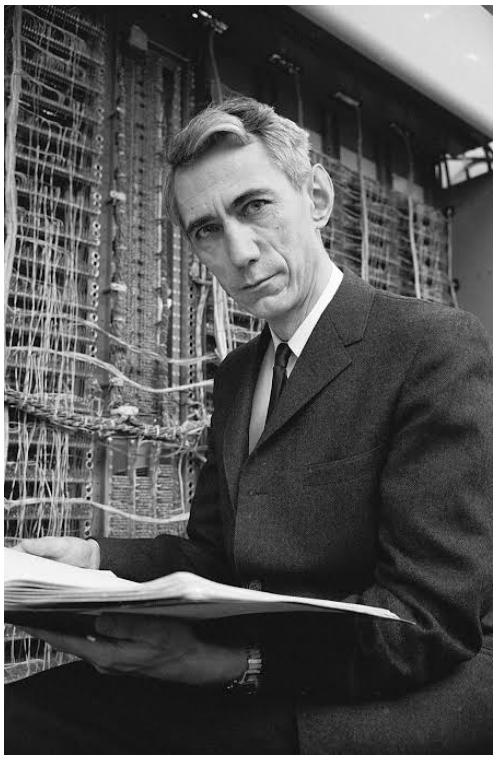
Autour de la théorie de l'information

ou de la communication

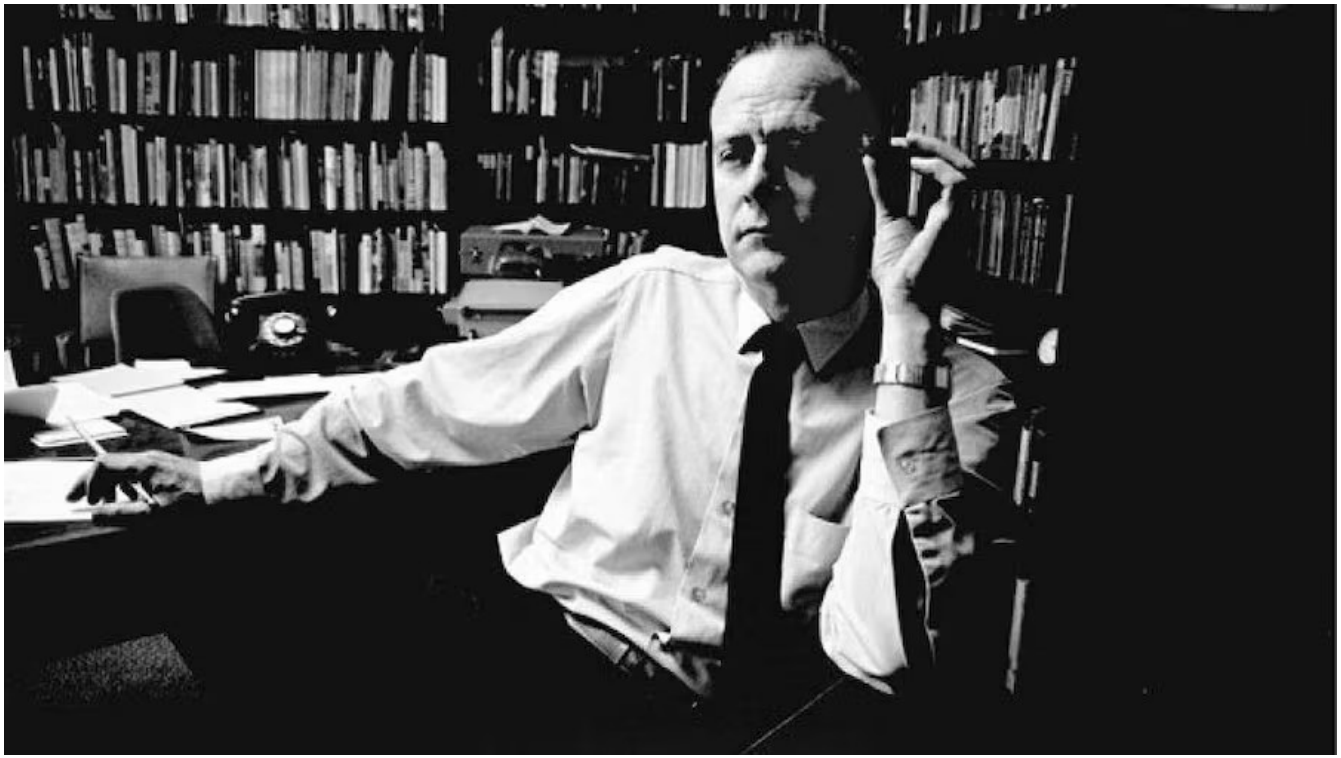
Djalil Chafaï

Après-midi mathématique pour lycéens
École normale supérieure – PSL
Mercredi 24 avril 2024

https://rdv-des-lyceen-ne-s.dma.ens.fr/

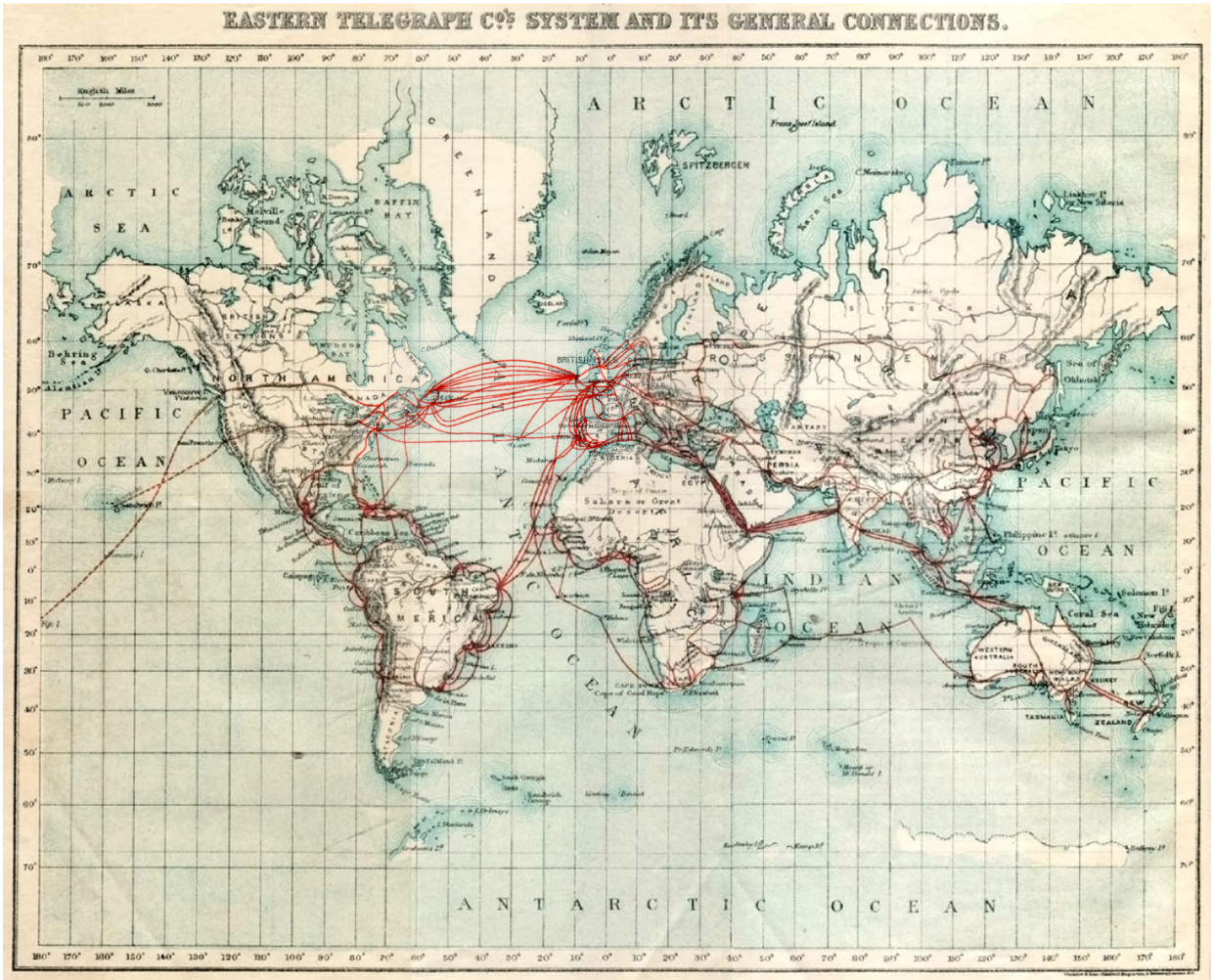


Claude Elwood Shannon (1916 – 2001)
Ingénieur en génie électrique et mathématicien américain.
Fondateur principal de la théorie de l'information.



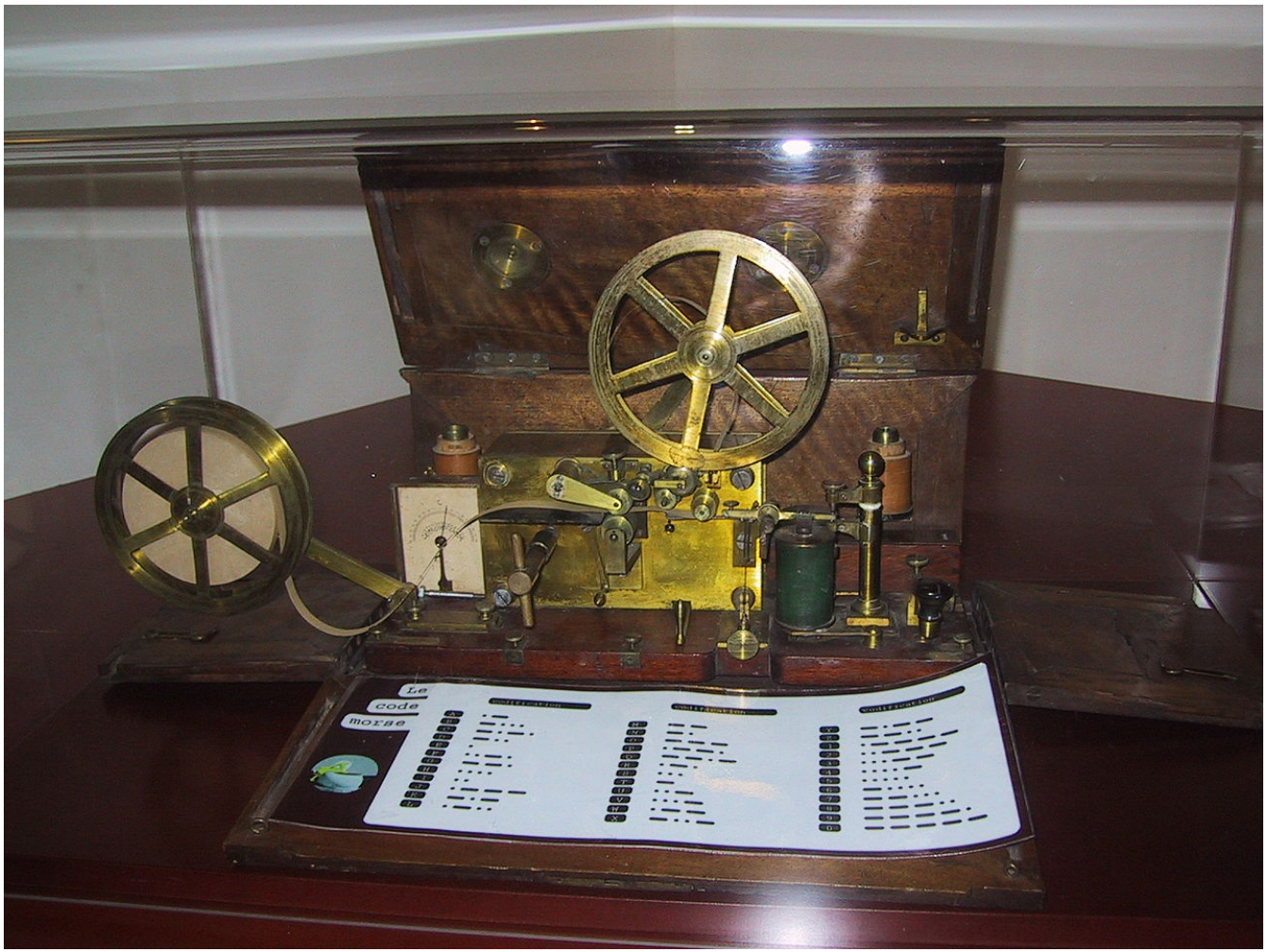
Marshal McLuhan (1911 – 1980)
Professeur de littérature anglaise et théoricien de la communication canadien, l'un des fondateurs de l'étude contemporaine des médias.
Global Village dans *The Medium is the Massage* (1967)

Télégraphe et code Morse



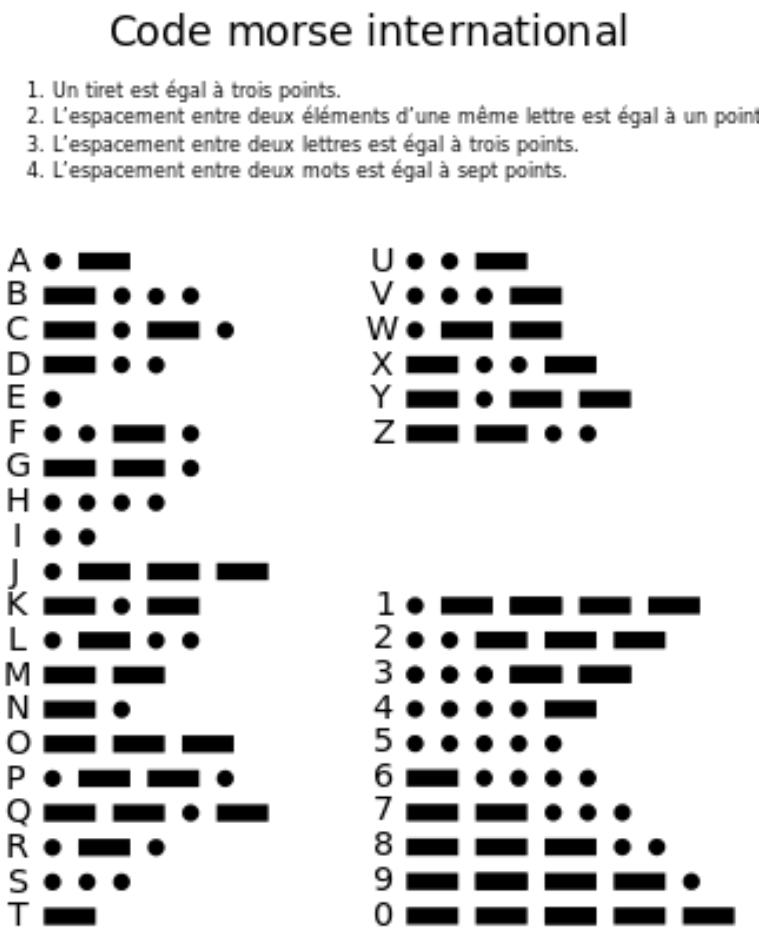
Réseau international de télégraphe en 1901.

Télégraphe et code Morse



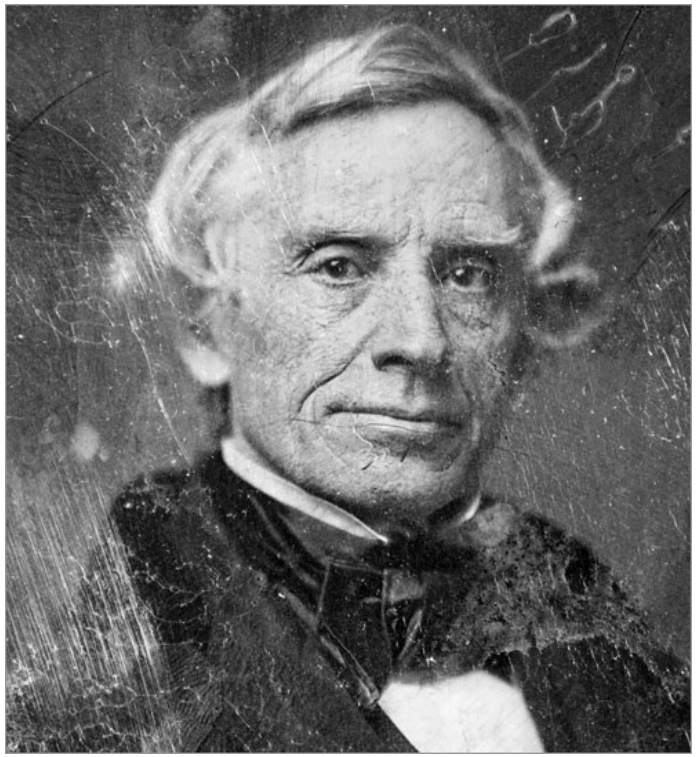
Télégraphe de Morse.

Télégraphe et code Morse



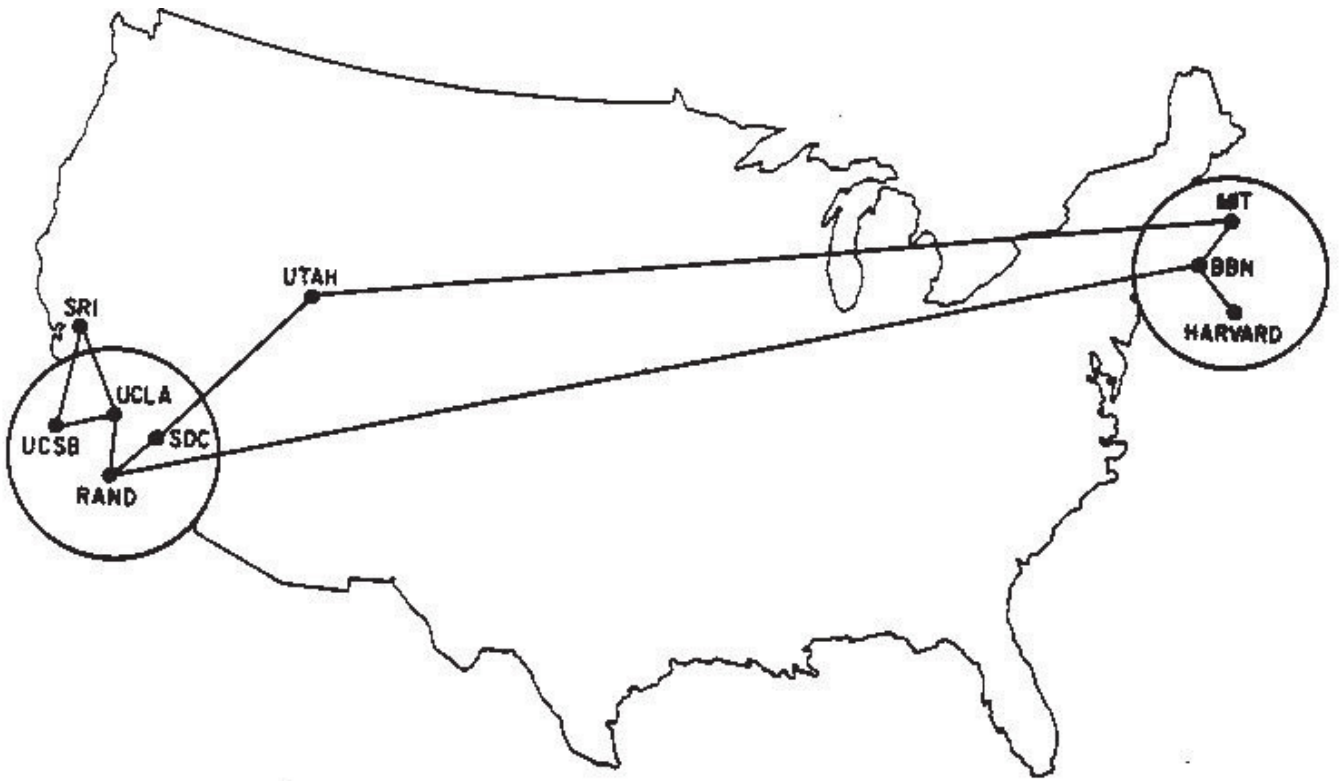
Un codage à longueur variable, avec espacement.

Télégraphe et code Morse



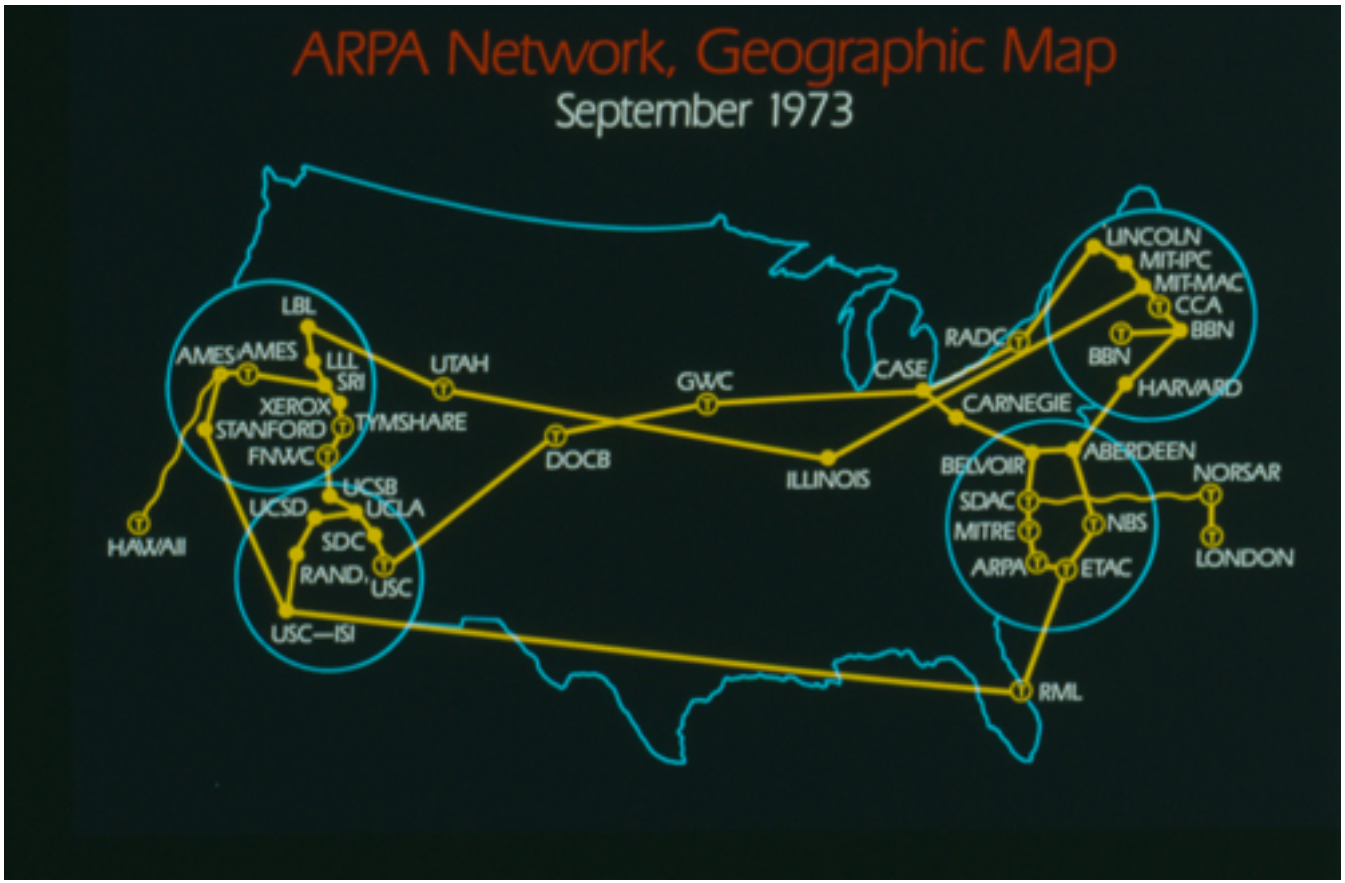
Samuel Morse (1791 – 1872)
Scientifique américain, développeur d'un télégraphe électrique et d'un alphabet qui portent tous deux son nom.

Réseau Internet



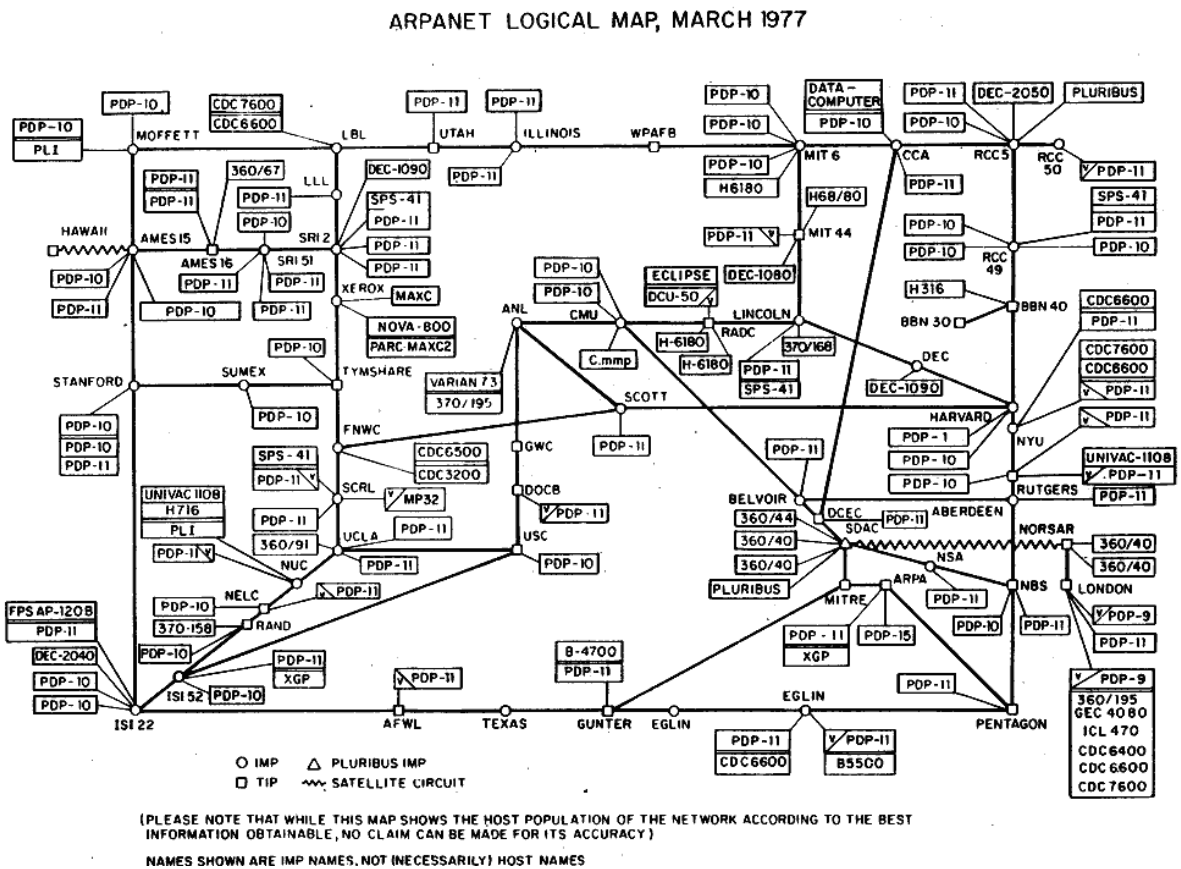
Arpanet en 1970.

Réseau Internet



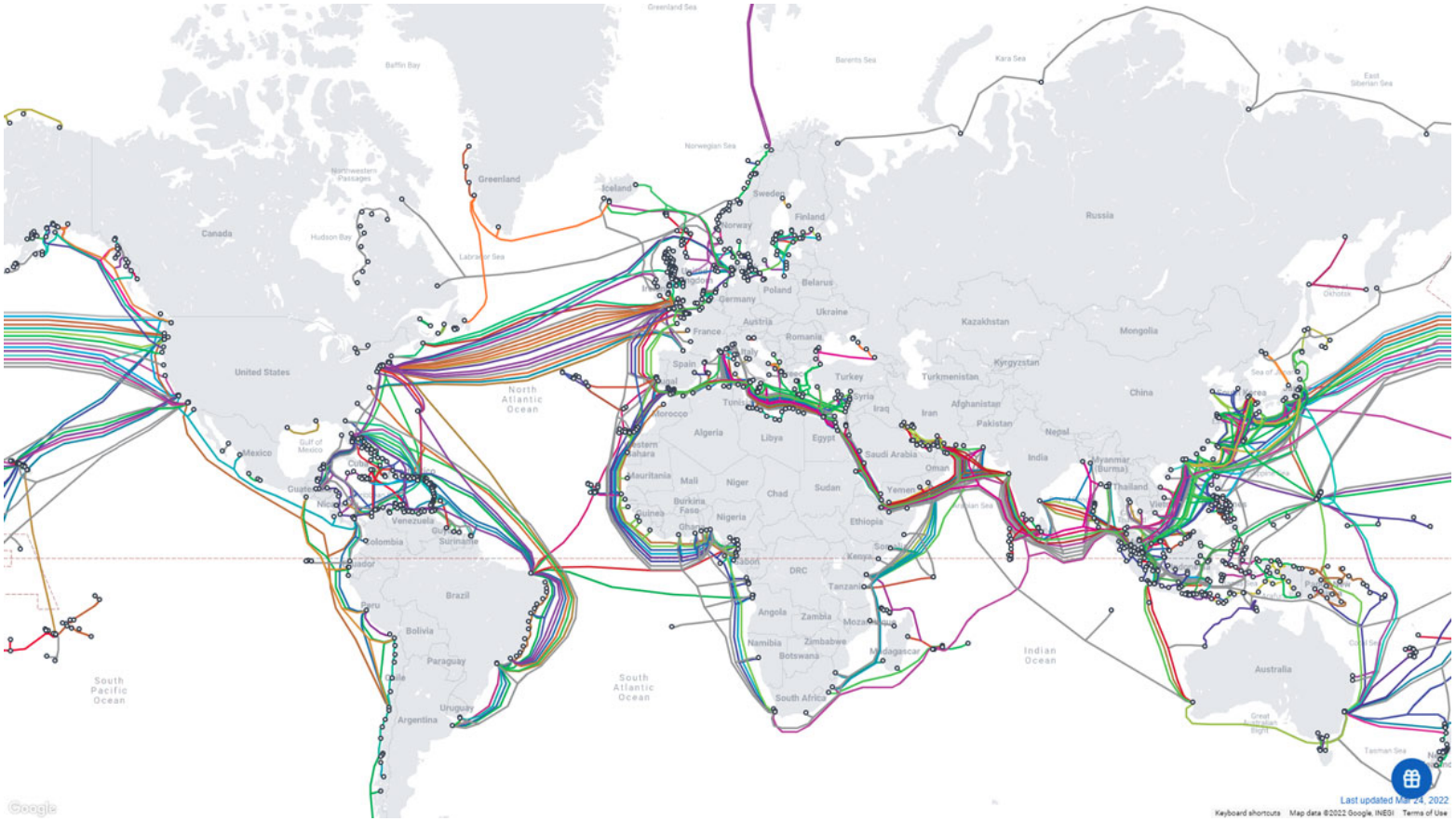
Arpanet en 1973.

Réseau Internet



Arpanet en 1977.

Réseau Internet



Câbles sous-marins en 2022.

Mais comment et sous quelle forme circule l'information ?

Circulation de l'information

- Codage

Circulation de l'information

- Codage
  - Codage binaire ASCII (1960'), ISO (1980'), UTF (1990')

Circulation de l'information

- Codage
  - Codage binaire ASCII (1960'), ISO (1980'), UTF (1990')
  - Compression de données avec ou sans perte

Circulation de l'information

- Codage
  - Codage binaire ASCII (1960'), ISO (1980'), UTF (1990')
  - Compression de données avec ou sans perte
  - Codage correcteur, codage cryptographique

Circulation de l'information

- Codage
  - Codage binaire ASCII (1960'), ISO (1980'), UTF (1990')
  - Compression de données avec ou sans perte
  - Codage correcteur, codage cryptographique
  - Texte, son, image, modulation et échantillonnage, formats

Circulation de l'information

- Codage
  - Codage binaire ASCII (1960'), ISO (1980'), UTF (1990')
  - Compression de données avec ou sans perte
  - Codage correcteur, codage cryptographique
  - Texte, son, image, modulation et échantillonnage, formats
- Transmission

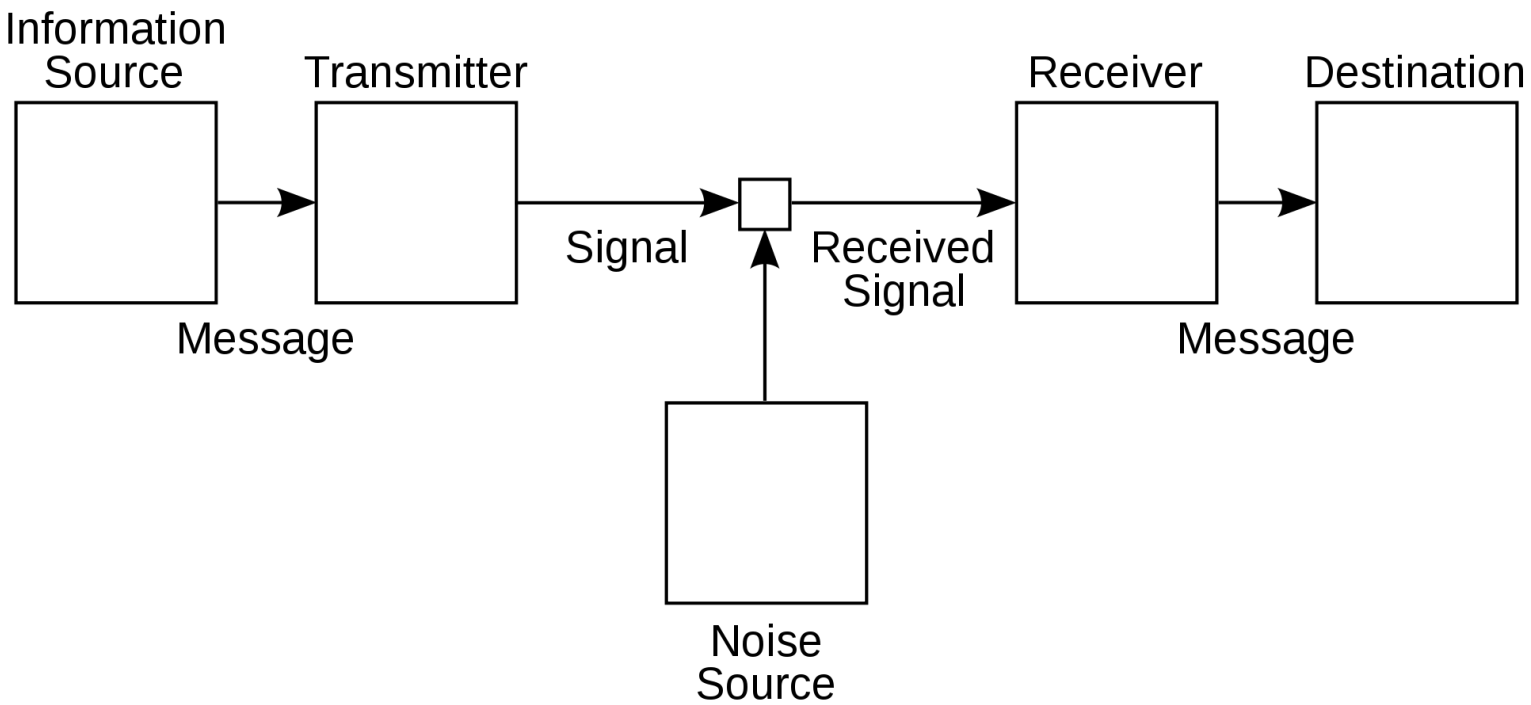
Circulation de l'information

- Codage
  - Codage binaire ASCII (1960'), ISO (1980'), UTF (1990')
  - Compression de données avec ou sans perte
  - Codage correcteur, codage cryptographique
  - Texte, son, image, modulation et échantillonnage, formats
- Transmission
  - Piles de protocoles

Circulation de l'information

- Codage
  - Codage binaire ASCII (1960'), ISO (1980'), UTF (1990')
  - Compression de données avec ou sans perte
  - Codage correcteur, codage cryptographique
  - Texte, son, image, modulation et échantillonnage, formats
- Transmission
  - Piles de protocoles
  - TCP/IP, routage

Schéma de communication



Claude Shannon, *A Mathematical Theory of Communication* (1948)

Codage ASCII

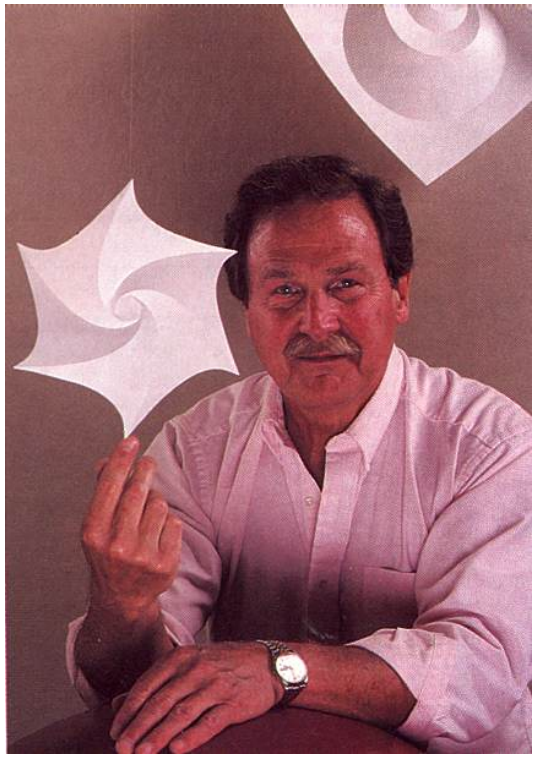
Numéro (0–255)	Code binaire 8 bits	Signification
⋮	⋮	⋮
13	00001101	Saut de page (CR)
⋮	⋮	⋮
64	01000000	@
65	01000001	A
66	01000010	B
67	01000011	C
⋮	⋮	⋮

Longueur fixe de 8 bits (ASCII ISO-8859)

$2^8 = 256$ symboles différents

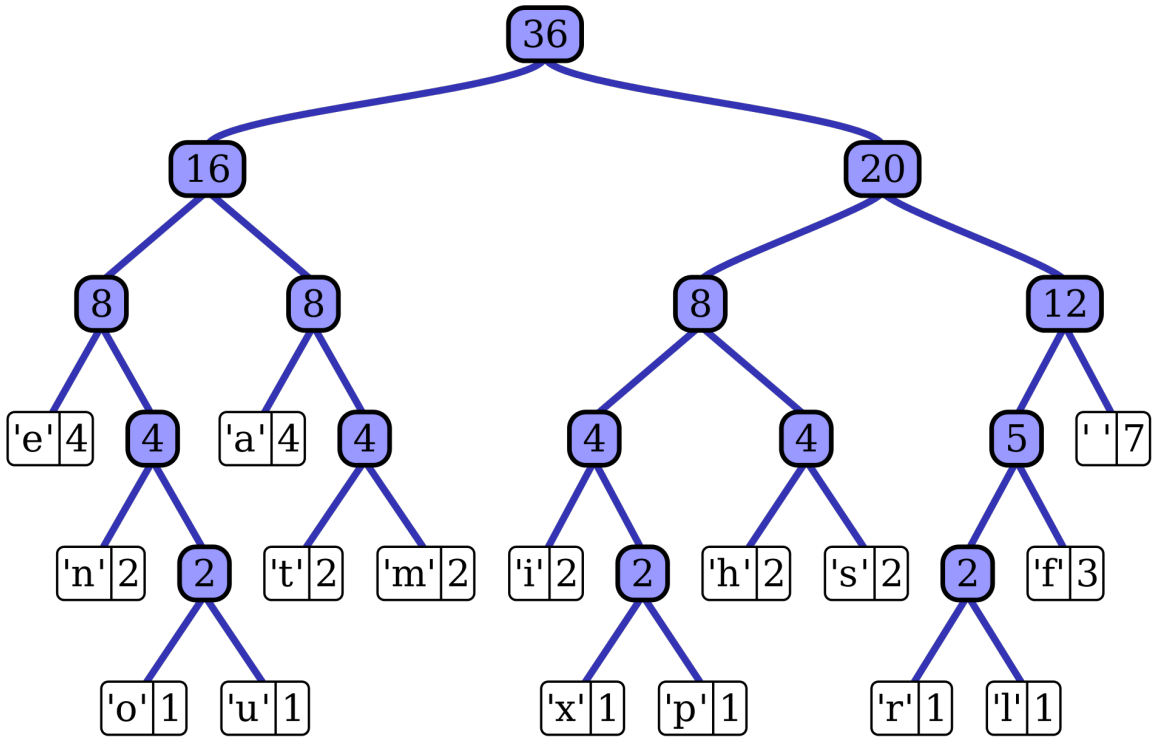
ABC devient 010000010100001001000011

Peut-on faire mieux ?



David Albert Huffman (1925 – 1999)
Informaticien américain, contributeur majeur
à la théorie du codage et de la compression de données.

Codage de Huffman



Arbre de Huffman du message

`this is an example of a huffman tree`

$n = 36$ symboles, $r = 16$ symboles distincts

Codage de Huffman

this is an example of a huffman tree

Symbole	Occurence	Fréquence	Code binaire
	7	0.194	111
a	4	0.111	010
e	4	0.111	000
f	3	0.083	1101
t	2	0.056	0110
h	2	0.056	1010
i	2	0.056	1000
s	2	0.056	1011
n	2	0.056	0010
m	2	0.056	0111
x	1	0.028	10010
p	1	0.028	10011
l	1	0.028	11001
o	1	0.028	00110
u	1	0.028	00111
r	1	0.028	11000

Propriété de prefixe $\Rightarrow$ décodage assuré malgré codes de longueurs variable

Inégalité de caractérisation de Kraft : $\sum_{i=1}^{r} s^{-\ell_i} \leq 1$ ici $r = 16$ et $s = 2$

Codage de Huffman

- Message de $n = 36$ symboles, $r = 16$ symboles distincts

Codage de Huffman

- Message de $n = 36$ symboles, $r = 16$ symboles distincts
- Codage de Huffman : 135 bits

Codage de Huffman

- Message de $n = 36$ symboles, $r = 16$ symboles distincts
- Codage de Huffman : 135 bits
- Codage fixe ASCII (8 bits par symbole) : 288 bits
  $(n \times 8 = 36 \times 8 = 288)$

Codage de Huffman

- Message de $n = 36$ symboles, $r = 16$ symboles distincts
- Codage de Huffman : 135 bits
- Codage fixe ASCII (8 bits par symbole) : 288 bits
  $(n \times 8 = 36 \times 8 = 288)$
- Codage fixe minimal (4 bits par symbole) : 144 bits
  $(n \times 4 = 36 \times 4 = 144$ car $\log_2(r) = 4$, $r = 16 = 2^4)$

Codage de Huffman

- Message de $n = 36$ symboles, $r = 16$ symboles distincts
- Codage de Huffman : 135 bits
- Codage fixe ASCII (8 bits par symbole) : 288 bits
  $(n \times 8 = 36 \times 8 = 288)$
- Codage fixe minimal (4 bits par symbole) : 144 bits
  $(n \times 4 = 36 \times 4 = 144$ car $\log_2(r) = 4$, $r = 16 = 2^4)$
- $\log_b(x) =$ nombre de chiffres en base b pour écrire x

Codage de Huffman

- Message de $n = 36$ symboles, $r = 16$ symboles distincts
- Codage de Huffman : 135 bits
- Codage fixe ASCII (8 bits par symbole) : 288 bits
  $(n \times 8 = 36 \times 8 = 288)$
- Codage fixe minimal (4 bits par symbole) : 144 bits
  $(n \times 4 = 36 \times 4 = 144$ car $\log_2(r) = 4$, $r = 16 = 2^4)$
- $\log_b(x) =$ nombre de chiffres en base b pour écrire x
- Concepts de codage : de longueur fixe ou variable, adaptatif ou préadaptatif, optimal, à la volée

Entropie de Shannon et théorème du codage

- Message aléatoire de n lettres indépendantes dans un alphabet de taille r et de loi de probabilité $p_1, \ldots, p_r$

Entropie de Shannon et théorème du codage

- Message aléatoire de n lettres indépendantes dans un alphabet de taille r et de loi de probabilité $p_1, \ldots, p_r$
- Les probabilités $p_1, \ldots, p_r$ sont les fréquences théoriques

Entropie de Shannon et théorème du codage

- Message aléatoire de n lettres indépendantes dans un alphabet de taille r et de loi de probabilité $p_1, \ldots, p_r$
- Les probabilités $p_1, \ldots, p_r$ sont les fréquences théoriques
- Théorème de codage source de Claude Shannon (1948)

$$\lim_{n \to \infty} \frac{\text{LongueurMinimaleCodage}}{n} = \mathrm{S}(p).$$

Il faut environ $n\mathrm{S}(p)$ bits par symbole

Entropie de Shannon et théorème du codage

- Message aléatoire de n lettres indépendantes dans un alphabet de taille r et de loi de probabilité $p_1, \ldots, p_r$
- Les probabilités $p_1, \ldots, p_r$ sont les fréquences théoriques
- Théorème de codage source de Claude Shannon (1948)

$$\lim_{n \to \infty} \frac{\text{LongueurMinimaleCodage}}{n} = \mathrm{S}(p).$$

  Il faut environ $n\mathrm{S}(p)$ bits par symbole
- Entropie d'une loi de probabilité $p_1, \ldots, p_r$

$$\mathrm{S}(p) = \sum_{i=1}^{r} p_i \log\left(\frac{1}{p_i}\right)$$

  Maximale pour la loi uniforme $(\frac{1}{r}, \ldots, \frac{1}{r})$
  Minimale pour les lois concentrées sur une seule valeur

Mesure du désordre, des possibles, de l'incertitude

- Coder revient à numéroter, à compter les possibles

Mesure du désordre, des possibles, de l'incertitude

- Coder revient à numéroter, à compter les possibles
- Nombre de messages de longueur n écrits dans un alphabet à r lettres comprenant n_i fois la lettre n°i pour tout i

$$\frac{n!}{n_1! \cdots n_r!}$$

Mesure du désordre, des possibles, de l'incertitude

- Coder revient à numéroter, à compter les possibles
- Nombre de messages de longueur n écrits dans un alphabet à r lettres comprenant n_i fois la lettre n°i pour tout i

$$\frac{n!}{n_1! \cdots n_r!}$$

- Avec formule de Stirling $n! \approx \sqrt{2\pi n}(n/\mathrm{e})^n$

$$\frac{n!}{n_1! \cdots n_r!} \approx \mathrm{e}^{n\mathrm{S}(\frac{n_1}{n},\ldots,\frac{n_r}{n})}.$$

Mesure du désordre, des possibles, de l'incertitude

- Coder revient à numéroter, à compter les possibles
- Nombre de messages de longueur n écrits dans un alphabet à r lettres comprenant n_i fois la lettre n°i pour tout i

$$\frac{n!}{n_1! \cdots n_r!}$$

- Avec formule de Stirling $n! \approx \sqrt{2\pi n}(n/\mathrm{e})^n$

$$\frac{n!}{n_1! \cdots n_r!} \approx \mathrm{e}^{n\mathrm{S}(\frac{n_1}{n},\ldots,\frac{n_r}{n})}.$$

- Preuve du théorème de codage source de Shannon

Mesure du désordre, des possibles, de l'incertitude

- Coder revient à numéroter, à compter les possibles
- Nombre de messages de longueur n écrits dans un alphabet à r lettres comprenant n_i fois la lettre n°i pour tout i

$$\frac{n!}{n_1! \cdots n_r!}$$

- Avec formule de Stirling $n! \approx \sqrt{2\pi n}(n/\mathrm{e})^n$

$$\frac{n!}{n_1! \cdots n_r!} \approx \mathrm{e}^{n\mathrm{S}(\frac{n_1}{n},\ldots,\frac{n_r}{n})}.$$

- Preuve du théorème de codage source de Shannon
- Atteint par codage de Huffman, codage arithmétique

Caractérisation axiomatique de l'entropie

- pour tout n, la fonction $p \mapsto \mathrm{S}_n(p)$ est continue

Caractérisation axiomatique de l'entropie

- pour tout n, la fonction $p \mapsto \mathrm{S}_n(p)$ est continue
- pour tout n, $\mathrm{S}_n(\frac{1}{n}, \ldots, \frac{1}{n}) < \mathrm{S}_{n+1}(\frac{1}{n+1}, \ldots, \frac{1}{n+1})$

Caractérisation axiomatique de l'entropie

- pour tout n, la fonction $p \mapsto \mathrm{S}_n(p)$ est continue
- pour tout n, $\mathrm{S}_n(\frac{1}{n}, \ldots, \frac{1}{n}) < \mathrm{S}_{n+1}(\frac{1}{n+1}, \ldots, \frac{1}{n+1})$
- pour tout $n = n_1 + \cdots + n_r$,

$$\mathrm{S}_n(\tfrac{1}{n}, \ldots, \tfrac{1}{n}) = \mathrm{S}_r(\tfrac{n_1}{n}, \ldots, \tfrac{n_r}{n}) + \sum_{i=1}^{r} \frac{n_i}{n} \mathrm{S}_{n_i}(\tfrac{1}{n_i}, \ldots, \tfrac{1}{n_i})$$

Compression sans perte

- Codage entropique de Huffman, ou arithmétique

Compression sans perte

- Codage entropique de Huffman, ou arithmétique
  - Développé par David Huffman (1952)

Compression sans perte

- Codage entropique de Huffman, ou arithmétique
  - Développé par David Huffman (1952)
  - Amélioré par Jorma Rissanen et Richard Pasco (1976)

Compression sans perte

- Codage entropique de Huffman, ou arithmétique
  - Développé par David Huffman (1952)
  - Amélioré par Jorma Rissanen et Richard Pasco (1976)
  - Utilisé partout et tout le temps !

Compression sans perte

- Codage entropique de Huffman, ou arithmétique
  - Développé par David Huffman (1952)
  - Amélioré par Jorma Rissanen et Richard Pasco (1976)
  - Utilisé partout et tout le temps !
- Préadaptation, adaptation, fenêtre glissante ou bloc

Compression sans perte

- Codage entropique de Huffman, ou arithmétique
  - Développé par David Huffman (1952)
  - Amélioré par Jorma Rissanen et Richard Pasco (1976)
  - Utilisé partout et tout le temps !
- Préadaptation, adaptation, fenêtre glissante ou bloc
- Codage par dictionnaire LZ, ou LZW

Compression sans perte

- Codage entropique de Huffman, ou arithmétique
  - Développé par David Huffman (1952)
  - Amélioré par Jorma Rissanen et Richard Pasco (1976)
  - Utilisé partout et tout le temps !
- Préadaptation, adaptation, fenêtre glissante ou bloc
- Codage par dictionnaire LZ, ou LZW
  - Développé par Abraham Lempel et Jacob Ziv (1977, 1978)

Compression sans perte

- Codage entropique de Huffman, ou arithmétique
  - Développé par David Huffman (1952)
  - Amélioré par Jorma Rissanen et Richard Pasco (1976)
  - Utilisé partout et tout le temps !
- Préadaptation, adaptation, fenêtre glissante ou bloc
- Codage par dictionnaire LZ, ou LZW
  - Développé par Abraham Lempel et Jacob Ziv (1977, 1978)
  - Amélioré par Terry Welsh (1984), notamment sur 12 bits

Compression sans perte

- Codage entropique de Huffman, ou arithmétique
  - Développé par David Huffman (1952)
  - Amélioré par Jorma Rissanen et Richard Pasco (1976)
  - Utilisé partout et tout le temps !
- Préadaptation, adaptation, fenêtre glissante ou bloc
- Codage par dictionnaire LZ, ou LZW
  - Développé par Abraham Lempel et Jacob Ziv (1977, 1978)
  - Amélioré par Terry Welsh (1984), notamment sur 12 bits
  - Utilisé par le format d'image GIF et d'archivage ZIP

Compression sans perte

- Exploitation de la redondance dans les données

Compression sans perte

- Exploitation de la redondance dans les données
- Sous-dimensionalité : crucial en sciences des données

Compression sans perte

- Exploitation de la redondance dans les données
- Sous-dimensionalité : crucial en sciences des données
- Complexité des algorithmes : mémoire, codage, décodage

Compression sans perte

- Exploitation de la redondance dans les données
- Sous-dimensionalité : crucial en sciences des données
- Complexité des algorithmes : mémoire, codage, décodage
- Fable de La Fontaine : vainqueur $\neq$ meilleur

Compression avec perte

- Comment compresser son et image, audio et vidéo

Compression avec perte

- Comment compresser son et image, audio et vidéo
- Numérisation : passage de l'analogique au numérique

Compression avec perte

- Comment compresser son et image, audio et vidéo
- Numérisation : passage de l'analogique au numérique
- Perception humaine : psychoacoustique, phychovisuel

Compression avec perte

- Comment compresser son et image, audio et vidéo
- Numérisation : passage de l'analogique au numérique
- Perception humaine : psychoacoustique, phychovisuel
- Échantillonnage et modulation : CD = 44 kHz 2×16 bits

Compression avec perte

- Comment compresser son et image, audio et vidéo
- Numérisation : passage de l'analogique au numérique
- Perception humaine : psychoacoustique, phychovisuel
- Échantillonnage et modulation : CD = 44 kHz 2×16 bits
- Théorème d'échantillonnage de Nyquist–Shannon : $\times 2$!

Compression avec perte

- Perte de détails de moindre importance perceptuelle

Compression avec perte

- Perte de détails de moindre importance perceptuelle
- Codage sans perte (entropie) après élimination des détails

Compression avec perte

- Perte de détails de moindre importance perceptuelle
- Codage sans perte (entropie) après élimination des détails
- Compromis entre qualité et taux de compression

Compression avec perte

- Perte de détails de moindre importance perceptuelle
- Codage sans perte (entropie) après élimination des détails
- Compromis entre qualité et taux de compression
- Image fixe : JPEG, ...

Compression avec perte

- Perte de détails de moindre importance perceptuelle
- Codage sans perte (entropie) après élimination des détails
- Compromis entre qualité et taux de compression
- Image fixe : JPEG, ...
- Son et vidéo : MP3, MP4, ...

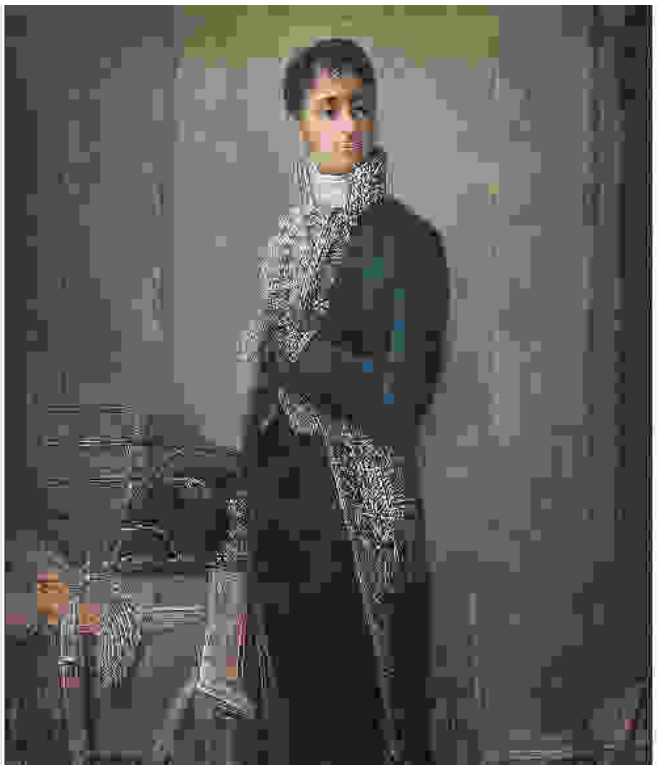
Exemple du JPEG (1991)

87 kB

Exemple du JPEG (1991)

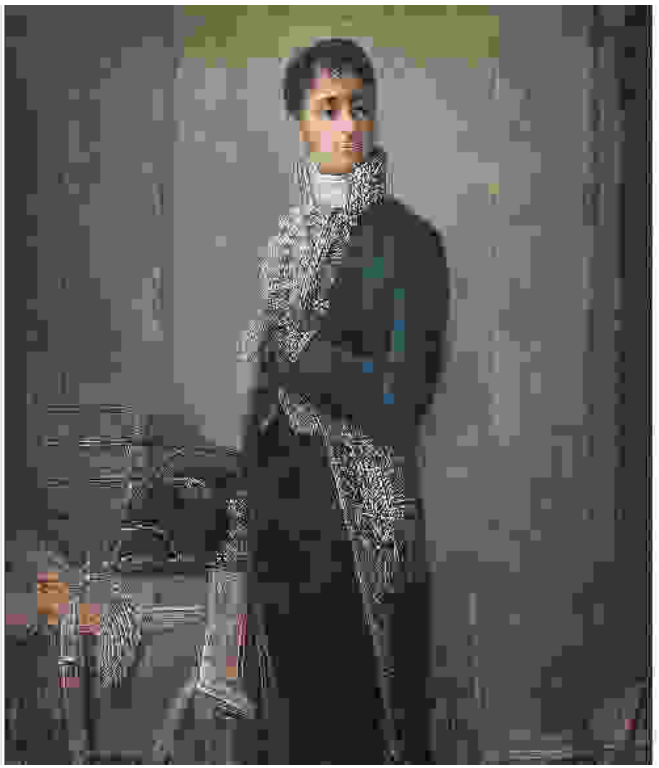
15 kB

Exemple du JPEG (1991)



11 kB

Exemple du JPEG (1991)



11 kB

DFT par bloc 8×8, seuillage HF, puis codage entropique !

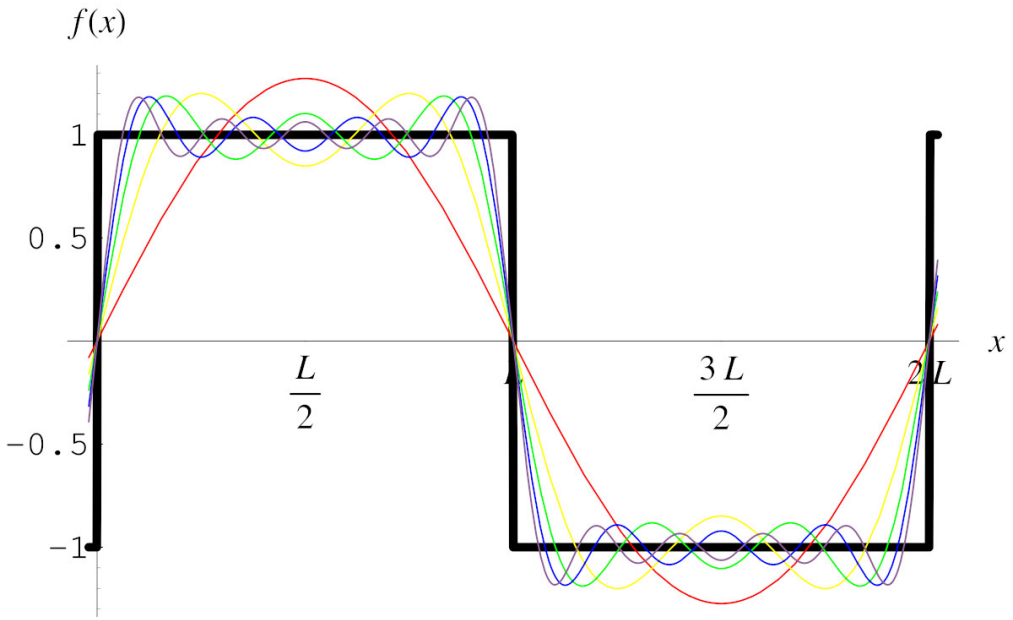
Exemple du JPEG (1991)

87 kB

DFT par bloc 8×8, seuillage HF, puis codage entropique !

Joseph Fourier (1768 – 1830) inventeur de l'analyse harmonique

Traitement du signal et analyse harmonique



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

Traitement du signal et analyse harmonique

- Signal à temps discret $f(0), f(1), \ldots, f(N-1)$

Traitement du signal et analyse harmonique

- Signal à temps discret $f(0), f(1), \ldots, f(N-1)$
- Transformée de Fourier discrète (DFT) :

$$\widehat{f}(k) = \sum_{n=0}^{N-1} f(n) \mathrm{e}^{2\pi \mathrm{i} k \frac{n}{N}} \quad 0 \leq k < N$$

Traitement du signal et analyse harmonique

- Signal à temps discret $f(0), f(1), \ldots, f(N-1)$
- Transformée de Fourier discrète (DFT) :

$$\widehat{f}(k) = \sum_{n=0}^{N-1} f(n) \mathrm{e}^{2\pi \mathrm{i} k \frac{n}{N}} \quad 0 \leq k < N$$

- Reconstruction par superposition

$$f(n) = \frac{1}{N} \sum_{k=0}^{N-1} \widehat{f}(k) \mathrm{e}^{2\pi \mathrm{i} k \frac{n}{N}}$$

Traitement du signal et analyse harmonique

- Signal à temps discret $f(0), f(1), \ldots, f(N-1)$
- Transformée de Fourier discrète (DFT) :

$$\widehat{f}(k) = \sum_{n=0}^{N-1} f(n) \mathrm{e}^{2\pi \mathrm{i} k \frac{n}{N}} \quad 0 \leq k < N$$

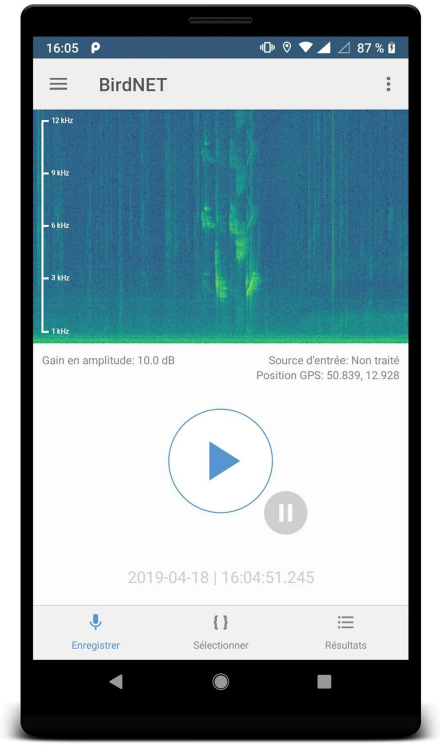
- Reconstruction par superposition

$$f(n) = \frac{1}{N} \sum_{k=0}^{N-1} \widehat{f}(k) \mathrm{e}^{2\pi \mathrm{i} k \frac{n}{N}}$$

- Géométrie de l'algèbre linéaire en analyse : base de Fourier

$$\widehat{f}(k) = \langle f, \mathrm{e}^{2\pi \mathrm{i} k \frac{\cdot}{N}} \rangle$$

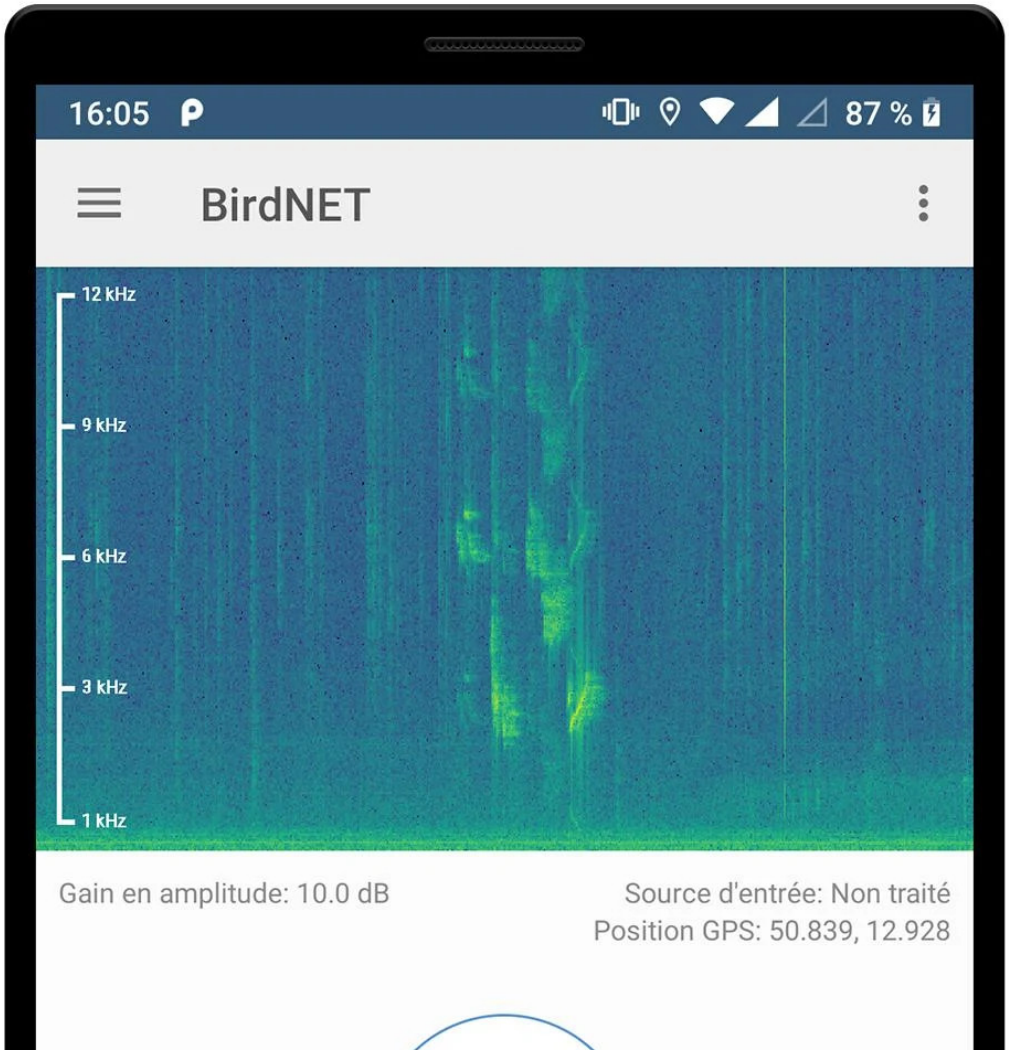
Traitement du signal et analyse harmonique



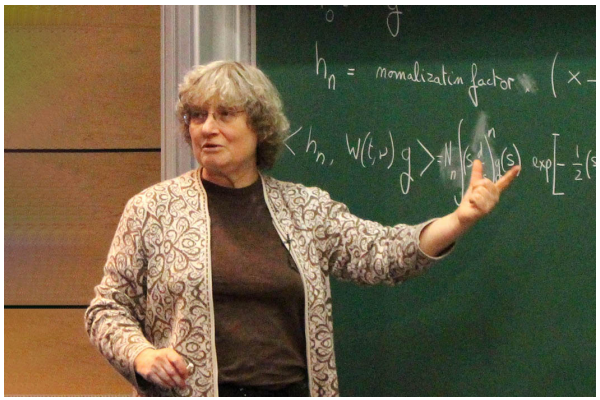
Enregistrez en continu les sons de votre environnement.

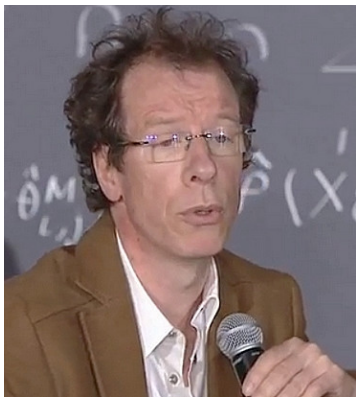
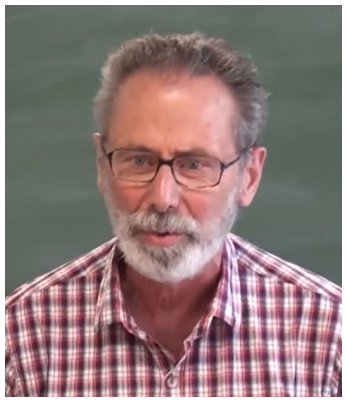
Reconnaissance vocale ($\neq$ compression) : Shazam, BirdNet, Siri, Alexa, GoogleHome, ...

Traitement du signal et analyse harmonique



Traitement du signal et analyse harmonique

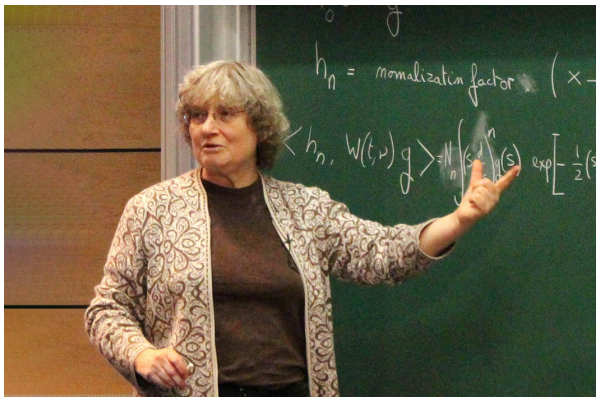


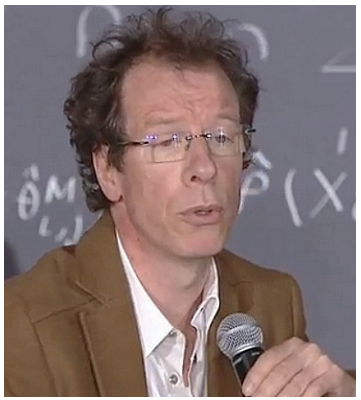
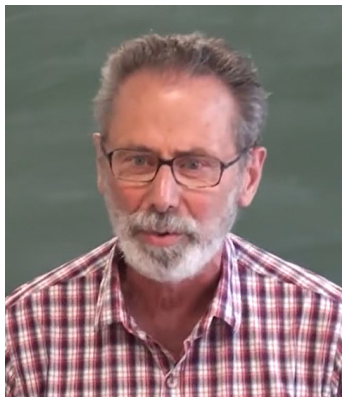



Ingrid Daubechies, Stéphane Mallat, Yves Meyer

- Transformée de Fourier rapide (FFT)

Traitement du signal et analyse harmonique

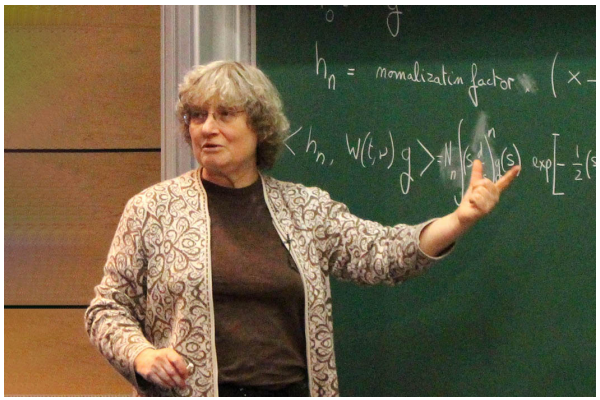


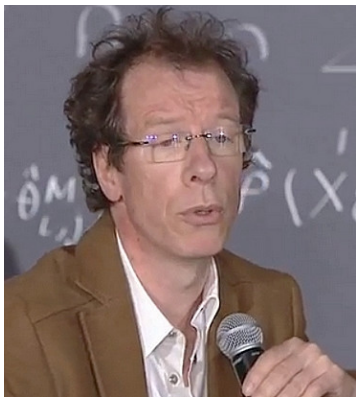
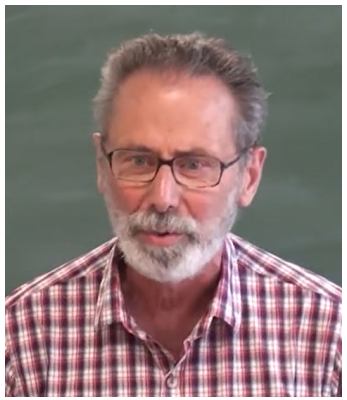



Ingrid Daubechies, Stéphane Mallat, Yves Meyer

- Transformée de Fourier rapide (FFT)
- Algorithmes pyramidaux

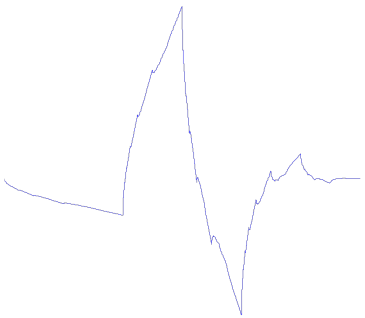
Traitement du signal et analyse harmonique



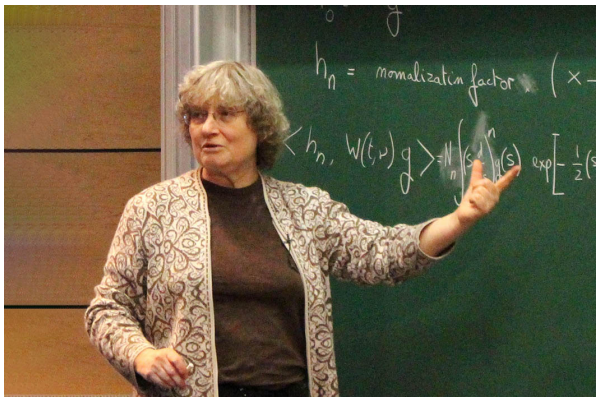



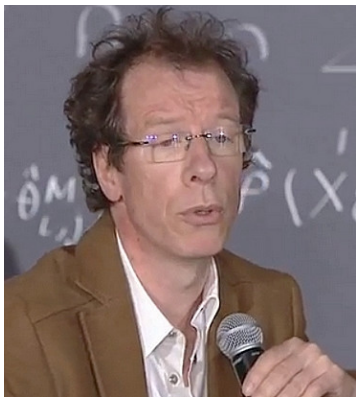
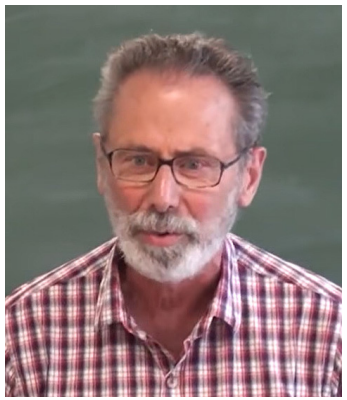
Ingrid Daubechies, Stéphane Mallat, Yves Meyer

- Transformée de Fourier rapide (FFT)
- Algorithmes pyramidaux
- Transformée en ondelettes



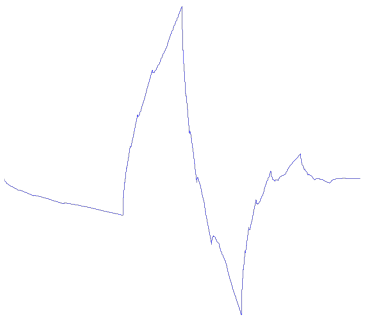
Traitement du signal et analyse harmonique



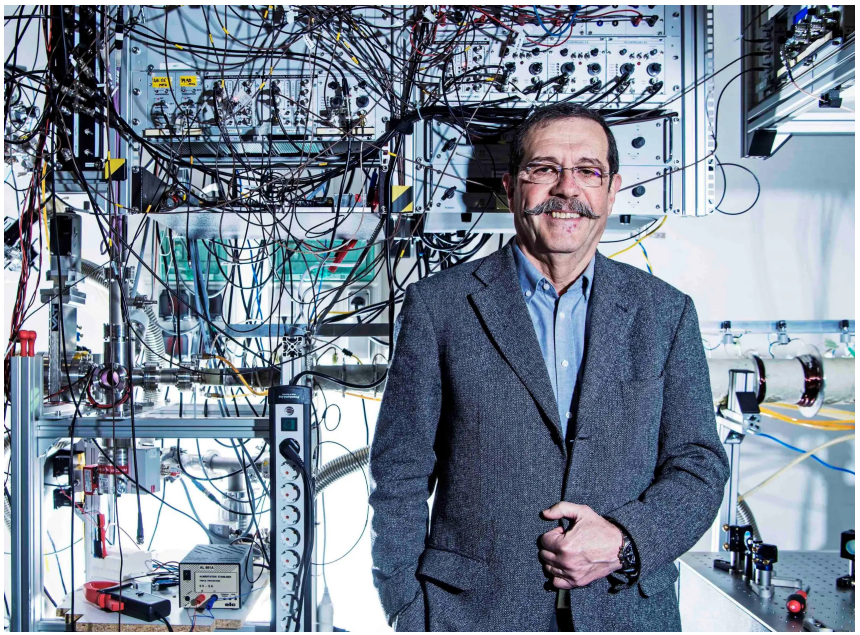



Ingrid Daubechies, Stéphane Mallat, Yves Meyer

- Transformée de Fourier rapide (FFT)
- Algorithmes pyramidaux
- Transformée en ondelettes
- Transformée en ondelettes rapide (FWT)



Futur



Alain Aspect

- Triangle informatique-mathématiques-physique

Futur

Ordinateur quantique

- Triangle informatique-mathématiques-physique