À propos d'une question épineuse: À quoi ça sert les Mathématiques???

Par Mohamed Rachid HILALI

Jean Prestet (1648 - 1690) prêtre et Mathématicien Français a écrit dans la préface de son livre "Nouvaux éléments de Mathématiques" :

Je conseille l'étude des Mathématiques, parce que plusieurs expériences aussi bien que la raison m'ont pleinement convaicu qu'elles sont très utiles et même nécessaires non seulement dans les sciences et dans les arts, qui en tirent toute leur perfection ; mais aussi pour donner à l'esprit plus de force et plus d'étendue, et même pour régler en quelque sorte les mouvement du cœur . Car les sens, l'imagination, et les passions sont les sources générales des erreurs dans notre esprit, et du désordre ou de la corruption de notre cœur. Or l'étude des Mathématiques est très propre pour apprendre à dissiper les illusions des sens, à corriger le déréglement de l'imagination, et à modérer la fière impétuosité de nos passions. L'esprit et le cœur en deviennent donc plus purs, et mieux disposés à recevoir les vérités et les maximes saintes de la Religion.

1 Motivation

Motivation

À quoi servent les mathématiques ? Pourquoi on fait les mathématiques ? Voici des questions bien naturelles pour de jeunes étudiants universitaires. Les réponses de leurs professeurs sont, la plupart du temps, rapides. En effet, les cours, structurés et chargés ne permettraient de donner des exemples d'applications. Les mêmes questions sont posées dans les écoles d'enseignement secondaire avec plus d'insistance. Les professeurs de ces écoles ont évidemment la vie plus dure que les professeurs d'université. S'ils savent répondre de façon compétente à ces questions, c'est souvent qu'ils l'ont appris auprès de leurs formateurs. Et s'ils ne le savent pas, à qui la faute ?

Motivation

Dans cet exposé on va donner un survey sur l'importance des Mathématiques dans plusieurs domaines.

2 Sur le plan personnel:

Sur le plan personnel:

- Les Mathématiques apportent beaucoup de choses, elles contribuent essentiellement à:
- La purification du raisonnement
- Le développement de l'intuition et de la logique
- La régulation du flux des neuronnes
- La sélection par excellence des candidats aux concours.

3 Sur le plan technologique

Sur le plan technologique

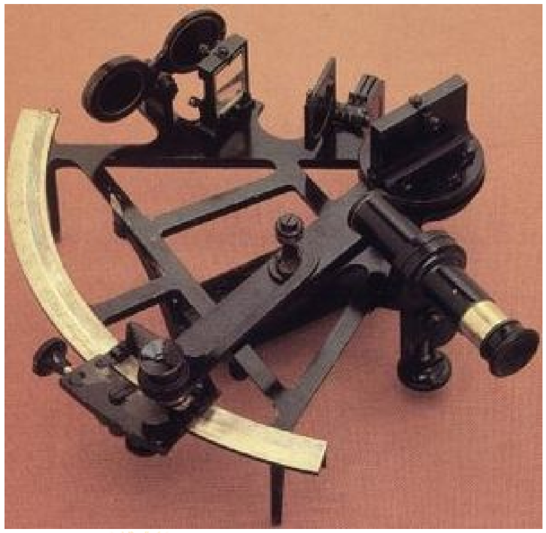
Les Mathématiques sont omniprésents dans le développement de nouvelles (et anciennes) technologies. Nous allons donner quelques exemples tangibles d'applications qui ont façonné l'environnement humain et sa compréhension.

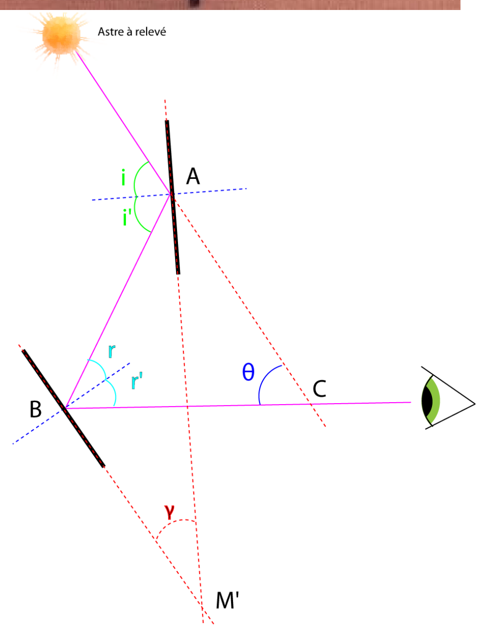
4 LE GPS

LE GPS (Global Positioning System)

Pour pouvoir déterminer la position d'un objet dans notre espace, l'Homme a uilisé au fil des temps plusieurs techniques citons par exemple:

- Le sextant en navigation qui détermine l'angle entre 2 points





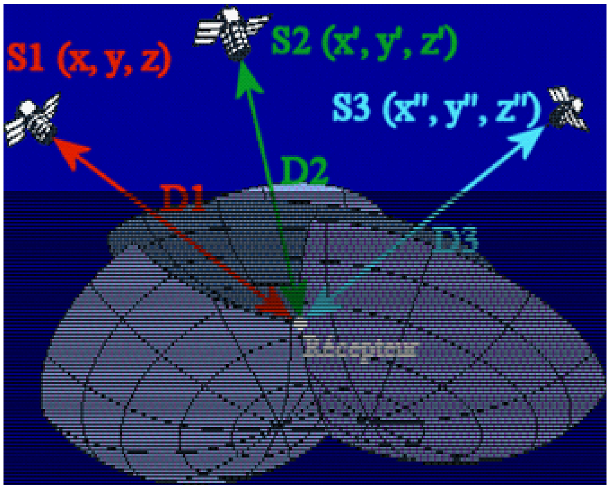
- La boussole magnétique

- L'astrolabe
- Le compas magnétique

Actuellement c'est l'ère du GPS

Prérequis Mathématiques: Géométrie euclidienne, systèmes d'équations linéaires ou non linéaires,corps finis

Nous allons décrire succinctement les fondements de son fonctionnement



Les satellites émettent des signaux répétés périodiquement.

Les signaux sont captés à l'aide du récepteur du GPS, qui captera le signal des satellites et calculera sa position.

Le récepteur a en mémoire un almanach, lequel contient la position prévue des satellites à chaque instant.

Lorsque le récepteur capte le signal d'un satellite, il se met lui-même à générer les signaux des différents satellites et il les compare avec les signaux reçus.

En général, les signaux ne concordent pas. Il translate alors les signaux qu'il génère jusqu'à ce qu'un des signaux qu'il génère soit en accord parfait avec le signal reçu (il mesure ceci en calculant la corrélation entre les deux signaux).

Il peut alors calculer le temps de parcours du signal depuis le satellite

Le GPS de coordonnées cartésiennes (x, y, z) se trouve sur la sphère de centre $A_i(a_i, b_i, c_i)$ position du satellite (S_i) capté et de rayon $D_i = c(T_i - \tau)$, où τ désigne le défaut de synchronisation de l'horloge ordinaire du GPS avec celles (de très haute précision: horloge atomique) des satellites, et T_i le temps affiché par le GPS. On a alors quatre inconnues x, y, z, τ à déterminer

Le système d'équations qui doit vérifier les coordonnées cartésiennes de la position du GSM est:

$$\begin{cases}(x-a_1)^2+(y-b_1)^2+(z-c_1)^2=c^2(T_1-\tau)^2\\(x-a_2)^2+(y-b_2)^2+(z-c_2)^2=c^2(T_2-\tau)^2\\(x-a_3)^2+(y-b_3)^2+(z-c_3)^2=c^2(T_3-\tau)^2\\(x-a_4)^2+(y-b_4)^2+(z-c_4)^2=c^2(T_4-\tau)^2\end{cases}$$

5 Signal du GPS et du satellite

Signal du GPS et du satellite

Prérequis Mathématiques: théorie des corps finis

Le GPS doit reconnaître chaque satellite, le localiser et déduire la distance associée, cette fonctionnalité repose sur l'émission, la réception des signaux et la génération de signaux periodiques.

Chaque satellite est codé par deux suites de r-uplets dans $\mathbb{F}_{2^r} \simeq (\mathbb{Z}/2\mathbb{Z})^r$, $(q_0, ..., q_{r-1})$ et $(a_0, ..., a_{r-1})$ (qui est émis de façon periodique) ayant les propriétés suivantes:

Par récurrence on construit la suite $(a_n)_{r\leq n}$ par: $a_n = \sum_{k=0}^{r-1} q_k a_{n-r+k,}$ on a évidemment $a_{n+2^r-1} = a_n$

Pour tout $n \geq r$, le registre à décalage du GPS génère la suite dite décalage: $u_n = (a_n, a_{n-1}, ..., a_{n-r}) \in \mathbb{F}_{2^r}$, et donne naissance aux (2^r-1)-uplets dites fenêtres $(0 \leq k \leq 2^r-1)$, $M_k = (a_k, a_{k+1}, ..., a_{k+2^r-2})$

Les propriétés exigées sont: $\mathbb{F}_{2^r} - \{0\} = \{u_n, n \geq r\}$ et la polynôme $P(x) = x^r + q_{r-1}x^{r-1} + ... + q_1 x + q_0$ est irréductibles dans $\mathbb{F}_2$

on démontre par la théorie des corps que de telles suites existent

La corrélation entre deux fenêtres $B = (b_1, ..., b_{2^r-1})$ et $C = (c_1, ..., c_{2^r-1})$ est définie par: $Cor(B,C) = Card\{i/b_i = c_i\} - Card\{i/b_i \neq c_i\}$. Un registre à décalage est mal corrélé si $Cor(B,C)$ est proche de 0 pour tous couple de fenêtres (B,C), ce qui permet au GPS de miex identifier le satellite. Pour le choix ci-dessus on a $Cor(B,C) = -1$.

6 Gestion des coups de foudre:

Gestion des coups de foudre:

Prérequis Mathématiques: ceux dux GPS, probabilité-statistique

Pour plusieurs raisons: installation électrique, installation des usines sensibles, transport électrique, préviion des catastrophes, la détection des zones à haut risque devient une nécessité. Une fois de plus les Mathématiques sont là pour remédier au problème, voyons comment

D'abord plusieurs GPS sont répartis sur plusieurs points et reliés à un système central, leurs position et leurs décalages sont données par un calcul statistique pour réduire les erreurs, ils sont parfaitement synchronisés entre eux et avec les satellites (ordre de l'erreur 100 nanosecondes près, ainsi ils peuvent envoyer une pulsation toutes les secondes au même instant.

Les coups de foudres génèrent des ondes électromagnétiques, lorsqu'ils sont interceptés par les GPS, le système central localise par triangulation leur position.

7 Cartographie:

Cartographie:

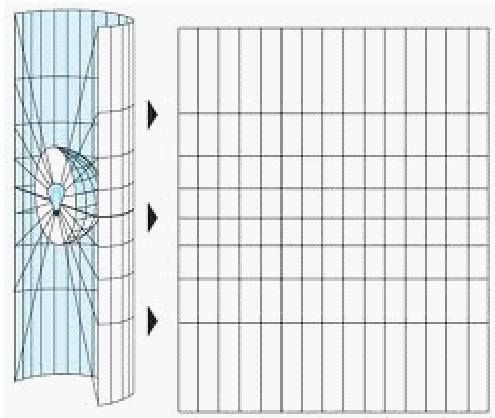
Prérequis Mathématiques: Géométrie différentielle

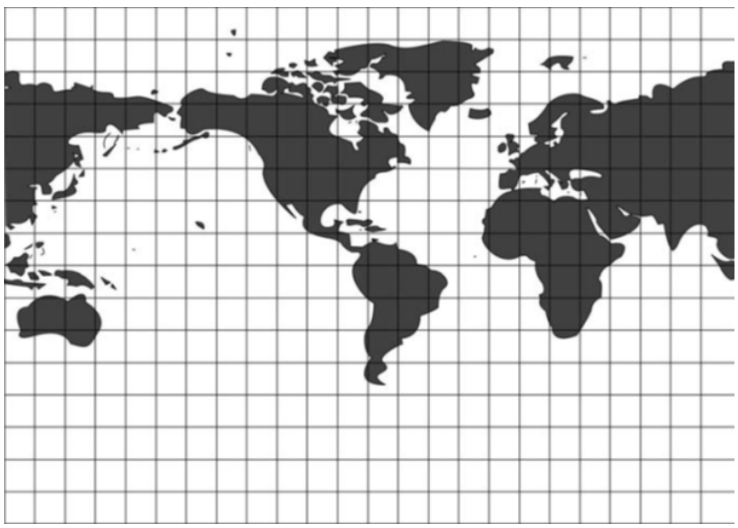
Le GPS utilise une carte pour pouvoir se diriger, alors comment on peut représenter cette carte

D'abord rappelons un théorème en Géométrie différentielle:on ne peut jamais cartographier une portion de sphère par une portion de plan en préservant les distances et les angles.

On utilise souvent la projection de Lambert sur le cylindre de base l'équateur et de génératrice perpendiculaire au plan équatoriale qui a l'avantage de préserver les aires:

Une autre projection dite de Mercator sur le cylindre, qui elle, conserve les angles





8 Cryptographie à clé publique

Cryptographie à clé publique: code RSA (Rivest-Shamir-Adleman) (cassé Janvier 2010)

Prérequis Mathématiques: Arithmétique

Échanger des informations demande souvent une sécurité totale

La manière alors est de crypter les messages, ce qui exige la connaissance du mode d'emploi entre l'expéditeur et le receveur, mais ceci présente présente beaucoup de risques lors de sa communication

L'idée géniale se repose sur le mode de fonctionnement entièrement publique du code.

Principe du code RSA qui a résisté 40 ans et qui est encore opérationnel:

Le receveur R (banque, institution, société de vente...) publie publiquement un grand nombre entier $n = pq$ qui se décompose comme produit de deux nombres premiers p et q gardés secrets (il est très difficile - même pour un ordinateur - de trouver p et q à partir de n)

R calcule $\Phi(n) = Card\{k \leq n \;/\; k$ et n sont premiers entre eux$\} = (p-1)(q-1)$ où Φ désigne la fonction d'Euler

R choisit une clé publique de cryptage $e \in \{1, ..., \Phi(n)\}$ premier avec $\Phi(n)$

La clé de décryptage est le nombre $d \in \{1, ..., \Phi(n)\}$ vérifiant $d.e \equiv 1[\Phi(n)]$

L'expéditeur écrit un message $m,$ le convertit en nombre décimal par exemple (selon la position de l'alphabet, de l'espace ou du chiffre),le découpé en r blocs $m_i \leq n-1,$ premiers avec $n,$ puis le crypte par $c = c_1\ c_2 ... c_r$ selon la relation $m_i^e \equiv c_i\ [n]$

R décrypte le message codé c par la relation $m_i \equiv c_i^d\ [n]$

9 Google

Google

Prérequis Mathématiques: réduction des matrices, probabilité, chaîne de Markov, théorie des graphe

Certes Google doit sa suprématie grace à l'algorithme PageRank

L'utilisation d'un moteur de recherche est simple. Quelqu'un, assis à un ordinateur relié à la Toile, désire connaître les meilleures sources d'information sur un sujet particulier.

Il choisit d'interroger le moteur de Google à l'aide de plusieurs mots en rapport avec le sujet.

Google parvient à ordonner les pages qu'il propose en mettant en premier celles qui sont les plus susceptibles de répondre aux

Alors comment Google a pu deviner les désirs de l'utilisateur?

Le principe fondamental de l'algorithme PageRank est l'ordonnancement des pages de la Toile qui tient compte de la structure des liens entre elles et non pas de leurs contenus et sont disposées sous forme de graphes orientés. Le parcours d'un chemin du graphe a pour probabilité 1.

Ceci peut être modélisé par une chaîne de Markov $(X_n)_{n \in \mathbb{N}},$ sa matrice de transition $T = (p_{ij} = P(X_n = i / X_{n-1} = j)$ est une matrice stochastique par colonne, c'est à dire $\sum_i p_{ij} = 1$

Toutes les valeurs propres de la matrice T sont dont le disque unité et 1 est une valeur propre

T possède un vecteur propre $\pi = (\pi_i) = \lim_{n\to\infty} T^n(P(X_0 = i))$ associé à la valeur propre $1,$ avec $\pi_i \geq 0$ et $\sum_i \pi_i = 1$

La page i sera affectée du rang π_i ce qui permet dde ranger les pages dans le résultat de recherche selon la grandeur de leur rang π_i.