную группу несовместимых событий; требуется определить вероятность события А.

$$P(A) = \sum_{i=1}^{n} P(AH_i)$$

Применив теорему умножения вероятностей к правой части последнего равенства, окончательно имеем

$$P(A) = -\sum_{i=1}^{n} P(H_i)P(H_i/A)$$

Случайные величины

Случайная величина (ранее рассматривалось случайное событие) – класс случайных событий, имеющих числовые значения. Например в игральной кости 1, 2, 3, 4, 5, 6 говорят о возможных значениях случайной величины. Например, время от 0 до 24 часов, а 25 часов не бывает. В зависимости от того, какова мощность множества возможных значений случайной величины, различают дискретные и непрерывные случайные величины. Множество возможных значений дискретной случайной величины конечно (счетно). Например исходы бросания кости. Для каждой характеристики дискретной случайной величины достаточно пересчитать все возможные значения вероятностей этих значений.

Например

	x_i	1	2	3	4	5	6
Для кости	$P(x_i)$	1/6	1/6	1/6	1/6	1/6	1/6

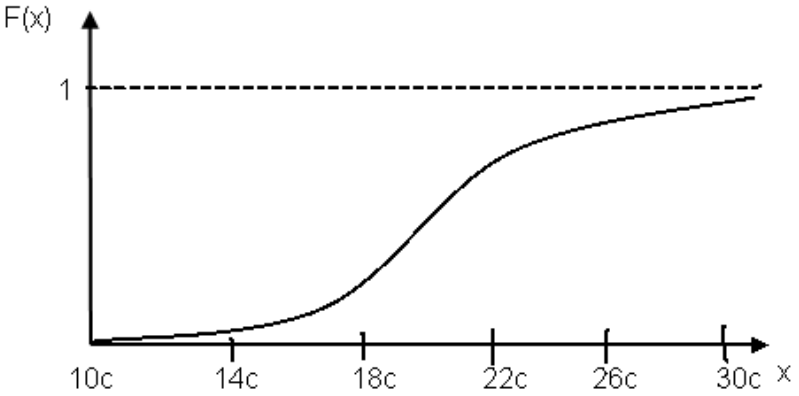
Могут быть и разные $P(x_i)$, например при стрельбе по мишени.

Случайные величины в отличии от их возможных значений обычно обозначаются большими буквами латинского алфавита (это не обязательно, могут быть и малые буквы греческого алфавита).

Множество значений (возможных!) непрерывной случайной величины континуально. Для описания непрерывной случайной величины обычно используется либо функция распределения, либо плотность вероятности.

Функция распределения определяется как вероятность того, что случайная величина X меньше некоторого наперед

заданного её значения x (действительного числа), выступающего в качестве аргумента функции F(x) = P(X<x). Например находится среднее время, за которое группа пробежит 100 метров. Считают, что X – это непрерывная величина, распределенная в интервале от 11с до 30с.



Плотность вероятности распределения определяется как предел отношения вероятности попадания случайной величины X в интервал ΔX, примыкающих непосредственно к точке x к этому интервалу при стремлении к нулю последнего

$$f(x) = \lim_{\Delta x \to 0} \frac{P(x \le X < x + \Delta x)}{\Delta x}$$

Т.е. это скорость изменения функции в рейтинге значения x. Отсюда $f(x) = F'(x)$ $f(x)$ – так обозначается плотность распределения случайной величины (или плотность вероятности). Существует и другие формы описания случайной величины. Все они имеют общее название - законы распределения.

2. Энтропия дискретных сообщений

Рассмотрим некоторый объект (назовем его источником информации), который участвует в эксперименте. Пусть это будет монета (два возможных состояния) или игральная кость (шесть состояний) или рулетка клуба знатоков (множество возможных состояний). После проведения эксперимента источник моет находится в одном из множества состояний { $a_1,a_2,...,a_m$} = {a_k} с вероятностями { $p_1,p_2,...,p_m$} = {p_k}, где k = 1,m. Т.к. состояния {a_k} составляют полную группу событий, то

$$\sum_{k=1}^{m} p_k = 1$$

Заметим, что при m = 1 результат эксперимента известен заранее (априори). С возрастанием m возрастает неопределенность исхода опыта (эксперимента). Это говорит о том, что неопределенность исхода опыта (назовем её численной характеристикой f степени неопределенности) должна зависеть от m, т.е. являться функцией f(m). При этом при m = 1. Эта функция должна обращаться в нуль (т.е. неопределенность полностью отсутствует), а при возрастании m она должна увеличиваться.

Если событие сложное, состоящее из нескольких независимых событий r и q, то функция f(r,q) должна возрастать. Считается, что неопределенность сложного опыта должна быть больше и равна сумме неопределенности составляющих.

$$f(r,q) = f(r) + f(q)$$

Если система передает информацию о двух независимых параметрах X и Y с числом возможных значений этих параметров m и n, соответственно, то общее число сообщений будет N = m*n. Следовательно неопределенность в этом случае больше. Но и информации при получении результатов сложного опыта также больше.

Отсюда требования, которые предъявляются к мере количества информации. Для равновероятных событий (результат опыта) они будут следующие:

- Мера количества информации равна нулю для опыта с одним исходом;
- Она должна быть пропорциональна количеству равновероятных исходов;
- Мера должна обладать свойством аддитивности (сложения) результатов опытов, т.е. формация сложного опыта должна составлять сумму информаций, составляющих опыт.

Этим требования удовлетворяет единственная функция – это логарифм числа равновероятных исходов, т.е. log N

а) Если N = 1 → log 1 = 0

б) С ростом N – log N возрастает

в) Для сложного опыта число исходов N = m*n и тогда logN = log m*n = log m + log n

т.е. выполняется свойство аддитивности.

Пример. Опыт содержит 16 равновероятных исходов. Определить количество информации на один исход опыта

$\log_2 16 = 4$ $\left(\frac{\text{дв.ед}}{\text{исход}}\right)$

Если результатом опыта (всего их n) имеют неравные вероятности, то рассуждения принимают вид:

x	x_1	x_2	x_3	…	x_n
p(x)	$p(x_1)$	$p(x_2)$	$p(x_3)$	…	$p(x_n)$

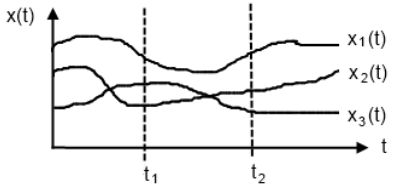
Какое количество информации получит наблюдатель от одного исхода? Чем большей вероятностью обладает исход, тем меньшей неопределенностью и меньше количество информации. Отсюда требование к мере количества информации: исходам с меньшей вероятностью должно соответствовать большее количество информации. Такому требованию удовлетворяет только функция:

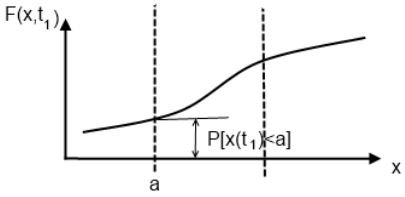
$$log_2 \frac{1}{p(x_i)} = -log_2 p(x_2)$$

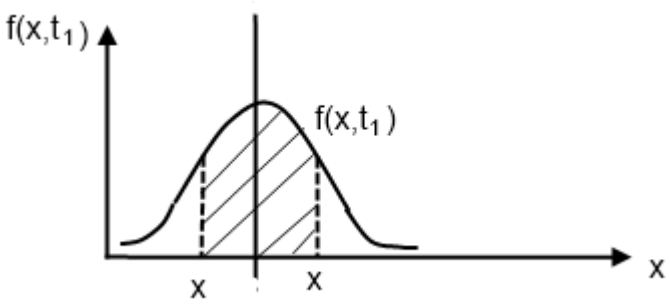
В общем случае переносчиками информации являются сигналы, имеющие случайный характер. Сигналам мешают выполнять свои функции помехи – тоже случайные. Во времени сигналы и помехи являются случайными процессами. Случайные процессы описываются случайными функциями. Это таки функции, которые при каждом фиксированном значении своего аргумента являются случайной величиной. Если аргумент время, то случайная функция называется случайным процессом.

Законы распределения характеризуют случайные величины (F(x) – универсальная форма; f(x) – для непрерывной случайной величины). Плотность распределения случайной величины f(x) может быть одномерной и двумерной. Одномерная плотность распределения не учитывает статистические связи между отдельными сочетаниями случайного процесса $f(x_1,t_1)$ сечение по t_1.

Двумерная плотность распределения учитывает вероятность статистической взаимосвязи между двумя сечениями x(t) в момент времени t_1 и t_2







Основные соотношения:

1. $x_1(t_1)$ – это фактически не функция времени, а случайная величина.
2. $f(x_1,t_1) = \frac{\partial F(x,t_1)}{\partial x}$
3. $F(x_b,t_1) - F(x_a,t_1) = P(x_a \le x(t1) \le x_b) = \int_{x_a}^{x_b} f(x1,t1)dx$

Двумерная плотность распределения – это, как частный случай совместной двумерной плотности вероятности двух процессов X(t) и Y(t). Т.е. можно рассматривать, как t^o в 7 и 20 часов или, как t^o и давление в t_1

Эта функция определяет количество информации при наступлении x_i исхода опыта X_i. Она называется индивидуальной (частной) информацией.

$i(x_i) = -log_2 p(x_i)$

Если число исходов опыта n и они равновероятны, то:

$p(x_i) = \frac{1}{n}$; $i(x_i) = -log_2 \frac{1}{n} = log_2 n$

Последнее соответствует ранее приведенным результатам.

3. Приближенное описание случайных величин. Случайные процессы