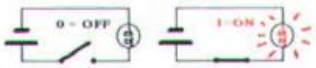
Massachusetts Institute of Technology (MIT)

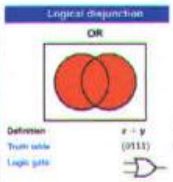
Lecture by Pr. Bob Gallagher
Boole (1815-1864) & **Shannon** (1916-2001)



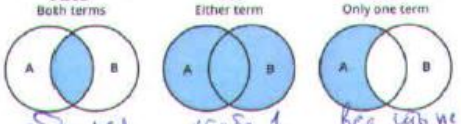
Logical addition (disjunction)

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



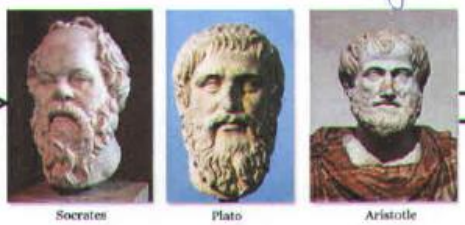
BOOLEAN LOGIC



Good logic

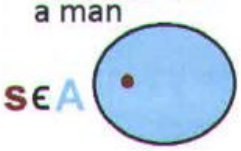

Socrates

Socrates was a philosopher



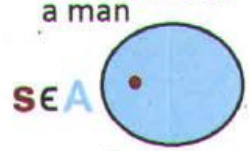
philosophers are men

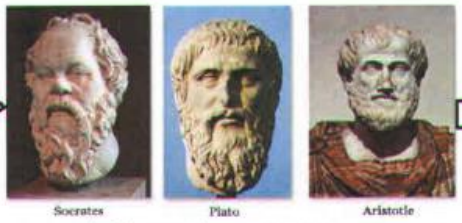
Socrates was a man



Bad logic

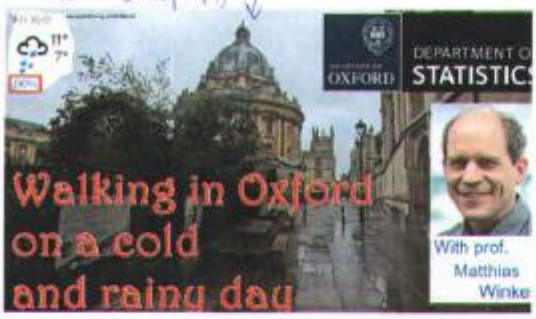
Socrates was a man

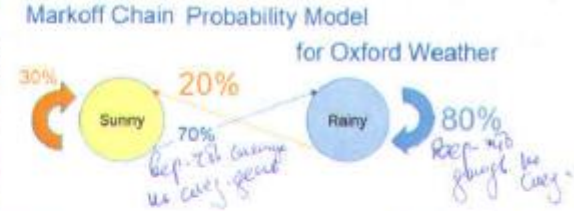




philosophers are men

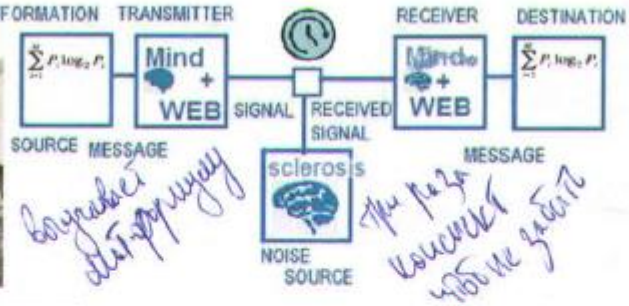
Socrates was a philosopher





Bad way

Good way
1. listening
2. first way of processing
3. Writing, incl. sth., you're not quite sure about



School ==formalism==> University

Motivation: 80% chance of rain

Let A_j be the event of rain at 9am on day j of this term, $1 \le j \le n$

Suppose the events A_i and A_j have probability p, independently

then take notes on the lecture yourself

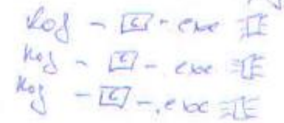
CFA экзамен
(Chartered Financial Analyst)

.NET Delphi / Андрес Хейлсберг
C# много книги

хотели назвать Oak
↓ многие з/п

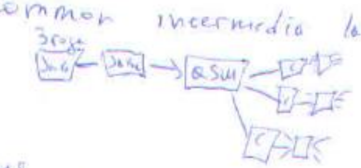
C++ D. Ритчи   C+ classes   П. Нортон Java (от C++)
Хорошие з/п
4.5 года

1) убрали множественное наслед.
2) класс
3) указатели убрали



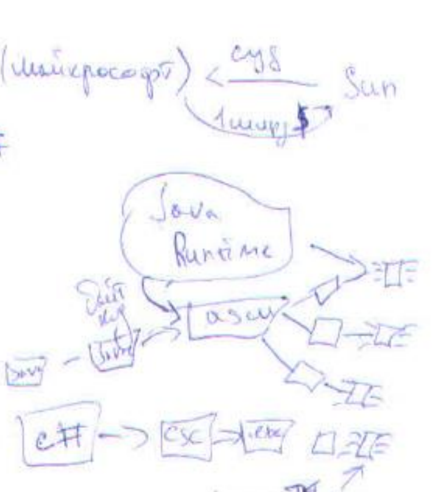
Main = main
Main() ≠ main()

common intermedia language



J++ (майкрософт) < суд — Sun
1 млрд $

C#



MS coree.dll

JIT compiler
just in time

.dll – только ядро системы пользователи не может запустить
.exe – уже пользователей

JedR.exe
010170
– пример из либа

инкапсуляция

static
Статический метод относится ко всему классу

Resume of Lecture by Pr. Bob Gallagher from MIT

Massachusetts Institute of Technology (MIT)

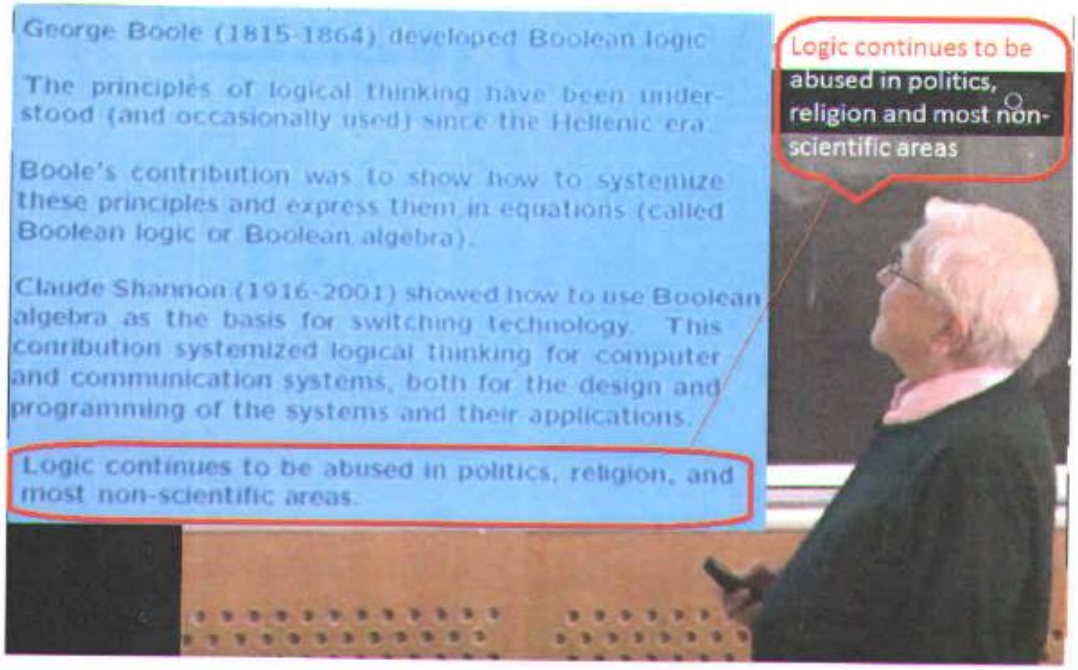
George Boole (1815-1864) developed Boolean logic

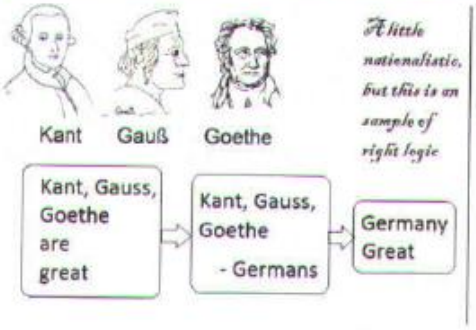
The principles of logical thinking have been understood (and occasionally used) since the Hellenic era.

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.

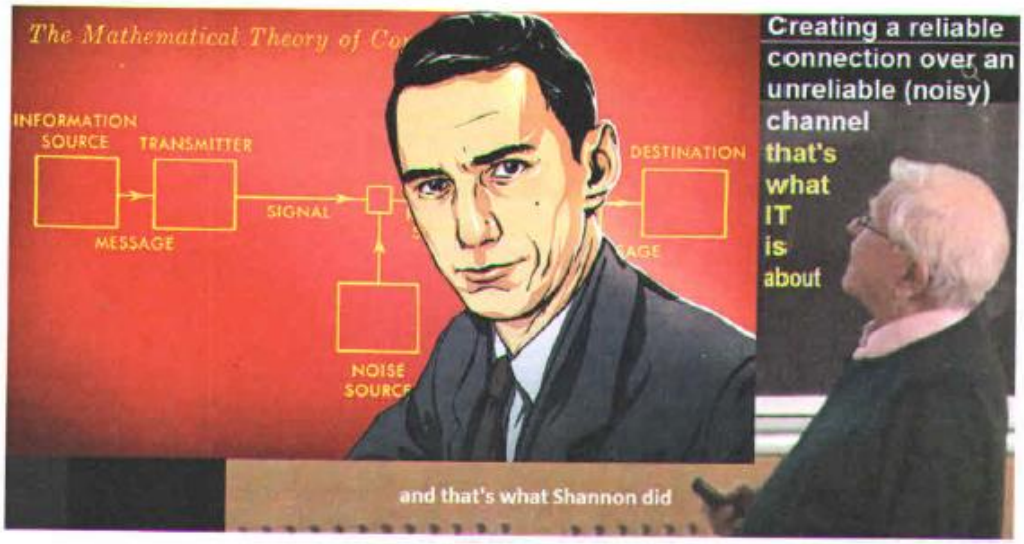
Logic continues to be abused in politics, religion, and most non-scientific areas.





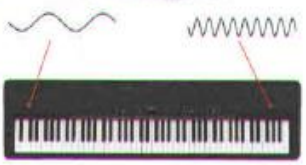
Bad logic (abuse of logic)

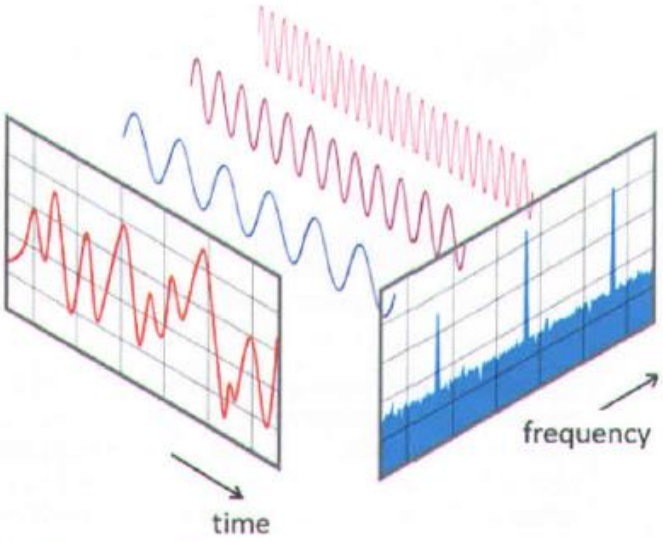
Плохие шутки



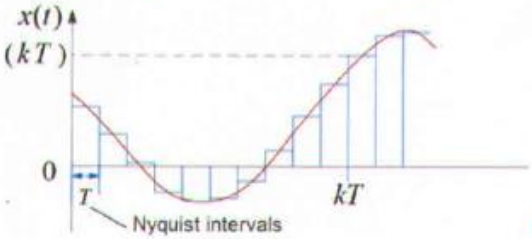
Fourier transform

$$\hat{f}(\xi) = \int_{-\infty}^{\infty} f(x)\, e^{-i2\pi\xi x}\, dx.$$

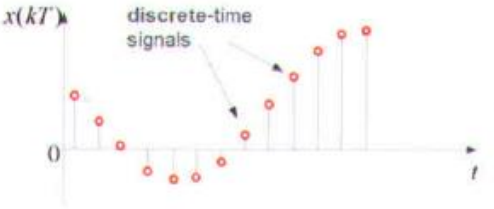


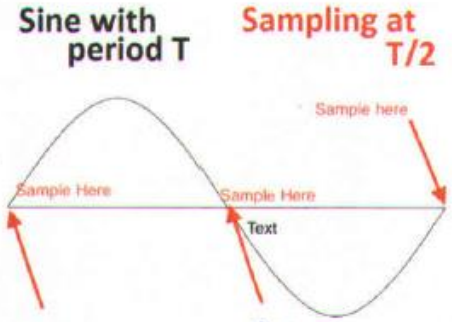


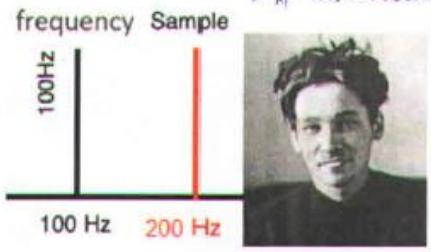
Sampling. Kotelnikov-Nyquist Theorem



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





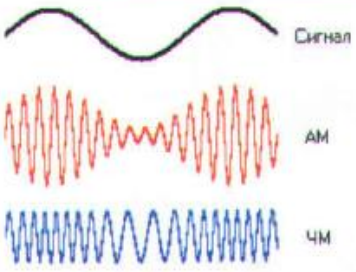


$$F_{sample} >= 2 * F_{max}$$

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

$$x(t) = \sum_{k=-\infty}^{\infty} x(k\Delta t)\, \frac{\sin 2\pi F (t - k\Delta t)}{2\pi F (t - k\Delta t)}$$

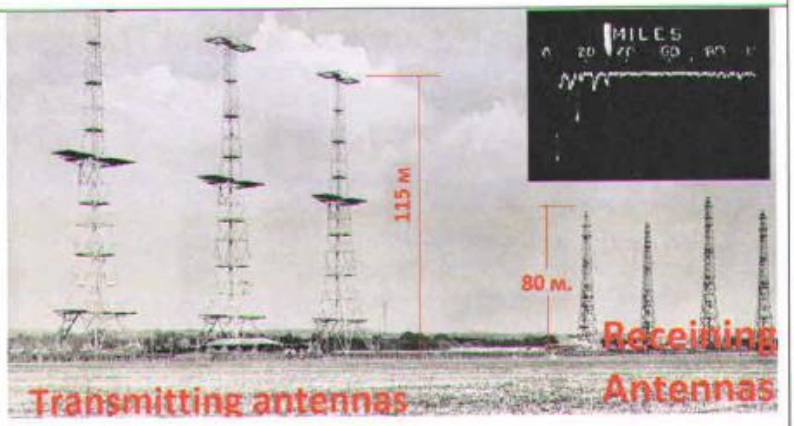
Reginald A. Fessenden
(October 6, 1866 – July 22, 1932)



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

(1889-1976)

$$W = K \log m$$

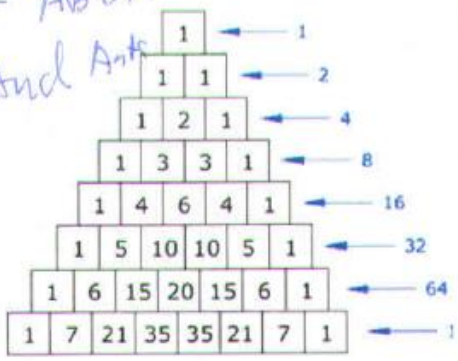
Where W is the speed of transmission of intelligence,
m is the number of current values,
and, K is a constant.

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

$$H = n \log_2 s$$

$$= \log s^n.$$

for ABBA And Ant



Shannon Hartley Theorem

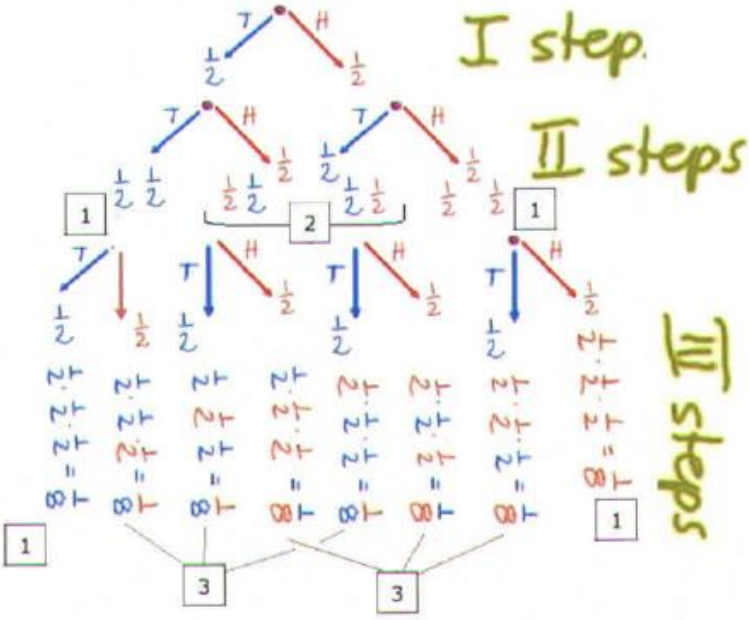
This is a measure of the *capacity* on a channel; it is impossible to transmit information at a faster rate without error.

$$C = B\log_2(1+S/N)$$

- C = capacity (in bit/s)
- B = bandwidth of channel
- S = signal power (in W)
- N = noise power (in W)

It is more usual to use SNR (in dB) instead of power ratio (as with terrestrial and commercial communications syste S/N >> 1, then rewriting in terms of log10.

$$C = B\frac{\log_{10}(S/N)}{\log_{10}2} = B\frac{10\log_{10}(S/N)}{10.\log_{10}2} = B\frac{SNR}{3.01}$$



+0,2 to Exam from Pascal

$(a+b)^0 = 1$

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

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

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

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

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

$(1+x)^5 = 1^5+5\cdot1^4x+10\cdot1^3x^2+10\cdot1^2x^3+5\cdot1\cdot x^4+x^5 =$

$= 1+5x+10x^2+10x^3+5x^4+x^5$

$(a+b)^6 = a^6+6a^5b+15a^4b^2+20a^3b^3+15a^2b^4+6ab^5+b^6$

É. Galois (1811-1832) [Les Misérables | Do You Hear the People Sing?]

Example

There are 6! ways to order the letters of GALOIS

If randomly reorder the letters what is probability that the vowels (A, O, I) are all before consonants (G, L, S)?

ABBA $\frac{4!}{4} = 6$

$n = m_1 \cdot m_2$

$\frac{n!}{m_1!\, m_2!}$ – кількість комбінацій.

$(1+x)^{13}$

$(1+x)^{13} = \binom{13}{0}x^0 + \binom{13}{1}x^1 + \binom{13}{2}x^2 + \binom{13}{3}x^3 + \binom{13}{4}x^4 + \binom{13}{5}x^5 + \binom{13}{6}x^6 + \binom{13}{7}x^7 + \binom{13}{8}x^8 + \binom{13}{9}x^9 + \binom{13}{10}x^{10} + \binom{13}{11}x^{11} + \binom{13}{12}x^{12} + \binom{13}{13}x^{13}$

$(1+x)^3 = 1 + 3x + 3x^2 + x^3$

There are 6! ways to order the letters of GALOIS.
Есть 6 способов расположить буквы GALOIS.

$2 \cdot 2 = 4$.

HOWARD
GARDNER

- DIFFERENT PEOPLE HAVE DIFFERENT KINDS of MINDS
- WE CAN BE SMART IN A LOT OF WAYS

MULTIPLE INTELLIGENCES

NATURALIST INTELLIGENCE

SCHOOL LIKES THESE

LINGUISTIC INTELLIGENCE — Words, Nerds

JOCKS

HARVARD SCHOOL of ED

SPIRITUAL INTELLIGENCE

LOGICAL MATHEMATICAL INTELLIGENCE

MORAL INTELLIGENCE

BODILY KINESTHETIC INTELLIGENCE

INTER PERSONAL INTELLIGENCE

SPATIAL INTELLIGENCE

Philosophers

EXISTENTIAL INTELLIGENCE

MUSICAL INTELLIGENCE

THE ARTS LIKE THESE

EMOS

INTRA PERSONAL INTELLIGENCE

... REPUBLIC HE HELPS US SEE HOW OUR KIDS ARE GIFTED - ALL OF THEM:

$\sum_{i=1}^{4} \log_2 \left(\frac{1}{Pi}\right) Pi$

$\log\left(\frac{1}{Pi}\right) = 3$

KNOW THYSELF

Socrates

1. 50% - 0,5
2. 16% - 0,32
3. 16% = 0,48
4. 16% = 0,48

1,78

Определение смысла

Як вывучыць новую мову – замежную ці мову праграмавання. Гэта залежыць ад шматлікіх фактараў: перш за ўсё, ад наяўнасці часу, які вы гатовыя выдаткаваць на вывучэнне мовы праграмавання C# і платформы .NET Framework (або Core). Нарэшце, здольнасці мець важна, але, на маю думку, гэта не галоўнае.

19 лютага 2024 г. – 23 лютага 2024 г.
https://bsu.by/news/nedelya-rodnogo-yazyk_a-startuet-v-bgu-d/

Kató Lomb (94: 8.2.1909 9.6.2003

Ёсць аналогія з вывучэннем замежнай мовы. Адна з першых у свеце сінхронных перакладчыкаў Като Ломб - яна раіла перад вывучэннем замежнай мовы даведацца, ці можна выдзяляць на заняткі хаця б 10-12 гадзін у тыдзень на працягу 2-х гадоў (ўсяго 1040-1248 гадзін). Калі не - і не падманвайце сябе.

Яе 10 запаведзяў па арганізацыі вывучэння натуральных моў з кнігі «Як я вывучаю мовы» (прыведзены ў дадатку), на мой погляд, актуальныя і для вывучэння моў шляхам праграмавання.

Адказаць на гэтае пытанне Вам дапаможа гэты тэсцік.
Выконваць яго трэба самастойна, на працягу 3-5 дзён.

Ад таго, колькі пунктаў Вы пройдзеце залежыць ад выбару хуткасці, з якой можна працаваць. Запускаць усе каманды лепш з кансолі Start|Run|cmd.

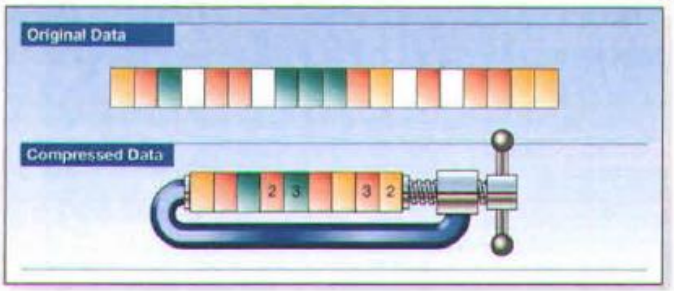
ПРАДМОВА. Адзін са стваральнікаў праекту Apple Macintosh. Джэф Раскін (61:09.03.1943 - 26.02.2005) высунуў на мой погляд зусім правільны лозунг **Your Time Is Sacred; Your Work Is Sacred** - з гэтага вынікае, што ў абавязковым парадку неабходна захоўваць праведзеную працу - яна святая, і час, на яе выдаткаваны, бясцэнны. ***[Jef Raskin. THE HUMAN INTERFACE. Chapter 1.6].***

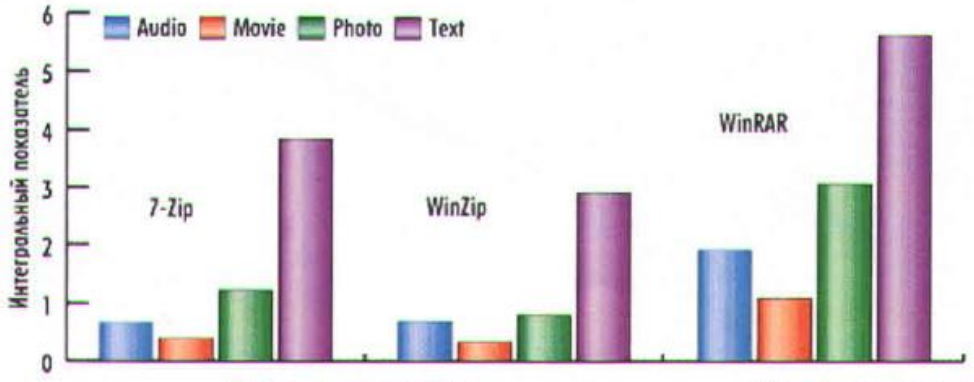
«Прыблізна кожную гадзіну я ствараю рэзервовую копію сваёй працы з дапамогай энерганезалежнай запамінальнай прылады, якая можа быць фізічна вынята з кампутара і такім чынам абаронена ад любых нечаканасцяў у яго працы.
Акрамя таго, кожны тыдзень я захоўваю рэзервовую копію сваёй сістэмы на вонкавым дыску.
Гэта не значыць, што я параноік, - я ўсяго толькі лічу, што такі падыход практычны…
Сістэма павінна разглядаць дадзеныя, якія ўводзяцца юзэрам, як неацэнныя»

10 запаведзяў К.Ломб - чалавека, які ведаў 16 моў

1. Займайся мовай штодня. Калі ўжо зусім няма часу, дык хаця б дзесяць хвілін. Асабліва добра займацца раніцай.
2. Калі жаданне займацца занадта хутка слабее, не «фарсіруй», але і не кідай вучобу. Прыдумай якую-небудзь іншую форму: адкладзі кнігу і паслухай радыё, пакінь практыкаванні падручніка і пагартай слоўнік і г.д.
3. Ніколі не зубры, не завучвай нічога па асобнасці, у адрыве ад кантэксту.
4. Выпісвай па-за чаргой і завучвай усе "гатовыя фразы", якія можна выкарыстоўваць у максімальна магчымай колькасці выпадкаў.
5. Старайся разумова перакладаць усё, што магчыма: прамільгнулае рэкламнае табло, надпіс на афішы, абрыўкі выпадкова пачутых размоў. Гэта заўсёды адпачынак, нават для стомленай галавы.
6. Вывучваць трывала варта толькі тое, што выпраўлена выкладчыкам. Не перачытвай уласных няправільных практыкаванняў: пры шматразовым чытанні тэкст запамінаецца мімаволі са ўсімі магчымымі памылкамі. Калі займаешся адзін, то вывучвай толькі загадзя правільнае.
7. Гатовыя фразы, ідыяматычныя выразы выпісвай і запамінай у першай асобе, адзінага ліку. Напрыклад: "I am only pulling your leg" (Я цябе толькі дражню).
8. Замежная мова - крэпасць, якую неабходна штурмаваць з усіх бакоў адначасова: чытаннем газет, слуханнем радыё, праглядам недубляваных фільмаў, наведваннем лекцый на замежнай мове, прапрацоўкай падручніка, перапіскай, сустрэчамі і гутаркамі з сябрамі - носьбітамі мовы.
9. Не бойся казаць, не бойся магчымых памылак, а прасі, каб іх выпраўлялі. І галоўнае, не хвалюйся і не крыўдуй, калі цябе сапраўды пачнуць папраўляць.
10. Будзь цвёрда ўпэўнены ў тым, што ў што б там ні стала дасягнеш мэты, што ў цябе нязломная воля і незвычайныя здольнасці да моў.

Comparison of the compression ratio of popular archivers





Before Compression **After Compression**

Data

AAAAAAABCCCCCCDDEEEEE →

Symbol	Frequency
A	7
B	1
C	6
D	2
E	5

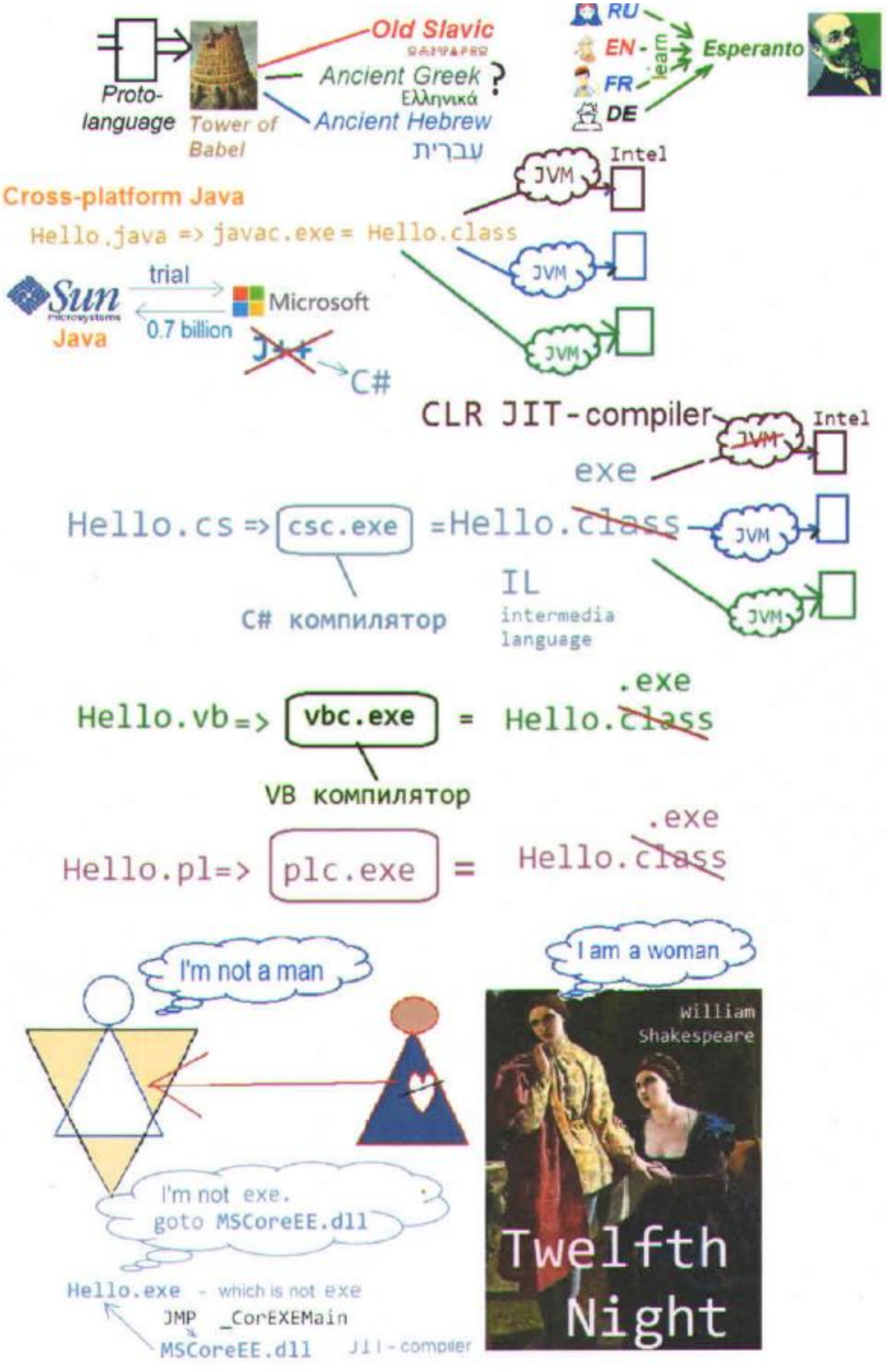
Symbol	Bit Code
A	00
B	111
C	01
D	110
E	10

Entropy compression ratio

Before Compression = 21 x 8 bits =198 bits
After Compression = 7 x 2 bits + 1 x 3 bits + 6 x 2 bits + 2 x 3 bits + 5 x 2 bits = 45 bits

$H = n * \log_2 S = \log_2 S^n$

+0.2 to Exam


Proto-language
Tower of Babel
Old Slavic
Ancient Greek
Ancient Hebrew
RU
EN
FR
DE
learn
Esperanto
Cross-platform Java
Hello.java => javac.exe = Hello.class
JVM
Intel
Sun microsystems
Java
trial
0.7 billion
Microsoft
J++
C#
CLR JIT-compiler
exe
Hello.cs => csc.exe =Hello.class
C# компилятор
IL
intermedia language
Hello.vb => vbc.exe = Hello.class
.exe
VB компилятор
Hello.pl=> plc.exe = Hello.class
I'm not a man
I am a woman
William Shakespeare
Twelfth Night
I'm not exe.
goto MSCoreEE.dll
Hello.exe - which is not exe
JMP _CorEXEMain
MSCoreEE.dll
JIT-compiler

```
class Dog
{
  public string name;
  public string bread;
  public int age;
```


```
  public void Bark()
  {
    Console.WriteLine("Woof woof!");
  }
```

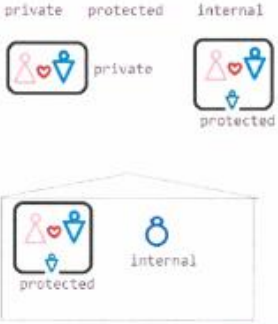
```
static void Main(string[] args)
{
    Dog dori = new Dog();  //Constructor works
    dori.age = 3;

    dori.name = "Dori";
    dori.breed = "Mongrel";
    dori.Bark();
}
```

```
public Dog()
{
}
public Dog(string name)
{
    this.name = name;
}
public Dog(string name, string breed)
{
    this.name = name;
    this.breed = breed;
}
```

1 - **constructor** no returns value

2. The name of the **constructor** is the same name is the class.

3. more than one **constructor**




```
class AFather
{
   protected string name;
   int age;
}
class ASon:AFather
{
    public ASon(string name)
    {
       base.age = 33;
       base.name = name;
    }
}
```

unavailable available

```
class Program
{
    static void Main(string[] args)
    {
        AFather af = new AFather();
        ASon andy = new ASon("Olaf");
    }
}
```

Program.exe

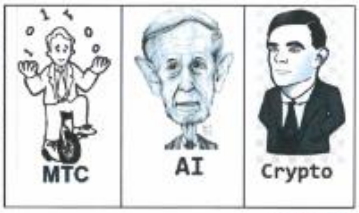
```
class AFather
{
   protected string name;
   internal int age;
}

class Program
{
    static void Main(string[] args)
    {
        AFather af = new AFather();
        af.age = 33;
        ASon andy = new ASon("Olaf");
    }
}
```

available
unavailable

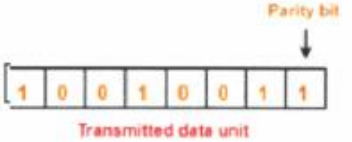
ASon.dll

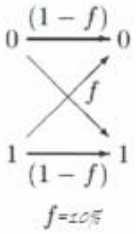
```
class ASon:AFather
{
    public ASon(string name)
    {
        base.name = name;
        base.age = 33;
    }
}
```

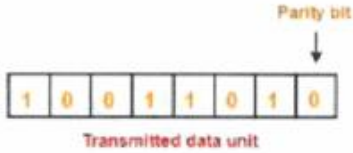
Sir **Dr. D. MacKay**,
University of Cambridge
(22 April 1967 – 14 April 2016)

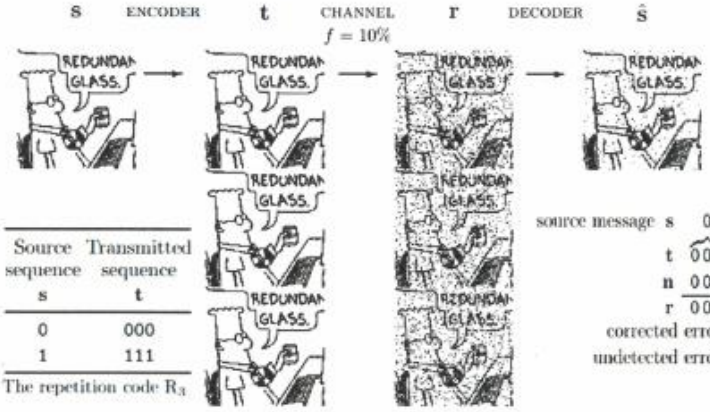


"I believe in clean energy,
but I also believe in mathematics"







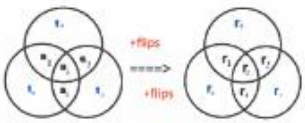


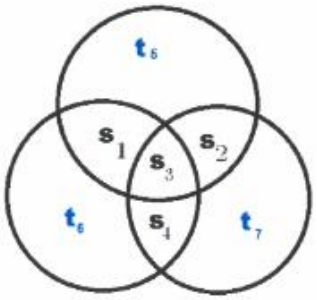
Source sequence s	Transmitted sequence t
0	000
1	111

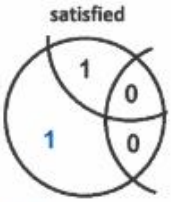
The repetition code R_3

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					*		

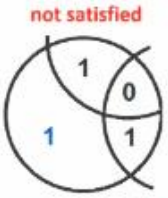
7.4. Hamming code. $\frac{4}{\Sigma} \rightarrow \frac{7}{t}$



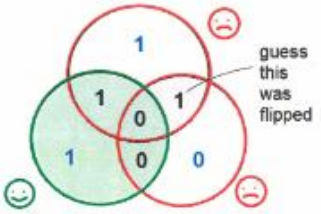


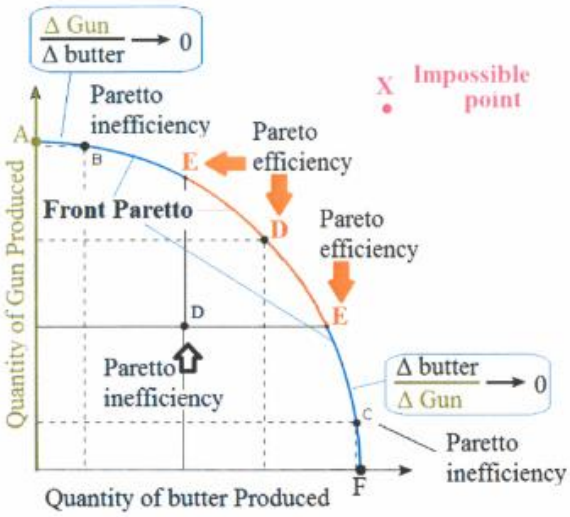


1+1+0+0=**0**



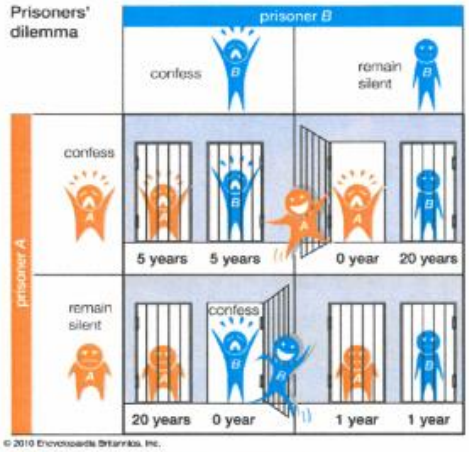
1+1+0+1=**1**

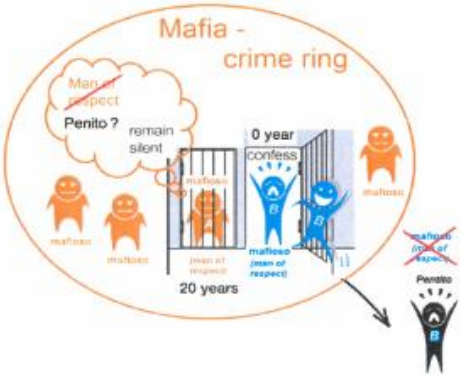




by Vilfredo Pareto

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





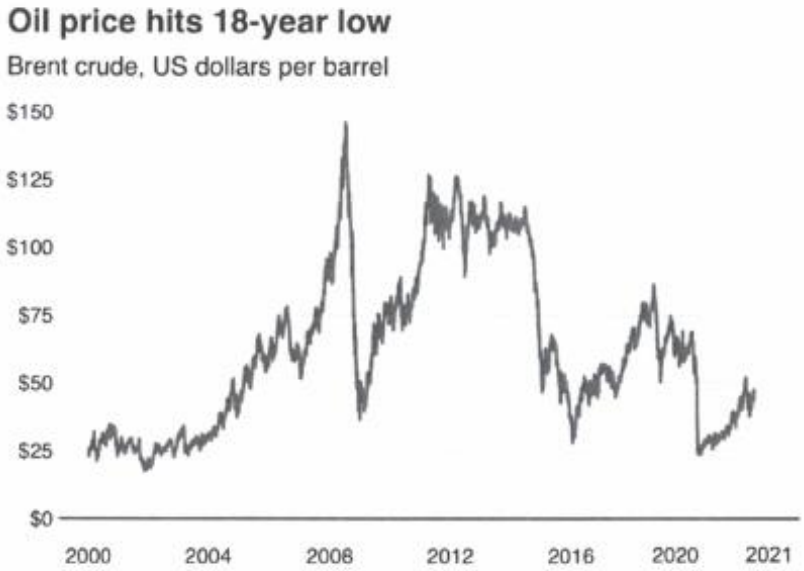
Game Theory

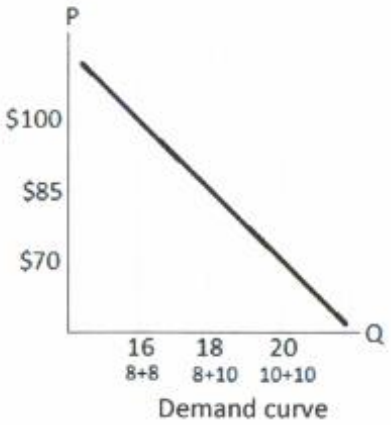
Nash Equilibrium

** => Nash equilibrium

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

-1-1 Pareto Optimality



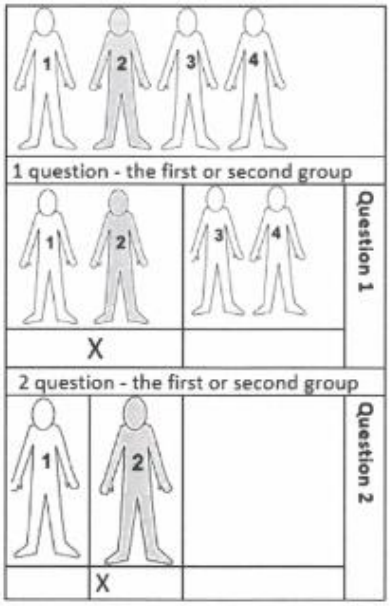


Barrel	1. $8 \cdot 10^6$ barrels/day	2. $10 \cdot 10^6$ barrels/day
1. $8 \cdot 10^6$ barrels/day	$800 millions per day $100 per barrel $800 millions per day	$850 millions per day $85 per barrel $680
2. $10 \cdot 10^6$ barrels/day	$680 millions per day $85 per barrel $850 millions per day	$700 millions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

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



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**

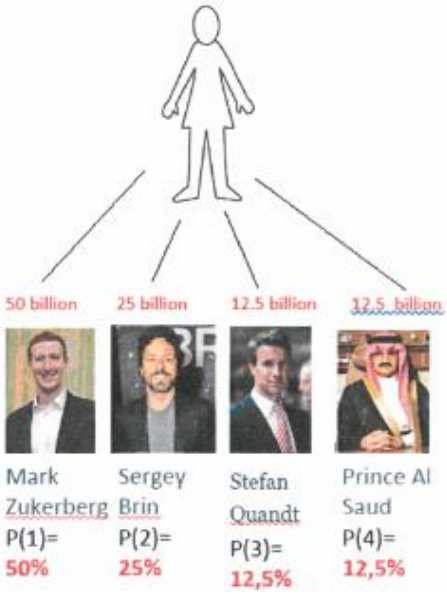
Quantifying information

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

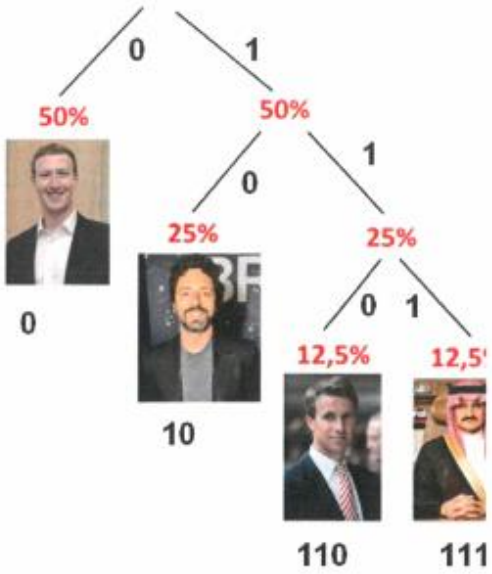
Quantifying information

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

number of bits required to encode choice



Huffman code



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		

лламаммар

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

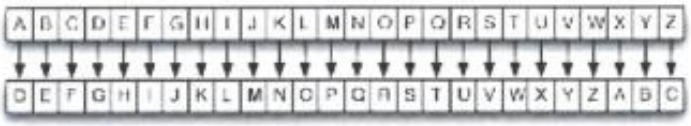
ам ыл ла ам ма ра ма ыл ла ам мы

мылла рама

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

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.