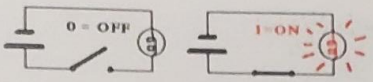
Massachusetts Institute of Technology (MIT)

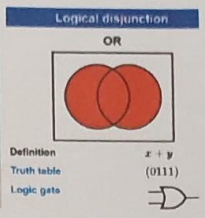
Lecture by Pr. Bob Gallagher
Boole (1815-1864) & **Shannon** (1916-2001)



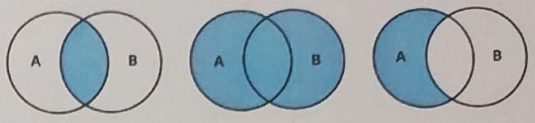
Logical addition (disjunction)

A	B	F=A∨B
0	0	0
0	1	1
1	0	1
1	1	1

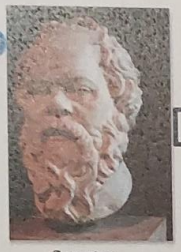
A	B	$A \vee B$
True	True	True
True	False	True
False	True	True
False	False	False



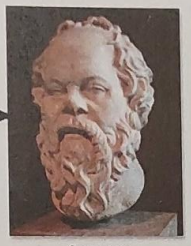
BOOLEAN LOGIC

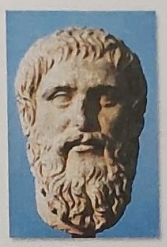


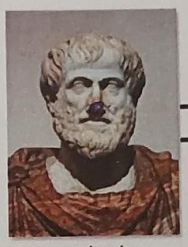
Good logic


Socrates

Socrates was a philosopher

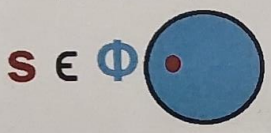

Socrates

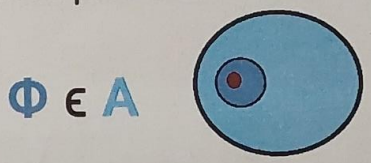

Plato

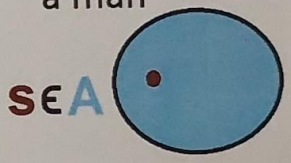

Aristotle

philosophers are men

Socrates was a man

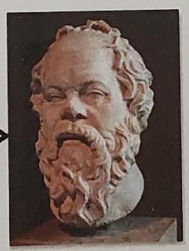


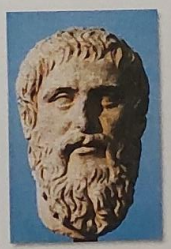


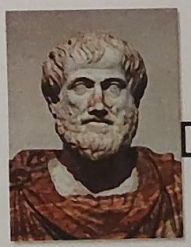


Bad logic

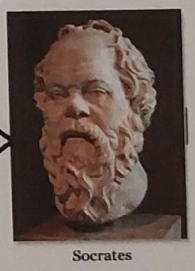
Socrates was a man


Socrates

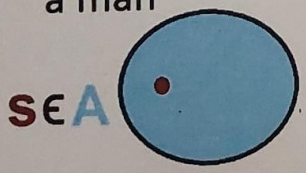

Plato

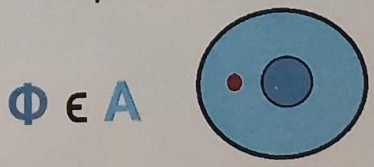

Aristotle

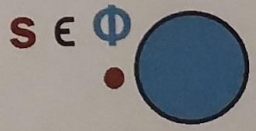
philosophers are men


Socrates

Socrates was a philosopher







Resume of Lecture by Pr. Bob Gallagher from MIT

Massachusetts Institute of Technology (MIT)

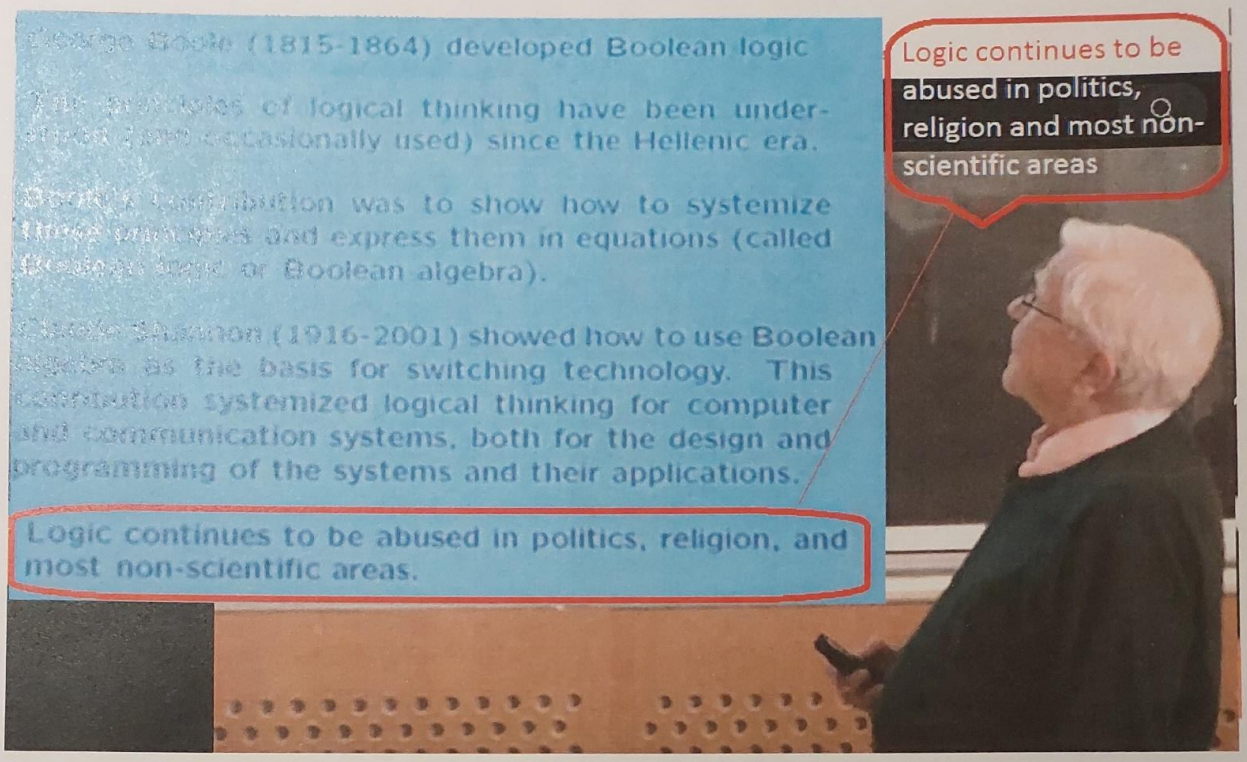
George Boole (1815-1864) developed Boolean logic

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

Boole's contribution was to show how to systemize those 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.

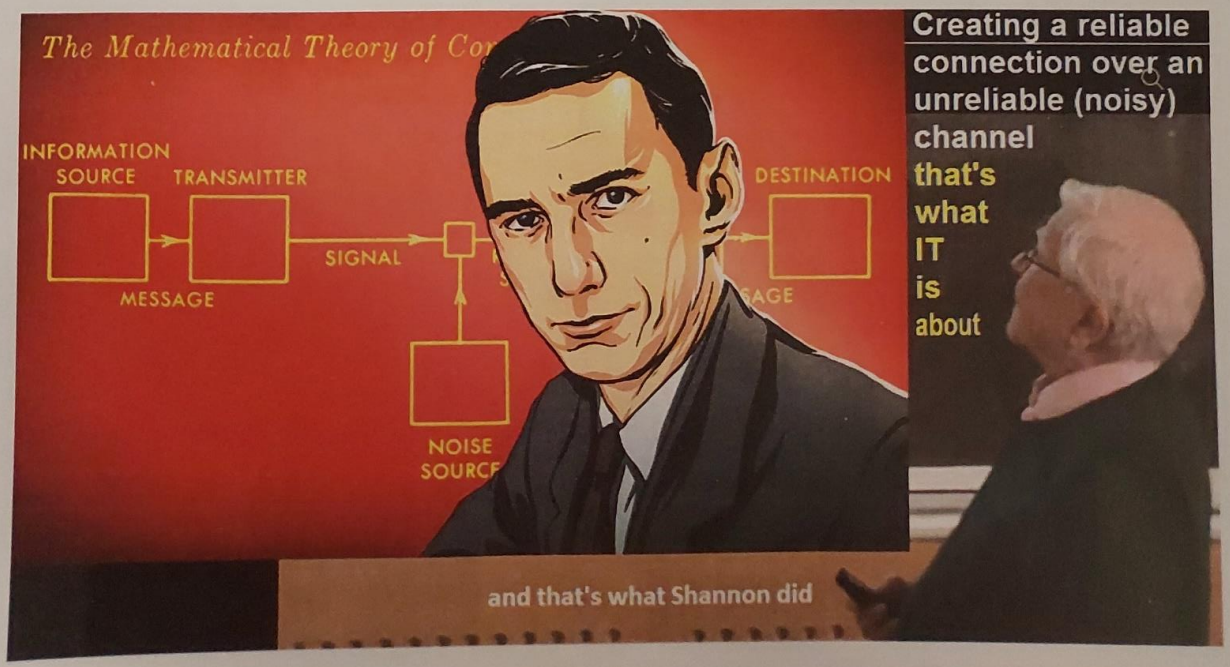


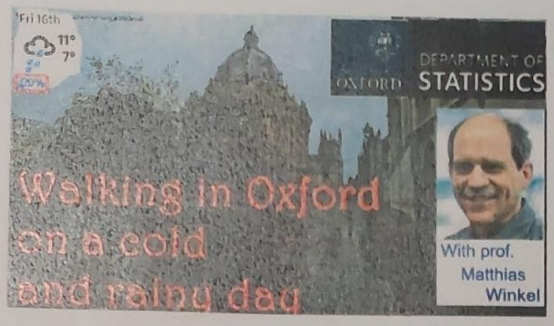
Kant Gauß Goethe

A little nationalistic, but this is an sample of right logic

Kant, Gauss, Goethe are great → Kant, Gauss, Goethe - Germans → Germany Great

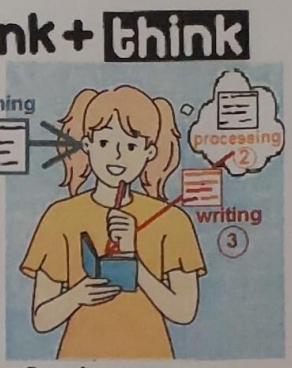
Bad logic (abuse of logic)

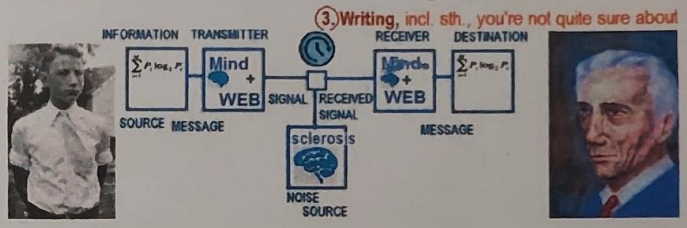




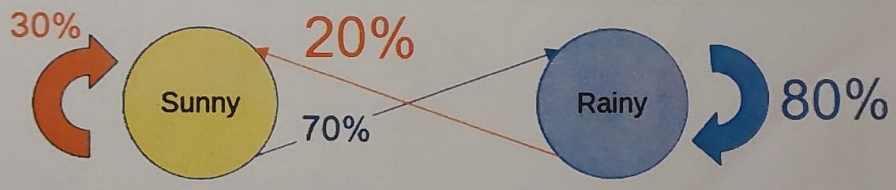
80% chance of rain

says the Met Office in its weather forecast for Oxford.

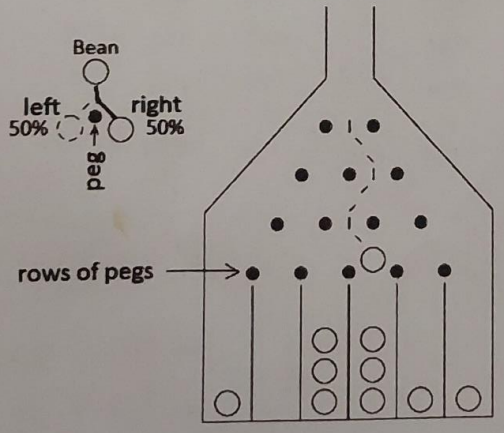


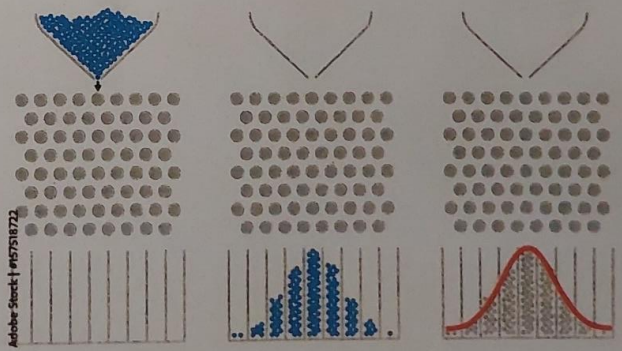


Markoff Chain Probability Model for Oxford Weather



If it is Rainy today => there is an 80% chance that it will be rainy tomorrow.



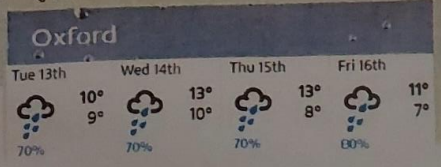


School gravity MOTION == formalism ==> University $E = MC^2$ $W = \vec{F} \cdot \vec{S}$

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_j each have probability p, independently



then take notes on the lecture yourself

1							← 1
1	1						← 2
1	2	1					← 4
1	3	3	1				← 8
1	4	6	4	1			← 16
1	5	10	10	5	1		← 32
1	6	15	20	15	6	1	← 64
1	7	21	35	35	21	7	1 ← 1

~~Ottica~~ Pascal's triangle (Binomial coefficients)

8 row 1 8 28 56 70 56 28 8 1

Shannon Hartley Theorem

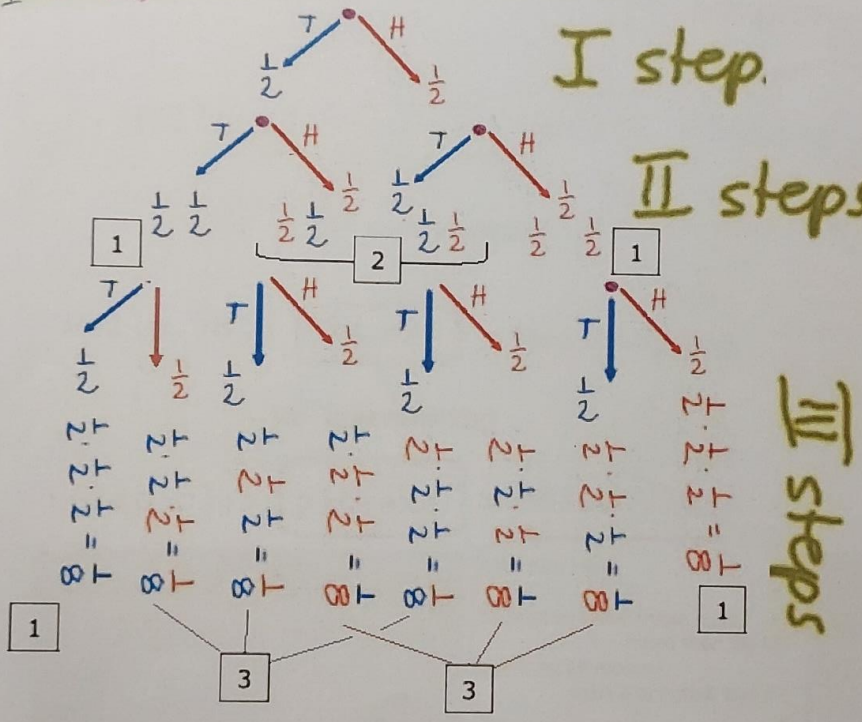
This is a measure of the *capacity* on a channel; it is impossible to transmit information at a faster rate without error.

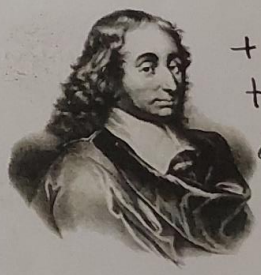
$$C = B\log_2(1+S/N)$$

- 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 B. Pascal

$$(a+b)^0 = 1$$
$$(a+b)^1 = a+b$$
$$(a+b)^2 = a^2+2ab+b^2$$
$$(a+b)^3 = a^3+3a^2b+3ab^2+b^3$$
$$(a+b)^4 = a^4+4a^3b+6a^2b^2+4ab^3+b^4$$
$$(a+b)^5 = a^5+5a^4b+10a^3b^2+10a^2b^3+5ab^4+b^5$$

$(1+x)^8 = 1^8 + 8x + 28x^2 + 56x^3 + 70x^4 + 56x^5 + 28x^6 + 8x^7 + x^8$

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

Generalization of The number of arrangements

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

$x_1 \dots x_1$ (m_1), $x_2 \dots x_2$ (m_2), $\dots$, $x_k \dots x_k$ (m_k)

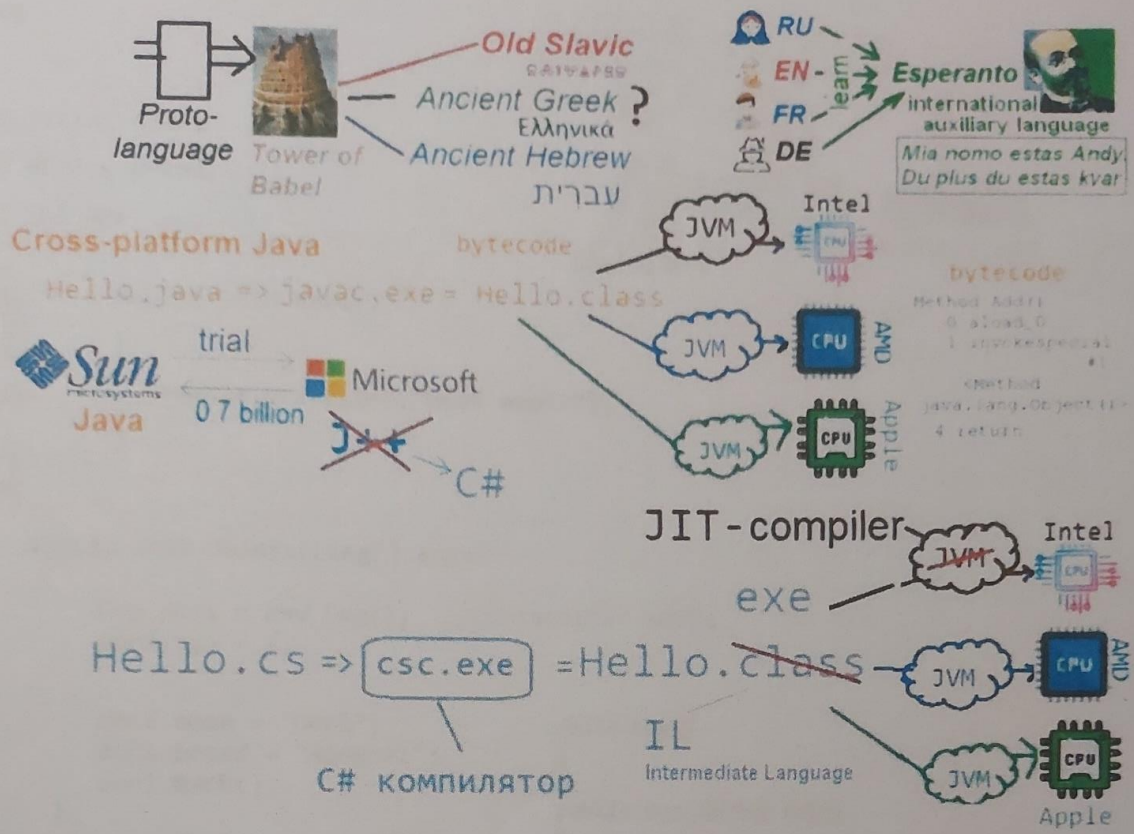
$m_1 + m_2 + m_k = n$

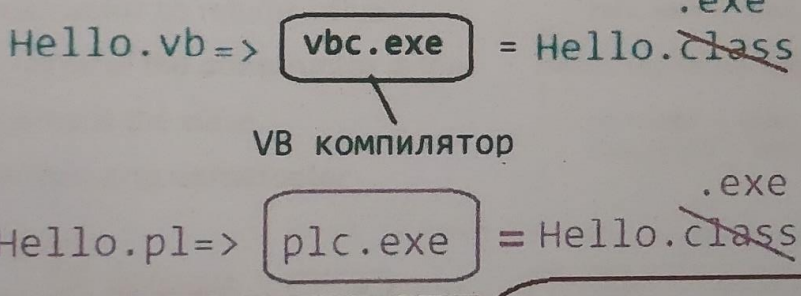
$$\frac{n!}{m_1!\,m_2!\dots m_n!}$$

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

Binomial coefficience: $x^0 + 4x^1 + 6x^2 + 4x^3 + x^4$

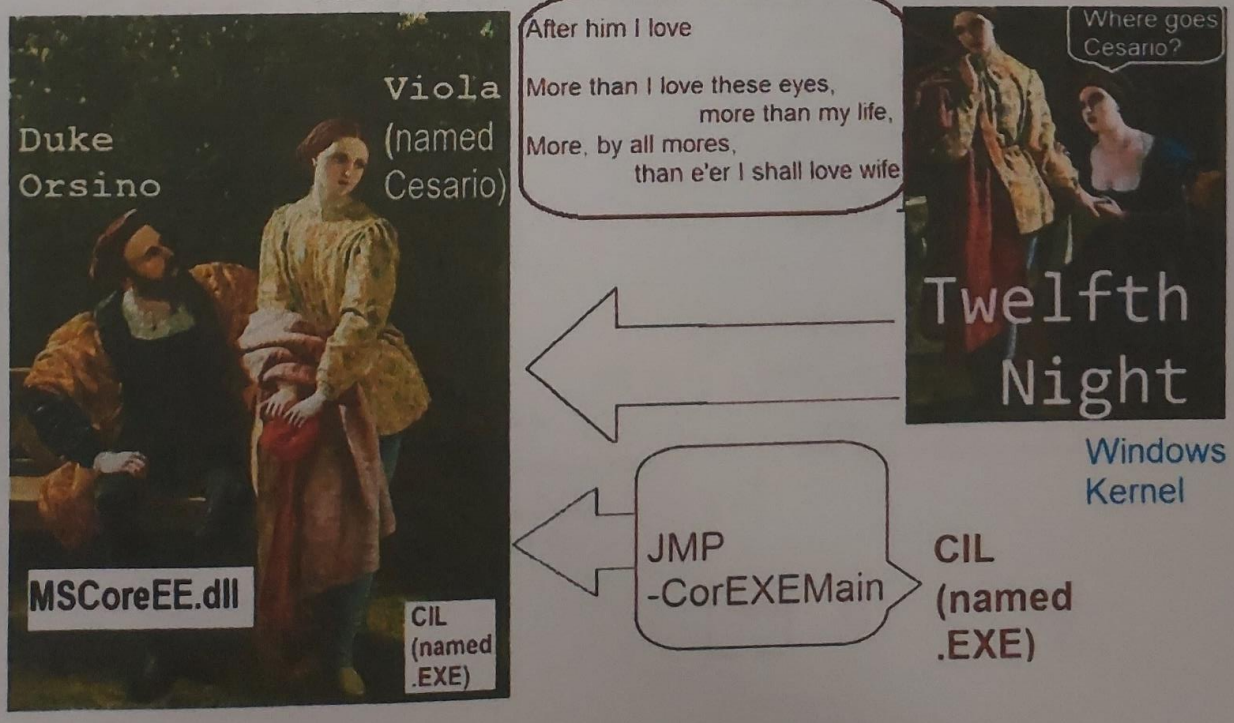
$\binom{4}{0}\ \binom{4}{1}\ \binom{4}{2}\ \binom{4}{3}\ \binom{4}{4}$





CIL - Common Intermediate Language

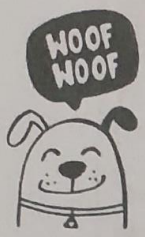
```
void .ctor() {
  .maxstack  1
  IL_0000:  ldarg.0
  IL_0001:  call instance
void
   System.Object::.ctor()
  IL_0006:  ret
} // end of
      method Add::.ctor
```



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

TU Du-blin

Pr. Bryan Duggan




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

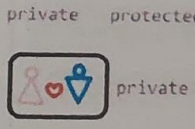
```
static void Main(string[] args)
{
    Dog dori = new Dog();  //Constructor works
    dori.age = 3;

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

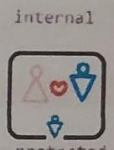
1 - **constructor** no returns value

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

3. more than one **constructor**

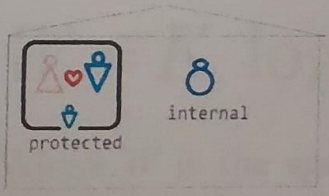
```
public Dog()
{
}
public Dog(string name)
{
    this.name = name;
}
public Dog(string name, string breed)
{
    this.name = name;
    this.breed = breed;
}
```






```
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

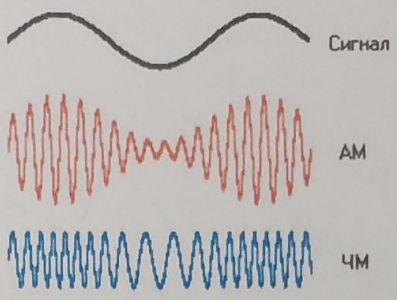
```
class AFather
{
   protected string name;
   internal int age;
}

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;
    }
}
```

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

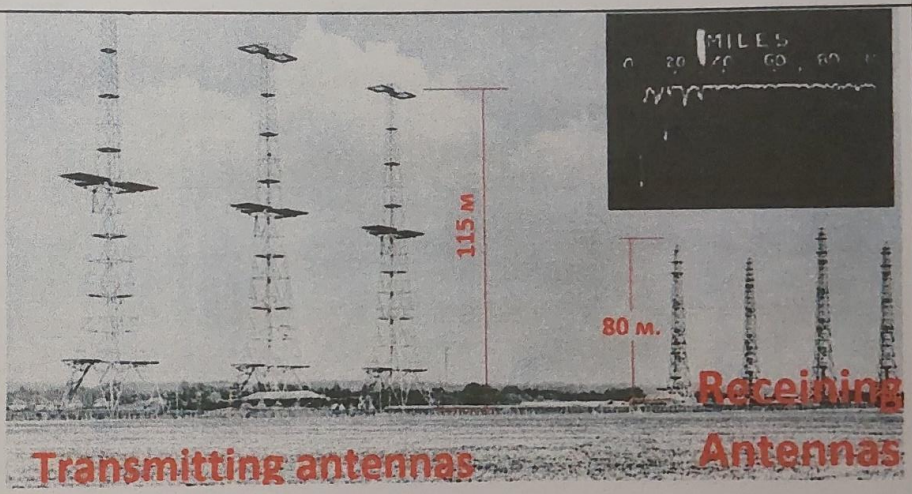


(October 6, 1866 – July 22, 1932)

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

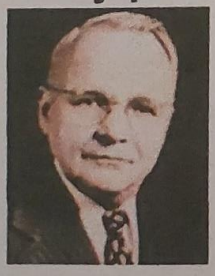
"Ни одна организация, занимающаяся какой-либо конкретной областью деятельности, никогда не изобретает какие-либо важные разработки в этой области или не внедряет какие-либо важные разработки в этой области до тех пор, пока она не будет вынуждена сделать это из-за внешней конкуренции.." Oxford University 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



$$W = K \log m$$

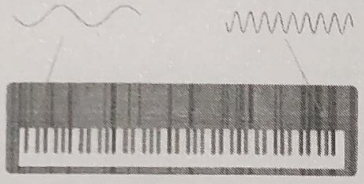
Where W is the speed of transmission of intelligence,
m is the number of current values,
and, K is a constant.

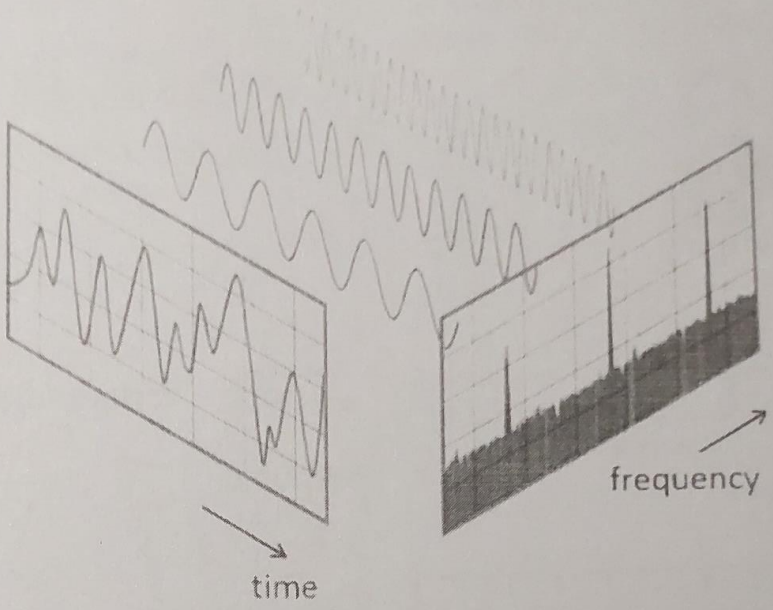
Ralph **Hartley**
(81:1888-1970)

$$H = n \log s$$

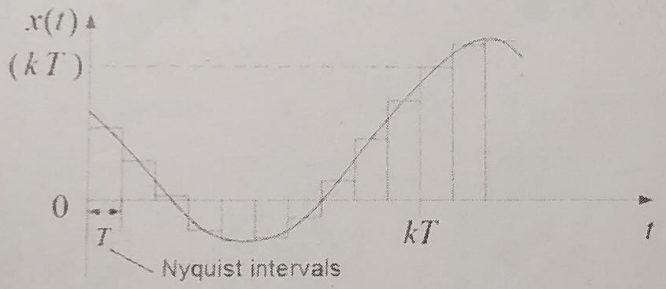
$$= \log s^n.$$

Fourier transform



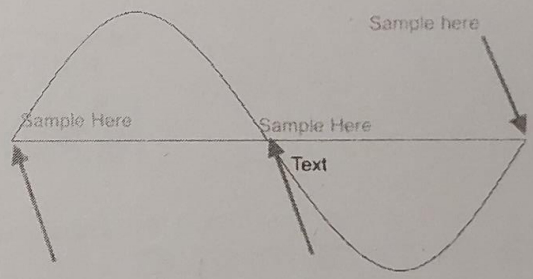


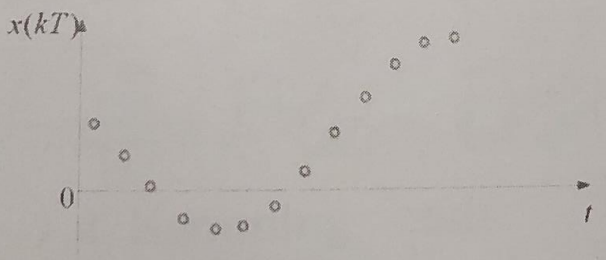
Sampling. Kotelnikov-Nyquist Theorem

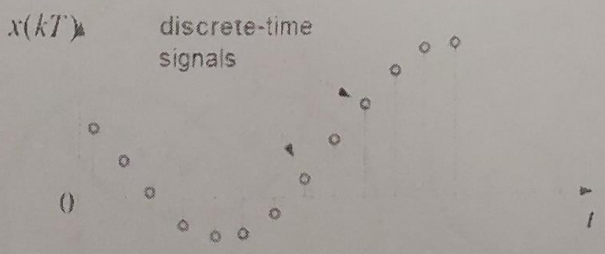


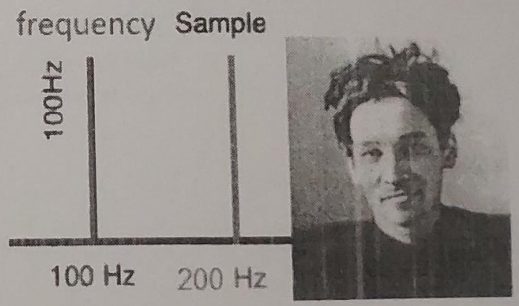
Time intervals T, through which readings s (kT) are taken, are called Nyquist intervals.

Sine with period T **Sampling at T/2**





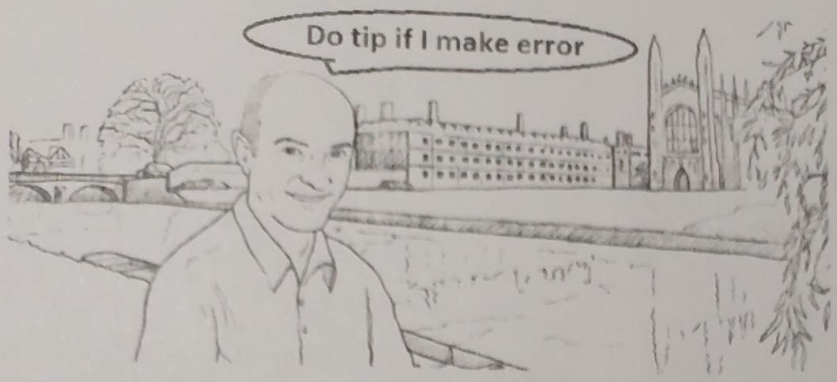




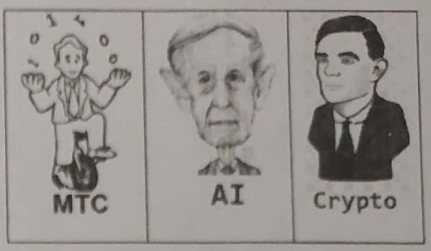
$F_{sample} >= 2 * F_{max}$

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

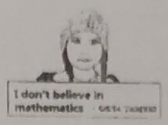
Котельников

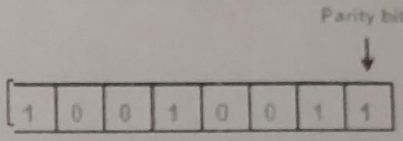


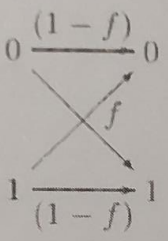
Sir **Dr. D. MacKay,**
University of Cambridge
(22 April 1967 – 14 April 2016)

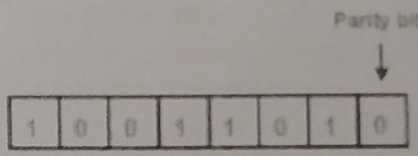


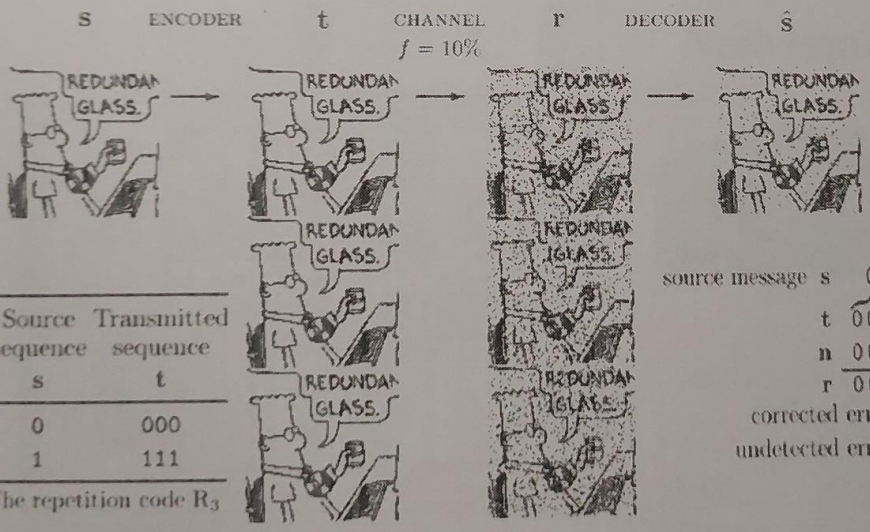
"I believe in clean energy,
but I also believe in mathematics"











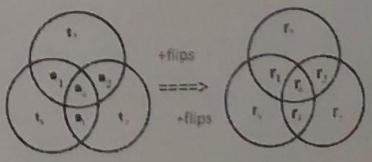
Source sequence s	Transmitted sequence t
0	000
1	111

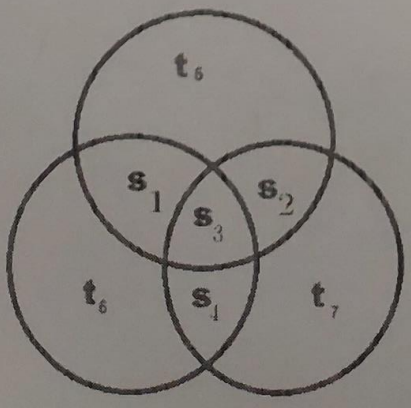
The repetition code R_3

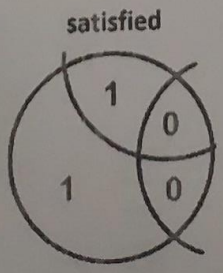
source message s	0	0	1	0	1	1	0
t	000	000	111	000	111	111	000
n	000	001	000	000	101	000	000
r	000	001	111	000	010	111	000
corrected errors		*					
undetected errors					*		

7.4. Hamming code.

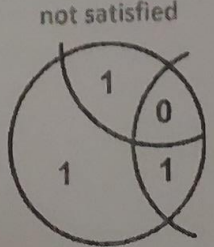
$$\frac{4}{\Sigma} \rightarrow \frac{7}{t}$$



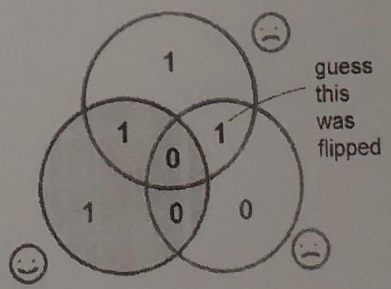


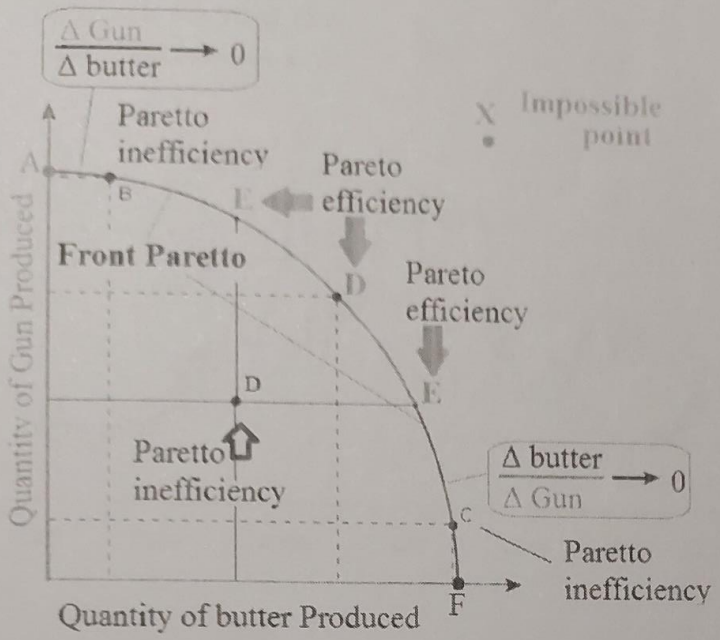


1+1+0+0=**0**



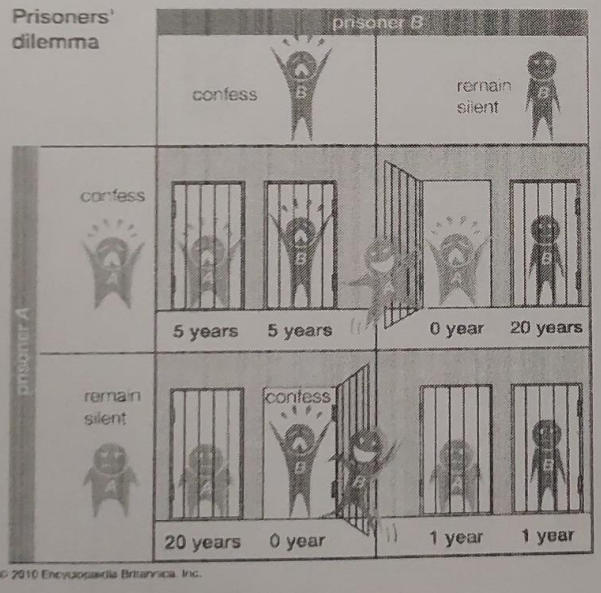
1+1+0+1=1





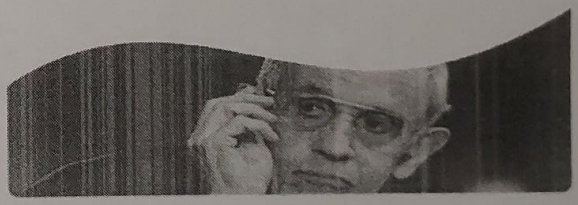
by Vilfredo Pareto

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

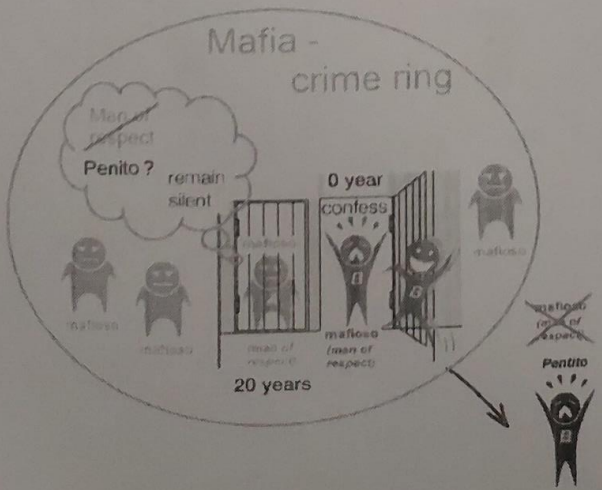


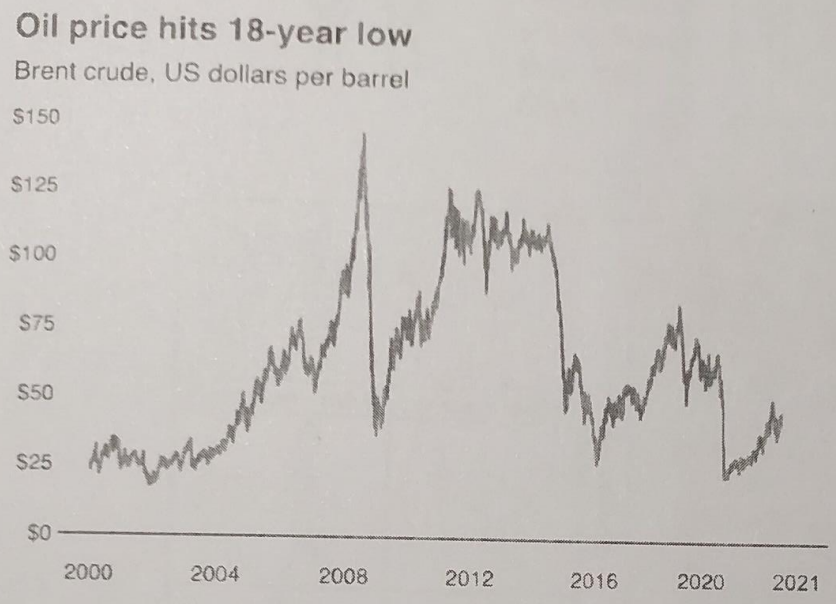
** => Nash equilibrium

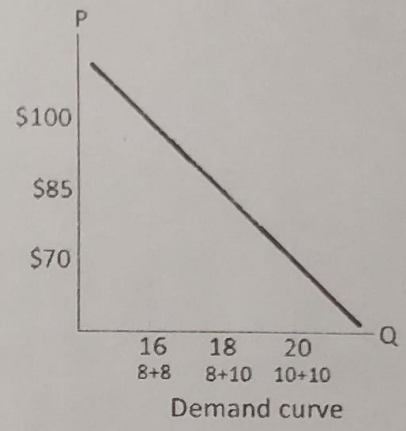
$H_2(x)$ / $H_1(x)$	*Player 2*	Recognition;	Non-recognition;
Player 1		1	2
Recognition;	1	* -5	-20 / 0
Non-recognition;	2	-5 * / -20	0 / -1 / -1

-1-1

Pareto Optimality





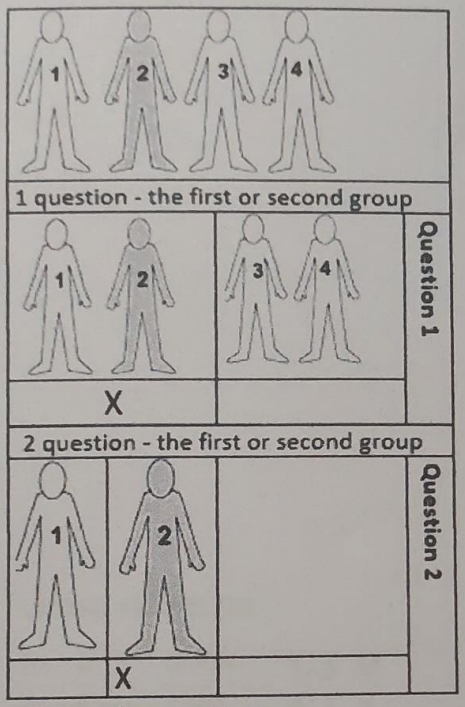


Barrel	1. $8 \cdot 10^6$ barrel/day	2. $10 \cdot 10^6$ barrel/day
1. $8 \cdot 10^6$ barrel/day	$800 millions per day $100 barrel $800 millions per day	$850 millions per day $85 barrel $680
2. $10 \cdot 10^6$ barrel/day	$680 millions per day $85 barrel $850 millions per day	$700 millions per day $70 barrel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

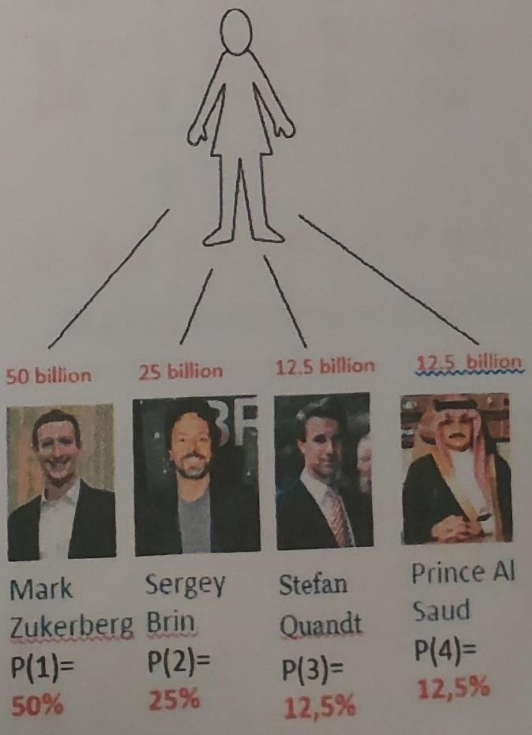
Quantifying information

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

Quantifying information

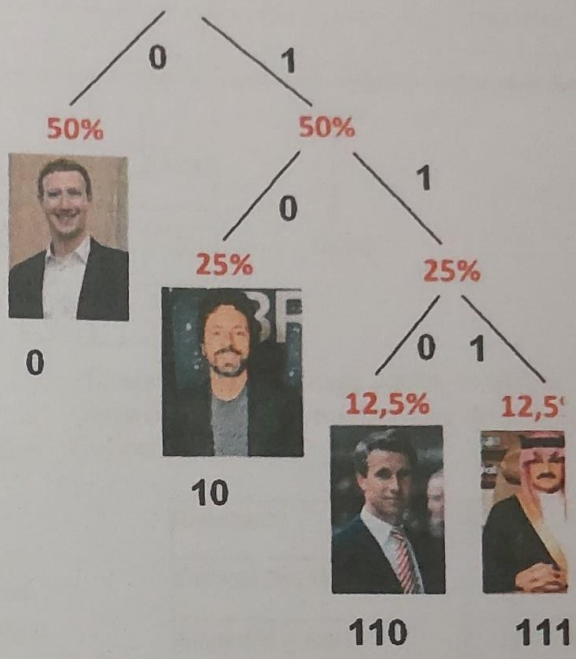
$$I(x_i) = \log_2\left(\frac{1}{p_i}\right)$$

number of bits required to encode choice



ce

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

лла мамма р

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
а р - 1	11%	8	ар
ра - 1	11%	9	ра

9

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

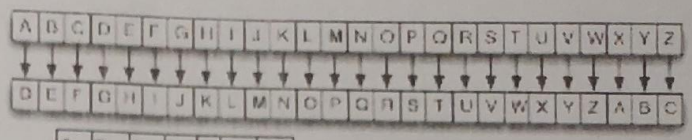
0. 4 6 7 3 1 9 1 6 7 3 5

ам ыл ла ам ма ра ма ыл ла ам мы

мылла рама

Caesar Cipher

$C=(p+3) \bmod 26$



- 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

ABBA

DEED

- 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

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=BqFJD7oCmDE

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.