

BCM0504

# Natureza da Informação

## História da Teoria da Informação

Prof. Alexandre Donizeti Alves



Universidade Federal do ABC

Bacharelado em Ciência e Tecnologia

Bacharelado em Ciências e Humanidades

Terceiro Quadrimestre - 2018

# Informação e Comunicação

- **Etimologia em latim**

*informatio, onis*: “delinear”, “conceber ideia”

- Existem diferentes visões
  - Biologia
  - Linguística
  - Física
  - Ciência da Computação



- **Qual é a relação entre informação e comunicação?**
  - **Comunicação**: intercâmbio de informação entre sujeitos ou objetos

# Informação e Comunicação



- **Informação** é a qualidade da **mensagem** que um emissor envia para um ou mais receptores
    - **Informação:** *resultado do processamento, manipulação e organização de dados em uma forma que se some ao conhecimento da pessoa que o recebe*
  - **Dicionário:**
    - Comunicação ou recepção de um conhecimento ou juízo
    - Conhecimento obtido por meio de investigação ou instrução, esclarecimento, explicação, indicação, comunicação, informe
-

# Teoria da Informação

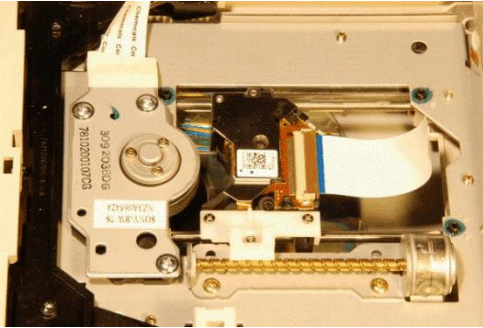
- É a probabilidade de ocorrência de um fato
  - Quanto maior a probabilidade desse fato, menos informação ele trará

## Exemplos:

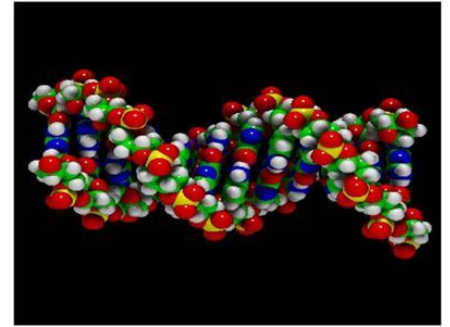


- A primeira vez que ouvimos um disco ele nos traz um novo conhecimento musical. Depois de ouvir várias vezes o mesmo disco, podemos prever os próximos acordes. Portanto, esse disco não nos traz mais informação
- Na palavra “**c\_mo**”, todos podem prever que a letra faltando é “o”. Portanto, é desnecessário escrever essa letra naquela posição

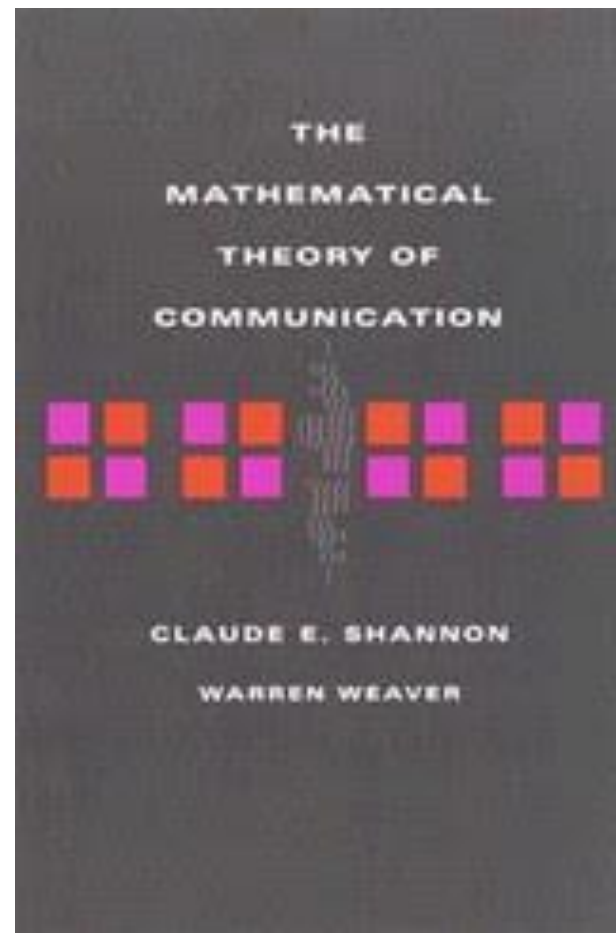
Este curso relaciona assuntos diferentes através de um conceito comum: a **informação**!



- Computadores
- DNA
- Redes Neurais
- Universo



# História da Teoria da Informação



Claude E. Shannon (1916-2001), considerado o **pai** da **Teoria da Informação**, e seu **livro** publicado em 1949, **Teoria Matemática da Comunicação**

[https://pt.wikipedia.org/wiki/Claude\\_Shannon](https://pt.wikipedia.org/wiki/Claude_Shannon)

# Shannon



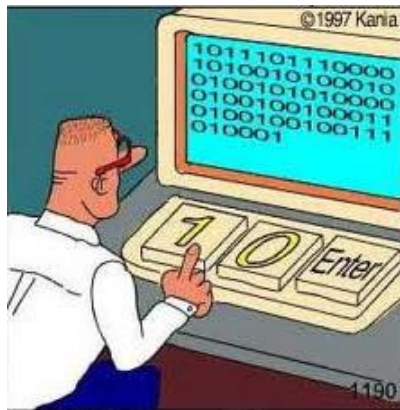
- Em 1948, Shannon publica seu artigo “*A Mathematical Theory of Communication*”, publicado na forma de livro no ano seguinte
- Antes dele, trabalhos isolados caminhavam passo a passo em direção a uma teoria geral de comunicação
- Hoje em dia, **Teoria da Comunicação** (ou **Teoria da Informação**) é uma área imensa de pesquisa, e muitos livros e simpósios internacionais sobre este assunto são publicados e realizados



# Teoria da Informação



- **Teoria da Informação** é uma teoria muito geral e que envolve muita matemática
- A unidade fundamental, o **bit (binary digit)**, é uma medida universal da quantidade de informação



# Teoria da Informação



- Teoria da Informação nos permite:
    - Dizer quantos bits de informação podem ser enviados por segundo através de certos *canais* de comunicação denominados perfeitos ou imperfeitos
    - Medir a taxa na qual uma fonte pode gerar informação
    - Dizer como representar, ou *codificar*, mensagens de uma determinada fonte eficientemente para transmitir através de algum tipo de *canal*, e como podemos evitar erros nesta transmissão
-

# Origens da Teoria da Informação

- Encontraremos as origens da extensa e elegante Teoria da Comunicação de Shannon no simples e aparentemente fácil de compreender fenômeno do **Telégrafo**



- Entretanto, várias pessoas, ao longo do tempo, contribuíram pouco a pouco com a construção desta teoria

# Os pilares da Teoria da Informação

- Os estudos da criptografia desenvolvidos na 2ª Guerra Mundial
- Os estudos da termodinâmica
- As tecnologias de transmissão de informação (começando pelo código Morse e pela telefonia)

# Criptografia na II Guerra

# “Está faltando água em AF”

## “AF is short of water”

- Estas palavras reverteram o curso da guerra do pacífico
- Criptografia e código japonês (J-25) decifrado pelos americanos



# “A ilha Midway está sem água”

Vamos atacar AF!



Almirante Yamamoto

AF??? O que é AF?



Comandante Rochester

# “A ilha Midway está sem água”

A ilha Midway está  
sem água!



AHA!!! Te peguei! 😊

Comandante Rochester

AF está sem água!



Almirante Yamamoto



# Fim da Guerra

- Os americanos aguardaram a chegada dos japoneses
- Começou o fim da II Guerra Mundial



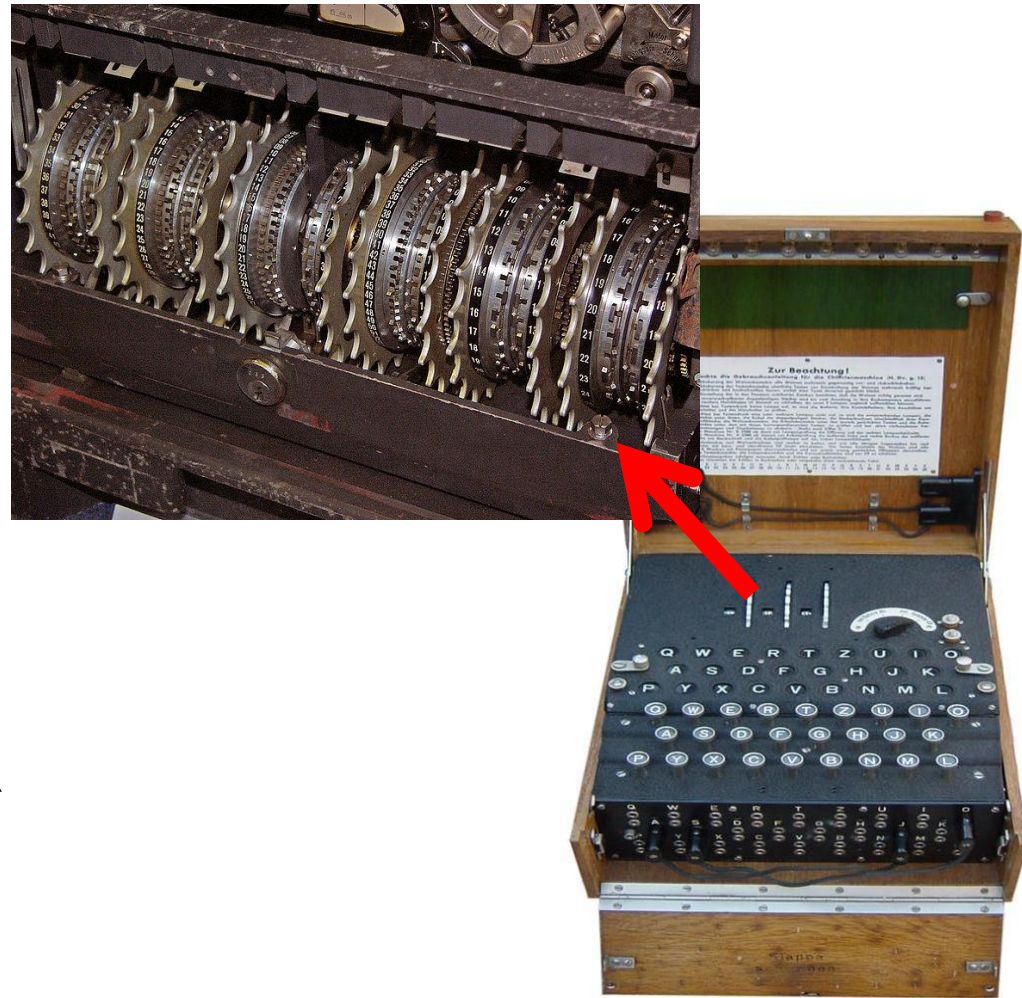
# Enigma

- O alemão Arthur Scherbius inventou a máquina para cifrar mensagens “Enigma”
- $3 \times 10^{114}$  configurações diferentes
- Força bruta: cada átomo do universo tentando um trilhão de combinações por segundo desde o início do universo



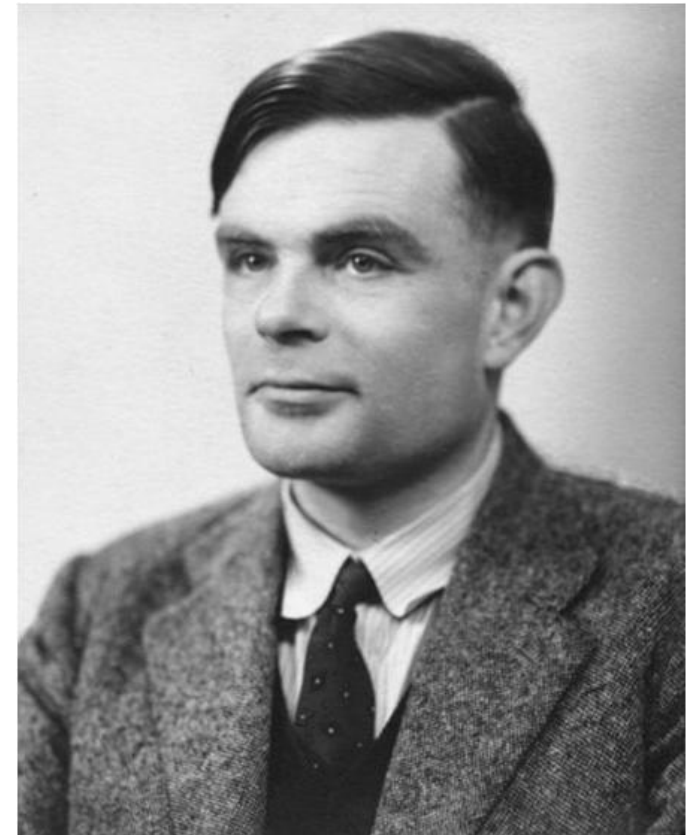
# Enigma

- Aliados capturaram uboats com Enigma e livros de código
- Mas a configuração dos rotores mudava a cada mês
- Mesmo conhecendo a máquina, decifrar não é trivial!



# Turing e seus colegas quebraram o código do Enigma

- Todas as letras eram trocadas de cada vez
- Enigma nunca deixava nenhuma letra sem trocar (**Exemplo**: o correspondente à letra “F” nunca era “F”)
- Frases comuns (**Exemplo**: o clima está bom hoje)
- Permitiu a destruição dos “U-boats” e o fim da guerra

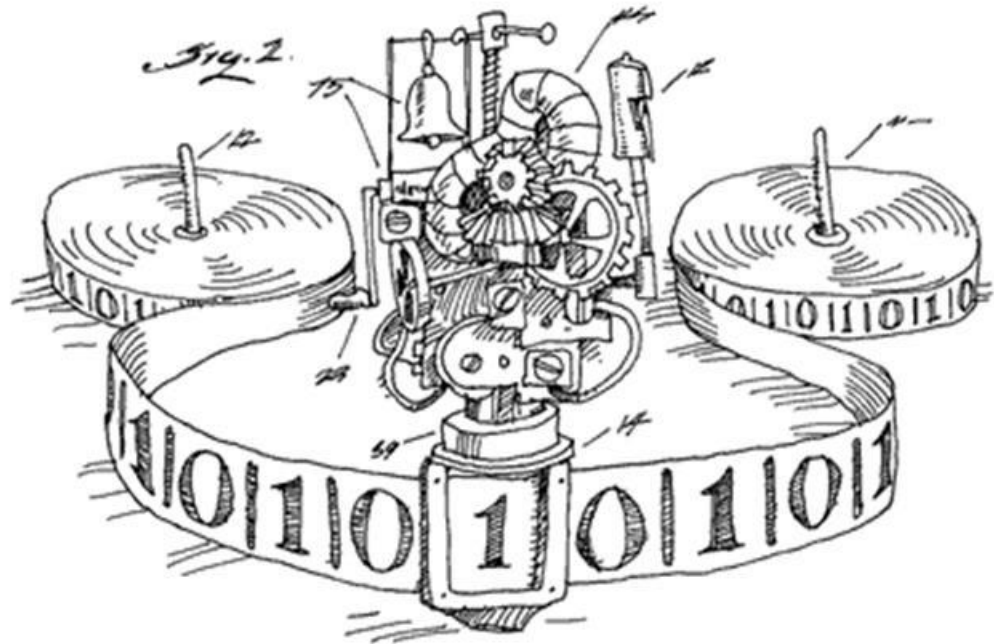




# Máquina teórica de Turing

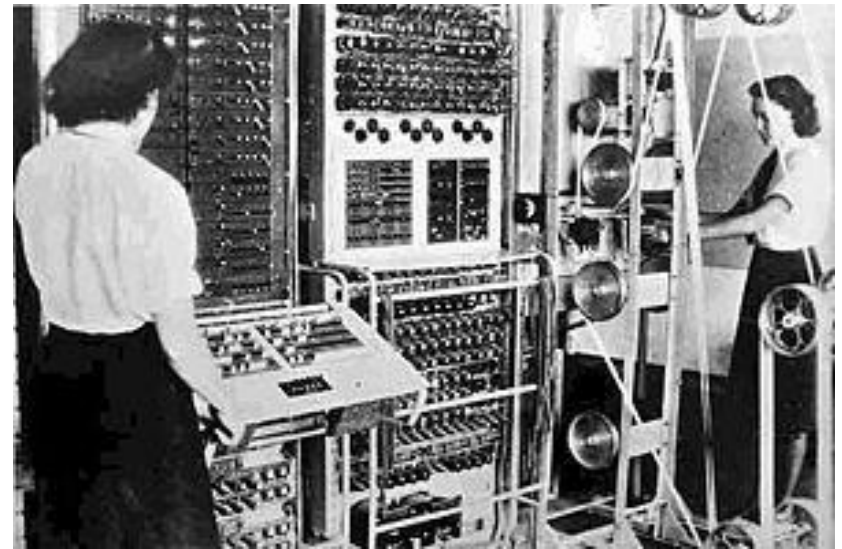


- Fita sem fim
- A máquina lia, escrevia, e apagava
- A máquina de Turing possuía “computabilidade universal”



# Colossus – um dos 10 computadores

- Construído apenas para quebrar Enigma
- Em 1945 Churchill mandou partir os 10 colossus “*in pieces no bigger than a man's hand*”
- Segredo até 1970



A **Criptografia** aliada fez  
terminar a II Guerra e começou  
a **era da informação**

Turing  
contribuiu para  
a II Guerra  
Mundial acabar



# Criptografia

- Um método muito simples para criptografar uma mensagem consiste em substituir cada letra pela que esta n posições na frente
  - Cifra de César



# Criptografia

Tente decifrar a mensagem seguinte:

**Q xgpvq jqlg guvcxc owkvq hqtg**

# Criptografia

Tente decifrar a mensagem seguinte:

**Q xgpvq jqlg guvcxc owkvq hqtvq**

**n = -2**

**O vento hoje estava muito forte**

# Redundância

-s -v-nç-s d- c--nc-- e d- t-cn-l-g-- -  
st-- m-lt-pl-c-ndo -s n-ss-s  
c-p-c-d-d-s d- c-l-t-r, tr-t-r, g-r-r  
- -t-l-z-r -nf-rm-ç-es.

## **Nosso cérebro aproveita a redundância para conseguir entender textos como o seguinte:**

De aorcdo com uma peqsiusa de uma uinrvesriddae ignlsea, não ipomtra em qaul odrem as Lteras de uma plravaa etãso, a úncia csioa iprotmatne é que a piremria e útmlia Lteras etejasm no lgaur crteo. O rseto pdoe ser uma bçguana ttaol, que vcoê anida pdoe ler sem pobrlmea. Itso é poqrue nós não lmeos cdaa Ltera isladoa, mas a plravaa cmoo um tdoo. Sohwa de bloa.

# Ou como este texto...

35T3 P3QU3N0 T3XTO 53RV3 4P3N45 P4R4 M05TR4R COMO  
NO554 C4B3Ç4 CONS3GU3 F4Z3R CO1545 MPR3551ON4ANT35!  
R3P4R3 N155O! NO COM3ÇO 35T4V4 M310 COMPL1C4DO, M45  
N3ST4 L1NH4 SU4 M3NT3 V41 D3C1FR4NDO O CÓD1GO  
QU453 4UTOM4T1C4M3NT3, S3M PR3C1S4R P3N54R MU1TO,  
C3RTO? POD3 F1C4R B3M ORGULHO5O D155O! SU4  
C4P4C1D4D3 M3R3C3! P4R4BÉN5!

# Métodos de compressão de informação

- Existem diversos métodos de compressão de informação
  - O que resta depois de comprimir um texto é um núcleo que não pode ser mais comprimido
  - Esse núcleo é a “informação”
-

# Uma primeira forma de quantificar a informação

- Informação é aquilo que sobra numa mensagem depois de eliminar a redundância



# Entropia e Termodinâmica



# Entropia e Termodinâmica



- Uma quantidade muito conhecida é a **Entropia**, muito utilizada em **Termodinâmica**
    - **Termodinâmica**: movimento da energia e como a energia cria movimento
    - **Entropia**: "grau de desordem" de um sistema termodinâmico
  - Uma quantidade **Entropia** também é utilizada em Teoria da Comunicação
    - E sabemos que a Termodinâmica é muito mais antiga que a Teoria da Informação
-

# Atenção!!!

Embora a **Entropia** da **Teoria da Comunicação** tenha uma analogia matemática com a **Entropia** da **Termodinâmica**, são conceitos diferentes, e usadas para medir quantidades completamente diferentes!



# Entropia em Termodinâmica



- Medida da reversibilidade de um processo:
  - Se não há mudança no valor da entropia do sistema, o sistema é reversível
- Mas a grande maioria dos fenômenos físicos não são reversíveis: a entropia do sistema envolvido aumenta
- Outra interpretação: quando a entropia de um sistema aumenta, diminui a energia disponível neste sistema para ser transformada em trabalho
  - Em Mecânica Estatística: aumento da entropia de um sistema significa um aumento da desordem deste sistema, em um sentido de imprevisibilidade

# Entropia em Comunicação



- Imaginem uma fonte de informação
    - **Exemplo:** um jogo de dado, sendo a informação o resultado do lançamento do dado
    - **Pergunta natural:** quantos bits seria necessário em uma codificação ideal (usando a menor quantidade de bits possível) para transmitir a informação de qualquer resultado possível?
      - A entropia da informação mediria este valor: a quantidade mínima de informação possível gerada por uma fonte
      - Quanto mais soubermos sobre a informação que vai ser gerada pela fonte, menor a sua entropia, e vice-versa
-

# Entropia em Comunicação

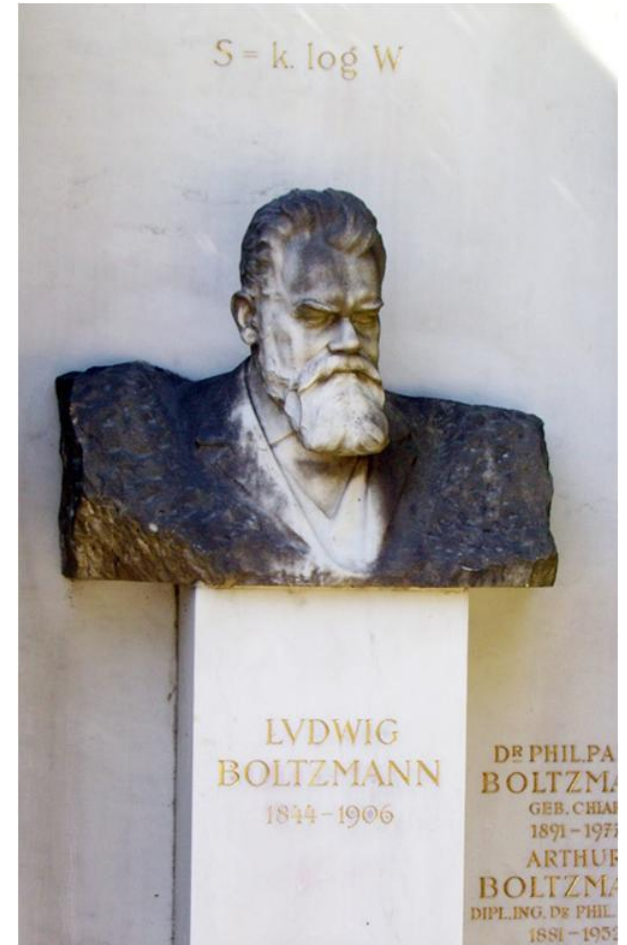


Portanto, **entropia da informação** está relacionada com a incerteza com que a informação vai ser gerada, e não com a quantidade de informação em si

---

# Boltzmann o pai da termodinâmica e da teoria da informação

- Inscrição no túmulo de Boltzmann
- As bases da teoria da informação estão nos estudos da termodinâmica



# Lavoisier

- Descreveu os elementos químicos e a lei de conservação da matéria
- Propôs o elemento chamado “calórico”.
- Fogo gera elemento “calórico”, transmitindo para o ferro e esquentando o ferro.
- Ao aproximar o ferro de outro objeto, parte do “calórico” passa para o 2º objeto.
- Problemas?
  - É verdade o “calórico”?



# Lavoisier

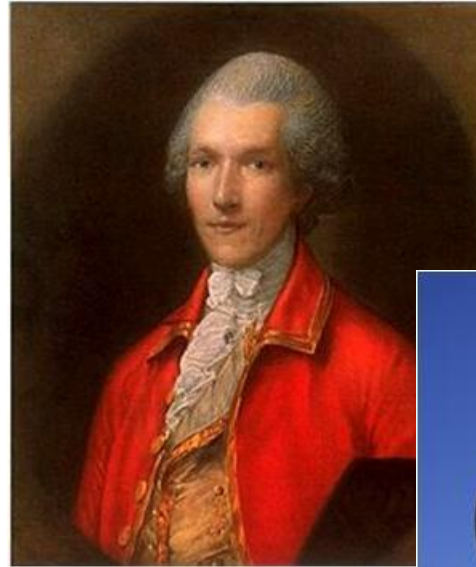


- Experimento para desacreditar o calórico:
  - Produzir calor por fricção
  - Ferramenta fria ao trabalhar sobre madeira fria gera calor
  - De onde viria o “calórico” se ambos estavam frios?
  - Desacreditada a teoria do “calórico”
- Conceito novo: trabalho gera calor.
- Se queremos trabalho, será que o calor pode gerar trabalho?



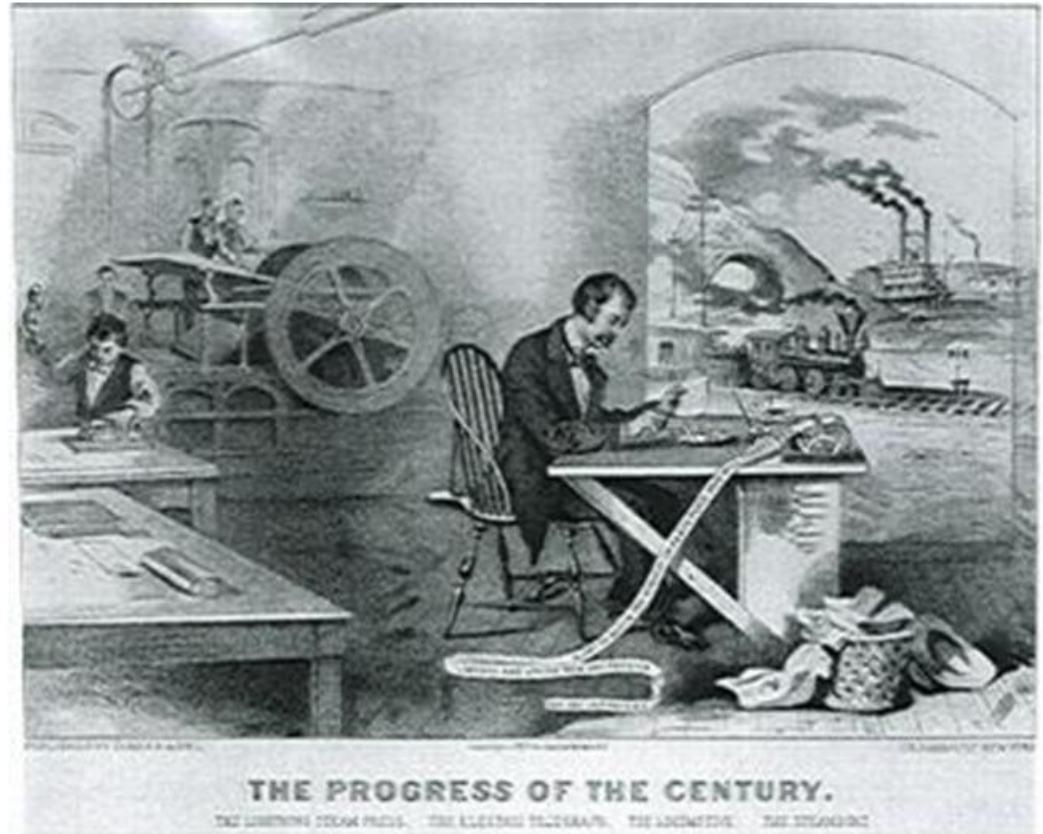
# Benjamim Thompson

- A viúva de Lavoisier casou com Benjamim Thomsom
- Thomson descobriu a equivalência de trabalho e calor

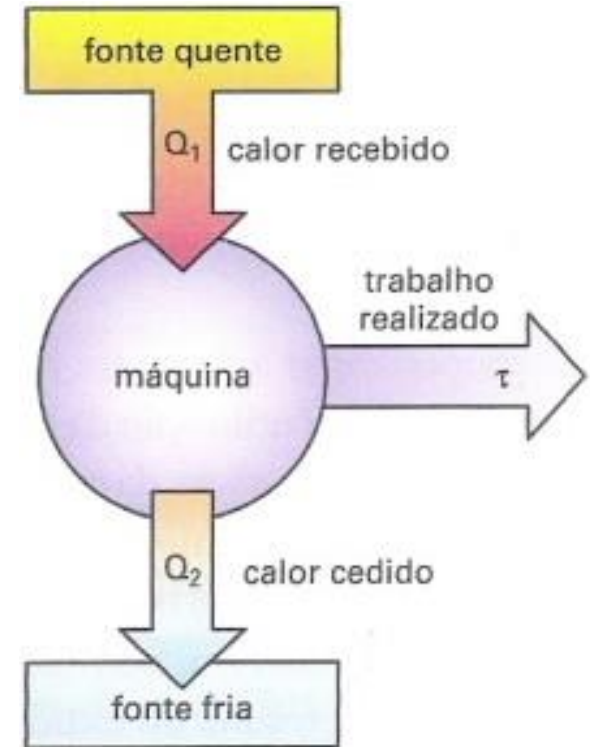


# Revolução Industrial

- 1769 Watt inventou máquina de vapor
- Pesquisa para aumentar eficiência das máquinas



# Máquina térmica de Carnot

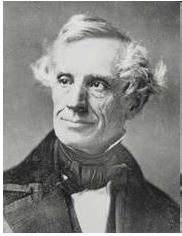


# Origem da moderna da Teoria da Informação

Embora haja analogia matemática da entropia da Informação com a entropia da Mecânica Estatística, dizemos que a origem real da **Teoria Moderna da Informação** tem suas raízes nas origens da **comunicação elétrica**



# Origens com o telégrafo



- **1832:** Samuel F. B. **Morse** colocou em funcionamento o primeiro telégrafo elétrico
    - Muito mais complicado que o que conhecemos atualmente
    - Considerava sequências de pulsos curtos e longos que representavam não letras do alfabeto, mas números correspondentes a palavras, onde a correspondência estava em um livro de códigos completado em 1837
    - Era uma forma eficiente de codificação, mas difícil de manusear
-

# Origens com o telégrafo



- **1838:** trabalhando com Alfred Vail, o **código Morse** como conhecemos hoje foi idealizado
    - Neste código, letras do alfabeto são representadas por espaços, pontos e traços
    - Para transmissão em um circuito elétrico, espaços eram representados por ausência de corrente, pontos por corrente de curta duração e traços por correntes de longa duração
    - Várias combinações de pontos e traços eram associadas a cada letra
- Exemplo:** letra E (que mais ocorre em textos em Inglês) era associada a um único ponto
-

# Código Morse

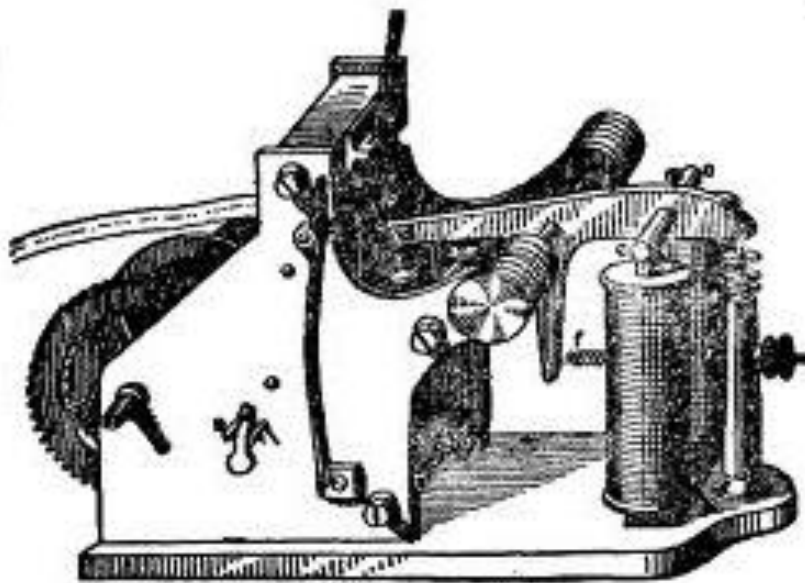


FIG. 103

## Morse Code Alphabet

The International morse code characters:

A	.-	N	-.	0	-----
B	-...	O	---	1	.----
C	-.-.	P	.-.	2	..---
D	-. .	Q	--.	3	...--
E	.	R	.-.	4	....-
F	.. .	S	...	5	.....
G	--.	T	-	6	-....
H	....	U	..-	7	--...
I	..	V	...-	8	----..
J	.-.	W	.-.	9	-----.
K	-. -	X	--.	Fullstop	....-
L	.-..	Y	-. -	Comma	--...-
M	--	Z	--..	Query	.....



# Código Morse e Teoria da Informação



- **Questão importante:**

- Uma outra associação entre os pontos, traços e espaços e as letras do alfabeto nos permitiria enviar textos em Inglês mais rápido pelo telégrafo?

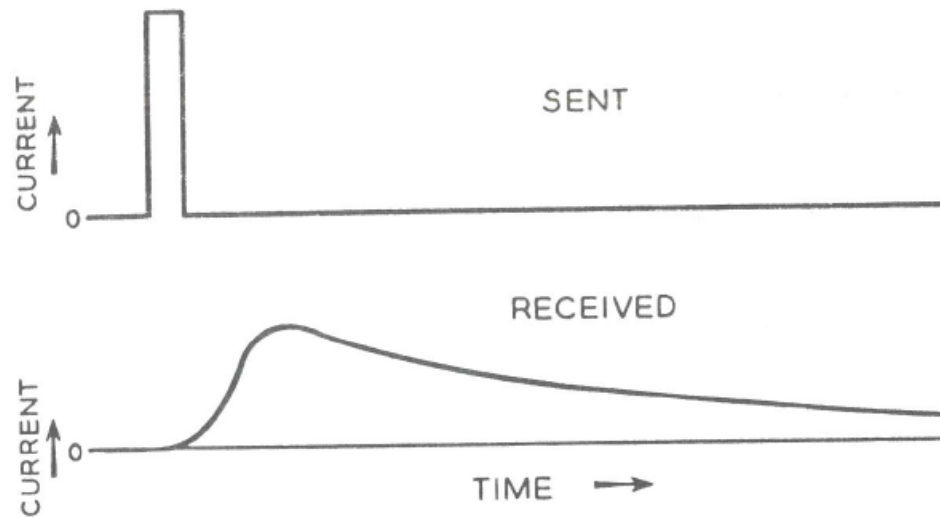
- **Resposta:**

- Usando nossa moderna Teoria de Informação, encontramos que teríamos, no máximo, um ganho de cerca de 15% sobre a velocidade de transmissão
- Isto mostra que Morse, intuitivamente, sabia o que estava fazendo, e atacou um assunto que está no centro da Teoria da Comunicação



# Limitações do telégrafo

- Quando os terminais dos cabos elétricos de um telégrafo estão muito longe (ou quando os cabos estão enterrados ou sob o mar), temos o problema da atenuação e espalhamento do sinal:



*Fig. II-1*



# Limitações do telégrafo



- Portanto, há um limite de velocidade de envios de sinais elétricos para que os sinais representando pontos e traços, no receptor, não se sobreponham todos e não se consiga decodificar coisa alguma
- Muitos tipos diferentes de correntes levam ao problema de identificação correta dos sinais pelo receptor (pelo problema de atenuação e espalhamento do sinal)

# Limitações do telégrafo



- Além disto, há outras **limitações**:
  - Interferências elétricas e magnéticas ocorridas durante o circuito dos sinais (ruídos)
  - Se quisermos aumentar a intensidade dos sinais para diferenciá-los melhor na recepção, podemos destruir o isolamento do cabo e criar um curto circuito
- Os primeiros telegrafistas já haviam percebido todos estes problemas

# Limitações do telégrafo



- Resumo das limitações apresentadas:
  - Limitação associada a velocidade de emissão do sinal
  - Interferências (ruídos)
  - Dificuldade em distinguir entre muitos valores possíveis de correntes
  - Limitação na intensidade de correntes a serem utilizadas (para não destruírem o isolamento dos cabos)
- Uma análise matemática mais precisa deste problema se tornou necessária

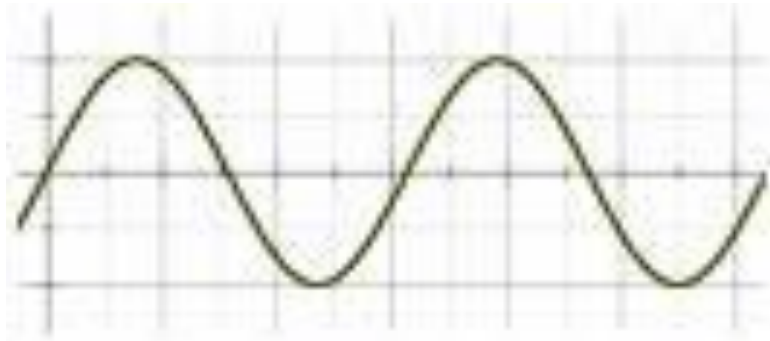
# Contribuições a Teoria da Informação



- No século XIX, várias pessoas contribuíram matematicamente para a teoria da Informação:
  - Lorde Kelvin (William Thomson)
  - Alexander Graham Bell (inventor do telefone em 1875)
  - Henri Poincaré
  - Oliver Heaviside
  - Michael Pupin
  - G. A. Campbell (ATTC)
- Mas sem dúvida alguma, a **grande contribuição** foi de **Joseph Fourier**

# A contribuição de Fourier

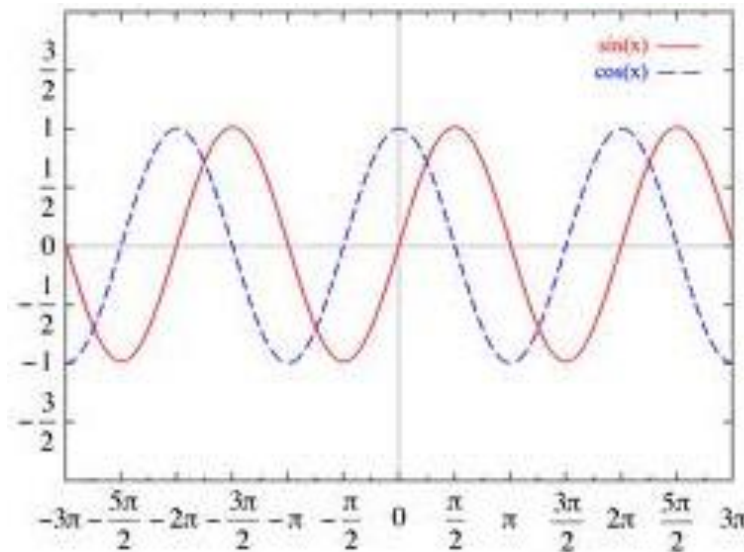
- Fourier baseou seus trabalhos na função seno:



- Demonstrou que toda função (incluindo os sinais elétricos) poderiam ser decompostas numa soma de funções senos com diferentes amplitudes, fases e frequências

# Função senoidal

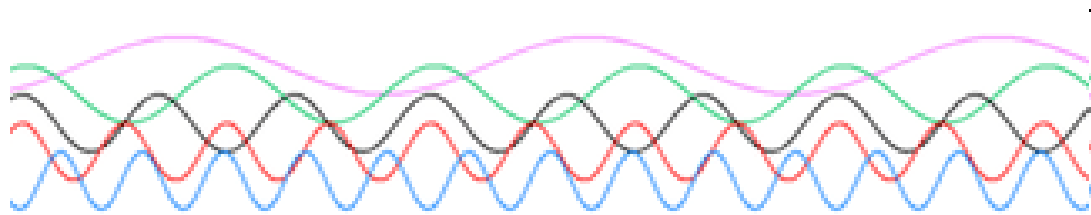
- Uma **senóide** ou **onda seno** ou **senoidal** é uma forma de onda cujo gráfico é de uma função seno generalizada



- Ondas podem ser descritas por variáveis como: amplitude, fase, comprimento de onda e frequência

# Frequência

- Indica o número de ocorrências de um evento (ciclos, voltas, oscilações etc.) em um determinado intervalo de tempo
  - Exemplo: Ondas senoidais com diferentes frequências
    - A azul é a de maior frequência

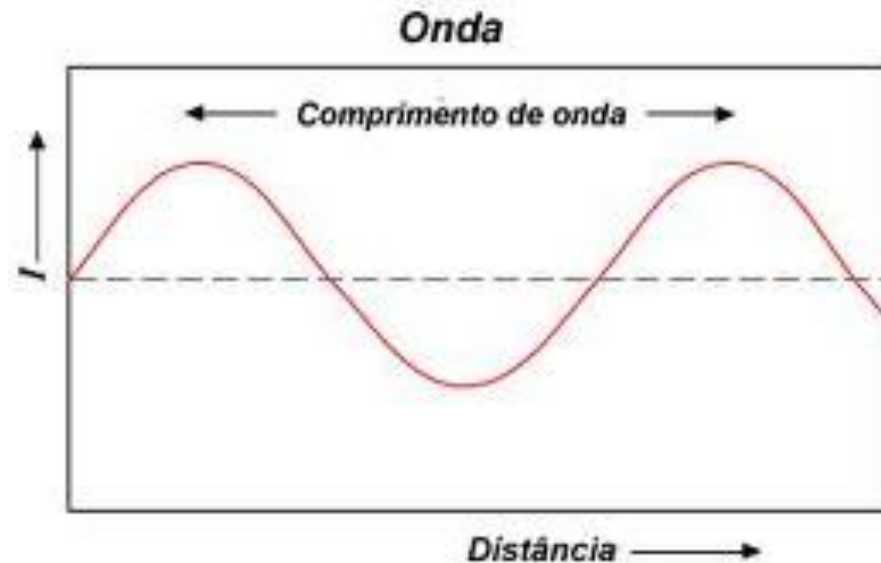


- O comprimento da onda é inversamente proporcional à sua frequência



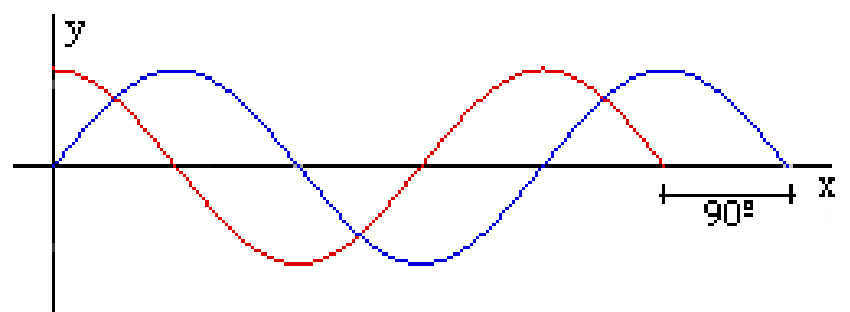
# Comprimento de onda

- Distância entre valores repetidos em um padrão de onda
  - Denotada por  $\lambda$



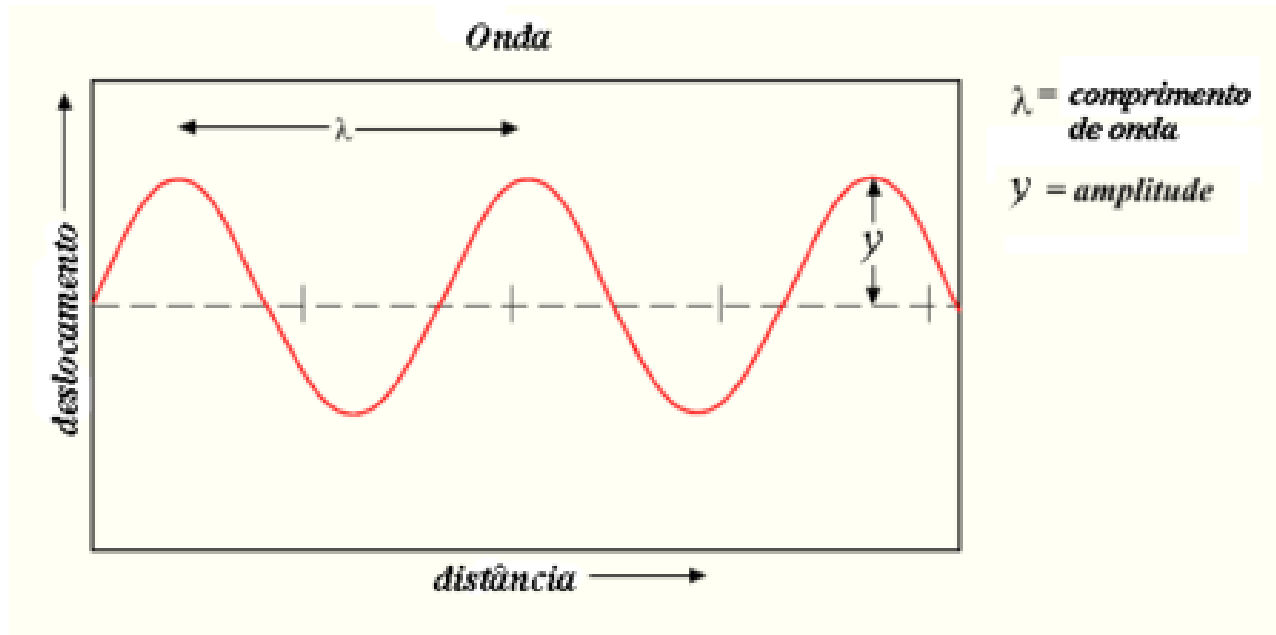
# Fase

- De quanto uma onda difere de outra de igual frequência e comprimento de onda no que toca às diferenças de fase em cada um dos seus pontos em igual distância da fonte e igual tempo
- **Exemplo:** duas senóides defasadas de  $90^\circ$



# Amplitude

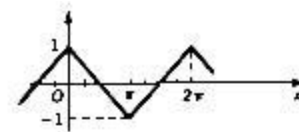
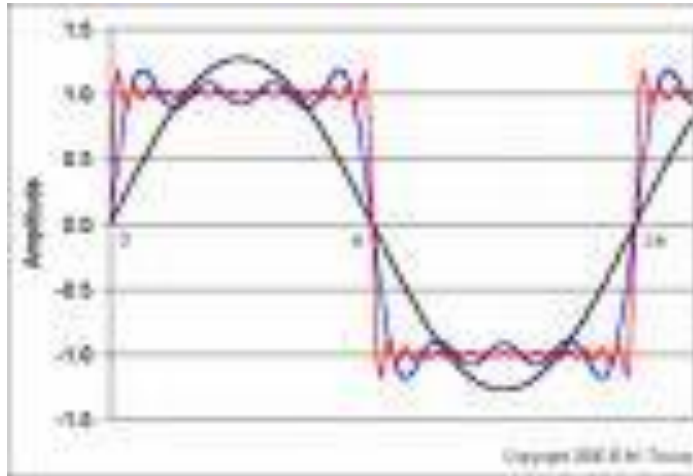
- Medida da magnitude de oscilação de uma onda



# A contribuição de Fourier

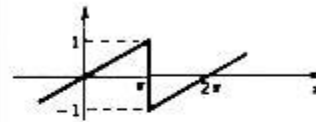


- Alguns exemplos de sinais elétricos escritos como uma soma de funções senos:



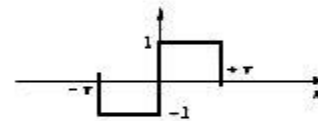
Triangular wave:

$$\frac{8}{\pi^3} \sum_{n=0}^{\infty} \frac{1}{(2n+1)^3} \cos(2n+1)x$$



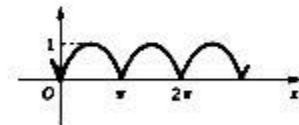
Rectangular sawtooth wave:

$$\frac{2}{\pi} \sum_{n=1}^{\infty} (-1)^{n+1} \frac{1}{n} \sin nx$$



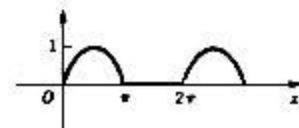
Square wave:

$$\frac{4}{\pi} \sum_{n=0}^{\infty} \frac{1}{2n+1} \sin(2n+1)x$$



Absolute value sine wave:

$$\frac{2}{\pi} - \frac{4}{\pi} \sum_{n=1}^{\infty} \frac{1}{4n^2-1} \cos 2nx$$



Half sine wave:

$$\frac{1}{\pi} + \frac{1}{2} \sin x - \frac{2}{\pi} \sum_{n=1}^{\infty} \frac{1}{4n^2-1} \cos 2nx$$

# A contribuição de Fourier



- Mostrou-se que, em uma transmissão de sinais elétricos tipo seno, a frequência não varia desde o emissor até o receptor (embora a amplitude e a fase possam variar)
  - Portanto, podemos agora emitir uma infinidade de sinais sem perigo de perdermos a informação de qual sinal foi emitido ao chegar no receptor
-

# A contribuição de Nyquist



- 1924: Harry Nyquist publicou seu importante artigo: *"Certain Factors Affecting Telegraph Speed"*
- Discutiu a relação entre a velocidade de transmissão e o número de símbolos (traduzidos em correntes) possíveis de serem transmitidos
- Exemplos:
  - 2 símbolos apenas, representados pelas correntes +1 e -1 ou
  - 4 símbolos representados pelas correntes +3, +1, -1 e -3 ou ainda
  - vários símbolos representados por diferentes frequências da função seno

# A contribuição de Nyquist

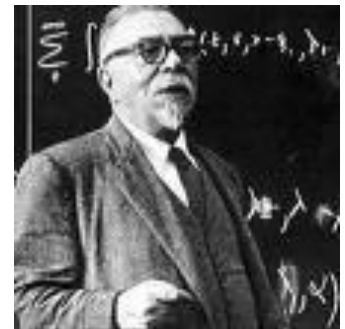


- Nyquist também conseguiu conciliar a transmissão telefônica e telegráfica sobre o mesmo fio (ao mesmo tempo)
  - Definindo sinais com frequências maiores que 150 hz para a telefonia e menores para a telegrafia
- Ainda fez vários estudos sobre quais frequências em determinados tipos de transmissões poderiam ser desprezadas sem prejuízo para o entendimento do sinal emitido

# Contribuições de Kolmogoroff e Wiener



- Na década de 40, ambos independentemente, um na Rússia e outro nos EUA, resolveram o problema de como, a partir de um sinal desconhecido com ruído, estimar qual o melhor sinal correto sem a presença do ruído





# E chegamos a Shannon



- Portanto, quando Shannon publica seu trabalho em 1947, muito já se havia feito anteriormente
  - De certa maneira, ele resumiu e trouxe mais conhecimento a todos estes problemas já estudados anteriormente
-

# Contribuição de Shannon



- Mas podemos dizer que a grande contribuição da sua teoria foi responder as perguntas:
  - Como podemos codificar (em termos de sinais elétricos) uma mensagem a partir de uma fonte para poder transmiti-la o mais rápido possível através de um canal que introduz ruídos com certas características?
  - O quão rápido podemos transmitir um tipo de mensagem através de um determinado canal sem erros?
- Tudo isto que vimos faz parte do que chamamos de **Teoria da Informação** e veremos alguns tópicos introdutórios ao longo deste curso

# Filmes

