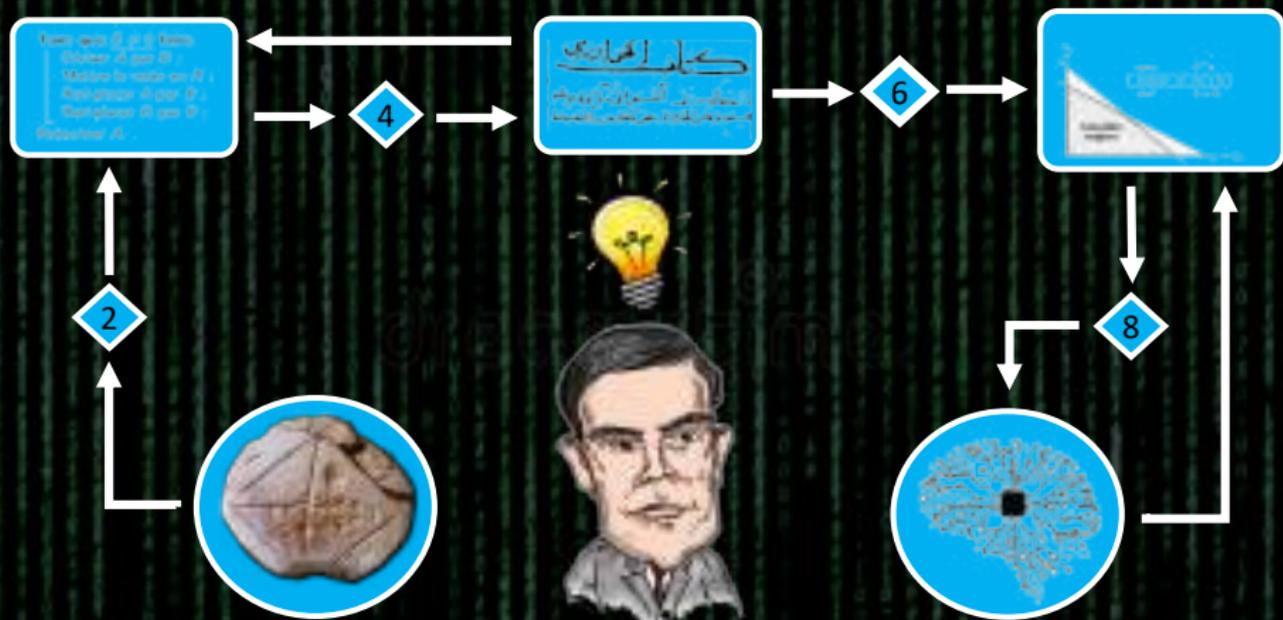


Les Algorithmes

Des origines à
l'Intelligence Artificielle



Qu'est-ce qu'un algorithme ?

Les algorithmes peuvent-ils tout faire ?

Doit avoir peur des algorithmes ?

Quels enjeux autour des algorithmes ?



Qu'est-ce qu'un algorithme ?

Entrées

Algorithme

=

Suite d'instructions

Sorties

Qu'est-ce qu'un algorithme ?

Entrées

Algorithme

=

Suite d'instructions

Sorties

Ingrédients :

Farine, œufs, sucre, huile, lait.

1. Mettre la farine dans une terrine.
2. Y déposer les œufs, le sucre, et l'huile.
3. Mélanger en ajoutant au fur et à mesure le lait.

Résultat : Pâte à crêpe.

Qu'est-ce qu'un algorithme ?

Entrées

Algorithme

=

Suite d'instructions

Sorties

Ingrédients :

Farine, œufs, sucre, huile, lait.

1. Mettre la farine dans une terrine.
2. Y déposer les œufs, le sucre, et l'huile.
3. Mélanger en ajoutant au fur et à mesure le lait.

Résultat : Pâte à crêpe.

Un **algorithme** résoud un problème de **manière constructive** en le décomposant en **opérations simples**.

Qu'est-ce qu'un algorithme ?

Entrées

Algorithme

=

Suite d'instructions

Sorties

Ingrédients :

Farine, œufs, sucre, huile, lait.

1. Put the flour in a bowl.
2. Add the eggs, sugar, and oil.
3. Mix delicately, gradually adding the milk.

Résultat : Pâte à crêpe.

Un **algorithme** résoud un problème de **manière constructive** en le décomposant en **opérations simples**.

Apparition des algorithmes

Quand sont apparus les algorithmes ?

Quand sont apparus les algorithmes ?

-3000 : Description de déroulés d'algorithme.

-300 : **Algorithme d'Euclide.**

Grands problèmes mathématiques de l'antiquité sont des questions d'algorithmes (géométriques).

Duplication du cube, trisection de l'angle, quadrature du cercle.

Moyen âge : **Apparition du mot algorithme**

Systeme de numération indo-arabe.

Années 1940 : **Apparition des ordinateurs**

Années 2000 : Puissance de calcul + données en quantité.

Apprentissage automatique

Quand sont apparus les algorithmes ?

-3000 : Description de déroulés d'algorithme.

-300 : **Algorithme d'Euclide.**

Grands problèmes mathématiques de l'antiquité sont des questions d'algorithmes (géométriques).

Duplication du cube, trisection de l'angle, quadrature du cercle.

Moyen âge : **Apparition du mot algorithme**

Système de numération indo-arabe.

1ère révolution algorithmique.

Années 1940 : **Apparition des ordinateurs**

2ème révolution algorithmique.

Années 2000 : Puissance de calcul + données en quantité.

Apprentissage automatique **3ème révolution algorithmique.**

Les algorithmes babyloniens

Tablettes mathématiques babyloniennes avec listes de problèmes mathématiques avec (ou sans) solutions.

BM 13901 (British Museum)
XVIII^e siècle av. J.-C.

24 problèmes et solutions.

Écriture cunéiforme.

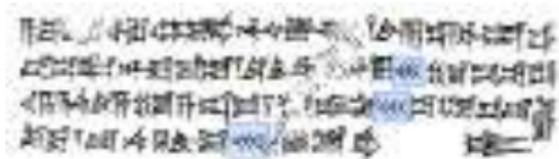
Système sexagésimal

Modèles de résolution des
équations du 2nd degré



Les algorithmes babyloniens

Problème 1 de BM 13901



J'ai additionné la surface et le côté de mon carré : 45'.

Tu poseras 1, l'unité. Tu fractionneras en deux 1 : 30'.

Tu croiseras 30' et 30' : 15'.

Tu ajouteras 15' à 45' : 1. C'est le carré de 1.

Tu soustrairas 30', que tu as croisé, de 1 : 30', le côté du carré.

F. Thureau-Dangin,
Revue d'assyriologie (1936)

$$\text{Equation : } x^2 + x = \frac{3}{4}.$$

$$x^2 + ax = B$$

$$\frac{1}{2}$$

Calculer $\frac{a}{2}$;

$$\frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$$

Calculer $\frac{a^2}{4}$;

$$x^2 + x + \frac{1}{4} = 1 = \left(x + \frac{1}{2}\right)^2$$

Calculer $S = B + \frac{a^2}{4}$;

$$x + \frac{1}{2} = \sqrt{1} = 1 \quad \text{Calculer } \sqrt{S};$$

$$x = 1 - \frac{1}{2} = \frac{1}{2}. \quad x = \sqrt{S} - \frac{a}{2};$$

$$x(x + a) + \frac{a^2}{4} = \left(x + \frac{a}{2}\right)^2$$

Algorithme d'Euclide. (\sim 300 av. J. C.)

PGCD(A, B) : plus grand entier C qui divise A et qui divise B .

Etant donné deux entiers A et B avec $A \geq B$, comment trouver PGCD(A, B) ?

Exemple : $A = 390$ et $B = 135$

Tant que $B \neq 0$ faire

Diviser A par B ;

Mettre le reste en R

;

Remplacer A par B ;

Remplacer B par R ;

Retourner A .

$$390 = 135 \times 2 + 120$$

$$A = 135 \text{ et } B = 120$$

$$135 = 120 \times 1 + 15$$

$$A = 120 \text{ et } B = 15$$

$$120 = 15 \times 8 + 0$$

$$A = 15 \text{ et } B = 0$$

PGCD(390, 135) = 15.

Algorithme d'Euclide. (\sim 300 av. J. C.)

PGCD(A, B) : plus grand entier C qui divise A et qui divise B .

Etant donné deux entiers A et B avec $A \geq B$, comment trouver PGCD(A, B) ?

Premier algorithme certifié :

Tant que $B \neq 0$ faire

Diviser A par B ;

Mettre le reste en R

;

Remplacer A par B ;

Remplacer B par R ;

Retourner A .

Algorithme d'Euclide. (\sim 300 av. J. C.)

PGCD(A, B) : plus grand entier C qui divise A et qui divise B .

Etant donné deux entiers A et B avec $A \geq B$, comment trouver PGCD(A, B) ?

Tant que $B \neq 0$ faire

Diviser A par B ;

Mettre le reste en R

;

Remplacer A par B ;

Remplacer B par R ;

Retourner A .

Premier algorithme certifié :

Termine :

B décroît et atteindra 0.

Algorithme d'Euclide. (\sim 300 av. J. C.)

PGCD(A, B) : plus grand entier C qui divise A et qui divise B .

Etant donné deux entiers A et B avec $A \geq B$, comment trouver PGCD(A, B) ?

Tant que $B \neq 0$ faire

Diviser A par B ;

Mettre le reste en R

;

Remplacer A par B ;

Remplacer B par R ;

Retourner A .

Premier algorithme certifié :

Termine :

B décroît et atteindra 0.

Valide :

$\text{PGCD}(A, B) = \text{PGCD}(B, R)$;

$\text{PGCD}(A, 0) = A$.

Origine du mot algorithme



Abû 'Abd Allah Muhammad ben Mūsā **al-Khawārizmī**
(vers 780, Khiva, Khwarezm ; vers 850, Bagdad)

Traité du système de numération des Indiens.

Recense des algorithmes de calcul avec les chiffres “arabes”.



Algorithmes de l'addition et de la multiplication.

$$\begin{array}{r} 1 \\ + 523 \\ 768 \\ \hline 1291 \end{array}$$

$$\begin{array}{r} 11 \quad 1 \quad 11 \\ + 2930172493 \\ 3473076891 \\ \hline 6403249384 \end{array}$$

$$\begin{array}{r} 4514 \\ \times 7654 \\ \hline 18056 \\ 22570 \cdot \\ 27084 \cdot \cdot \\ 31598 \cdot \cdot \cdot \\ \hline 34550156 \end{array}$$

Adoption du système de numération indo-arabe.

- ▶ Fin Xème : Gerbert d'Aurillac (Sylvestre II) rapporte les chiffres arabes. Abaque de Gerbert.
- ▶ 1085 Tolède : *Liber Algorismi de numero Indorum* sous l'impulsion de l'évêque Raimond
- ▶ 1130 Angleterre : *Algoritmi de numero indorum* par Adélard de Bath.
- ▶ 1202 : *Liber abaci* Fibonacci (Léonard de Pise)



In *Margarita philosophica*, de G. Reisch

Algoristes

Calcul à la plume
avec chiffres arabes

Abacistes

Calcul avec jetons
ou boulier

jusqu'à la révolution française

Querelle

Apparition des premiers ordinateurs.

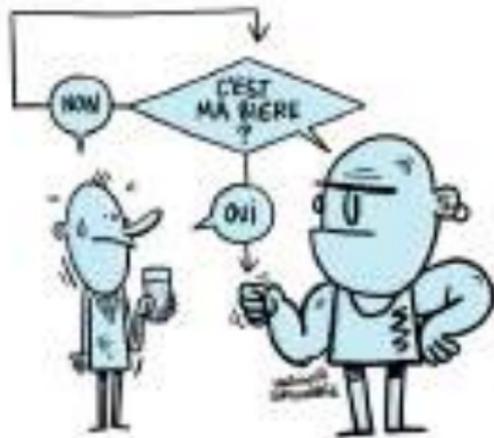
1944 : Décryptage d'Enigma par A. Turing et son équipe à l'aide de "bombes".



1945 : Premier ordinateur ENIAC électronique
30 tonnes, 19 000 lampes,
5 000 opérations par secondes.



Exemple d'algorithme. Analyse et applications.



Le problème des mariages stables

Préférences des hommes

Préférences des femmes

William	B	D	A	C	Alice	X	W	Z	Y
Xavier	C	A	D	B	Betty	Z	Y	W	X
Yvan	B	C	A	D	Clara	W	Z	Y	X
Zack	D	A	C	B	Denise	X	W	Z	Y

Le problème des mariages stables

Préférences des hommes

Préférences des femmes

William	B	D	A	C	Alice	X	W	Z	Y
Xavier	C	A	D	B	Betty	Z	Y	W	X
Yvan	B	C	A	D	Clara	W	Z	Y	X
Zack	D	A	C	B	Denise	X	W	Z	Y

Un **mariage**

William – **Alice**
Xavier – **Betty**
Yvan – **Clara**
Zack – **Denise**

Le problème des mariages stables

Préférences des hommes

Préférences des femmes

William	B	D	A	C	Alice	X	W	Z	Y
Xavier	C	A	D	B	Betty	Z	Y	W	X
Yvan	B	C	A	D	Clara	W	Z	Y	X
Zack	D	A	C	B	Denise	X	W	Z	Y

Un **mariage instable**

William – **Alice**
Xavier – **Betty**
Yvan – **Clara**
Zack – **Denise**

Le problème des mariages stables

Préférences des hommes

Préférences des femmes

William	B	D	A	C	Alice	X	W	Z	Y
Xavier	C	A	D	B	Betty	Z	Y	W	X
Yvan	B	C	A	D	Clara	W	Z	Y	X
Zack	D	A	C	B	Denise	X	W	Z	Y

Un **mariage instable**

William – **Alice**
Xavier – **Betty**
Yvan – Clara
Zack – Denise

Le problème des mariages stables

Préférences des hommes

Préférences des femmes

William	B	D	A	C	Alice	X	W	Z	Y
Xavier	C	A	D	B	Betty	Z	Y	W	X
Yvan	B	C	A	D	Clara	W	Z	Y	X
Zack	D	A	C	B	Denise	X	W	Z	Y

Un **mariage STABLE**

William – **Denise**
Xavier – **Clara**
Yvan – **Betty**
Zack – **Alice**

Le problème des mariages stables

Préférences des hommes

Préférences des femmes

William	B	D	A	C	Alice	X	W	Z	Y
Xavier	C	A	D	B	Betty	Z	Y	W	X
Yvan	B	C	A	D	Clara	W	Z	Y	X
Zack	D	A	C	B	Denise	X	W	Z	Y

Un **mariage STABLE**

William – Denise
Xavier – Clara
Yvan – Betty
Zack – Alice

Le problème des mariages stables

Préférences des hommes

Préférences des femmes

William	B	D	A	C	Alice	X	W	Z	Y
Xavier	C	A	D	B	Betty	Z	Y	W	X
Yvan	B	C	A	D	Clara	W	Z	Y	X
Zack	D	A	C	B	Denise	X	W	Z	Y

Un **mariage STABLE**

William – **Denise**
Xavier – **Clara**
Yvan – **Betty**
Zack – **Alice**

L'algorithme de Gale et Shapley

Les hommes proposent, les femmes disposent.

Préférences des hommes

Préférences des femmes

William	B	D	A	C	Alice	X	W	Z	Y
Xavier	C	A	D	B	Betty	Z	Y	W	X
Yvan	B	C	A	D	Clara	W	Z	Y	X
Zack	D	A	C	B	Denise	X	W	Z	Y

William –
Xavier –
Yvan –
Zack –

L'algorithme de Gale et Shapley

Les hommes proposent, les femmes disposent.

Préférences des hommes

Préférences des femmes

William	B	D	A	C	Alice	X	W	Z	Y
Xavier	C	A	D	B	Betty	Z	Y	W	X
Yvan	B	C	A	D	Clara	W	Z	Y	X
Zack	D	A	C	B	Denise	X	W	Z	Y

William – **Betty**

Xavier –

Yvan –

Zack –

L'algorithme de Gale et Shapley

Les hommes proposent, les femmes disposent.

Préférences des hommes

Préférences des femmes

William	B	D	A	C	Alice	X	W	Z	Y
Xavier	C	A	D	B	Betty	Z	Y	W	X
Yvan	B	C	A	D	Clara	W	Z	Y	X
Zack	D	A	C	B	Denise	X	W	Z	Y

William – Betty
Xavier – Clara
Yvan –
Zack –

L'algorithme de Gale et Shapley

Les hommes proposent, les femmes disposent.

Préférences des hommes

Préférences des femmes

William	B	D	A	C	Alice	X	W	Z	Y
Xavier	C	A	D	B	Betty	Z	Y	W	X
Yvan	B	C	A	D	Clara	W	Z	Y	X
Zack	D	A	C	B	Denise	X	W	Z	Y

William – ~~Betty~~
Xavier – Clara
Yvan – Betty
Zack –

L'algorithme de Gale et Shapley

Les hommes proposent, les femmes disposent.

Préférences des hommes

Préférences des femmes

William	B	D	A	C	Alice	X	W	Z	Y
Xavier	C	A	D	B	Betty	Z	Y	W	X
Yvan	B	C	A	D	Clara	W	Z	Y	X
Zack	D	A	C	B	Denise	X	W	Z	Y

William –
Xavier – **Clara**
Yvan – **Betty**
Zack –

L'algorithme de Gale et Shapley

Les hommes proposent, les femmes disposent.

Préférences des hommes

Préférences des femmes

William	B	D	A	C	Alice	X	W	Z	Y
Xavier	C	A	D	B	Betty	Z	Y	W	X
Yvan	B	C	A	D	Clara	W	Z	Y	X
Zack	D	A	C	B	Denise	X	W	Z	Y

William – **Denise**
Xavier – Clara
Yvan – Betty
Zack –

L'algorithme de Gale et Shapley

Les hommes proposent, les femmes disposent.

Préférences des hommes

Préférences des femmes

William	B	D	A	C	Alice	X	W	Z	Y
Xavier	C	A	D	B	Betty	Z	Y	W	X
Yvan	B	C	A	D	Clara	W	Z	Y	X
Zack	D	A	C	B	Denise	X	W	Z	Y

William – **Denise**
Xavier – **Clara**
Yvan – **Betty**
Zack –

L'algorithme de Gale et Shapley

Les hommes proposent, les femmes disposent.

Préférences des hommes

Préférences des femmes

William	B	D	A	C	Alice	X	W	Z	Y
Xavier	C	A	D	B	Betty	Z	Y	W	X
Yvan	B	C	A	D	Clara	W	Z	Y	X
Zack	D	A	C	B	Denise	X	W	Z	Y

William – **Denise**
Xavier – **Clara**
Yvan – **Betty**
Zack – **Alice**

L'algorithme de Gale et Shapley : certification

Terminaison :

Les hommes ne se proposent qu'une seule fois à chaque femme. Leur préférence décroît. A l'inverse, la préférence des femmes croît. On termine en $n \times n = n^2$ étapes au plus.

Validité :

Mariage : A chaque instant, un homme est au plus avec une femme et inversement. A la fin, tous les hommes sont avec une femme.

Stable : Couples (H1, F1) et (H2,F2).

Supposons que H2 préfère F1 à F2.

H2 s'est proposé à F1, mais n'est pas avec elle.

- ▷ Soit F1 l'a refusé car avec un homme qu'elle préférerait à H2.
- ▷ Soit F1 l'a ensuite quitté pour un homme qu'elle préférerait à H2.

Dans les deux cas, F1 préfère H1 à H2, **pas d'instabilité**.

L'algorithme de Gale et Shapley : applications

1968 : **Gale and Shapley**. Travaux purement **théoriques**.



David Gale (1921-2008)



Lloyd Shapley (1923-2016)

L'algorithme de Gale et Shapley : applications

1968 : **Gale and Shapley**. Travaux purement **théoriques**.



David Gale (1921-2008)



Lloyd Shapley (1923-2016)



Alvin Roth (1951-)

1980 : **Roth**. Affectation d'internes dans les hopitaux américains.

L'algorithme de Gale et Shapley : applications

1968 : **Gale and Shapley**. Travaux purement **théoriques**.



David Gale (1921-2008)



Lloyd Shapley (1923-2016)



Alvin Roth (1951-)

1980 : **Roth**. Affectation d'internes dans les hopitaux américains.

2004 : Appariement donneur/receveur greffe de rein.

L'algorithme de Gale et Shapley : applications

1968 : **Gale and Shapley**. Travaux purement **théoriques**.



David Gale (1921-2008)



Lloyd Shapley (1923-2016)



Alvin Roth (1951-)

1980 : **Roth**. Affectation d'internes dans les hopitaux américains.

2004 : Appariement donneur/receveur greffe de rein.

2012 : Prix Nobel d'économie Shapley et Roth.

L'algorithme de Gale et Shapley : applications

1968 : **Gale and Shapley**. Travaux purement **théoriques**.



David Gale (1921-2008)



Lloyd Shapley (1923-2016)



Alvin Roth (1951-)

1980 : **Roth**. Affectation d'internes dans les hopitaux américains.

2004 : Appariement donneur/receveur greffe de rein.

2012 : Prix Nobel d'économie Shapley et Roth.

2009 : APB ; 2018: Parcours Sup.

L'algorithme de Gale et Shapley : asymétrie

Les hommes proposent, les femmes disposent.

Asymétrie :

- ▶ Un homme termine avec sa partenaire préférée parmi toutes celles possibles dans un mariage stable.
- ▶ Une femme termine avec son partenaire le moins aimé parmi tous les possibles.

L'algorithme de Gale et Shapley : asymétrie

Les hommes proposent, les femmes disposent.

Asymétrie :

- ▶ Un homme termine avec sa partenaire préférée parmi toutes celles possibles dans un mariage stable.
- ▶ Une femme termine avec son partenaire le moins aimé parmi tous les possibles.

Sincérité :

- ▶ Un homme n'a aucun intérêt à mentir sur ses préférences.
- ▶ Une femme peut avoir intérêt à mentir pour obtenir un meilleur partenaire.

APB et ParcoursSup

APB : étudiants \equiv hommes.

Un étudiant obtient sa formation préférée parmi celles possibles.

MAIS impression de boîte noire. **Rejet du public.**

ParcoursSup : étudiants \equiv femmes.

Un étudiant obtient sa formation la moins aimée parmi celles possibles.

MAIS impression de choix dans la procédure.



Nécessité d'**algorithmes acceptables**, donc **compréhensibles**.

3ème révolution algorithmique : Intelligence Artificielle



Qu'est-ce que l'Intelligence Artificielle

Intelligence : ensemble de facultés cognitives très variées.

- ▶ **fonctions réceptives** : acquisition de l'information, ...
- ▶ **mémoire et apprentissage** : stockage et rappel de l'information (cf. représentation des connaissances)
- ▶ **raisonnement et pensée**
- ▶ **fonctions exécutives** : décision, action
- ▶ **fonctions expressives** : communication (langage naturel, oral écrit, etc.)

L'IA vise à **étudier et simuler** ces fonctions.

- ▶ **Comprendre le cerveau** grâce au numérique.
(Neurosciences)
- ▶ **S'inspirer du cerveau** pour créer des algorithmes.
Bio-inspiration

Origine de l'Intelligence Artificielle

1950 : Test de Turing : “ *un ordinateur mériterait d'être intelligent s'il pouvait interagir avec un humain en lui faisant croire qu'il est humain* ”

1956 : Conférence de Darmouth : Minsky, McCarthy, Shannon, Rochester, ...

- ▶ 1943 : 1er modèle mathématique d'un neurone artificiel (Pitts, McCulloch)
- ▶ 1954 : naissance du traitement automatique du langage naturel
- ▶ 1958 : premier algorithme d'apprentissage avec réseau de neurones (F. Rosenblatt)
- ▶ 1960 : premiers systèmes experts.

Origine de l'Intelligence Artificielle

1997 : Deep Blue (**système expert**) bat Kasparov aux échecs.

1990 : Apparition d'internet ⇒ **données en quantité**.

Augmentation de la **puissance de calcul**.

2012 : Un algorithme **apprend** à reconnaître des chats (Google X).

2016 : AlphaGo (**apprentissage**) bat Lee Sedol, champion du monde de Go,

2017 : AlphaZero bat Stockfish 8 aux échecs (28 victoires, 72 nuls, 0 défaites)

2022 : ChatGPT

Apprentissage machine

Plusieurs types d'apprentissage:

- ▶ apprentissage par renforcement
- ▶ apprentissage machine
- ▶ apprentissage profond
- ▶ ...

Caractéristiques communes:

- ▶ solution non certifiée mais probabilité d'exactitude (vrai à X %).
- ▶ besoin d'un grand nombre de calculs et/ou de données.

Apprentissage par renforcement

Jeu des bâtonnets.

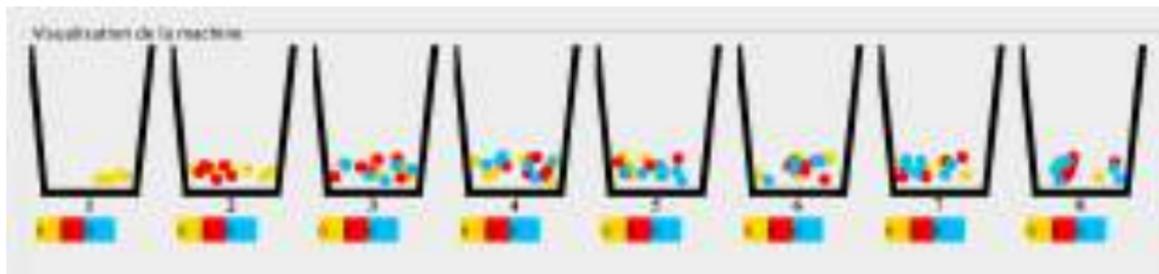


A tour de rôle, les joueurs enlèvent 1, 2 ou 3 bâtonnets.
Celui qui enlève le dernier bâtonnet gagne.

Apprentissage par renforcement

Jeu des bâtonnets.

On tire une boule au hasard dans chaque pot :
on ôte ● un, ● deux ou ● trois bâtonnets

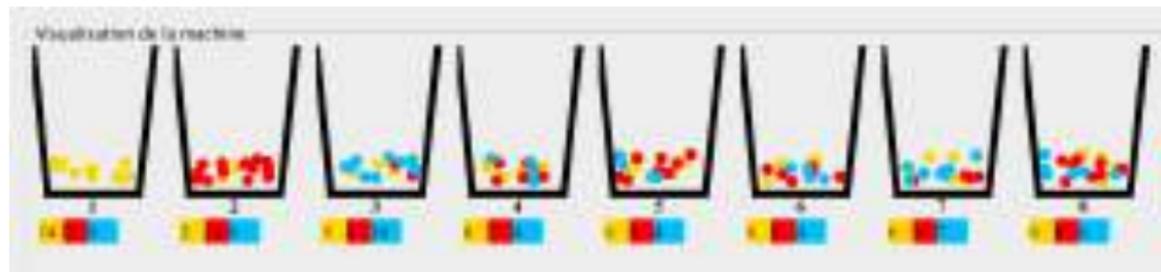


On joue. Si on gagne on remet chaque boule tirée dans son pot en ajoutant une autre de la même couleur. Si on perd on ne remet pas les boules tirées dans le pot.

Apprentissage par renforcement

Jeu des bâtonnets.

On tire une boule au hasard dans chaque pot :
on ôte ● un, ● deux ou ● trois bâtonnets

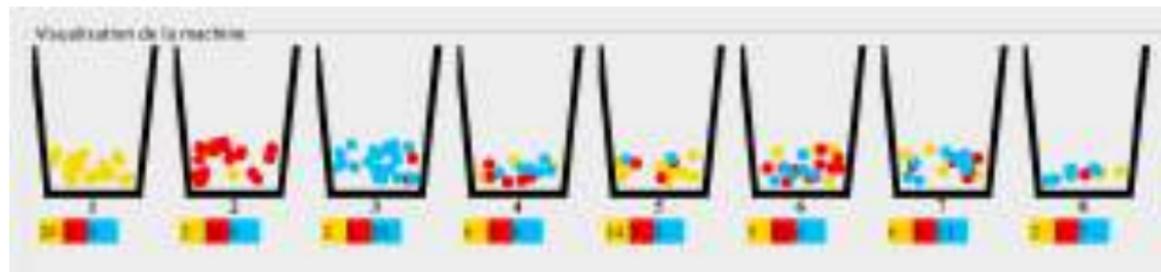


Après 20 parties.

Apprentissage par renforcement

Jeu des bâtonnets.

On tire une boule au hasard dans chaque pot :
on ôte ● un, ● deux ou ● trois bâtonnets

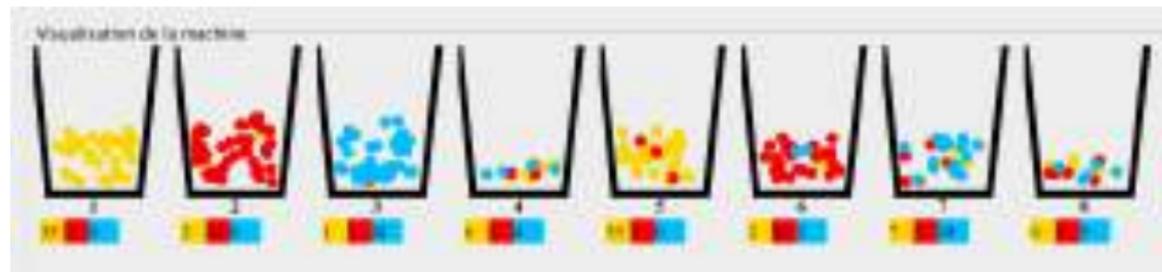


Après 50 parties.

Apprentissage par renforcement

Jeu des bâtonnets.

On tire une boule au hasard dans chaque pot :
on ôte ● un, ● deux ou ● trois bâtonnets

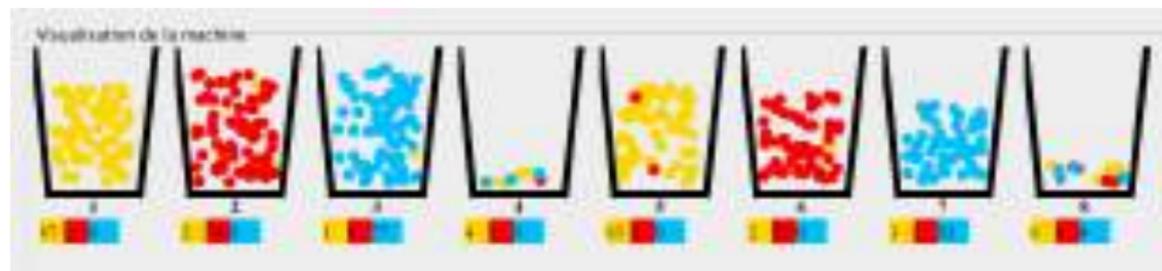


Après 100 parties.

Apprentissage par renforcement

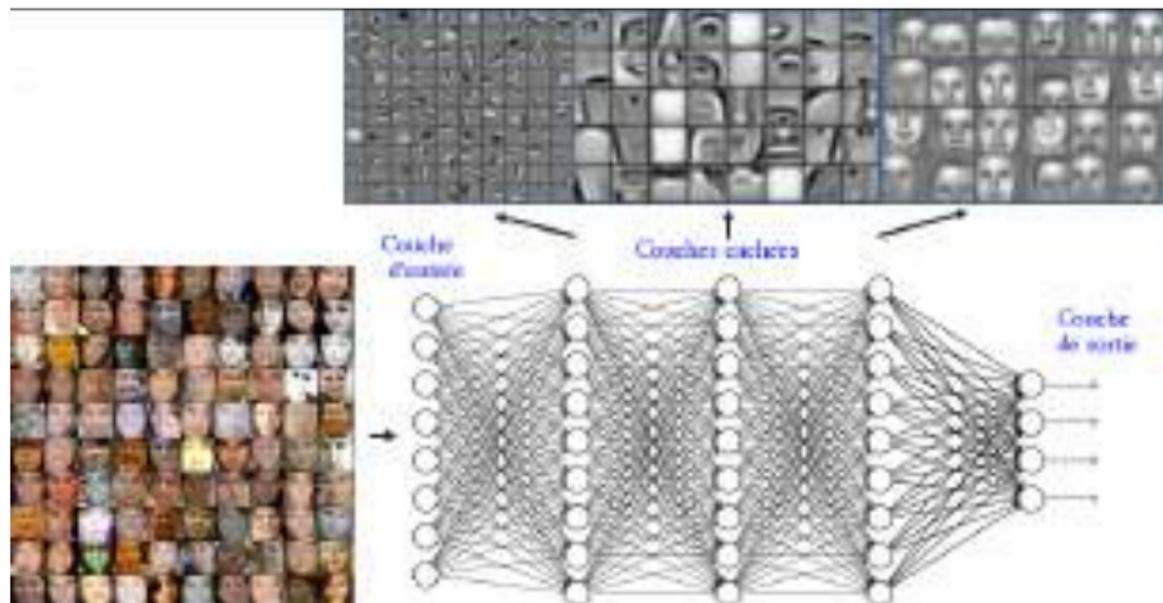
Jeu des bâtonnets.

On tire une boule au hasard dans chaque pot :
on ôte ● un, ● deux ou ● trois bâtonnets



Après 200 parties.

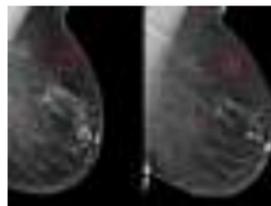
Réseaux de neurones



Applications de l'apprentissage automatique

Perception :

- ▶ Analyse d'image → diagnostic médical.
- ▶ Reconnaissance vocale → assistant intelligent.
- ▶ Language → traduction, détection de spams,



Imitation :

- ▶ Deep fake. Musique à la manière de.
- ▶ Synthèse vocale → assistant intelligent.
- ▶ Véhicule autonome.
- ▶ Jeux.



Attention à l'échantillonnage

Difficulté d'avoir un échantillonnage non biaisé.

- ▶ X. Wu and X. Zhang *Automated Inference on Criminality using Face Images*. Algorithme qui pouvait prédire à 90% si une personne était criminelle à partir d'une photo.



criminels
non-souriants



non-criminels
souriants

- ▶ Plante.net. Pour les photos de plantes prises dans des conditions lumineuses non ordinaires (la nuit, ...) il y a plus d'erreurs.
- ▶ Les algorithmes de reconnaissance de lésion par IRM doivent être entraînés avec des images de chaque machine.

Attention à l'échantillonnage

Reproduction ou amplification des biais humains

- ▶ Programme GloVe. Fleurs → bonheur. Insectes → mort, douleur, ...
- ▶ Chatbot Tay de Microsoft devenu raciste et négationniste en quelques heures.



Enjeux scientifiques : Les algorithmes peuvent-ils tout faire ?

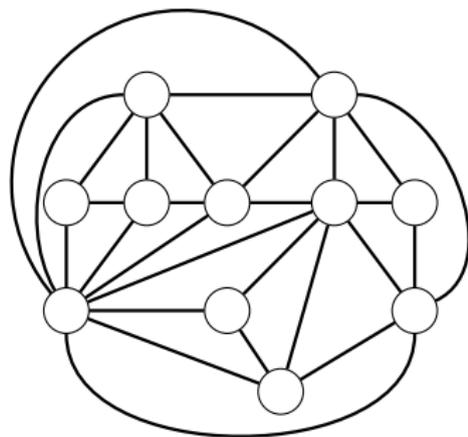


Coloration de graphes

4-coloration

Règle : Colorer les sommets d'un graphe de telle sorte que deux sommets reliés par une arête ont des couleurs différentes.

Question : est-ce possible avec 4 couleurs ?

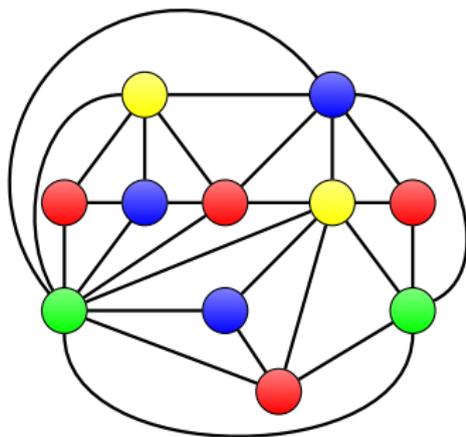


Coloration de graphes

4-coloration

Règle : Colorer les sommets d'un graphe de telle sorte que deux sommets reliés par une arête ont des couleurs différentes.

Question : est-ce possible avec 4 couleurs ?

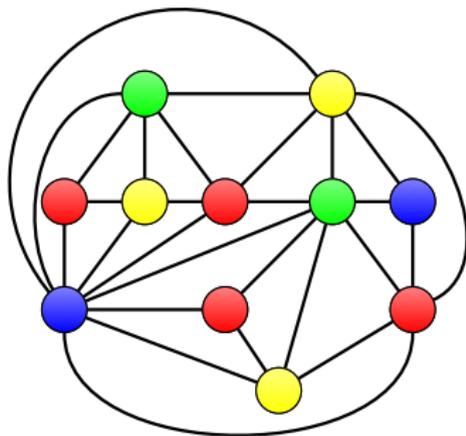


Coloration de graphes

4-coloration

Règle : Colorer les sommets d'un graphe de telle sorte que deux sommets reliés par une arête ont des couleurs différentes.

Question : est-ce possible avec 4 couleurs ?



Coloration de graphes : force brute

Algorithme **force brute** : tester **toutes les possibilités**.

Pour voir si un graphe à n sommets est colorable avec 4 couleurs : essayer toutes les combinaisons. On a 4 choix par sommet.

Au total, $\underbrace{4 \times 4 \times \cdots \times 4}_{n \text{ fois}} = 4^n$ possibilités.

Si $n = 135$, cela fait $4^{135} \simeq 10^{81}$ opérations.

$10^{81} \simeq$ nombre d'atomes dans l'univers.

Coloration de graphes : force brute

Algorithme **force brute** : tester **toutes les possibilités**.

Pour voir si un graphe à n sommets est colorable avec 4 couleurs : essayer toutes les combinaisons. On a 4 choix par sommet.

Au total, $\underbrace{4 \times 4 \times \cdots \times 4}_{n \text{ fois}} = 4^n$ possibilités.

Si $n = 135$, cela fait $4^{135} \simeq 10^{81}$ opérations.

$10^{81} \simeq$ nombre d'atomes dans l'univers.

Gale-Shapley : $135 \times 135 = 18225$ opérations.

Coloration de graphes : force brute

Algorithme **force brute** : tester **toutes les possibilités**.

Pour voir si un graphe à n sommets est colorable avec 4 couleurs : essayer toutes les combinaisons. On a 4 choix par sommet.

Au total, $\underbrace{4 \times 4 \times \dots \times 4}_{n \text{ fois}} = 4^n$ possibilités.

Si $n = 135$, cela fait $4^{135} \simeq 10^{81}$ opérations.

$10^{81} \simeq$ nombre d'atomes dans l'univers.

Gale-Shapley : $135 \times 135 = 18225$ opérations.

On recherche des **algorithmes RAPIDES**

Les 7 problèmes du millénaire

1. **Hypothèse de Riemann** (1859).
2. **Conjecture de Poincaré** (1904). **prouvée** (Perelman, 2003).
3. **Problème $P \neq NP$?** (1971).
4. **Conjecture de Hodge** (\sim 1930).
5. **Conjecture de Birch et Swinnerton-Dyer** (\sim 1960)
6. **Equations de Navier-Stokes** (19^{ème} siècle).
7. **Equations de Yang-Mills** (années 1950).

Clay Mathematical Institute offre 1 million de dollars pour la résolution de chacun des problèmes.

Le problème $P \neq NP$?

P résolubles rapidement

$+$, $-$, \times , \div

mariage stable

PGCD

tri

itinéraire

être premier ?

Le problème $P \neq NP$?

échecs

NP vérifiables rapidement

4-coloration sudoku voyageur de commerce
repliement de protéines ordonnancement
isomorphisme de graphes clé cryptographique

P résolubles rapidement

$+$, $-$, \times , \div mariage stable PGCD
tri itinéraire être premier ?

Le problème $P \neq NP$?

échecs

NP vérifiable rapidement

4-coloration sudoku voyageur de commerce

NP-complets

repliement de protéines ordonnancement

isomorphisme de graphes

clé cryptographique

P résolubles rapidement

$+$, $-$, \times , \div

mariage stable

PGCD

tri

itinéraire

être premier ?

Résoudre des problèmes NP-durs ?

Résoudre rapidement pour des **instances particulières**.

↪ Graphes planaires 4-colorables.

Algorithme approché : trouver une solution non-optimale.

↪ **certifier l'erreur**.

Heuristiques :

- ▶ Algorithme glouton. Haute proba. 2-approx pour coloration.
- ▶ Programmation linéaire + arrondi.
- ▶ Recherche tabou, Recuit simulé, Algorithmes génétiques.
- ▶ Intelligence distribuée: colonies de fourmis, ...
- ▶ Apprentissage automatique. (Machine Learning).

Programmation linéaire

Maximiser (ou minimiser): $c_1X_1 + c_2X_2 + \cdots + c_nX_n$

Soumis à $a_{11}X_1 + a_{12}X_2 + \cdots + a_{1n}X_n \leq b_1$

$a_{21}X_1 + a_{22}X_2 + \cdots + a_{2n}X_n \leq b_2$

\vdots

$a_{m1}X_1 + a_{m2}X_2 + \cdots + a_{mn}X_n \leq b_m$

Méthode de résolution développée
par George B. Dantzig.



Programmation linéaire

Une clé de la victoire en 1945.

Essentiel pour la bataille de Normandie.
Débarquement de trois millions de soldats
(150 000 le jour J) + matériel, vivres, ...



Rendue publique en 1947.

Très nombreuses applications :

Planification et contrôle de la production, distribution,

dans de très nombreux secteurs : industrie manufacturière, énergie, transports, télécommunications, finance, ...

Enjeux éthiques et sociétaux des algorithmes



Encadrer les algorithmes

Quel processus d'homologation d'un algorithme ?

► Validation scientifique.

Vérification.

Taux d'erreur acceptable ?

► Validation éthique.

Mercedes : *nos algorithmes favoriseront les passagers du véhicule.*



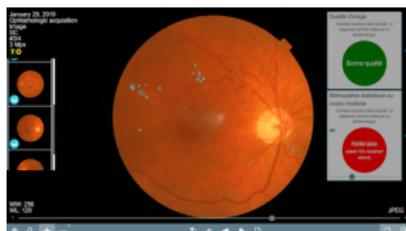
IBM ne fait plus de logiciel de reconnaissance et analyse faciale.

Encadrer les algorithmes

Responsabilité en cas d'erreur d'un algorithme/logiciel ?

► Diagnostic scientifique.

Avril 2018 : FDA autorise la mise sur le marché d'un logiciel de diagnostic de la rétinopathie diabétique **sans médecin**.



► Véhicule autonome.

Concepteur du logiciel, constructeur automobile, propriétaire du véhicule ?

Encadrer les algorithmes

Utilisation et propriété des données.

- ▶ Médecine. Qui est propriétaire des données ? malade ? médecin ?
hôpital ? data center ? financeurs du système de santé ?

Protection de l'individu – intérêt collectif.

Aux U.S.A., les GAFAM les collectent à foison.

En France, règles de la CNIL et du RGPD.

Minimisation de l'énergie

Le numérique consomme autant d'énergie que l'aviation civile.

Datacenters très énergivores.

Algorithmes d'apprentissage nécessite beaucoup de calcul donc d'énergie.

Green computing. I.A. frugale

Video en streaming gourmand.

Bitcoin : miner un bitcoin très onéreux énergétiquement (~ ville de 200 000 habitants).