

MAIS À QUOI PEUVENT BIEN SERVIR LES MATHÉMATIQUES ?

MAIS À QUOI PEUVENT BIEN SERVIR LES MATHÉMATIQUES ?

"Les domaines qui mobilisent les mathématiques avancées sont aujourd'hui considérablement plus nombreux qu'il y a vingt ans. Ils sont aussi plus stratégiques. (...) Nous voyons aujourd'hui apparaître de nouveaux métiers et de nouveaux modèles économiques dans lesquelles les statistiques et le traitement des données jouent un rôle important. La collecte, la structuration, la transformation et l'exploitation des données collectées passent par des processus mathématiques de très haut niveau. (...) Dans le nouveau paradigme, marqué par la continuité entre mathématiques fondamentales et appliquées et par la présence des mathématiques fondamentales au coeur du monde économique, la question de la communication est centrale."

Jean-Pierre Bourguignon, Président du Conseil Européen de la Recherche *in* "Un nouvel âge d'or pour les Mathématiques en entreprise (2014)

Au début de l'histoire

Au début de l'histoire

Il y a beaucoup de nombres simples, d'autres beaucoup plus compliqués, et puis des équations, beaucoup d'équations.

Au début de l'histoire

Il y a beaucoup de nombres simples, d'autres beaucoup plus compliqués, et puis des équations, beaucoup d'équations.

- ▶ Comment arrivent ces nombres,
- ▶ Comment arrivent ces équations,
- ▶ À quoi ces dernières peuvent-elles bien servir ?

Au début de l'histoire

Il y a beaucoup de nombres simples, d'autres beaucoup plus compliqués, et puis des équations, beaucoup d'équations.

- ▶ Comment arrivent ces nombres,
- ▶ Comment arrivent ces équations,
- ▶ À quoi ces dernières peuvent-elles bien servir ?

Un des premiers usages est sans doute...

Au début de l'histoire

Il y a beaucoup de nombres simples, d'autres beaucoup plus compliqués, et puis des équations, beaucoup d'équations.

- ▶ Comment arrivent ces nombres,
- ▶ Comment arrivent ces équations,
- ▶ À quoi ces dernières peuvent-elles bien servir ?

Un des premiers usages est sans doute... LE PARTAGE.

Au début de l'histoire

Il y a beaucoup de nombres simples, d'autres beaucoup plus compliqués, et puis des équations, beaucoup d'équations.

- ▶ Comment arrivent ces nombres,
- ▶ Comment arrivent ces équations,
- ▶ À quoi ces dernières peuvent-elles bien servir ?

Un des premiers usages est sans doute... LE PARTAGE.
Dans la vie, il nous faut **toujours** partager (*sic*)

- ▶ Parfois le partage est simple :

S'il n'y a qu'un gâteau et qu'il n'y a qu'une seule personne qui le convoite, l'affaire est entendue !

Formalisons ce processus de (faux) partage à la manière du mathématicien : désignons par X la part qui revient à chacun. Alors, la règle de partage se traduit par ...

Formalisons ce processus de (faux) partage à la manière du mathématicien : désignons par X la part qui revient à chacun. Alors, la règle de partage se traduit par ...

UNE ÉQUATION

Formalisons ce processus de (faux) partage à la manière du mathématicien : désignons par X la part qui revient à chacun. Alors, la règle de partage se traduit par ...

UNE ÉQUATION

$$X = 1$$

Formalisons ce processus de (faux) partage à la manière du mathématicien : désignons par X la part qui revient à chacun. Alors, la règle de partage se traduit par ...

UNE ÉQUATION

$$X = 1$$

Ici comme ailleurs, il s'agira de trouver X . Pour cette raison, X est appelé **l'inconnue**.

Formalisons ce processus de (faux) partage à la manière du mathématicien : désignons par X la part qui revient à chacun. Alors, la règle de partage se traduit par ...

UNE ÉQUATION

$$X = 1$$

Ici comme ailleurs, il s'agira de trouver X . Pour cette raison, X est appelé **l'inconnue**.

Mais le partage n'est pas toujours aussi simple...

- ▶ Il y a des cas où le partage est rationnel.

- ▶ Il y a des cas où le partage est rationnel.

Par exemple, lorsque six gâteaux doivent être répartis entre deux personnes (disons A et B), l'équation de répartition équitable ($x_A = x_B = X$) s'écrit

$$6 = x_A + x_B = 2X$$

de sorte que le rebouteux des équations (celui qui remet les quantités à la place qui doit être la leur) et que l'on qualifie d'algébriste (al Jabr...) écrira

$$X = \frac{6}{2} = 3$$

c'est-à-dire que trois gâteaux reviennent à chaque personne.

- ▶ Il y a des cas où le partage est rationnel.

Par exemple, lorsque six gâteaux doivent être répartis entre deux personnes (disons A et B), l'équation de répartition équitable ($x_A = x_B = X$) s'écrit

$$6 = x_A + x_B = 2X$$

de sorte que le rebouteux des équations (celui qui remet les quantités à la place qui doit être la leur) et que l'on qualifie d'algébriste (al Jabr...) écrira

$$X = \frac{6}{2} = 3$$

c'est-à-dire que trois gâteaux reviennent à chaque personne. Le partage est tout aussi rationnel lorsqu'il y a un nombre entier de gâteaux P et un nombre entier de personnes Q :

$$QX = P \quad \text{soit} \quad X = \frac{P}{Q}$$

Il s'agit encore une fois de résoudre une équation.

Il s'agit encore une fois de résoudre une équation.

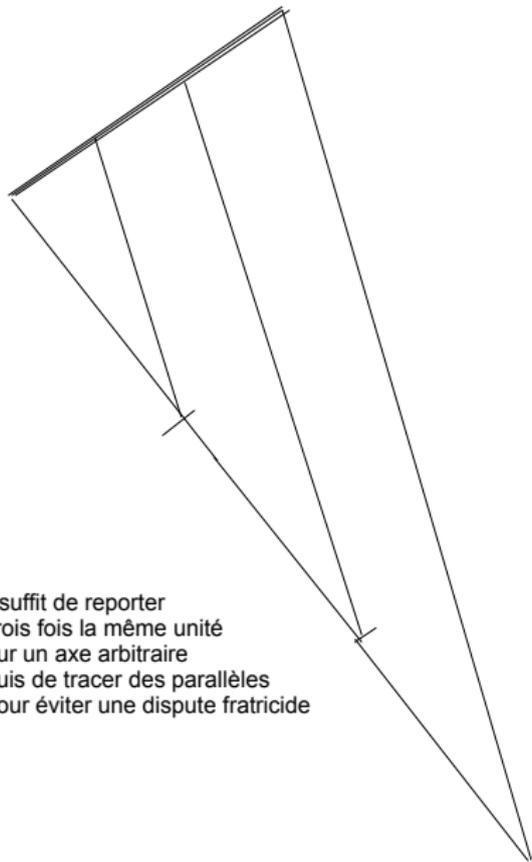
Parfois nous nous y perdons, même lorsque l'équation est relativement simple, et qu'elle nous contraint d'ajouter, de diviser, de multiplier, de retrancher. Lorsque l'on pèse le cochon lors de la pèlère, il faut ajouter, soustraire, multiplier, diviser pour trouver un prix sur lequel vont s'accorder acheteur et vendeur (du cochon). Parce qu'il y a le poids de l'échelle lors de la pesée, etc.

Il s'agit encore une fois de résoudre une équation.

Parfois nous nous y perdons, même lorsque l'équation est relativement simple, et qu'elle nous contraint d'ajouter, de diviser, de multiplier, de retrancher. Lorsque l'on pèse le cochon lors de la pèlère, il faut ajouter, soustraire, multiplier, diviser pour trouver un prix sur lequel vont s'accorder acheteur et vendeur (du cochon). Parce qu'il y a le poids de l'échelle lors de la pesée, etc.

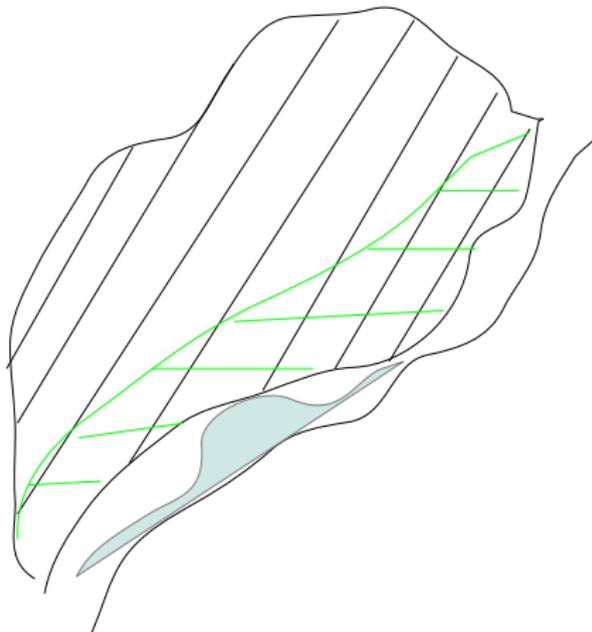
- ▶ Il y a des cas où le partage est une affaire de géométrie.

LE PARTAGE DE LA BAGUETTE DE PAIN EN TROIS



Il suffit de reporter
Trois fois la même unité
Sur un axe arbitraire
Puis de tracer des parallèles
Pour éviter une dispute fratricide

LE PARTAGE EST SOUVENT PLUS COMPLEXE



COMMENT SE PARTAGER UN LOPIN DE TERRE ?

La terre n'a pas la même valeur selon qu'elle se trouve près de la rivière ou non

Et puis, comment évaluer la superficie ? On voit que la question est ardue.

Et puis, dans le calcul des aires, des volumes, on doit prendre en compte des PUISSANCES de l'inconnue X , que l'on désigne par

$$X^2 = X \times X, \quad X^3 = X \times X \times X$$

et, de manière générale

$$X^n = \underbrace{X \times X \times X \times \cdots \times X}_{n \text{ fois}}$$

Et puis, dans le calcul des aires, des volumes, on doit prendre en compte des PUISSANCES de l'inconnue X , que l'on désigne par

$$X^2 = X \times X, \quad X^3 = X \times X \times X$$

et, de manière générale

$$X^n = \underbrace{X \times X \times X \times \cdots \times X}_{n \text{ fois}}$$

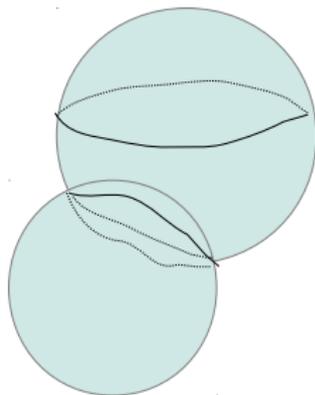
Par exemple l'inconnue X peut satisfaire une équation du second degré :

$$aX^2 + bX + c = 0$$

qui a pu occasionner quelques souffrances au lycée !

Cette équation est naturelle lorsque l'on cherche les lieux d'intersection, non pas de droites, mais de sphères ou de cercles, et l'on verra l'usage intéressant qui peut en être fait.

De l'usage des sphères pour comprendre...



L'intersection de deux sphères (moins cabossées)
Est un cercle et de trois sphères deux points (en général)

Les formules qui permettent d'obtenir ces intersections
font apparaître des objets **du second degré**.

Les formules sont connues depuis fort longtemps (les babyloniens ?).

Dans les bons cas, il y a deux solutions qui sont données au moyen des opérations élémentaires que l'on a rencontrées :

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

et d'une cinquième...

Les formules sont connues depuis fort longtemps (les babyloniens ?).

Dans les bons cas, il y a deux solutions qui sont données au moyen des opérations élémentaires que l'on a rencontrées :

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

et d'une cinquième...

$$\sqrt{\quad}$$

Les formules sont connues depuis fort longtemps (les babyloniens ?).

Dans les bons cas, il y a deux solutions qui sont données au moyen des opérations élémentaires que l'on a rencontrées :

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

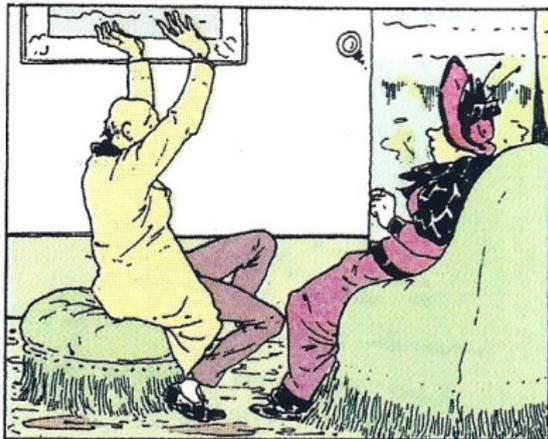
et d'une cinquième...

$$\sqrt{\quad}$$

Manipuler de manière répétée cette dernière opération, c'est, selon les mathématiciens, effectuer une succession de...

QUADRATURES

Le savant Cosinus savait, de longue date, extraire des racines.



— Une extraction de racine, s'exclame Zéphyrin ! Mais c'est ma spécialité, ça ! Dès ma plus tendre enfance, j'extrayais, par plaisir, toutes les racines de mes camarades ! et j'ose dire que j'ai acquis dans ce genre d'opérations une habileté extraordinaire. Je ne me vante pas, madame, je constate !.... Par quel procédé désirez-vous que j'opère ?

Par exemple, dans les bons cas, les solutions de l'équation du second degré sont données par

$$X_{\pm} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

c'est-à-dire que l'équation du second degré peut être résolue par quadrature.

On sait depuis la Renaissance italienne qu'une équation de degré trois (Cardan, Tartaglia, Bombelli, puis Ferrari) que les équations de degré 3 puis quatre peuvent être résolues par quadratures.

MÊME S'IL FAUT ÉCOUTER LES ANCIENS, TOUT CECI SENT
LA POUSSIÈRE !

MÊME S'IL FAUT ÉCOUTER LES ANCIENS, TOUT CECI SENT LA POUSSIÈRE !

ALORS TRANSPORTONS-NOUS AU XIX^{ème} SIÈCLE



Le jeune homme dont vous apercevez un portrait naît en 1811, obtient à 16 ans un premier prix au concours général, est refusé à l'X, écrit entre 17 et 18 ans son premier article de mathématiques, se range à 19 ans aux côtés des républicains activistes qui menacent (par la gauche) la souveraineté de Louis-Philippe (roi des français après la fuite de Charles X), est jugé le 14 juillet 1831, condamné à 6 mois de prison et sera tué en duel le 30 mai 1831, nous laissant un testament mathématique de première importance.

Le jeune homme dont vous apercevez un portrait naît en 1811, obtient à 16 ans un premier prix au concours général, est refusé à l'X, écrit entre 17 et 18 ans son premier article de mathématiques, se range à 19 ans aux côtés des républicains activistes qui menacent (par la gauche) la souveraineté de Louis-Philippe (roi des français après la fuite de Charles X), est jugé le 14 juillet 1831, condamné à 6 mois de prison et sera tué en duel le 30 mai 1831, nous laissant un testament mathématique de première importance. C'est le début de notre histoire !

Le jeune homme dont vous apercevez un portrait naît en 1811, obtient à 16 ans un premier prix au concours général, est refusé à l'X, écrit entre 17 et 18 ans son premier article de mathématiques, se range à 19 ans aux côtés des républicains activistes qui menacent (par la gauche) la souveraineté de Louis-Philippe (roi des français après la fuite de Charles X), est jugé le 14 juillet 1831, condamné à 6 mois de prison et sera tué en duel le 30 mai 1831, nous laissant un testament mathématique de première importance. C'est le début de notre histoire !

Nous allons un instant nous concentrer sur son héritage mathématique qui est, disons, le point de départ d'avancées technologiques actuelles que vous appréciez chaque jour sans exception, j'en prends le pari.

DE QUOI S'AGIT-IL ?

DE QUOI S'AGIT-IL ?

Niels Abels (Norvégien, 1802-1829) avait démontré que, *a contrario* des équations de degré 2, 3 ou 4, il n'était pas toujours possible de résoudre par quadrature une équation de degré inférieure ou égale à cinq. Il restait tout de même à donner un critère qui permettait de décider si oui ou non, une **équation algébrique**, c'est-à-dire du type

$$a_n X^n + a_{n-1} X^{n-1} + \dots + a_0 = 0$$

peut être résolue par une succession de quadratures. L'idée de génie de Galois illustre à merveille la démarche des mathématiciens lorsqu'ils sont en face d'une question ardue :

Tenter de formuler le problème autrement, pour le contourner,
l'aborder par une face par laquelle l'ascension est moins rude

La théorie disait déjà qu'il y avait n solutions, et Galois ne s'intéresse pas à la recherche des solutions elles-mêmes, mais plutôt à une famille de transformations qui laissent invariantes...

La théorie disait déjà qu'il y avait n solutions, et Galois ne s'intéresse pas à la recherche des solutions elles-mêmes, mais plutôt à une famille de transformations qui laissent invariantes...
les relations satisfaites par ces solutions.

La théorie disait déjà qu'il y avait n solutions, et Galois ne s'intéresse pas à la recherche des solutions elles-mêmes, mais plutôt à une famille de transformations qui laissent invariantes...
[les relations satisfaites par ces solutions.](#)

Le principe est le suivant.

- ▶ Il y a des relations qui relient les solutions et les coefficients a_n, \dots, a_0
- ▶ Il peut y en avoir d'autres. Plus il y en a, plus les solutions sont "proches" des coefficients et moins nous aurons besoin d'opérations pour les trouver, donc plus grande sera la chance que les solutions de l'équation puissent être obtenues au moyen de quadratures.
- ▶ Plus il y a de relations qui relient les solutions, moins il y a de chance qu'une permutation conserve ces relations (parce que certaines ne mettent pas en jeu *toutes* les solutions)

- ▶ Il existe évidemment des moyens pour trouver le groupe de Galois de certaines équations indépendamment de la connaissance des solutions de l'équation, et, à défaut de le déterminer explicitement, d'avoir suffisamment d'information sur sa structure pour décider si oui ou non il est possible d'exprimer les solutions de l'équation à partir des coefficients à l'aide de quadratures successives.

ENCORE UNE AVANCÉE IMPORTANTE DU JEUNE GALOIS.

Pour l'apprécier, il nous faut encore un petit effort. Mais c'est un effort auquel vous consentez au quotidien, (façon Monsieur Jourdain) lorsque vous regardez votre montre. Le cadran affiche les heures de 0 à 12, et vous pourriez me dire que, finalement,

ENCORE UNE AVANCÉE IMPORTANTE DU JEUNE GALOIS.

Pour l'apprécier, il nous faut encore un petit effort. Mais c'est un effort auquel vous consentez au quotidien, (façon Monsieur Jourdain) lorsque vous regardez votre montre. Le cadran affiche les heures de 0 à 12, et vous pourriez me dire que, finalement,

$$0 = 12.$$

ENCORE UNE AVANCÉE IMPORTANTE DU JEUNE GALOIS.

Pour l'apprécier, il nous faut encore un petit effort. Mais c'est un effort auquel vous consentez au quotidien, (façon Monsieur Jourdain) lorsque vous regardez votre montre. Le cadran affiche les heures de 0 à 12, et vous pourriez me dire que, finalement,

$$0 = 12.$$

Nous pouvons additionner, soustraire dans le nouvel ensemble formé où l'on ne considère que le reste de la division par 12, que l'on appelle l'ensemble des classes. Par exemple, s'il est 10h00, quatre heures plus tard il sera 2h et donc vous me dites que

$$10 + 4 = 2$$

ENCORE UNE AVANCÉE IMPORTANTE DU JEUNE GALOIS.

Pour l'apprécier, il nous faut encore un petit effort. Mais c'est un effort auquel vous consentez au quotidien, (façon Monsieur Jourdain) lorsque vous regardez votre montre. Le cadran affiche les heures de 0 à 12, et vous pourriez me dire que, finalement,

$$0 = 12.$$

Nous pouvons additionner, soustraire dans le nouvel ensemble formé où l'on ne considère que le reste de la division par 12, que l'on appelle l'ensemble des classes. Par exemple, s'il est 10h00, quatre heures plus tard il sera 2h et donc vous me dites que

$$10 + 4 = 2$$

De la même manière, si vous êtes seulement intéressés par le jour de la semaine (lundi, mardi, etc.), l'addition d'un multiple de 7 jours importe peu et vous devez calculer dans l'ensemble

$$\mathbb{Z}/7\mathbb{Z}$$

Dans l'ensemble $\mathbb{Z}/n\mathbb{Z}$, les additions, soustractions et multiplications sont permises, mais pas toujours les divisions. Par exemple, si $n = 12$

$$3 \times 4 = 12 = 0$$

alors que ni 3 ni 4 ne sont nuls. On ne pourra donc jamais inverser 3 ou 4 au sens de la multiplication, et ceci est un problème majeur. On pourra le faire si n est un nombre premier, et on obtient ainsi ce que les mathématiciens appellent un **corps fini** :

$$\mathbb{Z}/p\mathbb{Z}$$

avec p premier. Ce sont ces corps (les exemples les plus immédiats de corps finis - parce qu'il en existe d'autres), qui peuvent être appliqués à un problème tout à fait concret. Avant de le décrire...

UN PETIT INTERMÈDE

UN PETIT INTERMÈDE

Au bon souvenir de Camille et Perdican

Décryptons l'information

Pierre Repp cache avec habileté le texte d'Alfred de Musset. Ce dernier prend la plume en 1834 - un peu à contre coeur - pour s'ouvrir, entre les lignes d'une comédie, de la douleur causée par la rupture avec George Sand. La scène 5 de l'acte II, est une des plus connues. Nous y apprenons que...

Décryptons l'information

Pierre Repp cache avec habileté le texte d'Alfred de Musset. Ce dernier prend la plume en 1834 - un peu à contre coeur - pour s'ouvrir, entre les lignes d'une comédie, de la douleur causée par la rupture avec George Sand. La scène 5 de l'acte II, est une des plus connues. Nous y apprenons que...

Tous les hommes sont menteurs, inconstants, faux, bavards, hypocrites, orgueilleux et lâches, méprisables et sensuels ; toutes les femmes sont perfides, artificieuses, vaniteuses, curieuses et dépravées ;... ; mais il y a au monde une chose sainte et sublime, c'est l'union de deux êtres si imparfaits et si affreux...

LES CODES CORRECTEURS D'ERREURS

Le besoin de pouvoir corriger des erreurs dans la transmission de l'information est parfois crucial. Pensez par exemple à l'alphabet aéronautique (Alpha, Bravo, Charlie,...) qui exprime en creux la nécessité (vitale) de transmettre une information correcte.

LES CODES CORRECTEURS D'ERREURS

Le besoin de pouvoir corriger des erreurs dans la transmission de l'information est parfois crucial. Pensez par exemple à l'alphabet aéronautique (Alpha, Bravo, Charlie,...) qui exprime en creux la nécessité (vitale) de transmettre une information correcte.

Un message nous parvient souvent de manière erronée. Parfois, nous savons ce que notre interlocuteur (Pierre Repp) *a voulu dire*, c'est-à-dire qu'un processus mental nous permet à la fois :

- ▶ de **détecter** les erreurs contenues par le message,
- ▶ de **corriger** ces erreurs pour former le message que l'on a souhaité transmettre.

LES CODES CORRECTEURS D'ERREURS

Le besoin de pouvoir corriger des erreurs dans la transmission de l'information est parfois crucial. Pensez par exemple à l'alphabet aéronautique (Alpha, Bravo, Charlie,...) qui exprime en creux la nécessité (vitale) de transmettre une information correcte.

Un message nous parvient souvent de manière erronée. Parfois, nous savons ce que notre interlocuteur (Pierre Repp) *a voulu dire*, c'est-à-dire qu'un processus mental nous permet à la fois :

- ▶ de **détecter** les erreurs contenues par le message,
- ▶ de **corriger** ces erreurs pour former le message que l'on a souhaité transmettre.

Le principe de base du **code correcteur d'erreurs** est simple : on doit lui assigner les deux missions que nous venons de pointer : détecter puis corriger.

Aujourd'hui, la majorité des messages nous parvient sous forme...

Aujourd'hui, la majorité des messages nous parvient sous forme...

d'une succession de 0 et de 1

Aujourd'hui, la majorité des messages nous parvient sous forme...

d'une succession de 0 et de 1

Remarque : *Ce point de vue apparaît déjà dans les écrits de Leibniz ((1646-1716)...*

Aujourd'hui, la majorité des messages nous parvient sous forme...

d'une succession de 0 et de 1

Remarque : *Ce point de vue apparaît déjà dans les écrits de Leibniz ((1646-1716)...*

et chacun de ces zéros ou uns est appelé *binary digit* ou sous forme contractée : **bit**. Les $256 (= 2^8)$ **octets**, c'est-à-dire les successions de 8 symboles 0 ou 1 codent les principaux caractères typographiques utilisés (les lettres de l'alphabet, les signes de ponctuation, les caractères particuliers, etc).

L'information écrite n'est pas la seule à être numérisée.

- ▶ Le son l'est aussi : le son est une onde, qui se propage, avec pour effet d'augmenter ou de diminuer la densité de l'air à la fréquence de 440 fois par seconde (... à 440 chantent les musiciens...). L'onde de densité définit une fonction que l'on hache (les mathématiciens disent qu'ils la discrétisent). Sur un disque compact, le son est haché en...

L'information écrite n'est pas la seule à être numérisée.

- ▶ Le son l'est aussi : le son est une onde, qui se propage, avec pour effet d'augmenter ou de diminuer la densité de l'air à la fréquence de 440 fois par seconde (... à 440 chantent les musiciens...). L'onde de densité définit une fonction que l'on hache (les mathématiciens disent qu'ils la discrétisent). Sur un disque compact, le son est haché en...

44100 morceaux par seconde

L'information écrite n'est pas la seule à être numérisée.

- ▶ Le son l'est aussi : le son est une onde, qui se propage, avec pour effet d'augmenter ou de diminuer la densité de l'air à la fréquence de 440 fois par seconde (... à 440 chantent les musiciens...). L'onde de densité définit une fonction que l'on hache (les mathématiciens disent qu'ils la discrétisent). Sur un disque compact, le son est haché en...

44100 morceaux par seconde

et la valeur de la fonction en escalier sur chacune des fraction de ($\Delta = \frac{1}{44100}$) seconde est repérée sur une échelle de 2^{16} intensités possibles (Sony et Philips ont hésité entre 2^{14} et 2^{16} ...).

Livrons-nous à un petit calcul : À raison de 70mn par CD, en sachant que le son est reproduit en stéréo, il s'agira donc de transmettre fidèlement...

$$44100 \times 16 \times 2 \times 60 \times 70 = 5\,927\,040\,000 \text{ bits} \simeq 740 \text{ Mo}$$

$$44100 \times 16 \times 2 \times 60 \times 70 = 5\,927\,040\,000 \text{ bits} \simeq 740 \text{ Mo}$$

D' où l'intérêt de savoir corriger les erreurs, inévitables lors de la transmission de l'information (micro rayures, salissures, poussières, etc.).

$$44100 \times 16 \times 2 \times 60 \times 70 = 5\,927\,040\,000 \text{ bits} \simeq 740 \text{ Mo}$$

D' où l'intérêt de savoir corriger les erreurs, inévitables lors de la transmission de l'information (micro rayures, salissures, poussières, etc.).

- ▶ L'image est numérisée également, et elle nous apparaît sous forme de pixels, avec pour chacun - et pour une image noir et blanc - 2^8 niveaux de gris. Nous pourrions nous livrer à un calcul analogue pour connaître le nombre de méga-octets en jeu pour une petite image en noir et blanc, ou en couleur.

$$44100 \times 16 \times 2 \times 60 \times 70 = 5\,927\,040\,000 \text{ bits} \simeq 740 \text{ Mo}$$

D' où l'intérêt de savoir corriger les erreurs, inévitables lors de la transmission de l'information (micro rayures, salissures, poussières, etc.).

- ▶ L'image est numérisée également, et elle nous apparaît sous forme de pixels, avec pour chacun - et pour une image noir et blanc - 2^8 niveaux de gris. Nous pourrions nous livrer à un calcul analogue pour connaître le nombre de méga-octets en jeu pour une petite image en noir et blanc, ou en couleur.

Plusieurs systèmes de codages ont marqué - chacun à leur tour - une avancée significative, au plan théorique et bien entendu technologique.

- ▶ **Les codes de Hamming** ('50). Le principe : on ajoute au mot initial que l'on veut transmettre une information redondante qui permet par un phénomène (linéaire) d'inverser pour savoir où se trouvent les erreurs s'il y en a, et les corriger :

0011

On ajoute trois informations obtenues par des opérations élémentaires dans $\mathbb{Z}/2\mathbb{Z}$ - on somme les trois premiers bits - on somme les trois derniers bits - on somme les deux premières et la dernière.

- ▶ **Les codes de Hamming** ('50). Le principe : on ajoute au mot initial que l'on veut transmettre une information redondante qui permet par un phénomène (linéaire) d'inverser pour savoir où se trouvent les erreurs s'il y en a, et les corriger :

0011

On ajoute trois informations obtenues par des opérations élémentaires dans $\mathbb{Z}/2\mathbb{Z}$ - on somme les trois premiers bits - on somme les trois derniers bits - on somme les deux premières et la dernière. Cela donne

0011**101**

- ▶ **Les codes de Hamming** ('50). Le principe : on ajoute au mot initial que l'on veut transmettre une information redondante qui permet par un phénomène (linéaire) d'inverser pour savoir où se trouvent les erreurs s'il y en a, et les corriger :

0011

On ajoute trois informations obtenues par des opérations élémentaires dans $\mathbb{Z}/2\mathbb{Z}$ - on somme les trois premiers bits - on somme les trois derniers bits - on somme les deux premières et la dernière. Cela donne

0011**101**

S'il se présente un mot dont l'incorrection apparaît dans l'incohérence de la dernière présentation, le principe consiste à chercher des mots sans erreurs à proximité du mot présenté. Dans le cas présent, la redondance de l'information est construite par des opérations élémentaires. Ce code a servi pour la transmission de l'information à l'aide du Minitel.

- ▶ **Les codes de Reed et Solomon.** Ils sont, pour ce qui concerne les CD, très efficaces. Le Consultative Committee for Space Data System (créé en 1982) recommande ce code pour la transmission de données par satellites. Ils utilisent les calculs sur les polynômes qui ne font que représenter des mots à k lettres dans le corps

$$\mathbb{F}_{2^m}$$

L'encodage présente en général des erreurs et on utilise l'arithmétique sur les corps pour décoder les erreurs.

L'histoire ne s'arrête pas en si bon chemin. L'appréciation de l'efficacité d'un code dépend de l'utilisation que l'on en a. Les critères d'efficacité sont par exemple :

L'histoire ne s'arrête pas en si bon chemin. L'appréciation de l'efficacité d'un code dépend de l'utilisation que l'on en a. Les critères d'efficacité sont par exemple :

- ▶ La vitesse de transmission,

L'histoire ne s'arrête pas en si bon chemin. L'appréciation de l'efficacité d'un code dépend de l'utilisation que l'on en a. Les critères d'efficacité sont par exemple :

- ▶ La vitesse de transmission,
- ▶ La possibilité de commencer à corriger sans avoir l'intégralité du message,

L'histoire ne s'arrête pas en si bon chemin. L'appréciation de l'efficacité d'un code dépend de l'utilisation que l'on en a. Les critères d'efficacité sont par exemple :

- ▶ La vitesse de transmission,
- ▶ La possibilité de commencer à corriger sans avoir l'intégralité du message,
- ▶ Un bon compromis entre le volume de la redondance d'information (le plus petit possible) et leur efficacité (la plus grande possible) pour repérer et corriger les erreurs.

L'histoire ne s'arrête pas en si bon chemin. L'appréciation de l'efficacité d'un code dépend de l'utilisation que l'on en a. Les critères d'efficacité sont par exemple :

- ▶ La vitesse de transmission,
- ▶ La possibilité de commencer à corriger sans avoir l'intégralité du message,
- ▶ Un bon compromis entre le volume de la redondance d'information (le plus petit possible) et leur efficacité (la plus grande possible) pour repérer et corriger les erreurs.

Dans les années 50, des travaux ont montré l'existence théorique de codes correcteurs plus efficaces que le code de Hamming (qui lui est devenu un cas d'école), et, il y a une vingtaine d'années, de nouveaux codes très performants sont apparus, qui utilisent le calcul sur les corps de Galois différents et encore plus sophistiqués que ceux présentés.

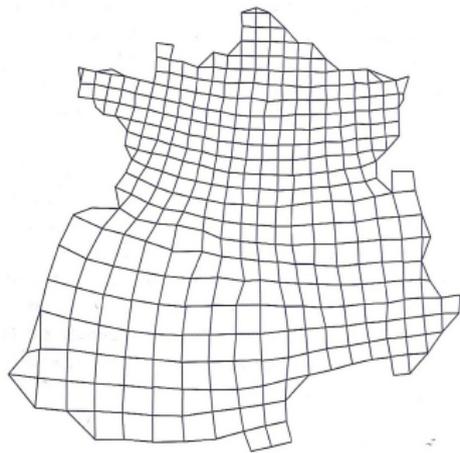
CE QUE J'AURAIS PU VOUS RACONTER

CE QUE J'AURAIS PU VOUS RACONTER

- ▶ **L'utilisation de mathématiques sophistiquées pour l'élaboration du GPS.**

CE QUE J'AURAIS PU VOUS RACONTER

- ▶ **L'utilisation de mathématiques sophistiquées pour l'élaboration du GPS.**
- ▶ **L'utilisation des mathématiques pour la prospection des énergies fossiles.**



?

- ▶ **L'utilisation des mathématiques en Sciences du vivant :**
génomique, biologie cellulaire, biologie animale, dynamique des populations, médecine santé, écologie et biodiversité.

- ▶ **L'utilisation des mathématiques en Sciences du vivant** : génomique, biologie cellulaire, biologie animale, dynamique des populations, médecine santé, écologie et biodiversité.
- ▶ **L'utilisation des mathématiques en sciences humaines et sociales** : Économie, finance, sociologie, politique.

This is one end

This is one end

but not *the* end !