



Современная теория информации

Лекция 1. Измерение информации. Энтропия.

Содержание лекции

- 1 Историческая заметка.
- 2 Дискретные ансамбли.
- 3 Измерение информации.
- 4 Энтропия

К. Шеннон, «отец» Теории информации



Клод Элвуд Шеннон, 1916–2001

Шеннон и информационный век

Мы пишем, чтобы предложить памятную [почтовую] марку в честь столетия со дня рождения Клода Элвуда Шеннона, отца информационного века. Информационные системы, такие как смартфоны, MP3-плееры и Интернет изменяют нашу жизнь. Они хранят наши воспоминания, объединяют наши сообщества и развлекают. Они облегчают доставку медицинских услуг и обеспечивают основы для наших финансовых, промышленных и правительственных организаций.

Шеннон и информационный век

Подобно тому как Ньютон открыл законы гравитации и движения, Шеннон открыл законы информации. Раскрывая простые законы, лежащие в основе таких чрезвычайно сложных проблем, как связь, вычислительная техника, память и криптография, Шеннон открыл дверь, которая привела нас к информационной эпохе. Его игривый дух и использование науки, технологии, техники и математики для решения реальных проблем, которые меняют мир, будут вдохновлять как молодых, так и старых... Настоящей петицией мы просим USPS [U.S. Postal Service] создать марку в его честь.¹

¹president of IEEE Mary Sue Coleman, president of Bell Labs Gee Rittenhouse and president of MIT Rafael Reif, 2013.

Реакция на работу Шеннона в 1940-х

Эта статья плохо мотивирована и чрезмерно абстрактна. Неясно, к какой практической проблеме она имеет отношение. Автор утверждает, что «семантические аспекты коммуникации не имеют отношения к инженерным проблемам», что, по-видимому, указывает на то, что его теория подходит в основном для передачи тарабарщины. Увы, люди не платят, чтобы тарабарщина передавалась повсюду.

Реакция на работу Шеннона в 1940-х

Я не понимаю значимости дискретных источников: независимо от того, что делается, в конце концов, сигнал ... всегда будет аналоговым. Автор упоминает вычислительные машины ... дюжины или около того таких машин будет достаточно для всех вычислений, которые нам ... нужны в обозримом будущем... IBM решил не заниматься бизнесом в сфере электронных вычислительных машин и этот журнал, вероятно, должен сделать тоже самое².

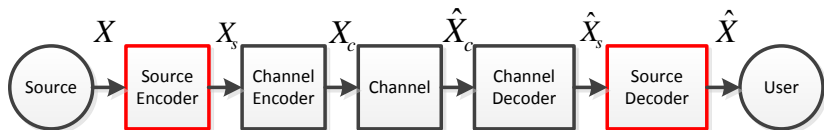
- С 1953 года издаётся журнал "IEEE Transactions on Information Theory".

²Santini S. We are sorry to inform you... IEEE Computer, 2005.

Теория информации в СССР и России

- В 1961 году был создан *Институт проблем передачи информации* (ИППИ) РАН.
 - ▶ С 1965 года издаётся журнал "Проблемы передачи информации".
- В 1962 году была образована *кафедра технической кибернетики* ЛИАП (ныне СПбГУАП).
 - ▶ В 1982 году издан учебник Колесник В.Д., Полтырев Г.Ш., "Курс теории информации".
 - ▶ В 2010 году издан учебник Кудряшов Б.Д., "Теория информации".

Общая схема системы связи³



- *Кодирование дискретных источников*: отвечает за представление сообщений источника в наиболее компактной форме для хранения или передачи.
- *Помехоустойчивое кодирование*: отвечает за защиту сообщений от помех в канале связи.

³Shannon, C.E. „A Mathematical Theory of Communication”, Bell System Technical Journal, 1948.

Практическое применение

- Архивирование данных (ZIP, RAR, 7-Zip);
- Сжатие речи (CELP);
- Сжатие звука (MP3);
- Сжатие изображений (JPEG, JPEG2000, PNG);
- Сжатие видео (MPEG-2, H.264/AVC, H.265/HEVC, H.266/VVC);

Практическое применение

- Архивирование данных (ZIP, RAR, 7-Zip);
- Сжатие речи (CELP);
- Сжатие звука (MP3);
- Сжатие изображений (JPEG, JPEG2000, PNG);
- Сжатие видео (MPEG-2, H.264/AVC, H.265/HEVC, H.266/VVC);

Практическое применение

- Архивирование данных (ZIP, RAR, 7-Zip);
- Сжатие речи (CELP);
- Сжатие звука (MP3);
- Сжатие изображений (JPEG, JPEG2000, PNG);
- Сжатие видео (MPEG-2, H.264/AVC, H.265/HEVC, H.266/VVC);

Практическое применение

- Архивирование данных (ZIP, RAR, 7-Zip);
- Сжатие речи (CELP);
- Сжатие звука (MP3);
- Сжатие изображений (JPEG, JPEG2000, PNG);
- Сжатие видео (MPEG-2, H.264/AVC, H.265/HEVC, H.266/VVC);

Практическое применение

- Архивирование данных (ZIP, RAR, 7-Zip);
- Сжатие речи (CELP);
- Сжатие звука (MP3);
- Сжатие изображений (JPEG, JPEG2000, PNG);
- Сжатие видео (MPEG-2, H.264/AVC, H.265/HEVC, H.266/VVC);

Практическое применение

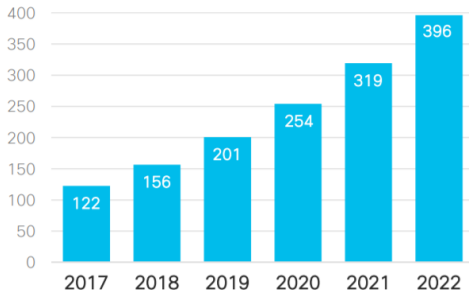
- Архивирование данных (ZIP, RAR, 7-Zip);
- Сжатие речи (CELP);
- Сжатие звука (MP3);
- Сжатие изображений (JPEG, JPEG2000, PNG);
- Сжатие видео (MPEG-2, H.264/AVC, H.265/HEVC, H.266/VVC);

Global IP Traffic Growth

Global IP traffic will increase 3-fold from 2017 to 2022

26% CAGR
2017-2022

Exabytes
per Month



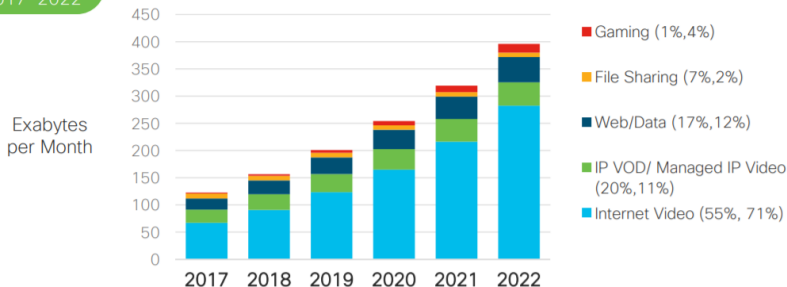
© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Source: Cisco VNI Global IP Traffic Forecast, 2017-2022

Global IP Traffic by Application Type

By 2022, video will account for 82% of global IP traffic

26% CAGR
2017-2022



* Figures (n) refer to 2017, 2022 traffic share

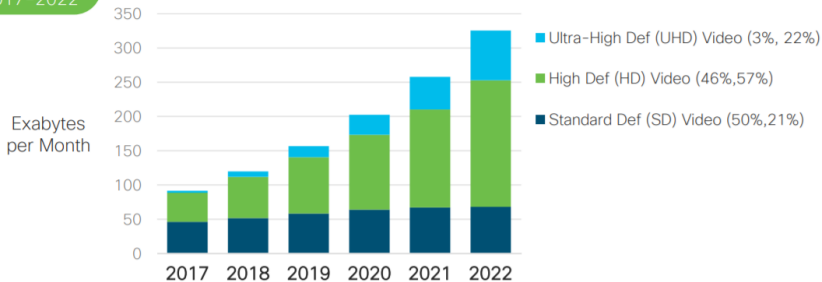
© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Source: Cisco VNI Global IP Traffic Forecast, 2017-2022

High Definition Content Impacts IP Video Growth

UHD IP video will account for 22% of global IP video traffic by 2022

29% CAGR
2017-2022



* Figures (n) refer to 2017, 2022 traffic share

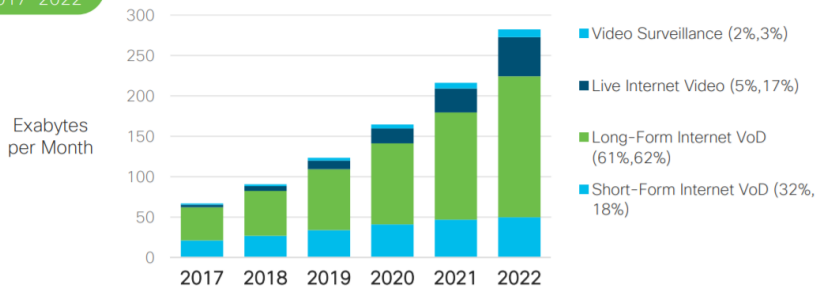
© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Source: Cisco VNI Global IP Traffic Forecast, 2017-2022

Global Internet Video Traffic by Type

By 2022, live video will increase 15-fold and reach 17% of Internet video traffic

33% CAGR
2017-2022



* Figures (n) refer to 2017, 2022 traffic share

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Source: Cisco VNI Global IP Traffic Forecast, 2017-2022

Дискретные ансамбли

- $X = \{x\}$ – дискретное множество, содержащее конечное число элементов (элементарных событий) $x \in X$.
- Множество чисел $\{p(x)\}$, $p(x) \geq 0$, $\sum_x p(x) = 1$ задаёт *распределение вероятностей*.
- $X = \{x, p(x)\}$ – **дискретный ансамбль**.
- $\Omega = \{A\}$ – множество всевозможных подмножеств X .
- Вероятность сложного события A :

$$P(A) = \sum_{x \in A} p(x), A \in \Omega.$$

Дискретные ансамбли

- Обозначим произведение событий A и B как $AB = A \cap B$.
- Для произвольной пары событий $A, B \subseteq X$ **условная вероятность**

$$P(A|B) = \frac{P(AB)}{P(B)}, \text{ если } P(B) \neq 0, \text{ иначе } 0.$$

- Пусть $X = \{00, 01, 10, 11\}$, где 0 – выпала решка, 1 – орёл. Пусть A означает, что два раза выпал орёл, $A = \{11\}$, B – что из двух раз хотя бы один раз выпал орёл, $B = \{01, 10, 11\}$.

$$P(A|B) = ?$$

Дискретные ансамбли

- Обозначим произведение событий A и B как $AB = A \cap B$.
- Для произвольной пары событий $A, B \subseteq X$ **условная вероятность**

$$P(A|B) = \frac{P(AB)}{P(B)}, \text{ если } P(B) \neq 0, \text{ иначе } 0.$$

- Пусть $X = \{00, 01, 10, 11\}$, где 0 – выпала решка, 1 – орёл. Пусть A означает, что два раза выпал орёл, $A = \{11\}$, B – что из двух раз хотя бы один раз выпал орёл, $B = \{01, 10, 11\}$.

$$P(A|B) = \frac{P\{11\}}{P\{01, 10, 11\}} = \frac{1/4}{3/4} = \frac{1}{3}.$$

Дискретные ансамбли

- Обозначим произведение событий A и B как $AB = A \cap B$.
- Для произвольной пары событий $A, B \subseteq X$ **условная вероятность**

$$P(A|B) = \frac{P(AB)}{P(B)}, \text{ если } P(B) \neq 0, \text{ иначе } 0.$$

- Из этого определения следует

$$P(AB) = P(A|B)P(B).$$

- В общем случае:

$$P(A_1 \dots A_n) = P(A_1)P(A_2|A_1)P(A_3|A_1A_2) \dots P(A_n|A_1 \dots A_{n-1}).$$

Дискретные ансамбли

- События $A, B \in \Omega$ независимы, если:

$$P(AB) = P(A)P(B).$$

- $A_1, \dots, A_n \in \Omega$ совместно независимы, если:

$$P(A_1 \dots A_n) = P(A_1)P(A_2) \dots P(A_n).$$

- Эквивалентно, $A, B \in \Omega$ независимы, если:

$$P(A|B) = P(A); P(B|A) = P(B).$$

- Вероятность объединения событий:

$$P(A \cup B) = P(A) + P(B) - P(AB);$$

$$P\left(\bigcup_{m=1}^M A_m\right) \leq \sum_{m=1}^M P(A_m)$$

Дискретные ансамбли

Задачи: найти вероятность существования пути из A в C

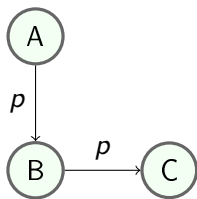


Рис.: Пример 1

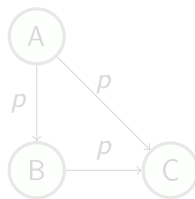


Рис.: Пример 2

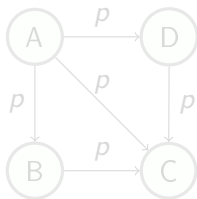


Рис.: Пример 3

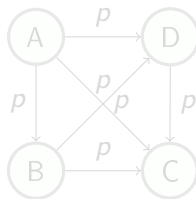


Рис.: Пример 4

Дискретные ансамбли

Задачи: найти вероятность существования пути из A в C

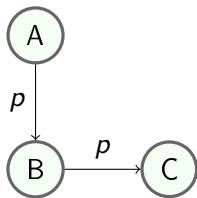


Рис.: Пример 1

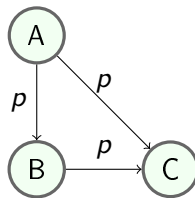


Рис.: Пример 2

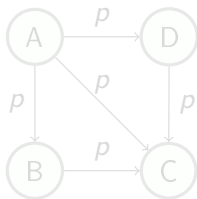


Рис.: Пример 3

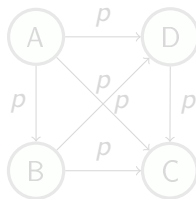


Рис.: Пример 4

Дискретные ансамбли

Задачи: найти вероятность существования пути из A в C

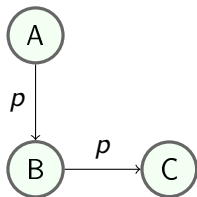


Рис.: Пример 1

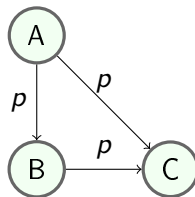


Рис.: Пример 2

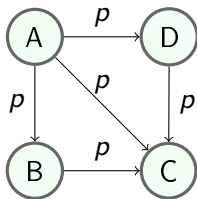


Рис.: Пример 3

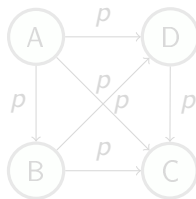


Рис.: Пример 4

Дискретные ансамбли

Задачи: найти вероятность существования пути из A в C

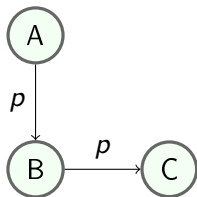


Рис.: Пример 1

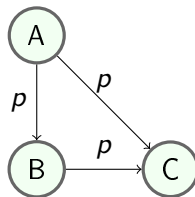


Рис.: Пример 2

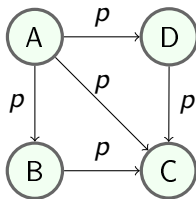


Рис.: Пример 3

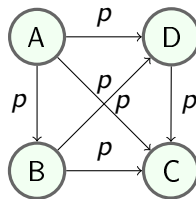


Рис.: Пример 4

Дискретные ансамбли

- Формула полной вероятности:

Пусть даны M несовместных событий⁴ H_1, \dots, H_M ("гипотез"), таких что

$P\left(\bigcup_{m=1}^M H_m\right) = 1$. Тогда вероятность произвольного события A

$$P(A) = \sum_{m=1}^M P(A|H_m)P(H_m).$$

$$P(AB) = P(A|B)P(B).$$

- Формула апостериорной вероятности (Байеса):

$$P(H_j|A) = \frac{P(AH_j)}{P(A)} = \frac{P(A|H_j)P(H_j)}{\sum_{m=1}^M P(A|H_m)P(H_m)}.$$

⁴пересечение – пустое множество

Дискретные ансамбли

Пример

- Формула апостериорной вероятности (Байеса):

$$P(H_j|A) = \frac{P(AH_j)}{P(A)} = \frac{P(A|H_j)P(H_j)}{\sum_{m=1}^M P(A|H_m)P(H_m)}.$$

- Пусть $p_1 = 0.9$ – вероятность бракованного изделия у первого рабочего, у второго – $p_2 = 0.5$, третьего – $p_3 = 0.2$. Первый изготовил $n_1 = 800$ деталей, второй – $n_2 = 600$, третий – $n_3 = 900$. Случайная деталь оказалась бракованной. Какова вероятность того, что её изготовил второй рабочий?

- ▶ H_1, H_2 и H_3 – гипотезы, что деталь произвёл первый, второй или третий рабочий, соответственно, $P(H_i) = \frac{n_i}{\sum n_i}$.
- ▶ A – событие, что деталь оказалась бракованной, $P(A|H_i) = p_i$.
- ▶

$$P(H_2|A) = \frac{P(A|H_2)P(H_2)}{P(A|H_1)P(H_1) + P(A|H_2)P(H_2) + P(A|H_3)P(H_3)} = 0.25.$$

Дискретные ансамбли

Пример

- Формула апостериорной вероятности (Байеса):

$$P(H_j|A) = \frac{P(AH_j)}{P(A)} = \frac{P(A|H_j)P(H_j)}{\sum_{m=1}^M P(A|H_m)P(H_m)}.$$

- Пусть $p_1 = 0.9$ – вероятность бракованного изделия у первого рабочего, у второго – $p_2 = 0.5$, третьего – $p_3 = 0.2$. Первый изготовил $n_1 = 800$ деталей, второй – $n_2 = 600$, третий – $n_3 = 900$. Случайная деталь оказалась бракованной. Какова вероятность того, что её изготовил второй рабочий?

- ▶ H_1, H_2 и H_3 – гипотезы, что деталь произвёл первый, второй или третий рабочий, соответственно, $P(H_i) = \frac{n_i}{\sum n_i}$.
- ▶ A – событие, что деталь оказалась бракованной, $P(A|H_i) = p_i$.
- ▶

$$P(H_2|A) = \frac{P(A|H_2)P(H_2)}{P(A|H_1)P(H_1) + P(A|H_2)P(H_2) + P(A|H_3)P(H_3)} = 0.25.$$

Дискретные ансамбли

Пример

- Формула апостериорной вероятности (Байеса):

$$P(H_j|A) = \frac{P(AH_j)}{P(A)} = \frac{P(A|H_j)P(H_j)}{\sum_{m=1}^M P(A|H_m)P(H_m)}.$$

- Пусть $p_1 = 0.9$ – вероятность бракованного изделия у первого рабочего, у второго – $p_2 = 0.5$, третьего – $p_3 = 0.2$. Первый изготовил $n_1 = 800$ деталей, второй – $n_2 = 600$, третий – $n_3 = 900$. Случайная деталь оказалась бракованной. Какова вероятность того, что её изготовил второй рабочий?
 - ▶ H_1, H_2 и H_3 – гипотезы, что деталь произвёл первый, второй или третий рабочий, соответственно, $P(H_i) = \frac{n_i}{\sum n_i}$.
 - ▶ A – событие, что деталь оказалась бракованной, $P(A|H_i) = p_i$.
 - ▶

$$P(H_2|A) = \frac{P(A|H_2)P(H_2)}{P(A|H_1)P(H_1) + P(A|H_2)P(H_2) + P(A|H_3)P(H_3)} = 0.25.$$

Дискретные ансамбли

Пример

- Формула апостериорной вероятности (Байеса):

$$P(H_j|A) = \frac{P(AH_j)}{P(A)} = \frac{P(A|H_j)P(H_j)}{\sum_{m=1}^M P(A|H_m)P(H_m)}.$$

- Пусть $p_1 = 0.9$ – вероятность бракованного изделия у первого рабочего, у второго – $p_2 = 0.5$, третьего – $p_3 = 0.2$. Первый изготовил $n_1 = 800$ деталей, второй – $n_2 = 600$, третий – $n_3 = 900$. Случайная деталь оказалась бракованной. Какова вероятность того, что её изготовил второй рабочий?

- ▶ H_1, H_2 и H_3 – гипотезы, что деталь произвёл первый, второй или третий рабочий, соответственно, $P(H_i) = \frac{n_i}{\sum n_i}$.
- ▶ A – событие, что деталь оказалась бракованной, $P(A|H_i) = p_i$.
- ▶

$$P(H_2|A) = \frac{P(A|H_2)P(H_2)}{P(A|H_1)P(H_1) + P(A|H_2)P(H_2) + P(A|H_3)P(H_3)} = 0.25.$$

Дискретные ансамбли

- Произведение ансамблей $X = \{x, p_X(x)\}$ и $Y = \{y, p_Y(y)\}$ определяется совместным распр. $\{p_{XY}(x, y)\}$, $\{(x, y) : x \in X, y \in Y\}$.
- Ансамбль произведений $XY = \{(x, y), p_{XY}(x, y)\}$.
- Условное распределение вероятностей:

$$p(x|y) = \begin{cases} \frac{p(x,y)}{p(y)}, & \text{if } p(y) \neq 0, \\ 0 & \text{иначе,} \end{cases} \quad x \in X.$$

- Ансамбли X и Y независимы, если

$$p(x, y) = p(x)p(y), \quad x \in X, \quad y \in Y.$$

Измерение информации

Интуитивный подход

Количество информации = затратам (во времени или пространстве), необходимым для передачи (хранения) данных.

Данные	Представление
Числа (измерения)	Длина зависит от диапазона
Текст	8 бит (1 байт) на букву
Цифровая речь	13 бит на отсчет
Изображения (bmp)	3 байта на пиксель

Измерение информации

Собственная информация

$X = \{x, p(x)\}$ – ансамбль, $\mu(x)$ – мера (количество) информации в x .

- Неотрицательность: $\mu(x) \geq 0$.
- $\mu(x)$ должна быть функцией от $p(x)$.
- Монотонность: если $x, y \in X$, $p(x) \geq p(y)$, тогда $\mu(x) \leq \mu(y)$.
- Аддитивность: Если x и y независимы, тогда $\mu(x, y) = \mu(x) + \mu(y)$.
- $\mu(p(x)^k) = k\mu(p(x))$.

Перечисленные требования приводят к следующему определению:

$$I(x) = -\log p(x), x \in X.$$

Измерение информации

Собственная информация

$X = \{x, p(x)\}$ – ансамбль, $\mu(x)$ – мера (количество) информации в x .

- **Неотрицательность:** $\mu(x) \geq 0$.
- $\mu(x)$ должна быть функцией от $p(x)$.
- **Монотонность:** если $x, y \in X$, $p(x) \geq p(y)$, тогда $\mu(x) \leq \mu(y)$.
- **Аддитивность:** Если x и y независимы, тогда $\mu(x, y) = \mu(x) + \mu(y)$.
- $\mu(p(x)^k) = k\mu(p(x))$.

Перечисленные требования приводят к следующему определению:

$$I(x) = -\log p(x), x \in X.$$

Измерение информации

Собственная информация

$X = \{x, p(x)\}$ – ансамбль, $\mu(x)$ – мера (количество) информации в x .

- *Неотрицательность*: $\mu(x) \geq 0$.
- $\mu(x)$ должна быть функцией от $p(x)$.
- *Монотонность*: если $x, y \in X$, $p(x) \geq p(y)$, тогда $\mu(x) \leq \mu(y)$.
- *Аддитивность*: Если x и y независимы, тогда $\mu(x, y) = \mu(x) + \mu(y)$.
- $\mu(p(x)^k) = k\mu(p(x))$.

Перечисленные требования приводят к следующему определению:

$$I(x) = -\log p(x), x \in X.$$

Измерение информации

Собственная информация

$X = \{x, p(x)\}$ – ансамбль, $\mu(x)$ – мера (количество) информации в x .

- *Неотрицательность*: $\mu(x) \geq 0$.
- $\mu(x)$ должна быть функцией от $p(x)$.
- *Монотонность*: если $x, y \in X$, $p(x) \geq p(y)$, тогда $\mu(x) \leq \mu(y)$.
- *Аддитивность*: Если x и y независимы, тогда $\mu(x, y) = \mu(x) + \mu(y)$.
- $\mu(p(x)^k) = k\mu(p(x))$.

Перечисленные требования приводят к следующему определению:

$$I(x) = -\log p(x), x \in X.$$

Измерение информации

Собственная информация

$X = \{x, p(x)\}$ – ансамбль, $\mu(x)$ – мера (количество) информации в x .

- *Неотрицательность*: $\mu(x) \geq 0$.
- $\mu(x)$ должна быть функцией от $p(x)$.
- *Монотонность*: если $x, y \in X$, $p(x) \geq p(y)$, тогда $\mu(x) \leq \mu(y)$.
- *Аддитивность*: Если x и y независимы, тогда $\mu(x, y) = \mu(x) + \mu(y)$.
- $\mu(p(x)^k) = k\mu(p(x))$.

Перечисленные требования приводят к следующему определению:

$$I(x) = -\log p(x), x \in X.$$

Измерение информации

Собственная информация

$X = \{x, p(x)\}$ – ансамбль, $\mu(x)$ – мера (количество) информации в x .

- *Неотрицательность*: $\mu(x) \geq 0$.
- $\mu(x)$ должна быть функцией от $p(x)$.
- *Монотонность*: если $x, y \in X$, $p(x) \geq p(y)$, тогда $\mu(x) \leq \mu(y)$.
- *Аддитивность*: Если x и y независимы, тогда $\mu(x, y) = \mu(x) + \mu(y)$.
- $\mu(p(x)^k) = k\mu(p(x))$.

Перечисленные требования приводят к следующему определению:

$$I(x) = -\log p(x), x \in X.$$

Измерение информации

Энтропия

Definition

$$H(X) = \mathbb{E}[I(x)].$$

$$H(X) = \sum_x p(x) I(x).$$

$$H(X) = \sum_x -p(x) \log p(x).$$

Энтропия

Примеры

A: $X = \{a, b, c\}; p(a) = p(b) = p(c) = 1/3,$
 $I(a) = I(b) = I(c) = H(X) = \log 3 = 1.59 \text{ бит},$

B: $X = \{a, b, c\}; p(a) = p(b) = 1/4, p(c) = 1/2$
 $I(a) = I(b) = 2, I(c) = 1$
 $H = 1.5 \text{ бита}.$

C: $X = \{0, 1\}; p(0) = 0.9, p(1) = 0.1 ,$
 $I(0) = 0.152, I(1) = 3.322;$
 $H = 0.469 \text{ бит}.$

D: $X = \{0, 1\}, p(0) = p(1) = 1/2$
 $I(0) = I(1) = H(X) = 1 \text{ бит}.$

Энтропия

Свойства энтропии

- 1 $H(X) \geq 0$.
- 2 $H(X) \leq \log |X|$. Равенство, если все элементы X равновероятны.
- 3 Если $X = \{x, p(x)\}$ и $Y = \{y = f(x), p(y)\}$, тогда $H(Y) \leq H(X)$ с равенством, если f обратима.
- 4 Если X и Y независимы, тогда

$$H(XY) = H(X) + H(Y).$$

Энтропия

Свойства энтропии

- 5 $H(X)$ – выпуклая \cap функция распределения вероятностей на элементах ансамбля X .
- 6 Пусть $X = \{x, p(x)\}$ и $A \subseteq X$. Введем ансамбль $X' = \{x, p'(x)\}$ и $p'(x)$ как:

$$p'(x) = \begin{cases} \frac{P(A)}{|A|}, x \in A, \\ p(x), x \notin A. \end{cases}$$

Тогда $H(X') \geq H(X)$.

- 7 Если для двух ансамблей X и Y распределения вероятностей отличаются только порядком следования элементов, то $H(X) = H(Y)$.

Доказательство свойства (2)

$$\begin{aligned} H(X) - \log |X| &\stackrel{(a)}{=} - \sum_{x \in X} p(x) \log p(x) - \sum_{x \in X} p(x) \log |X| = \\ &\stackrel{(b)}{=} \sum_{x \in X} p(x) \log \frac{1}{p(x)|X|} \leq \\ &\stackrel{(c)}{\leq} \log e \left[\sum_{x \in X} p(x) \left(\frac{1}{p(x)|X|} - 1 \right) \right] = \\ &= \log e \left(\sum_{x \in X} \frac{1}{|X|} - \sum_{x \in X} p(x) \right) = 0 \quad . \end{aligned}$$

Доказательство свойства (2)

$$\begin{aligned} H(X) - \log |X| &\stackrel{(a)}{=} - \sum_{x \in X} p(x) \log p(x) - \sum_{x \in X} p(x) \log |X| = \\ &\stackrel{(b)}{=} \sum_{x \in X} p(x) \log \frac{1}{p(x)|X|} \leq \\ &\stackrel{(c)}{\leq} \log e \left[\sum_{x \in X} p(x) \left(\frac{1}{p(x)|X|} - 1 \right) \right] = \\ &= \log e \left(\sum_{x \in X} \frac{1}{|X|} - \sum_{x \in X} p(x) \right) = 0 \quad . \end{aligned}$$

Доказательство свойства (2)

$$\begin{aligned} H(X) - \log |X| &\stackrel{(a)}{=} - \sum_{x \in X} p(x) \log p(x) - \sum_{x \in X} p(x) \log |X| = \\ &\stackrel{(b)}{=} \sum_{x \in X} p(x) \log \frac{1}{p(x)|X|} \leq \\ &\stackrel{(c)}{\leq} \log e \left[\sum_{x \in X} p(x) \left(\frac{1}{p(x)|X|} - 1 \right) \right] = \\ &= \log e \left(\sum_{x \in X} \frac{1}{|X|} - \sum_{x \in X} p(x) \right) = 0 . \end{aligned}$$

Доказательство свойства (2)

$$\begin{aligned} H(X) - \log |X| &\stackrel{(a)}{=} - \sum_{x \in X} p(x) \log p(x) - \sum_{x \in X} p(x) \log |X| = \\ &\stackrel{(b)}{=} \sum_{x \in X} p(x) \log \frac{1}{p(x)|X|} \leq \\ &\stackrel{(c)}{\leq} \log e \left[\sum_{x \in X} p(x) \left(\frac{1}{p(x)|X|} - 1 \right) \right] = \\ &= \log e \left(\sum_{x \in X} \frac{1}{|X|} - \sum_{x \in X} p(x) \right) = 0 \quad . \end{aligned}$$

Доказательство (с)

- $\ln x \leq x - 1 \iff \log x \leq (x - 1) \log e.$

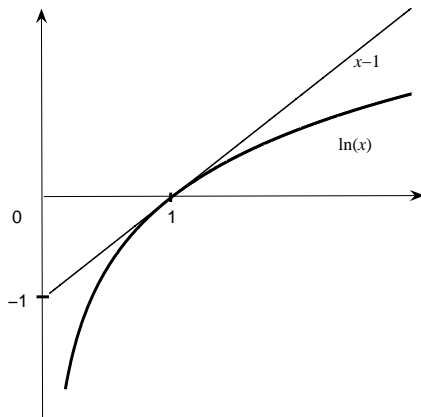


Рис.: Графическая интерпретация $\ln(x) \leq x - 1$