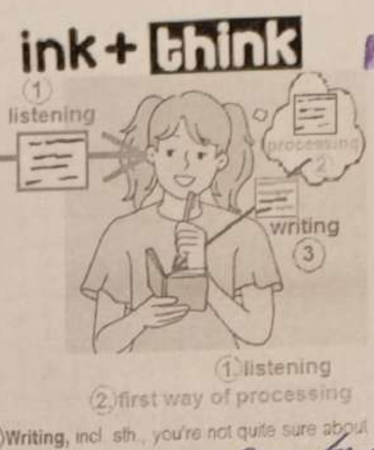
+0.1 +0.1 12.2 +0.1 4! +0.1 +0.1 +0.1

+0.1
6.3

занимает 1-ое место

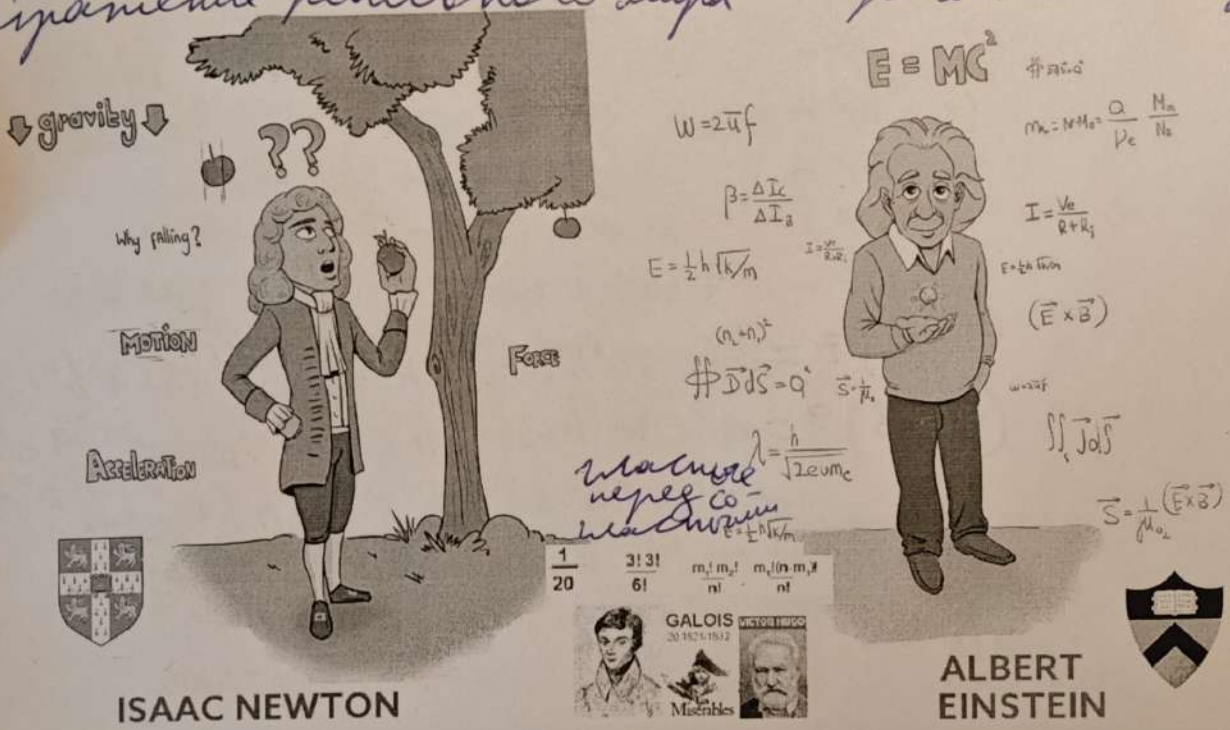


мелом и разговор запись обдумывание

School ⇩gravity⇩ MOTION ==formalism==> University $E = MC^2$ $\oint \vec{D}\,d\vec{S} = Q$ $\iint \vec{J}\,d\vec{S}$

CONCRETE AND ABSTRACT THINKING

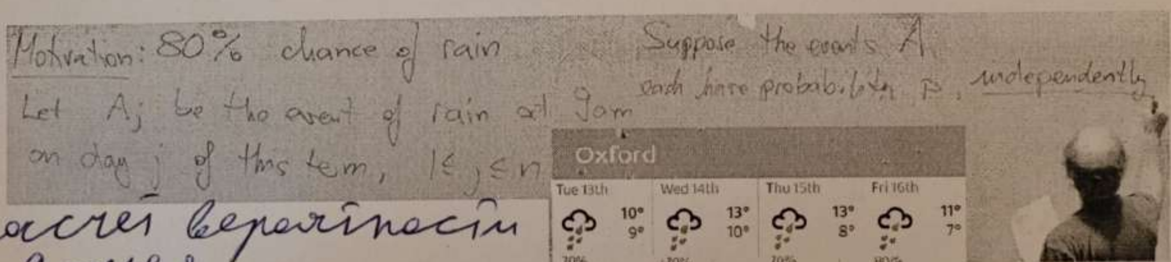
отражение реального мира реальный мир



гласные перед со-гласными

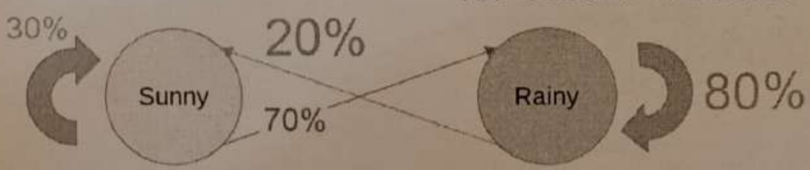
ISAAC NEWTON

ALBERT EINSTEIN



расчет вероятности дождя

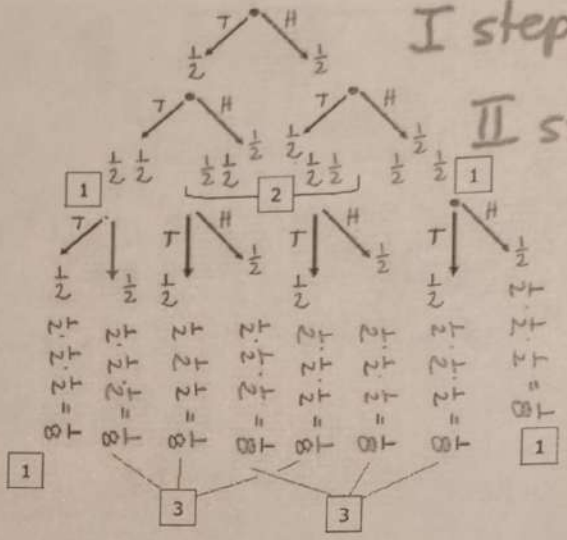
Markoff Chain Probability Model for Oxford Weather



Подреждане монетки

Pascal's triangle

0					1				→ 1
1				1		1			→ 2
2			1		2		1		→ 4
3		1		3		3		1	→ 8
4	1		4		6		4		1 → 16
5	1	5		10		10	5	1	→ 32
6	1	6	15		20	15	6	1	→ 64
7	1	7	21	35	35	21	7	1	→ 128
8	1	8	28	56	70	56	28	8	1 → 256
9	1	9	36	84	126	126	84	36	9 1 → 512



$(a+b)^0 = 1$

$(a+b)^1 = a+b$

$(a+b)^2 = a^2+2ab+b^2$

$(a+b)^3 = a^3+3a^2b+3ab^2+b^3$

$(a+b)^4 = a^4+4a^3b+6a^2b^2+4ab^3+b^4$

$(a+b)^5 = a^5+5a^4b+10a^3b^2+10a^2b^3+5ab^4+b^5$

Newton's Binomial

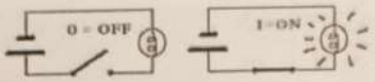
$(a+b)^7 = a^7 + 7a^6b + 21a^5b^2 + 35a^4b^3 + 35a^3b^4 + 21a^2b^5 + 7ab^6 + b^7$

$(a+b)^9 = a^9 + 9a^8b + 36a^7b^2 + 84a^6b^3 + 126a^5b^4 + 126a^4b^5 + 84a^3b^6 + 36a^2b^7 + 9ab^8 + b^9$

логика аристотеля → булева алгебра

Massachusetts Institute of Technology (MIT)

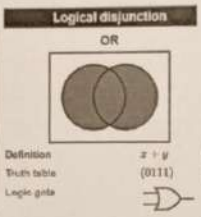
Lecture by Pr. Bob Gallagher
Boole (1815-1864) & Shannon (1916-2001)



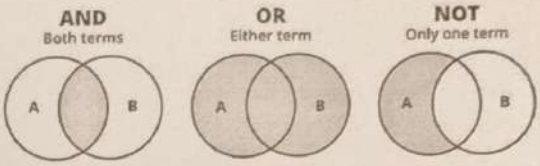
Logical addition (disjunction)

A	B	F=A∨B
0	0	0
0	1	1
1	0	1
1	1	1

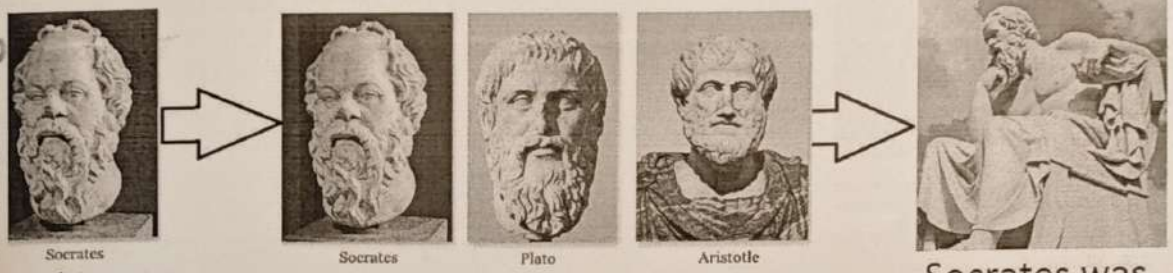
A	B	$A \vee B$
True	True	True
True	False	True
False	True	True
False	False	False



BOOLEAN LOGIC



Good logic



Socrates was a philosopher

$S \in \Phi$

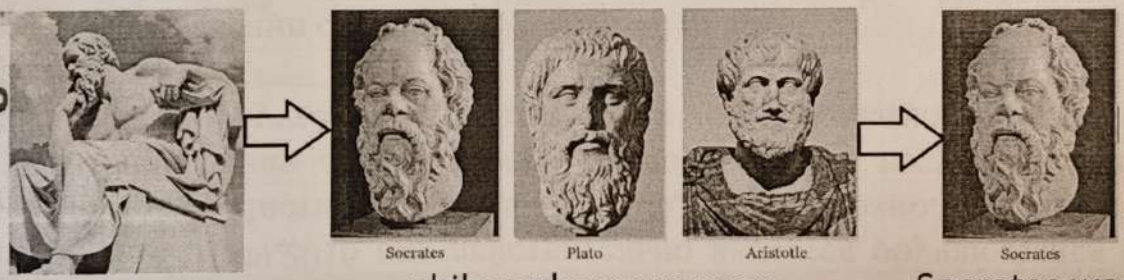
philosophers are men

$\Phi \in A$

Socrates was a man

$S \in A$

Bad logic



Socrates was a man

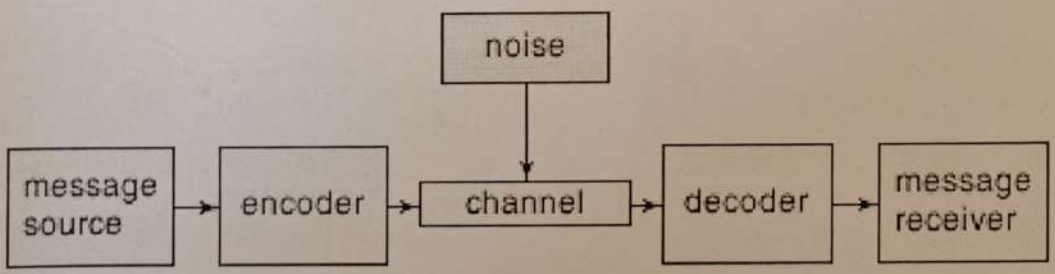
$S \in A$

philosophers are men

$\Phi \in A$

Socrates was a philosopher

$S \in \Phi$



Resume of Lecture by Pr. Bob Gallagher from MIT

Massachusetts Institute of Technology (MIT)

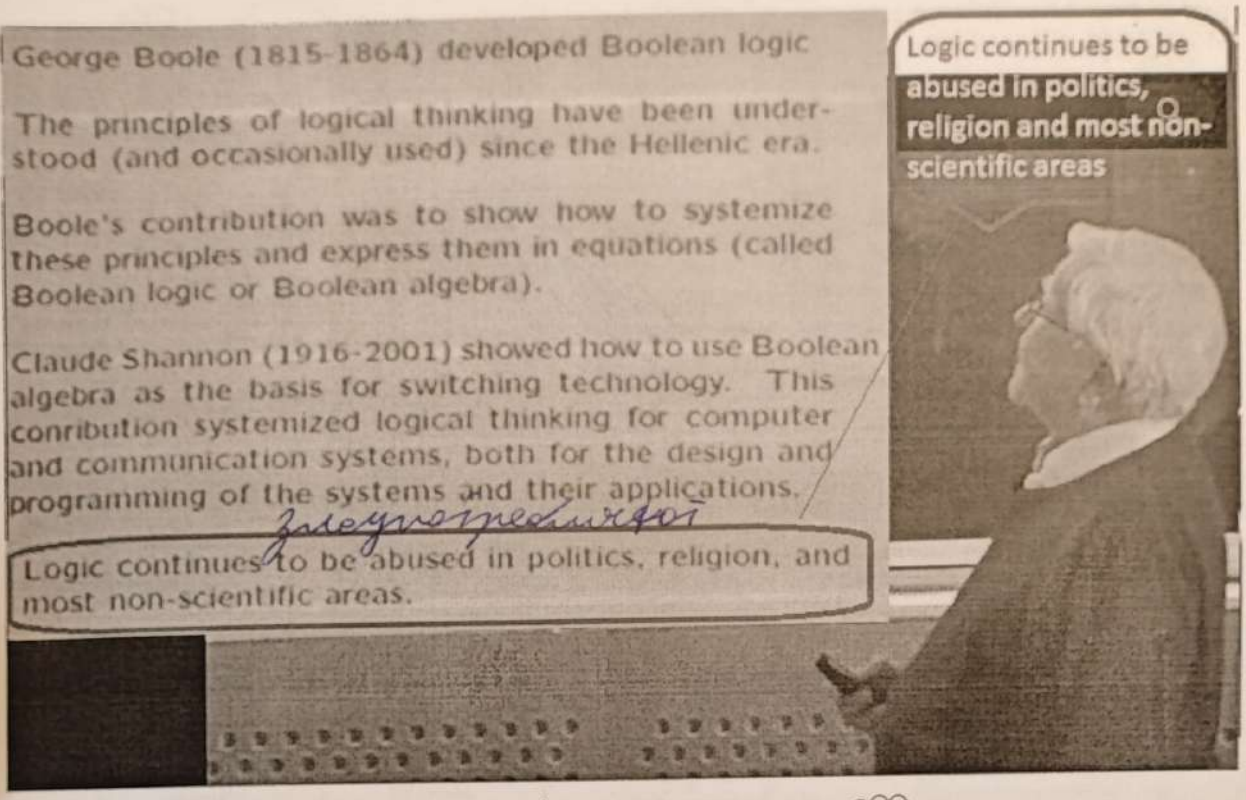
George Boole (1815-1864) developed Boolean logic

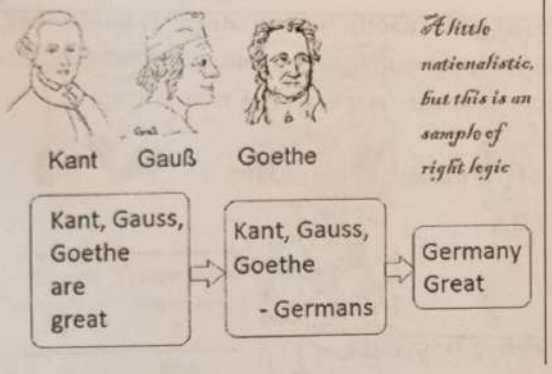
The principles of logical thinking have been understood (and occasionally used) since the Hellenic era.

Boole's contribution was to show how to systemize these principles and express them in equations (called Boolean logic or Boolean algebra).

Claude Shannon (1916-2001) showed how to use Boolean algebra as the basis for switching technology. This contribution systemized logical thinking for computer and communication systems, both for the design and programming of the systems and their applications.

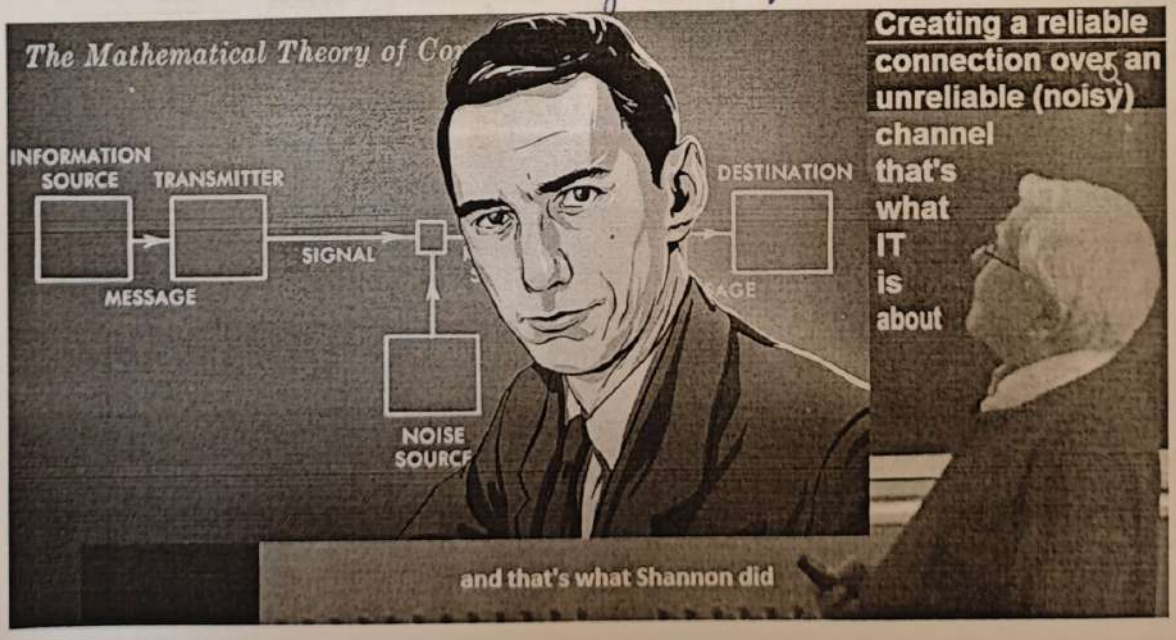
Logic continues to be abused in politics, religion, and most non-scientific areas.

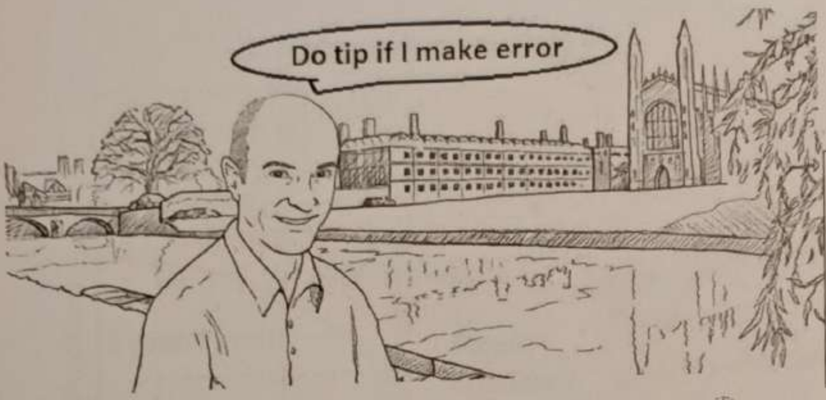




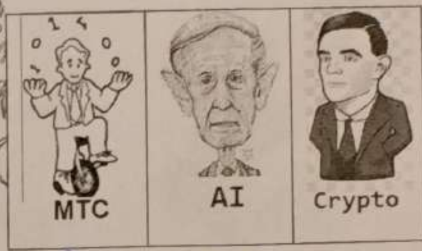
Bad logic (abuse of logic)

Любой гражданин может быть уличен или философом по такой логике.

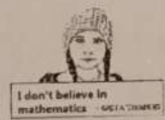




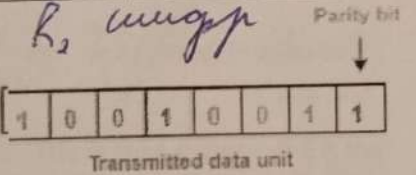
Sir Dr. D. MacKay,
University of Cambridge
(22 April 1967 – 14 April 2016)

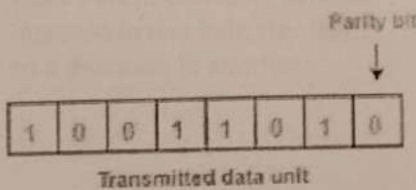


"I believe in clean energy,
but I also believe in mathematics"

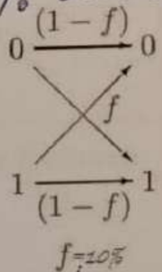


R_2 шифр

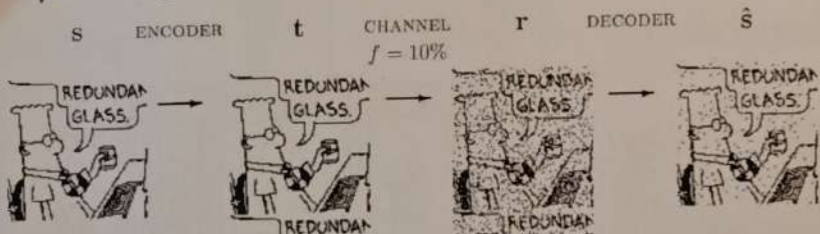




10% ошибки



binary simmetric channel



+0.2

R_3 шифр

Source sequence s	Transmitted sequence t
0	000
1	111

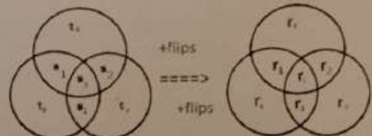
The repetition code R_3

source message s	0	0	1	0	1	1	0
t	000	000	111	000	111	111	000
n	000	001	000	000	101	000	000
r	000	001	111	000	010	111	000
corrected errors		⋆					
undetected errors					⋆		

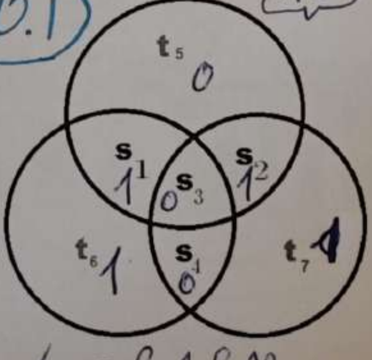
7.4. Hamming code.

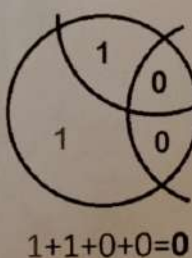
$$\frac{4}{\Sigma} \to \frac{7}{t}$$

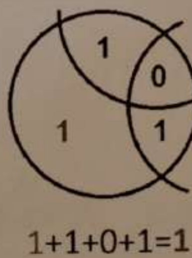
1100 011

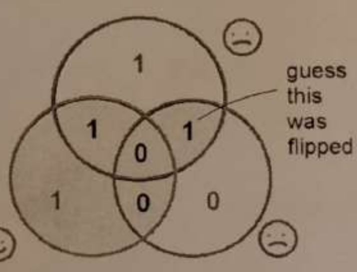


+0.1

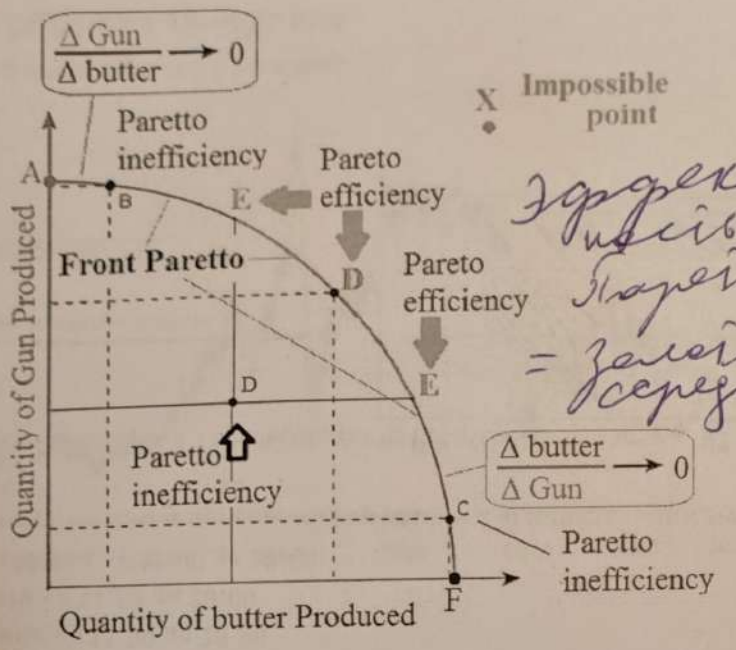








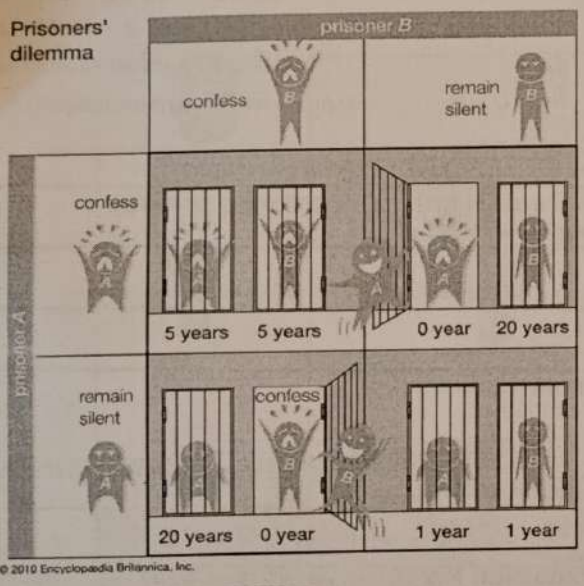
$t_5 = S_1 \wedge S_2 \wedge S_3$, если кол-во единиц чётное => 0



Эффективность по Парето = Заложил by Vilfredo Pareto

1848-1923

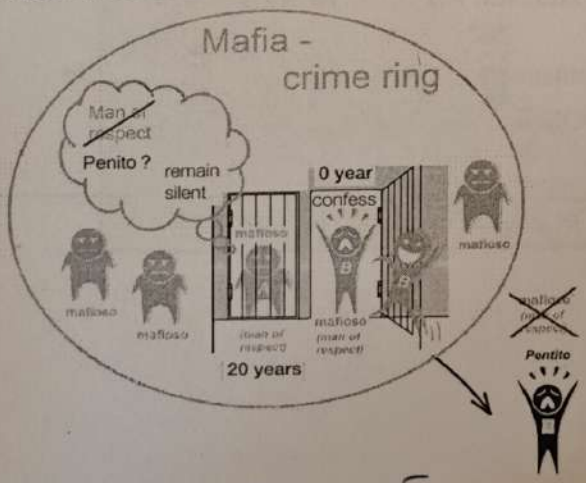
The orange sector E-D-E is the most Pareto efficient - since an increase in one indicator leads to a decrease in another.



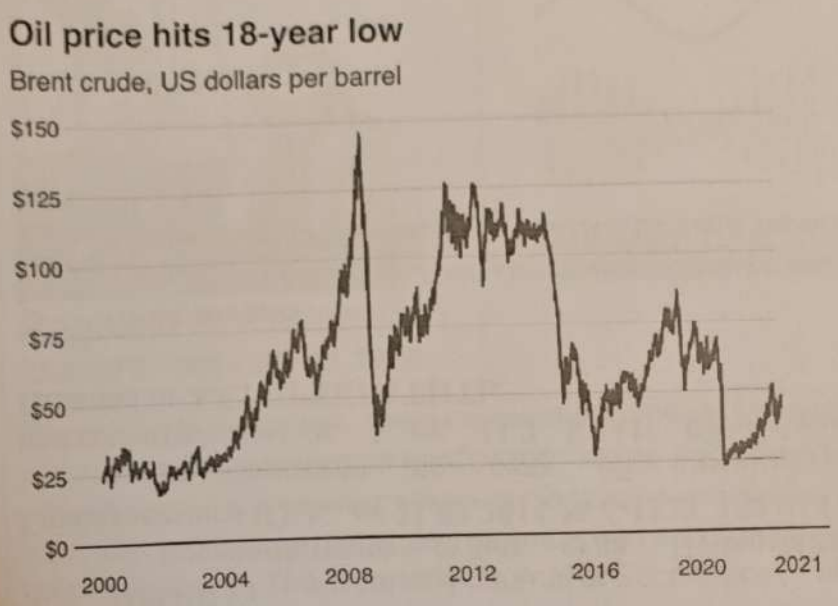
** => Nash equilibrium

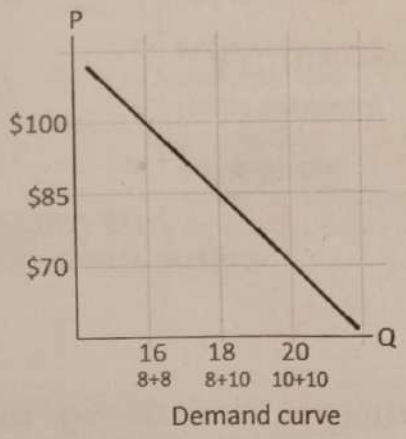
$H_2(x)$ / $H_1(x)$	*Player 2*	Recognition;	Non-recognition;
Player 1		1	2
Recognition;	1	* -5 / -5 *	-20 / 0
Non-recognition;	2	0 / -20	-1 / -1

-1-1 Pareto Optimality



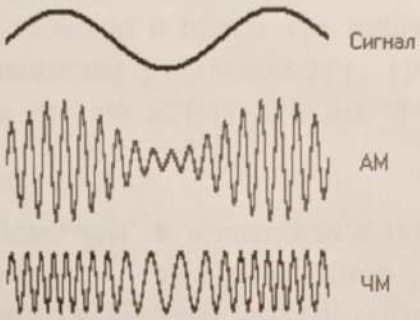
Вор своего не сдаст, т.к. в приватной ситуации его купят, а обычный человек думает о себе





Barrel	1. $8 \cdot 10^6$ barrels/day	2. $10 \cdot 10^6$ barrels/day
1. $8 \cdot 10^6$ barrels/day	$800 millions per day $100 per barrel $800 millions per day	$850 millions per day $85 per barrel $680
2. $10 \cdot 10^6$ barrels/day	$680 millions per day $85 per barrel $850 millions per day	$700 millions per day $70 per barrel $700 millions per day

Reginald A. Fessenden
(October 6, 1866 - July 22, 1932)

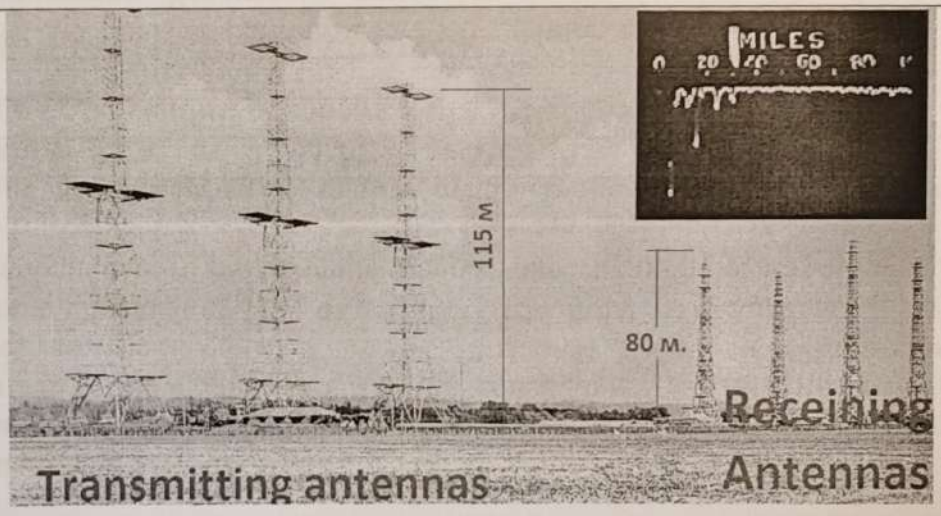


(October 6, 1866 - July 22, 1932)

first transmission of speech by radio (1900), and the first two-way radiotelegraphic communication across the Atlantic Ocean (1906)

"Ни одна организация, занимающаяся какой-либо конкретной областью деятельности, никогда не изобретает какие-либо важные разработки в этой области или не внедряет какие-либо важные разработки в этой области до тех пор, пока она не будет вынуждена сделать это из-за внешней конкуренции.." Oxford University Press. The Quarterly Journal of Economics , Feb., 1926, p. 262.

Battle of Britain
(3 month 3 weeks)
10.07-31.10.1940



Radar played a major role in the Battle of England

H. Nyquist

$$W = K \log m$$

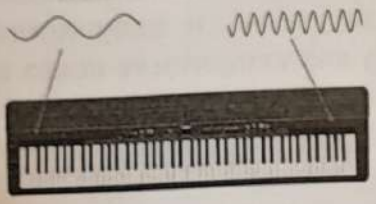
Where W is the speed of transmission of intelligence,
m is the number of current values,
and, K is a constant.

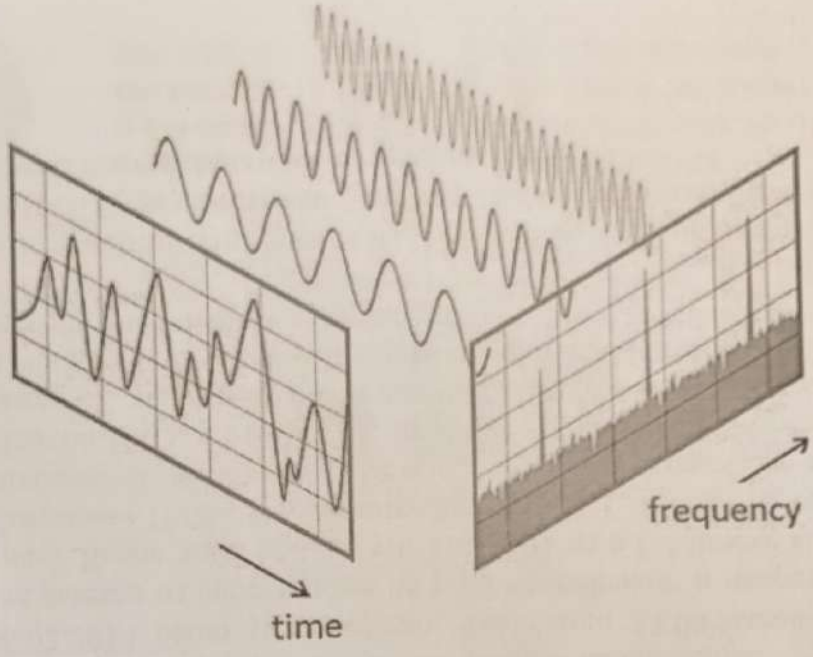
Ralph **Hartley**
(81:1888-1970)

$$H = n \log s$$

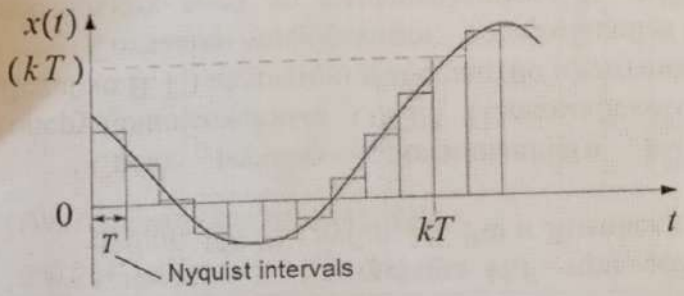
$$= \log s^n.$$

Fourier transform





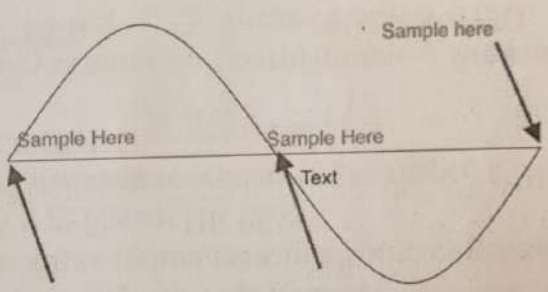
Sampling. Kotelnikov-Nyquist Theorem

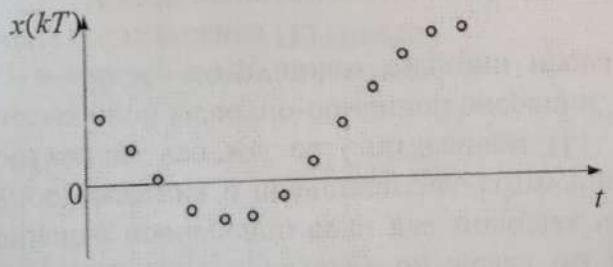


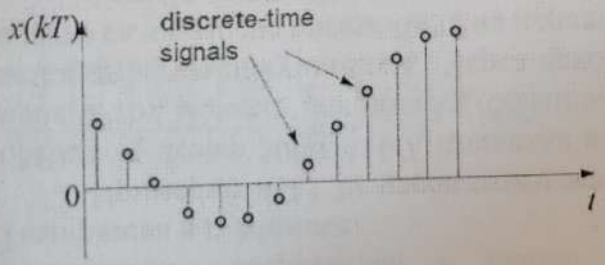
Time intervals T, through which readings s (kT) are taken, are called Nyquist intervals.

Sine with period T

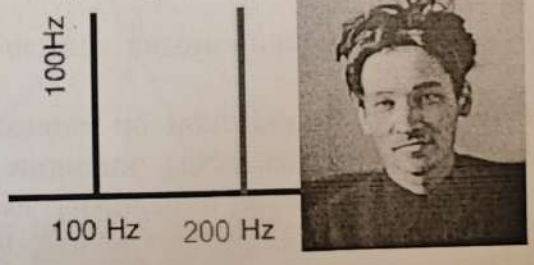
Sampling at T/2







frequency Sample



$F_{sample} >= 2 * F_{max}$

$(T_{sample} <= T_{min}/2)$

Say **NO** to the **first**

Say **YES** to the **second** if it is better than the first

Say **NO** to the **third** only if it is worse than all the others

Далее по условию - стратегия: выбирать 1 самый вероятный вариант

1	2	3	4

1 question - the first or second group

1	2	3	4	Question 1
X				

2 question - the first or second group

1	2		Question 2
	X		

Average number of questions =

2*0.25+ 2*0.25+ 2*0,25+ 2*0,25 =2

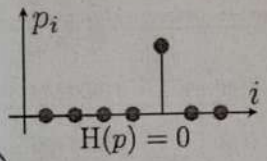
Average number of questions =

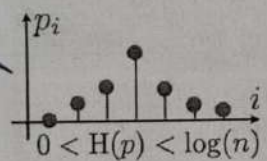
1*0.5+	2*0.25+	3*0,125+	3*0,125
			

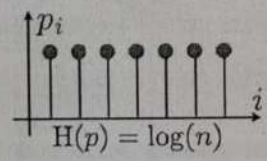
Question 1. Is this Zuckerberg?	 50%	1*0.5
Question 2. Is this Sergey Brin?	 25%	2*0.25
Question 3. Is this Stefan from BMW?	 12,5%	3*0,125
So Prince Saud	 12,5%	3*0,125
Average number of questions =		1,75

Теоретическая

$$H(X) = \sum_{i=1}^{n} p(x_i) \log_b \frac{1}{p(x_i)}$$







$$\sum_{i=1}^{n} p(i) \log_2 \frac{1}{p(i)}$$

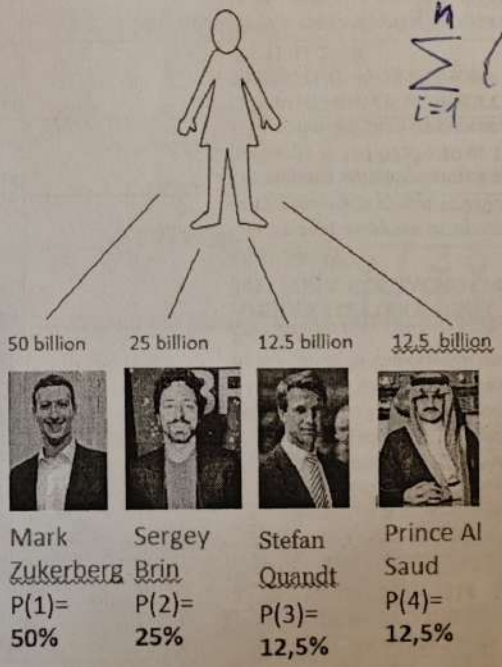
Quantifying information

$$I(x_i) = \log_2\left(\frac{1}{p_i}\right)$$

number of bits required to encode choice

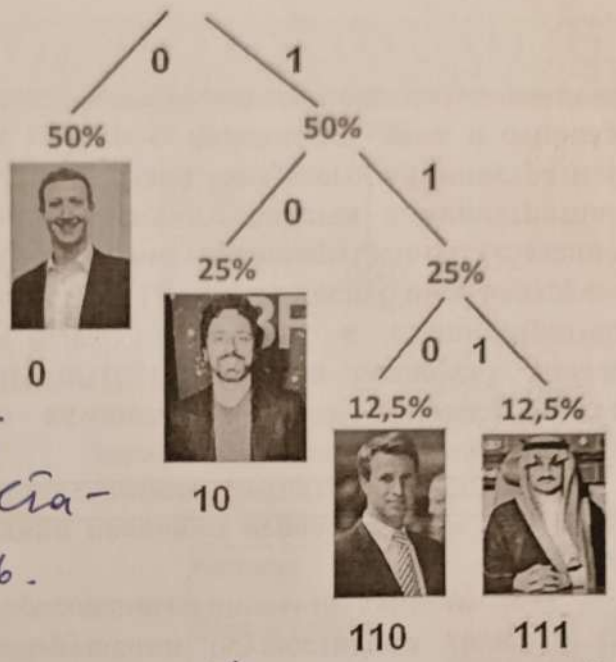
$$\sum_{i=1}^{n} p(x_i)\, I(x_i)$$

$$\sum_{i=1}^{n} \log_2 \frac{1}{p(x)} \cdot p(x)$$



1. считаем частоту символов (например, "а" – 5 раз, "б" – 7 раз)
2. строится дерево: берем 2 узла с наименьшей частотой, объединяем в родителя с суммой частот; повторяем, пока не останется 1 узел – корень.

Дерево Хаффмана



Такой же подход, как у Хаффмана, но с каждым звуком считаем частоту не 1 символа, а и символа, где и-целое.

First-order approximation (symbols independent but with frequencies of Belarusian txt).

Мама мыла ра

М - 3	— 30%	1-3 М
а - 4	— 40%	4-7 а
ы - 1	— 10%	8 -ы
л - 1	— 10%	9 -л
р - 1	— 10%	10 -р

10

лламмар

Second-order approximation (digram (2-symbols) structure as in Belarusian)

Мама мыла ра

Ма - 2	22%	1-2	ма
ам - 2	22%	3-4	ам
мы - 1	11%	5	мы
ыл - 1	11%	6	ыл
ла - 1	11%	7	ла
ар - 1	11%	8	ар
ра - 1	11%	9	ра

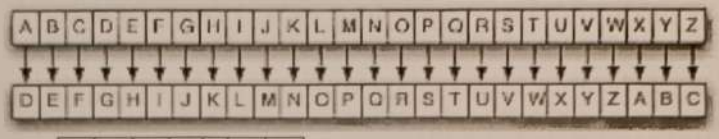
9

0. 4 6 7 3 1 9 1 6 7 3 5

ам ыл ла ам ма ра ма ыл ла ам мы

мылла рама

Caesar Cipher
C=(p+3) mod 26



- We can use the ordinal positions of letters in a cipher to generate this key:

A	B	C	D	...	Y	Z
1	2	3	4	...	25	26

- We can also rotate the starting point. If we add 3 to every number, we might use this key:

A	B	C	D	...	Y	Z
4	5	6	7	...	2	3

ABBA

↓

DEED

Vigenere Cipher

An improvement we can make to the Caesar cipher is to increase the number of keys.

While the Caesar cipher uses a single key, the **Vigenere** cipher uses multiple keys by selecting a keyword.

In the Vigenere cipher, for each new letter of message, it is enciphered using a different letter of the keyword.

https://www.youtube.com/watch?v=BgFJD7oCmDE

To encrypt the message **ABBA** using the keyword **LAW**, we might come up with the following table:

Plaintext	A	B	B	A
Ordinal Position	1	2	2	1
Keyword (LAW)	L	A	W	L
Keyword Ordinal Position	12	1	23	12
Sum	13	3	25	13
Ciphertext	M	C	Y	M

Frequency Analysis https://www.youtube.com/watch?v=sMOZf4GN3oc Khan

- Another issue with Caesar ciphers is that an adversary may be able to crack the code without a pin.
- For example, if we see a single letter word in the message, we might be able to guess that the character or number represents I or A. From there, we might be able to discover some patterns in the message.
- A pattern may be how frequently letters appear in the English language.

A	B	C	D	E	F	G	H	I	J	K	L	M
8.1%	1.5%	2.8%	4.3%	12.7%	2.2%	2.0%	6.1%	7.0%	0.2%	0.8%	4.0%	2.4%

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
6.7%	7.5%	1.9%	0.1%	6.0%	6.3%	9.1%	2.8%	1.0%	2.4%	0.2%	2.0%	0.1%

- Some letters appear very frequently, such as E or T and some letters appear very infrequently, such as J or K. Using these frequencies, we can look at what appears frequently or infrequently in the cipher-text and perhaps find certain patterns.
- While for humans it might be tedious to conduct frequency analysis to decode a message, a computer can do it very quickly.

voice —air→ ear
↑
noise

eye —nervous system→ brain

+0,1

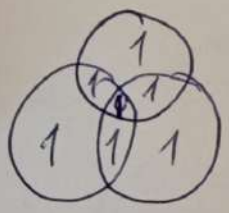
Received signal = transmited signal + noise

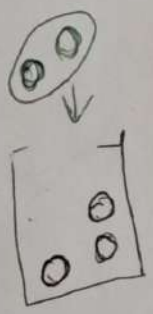
Solutions { physical / system

10 000 bit

+0.1
7.4.26
+0,2
+0.1
+0,1

0.3 Дисперсия





АНДРЕЙ
↓
ИСААК
ЗА

mamma mia
1 1

Школа 1

UNI

движ

~~10101~~

x x i a

1939
1
20

А Ў Я : ВУ
aeph.

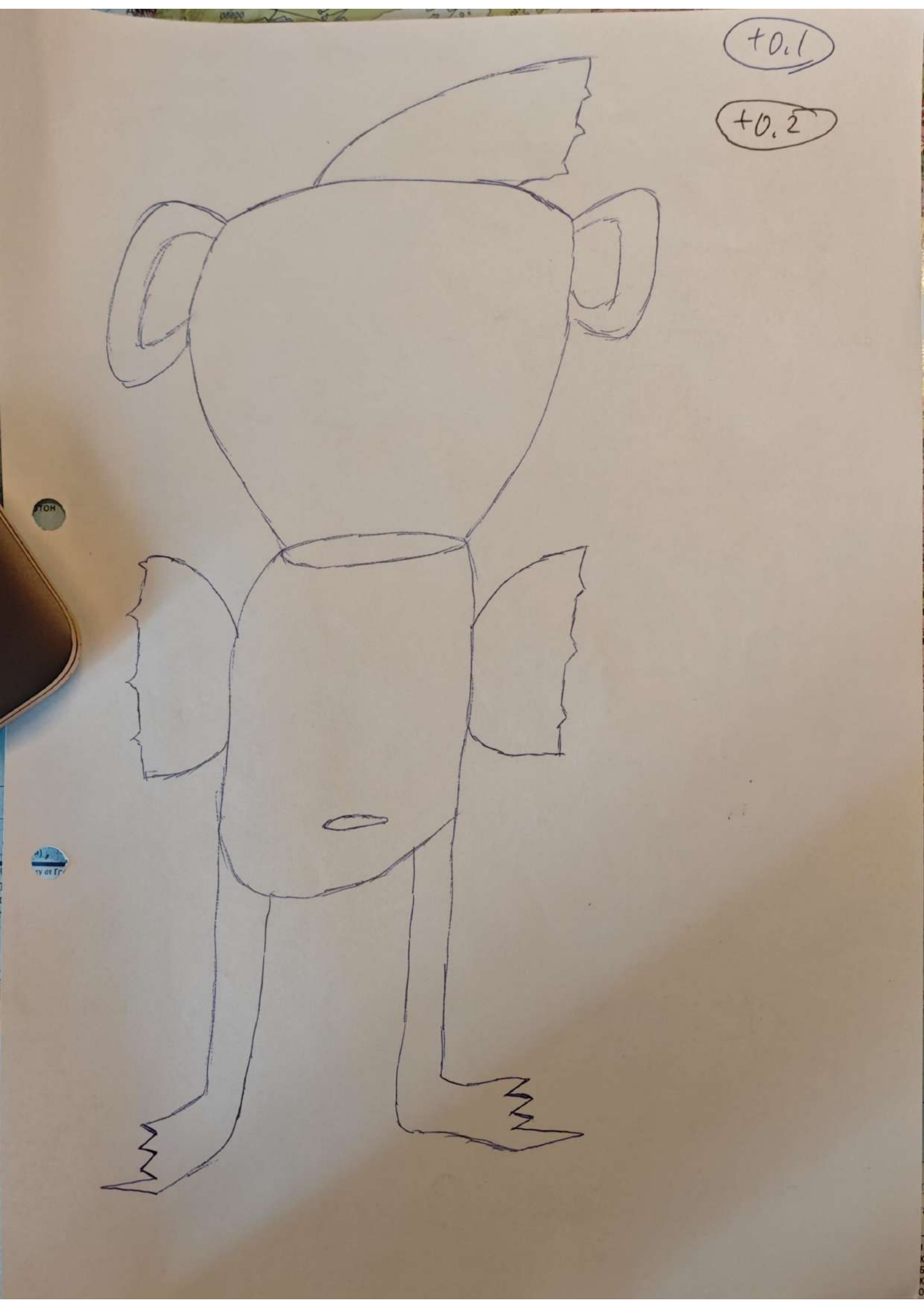
$\log_2 32 = 5$

3,5

Энтропийные
сжатие

confucious.by

ASP.NET 12р


+0.1
+0.2