Machines de Turing

La géométrie

- Descartes démontre l'équivalence géométrie euclidienne/géométrie analytique
- Lobai/Bolachevski/Riemman démontre l'indépendance du troisième axiome
- Différence entre axiomatique matérielle et axiomatique formelle

L’infini

- Galilée remarque que l’on peut mettre en bijection l’ensemble des entiers naturels et l’ensemble des carrés
- Cantor impose la notion de bijectivité pour dire « autant que » dans la théorie des ensembles
- Cantor pose les fondements des propriétés des cardinaux dits « transfinis »
- Le premier, aleph0, est le cardinal de N

Ensembles plus grands que N

- Cantor s'intéresse à l'ensemble des fonctions de N dans N
- Il suppose que l'on peut les énumérer et donc les numéroter sous la forme f_1, f_2, …., f_n,….
- Soit $f(i)=f_i(i)+1$
- f est une fonction de N dans N donc il existe un nombre n tel que pour tout i: $f(i)=f_n(i)$
- Mais alors on a aussi $f_n(n)=f(n)=f_n(n)+1$
- L'ensemble des fonctions de N dans N n'est pas énumérable

Paradoxe de Russel

- Soit E l'ensemble des ensembles qui ne se contiennent pas eux-mêmes.
- E se contient-il lui-même?
- Si E se contient lui-même alors par définition il ne se contient pas lui-même
- Si E ne se contient pas lui-même, alors il doit appartenir à E et donc se contenir
- Reformalisation de la théorie des ensembles par Goedel

Paradoxe de Berry

- Le plus petit nombre entier ne pouvant pas être exprimé en moins de quinze mots
- 1297297: un million deux cent quatre-vingt-dix-sept mille deux cent quatre-vingt-dix-sept
- Mais est aussi défini par la première phrase qui fait quatorze mots...
- Problème de l'utilisation du même langage pour décrire ce qui est observé.

Intuitionnistes

- Brouwer: Tous les objets mathématiques doivent se construire
- Pour un intuitionniste, pour prouver qu'il existe un objet possédant une propriété, il faut exhiber l'objet.
- Depuis 1918, les mathématiques intuitionnistes se sont développés parallèlement aux traditionnelles

Les formalistes

- Hilbert conduit les mathématiques vers un formalisme strict
- La propriété de consistance formelle demande simplement qu'à l'intérieur de la théorie formelle, on ne puisse avoir une formule qui soit démontrable et dont la négation soit démontrable (ce qui constituerait un paradoxe)

Décidabilité, calculabilité

- *Il existe une procédure algorithmique finie permettant de calculer en un nombre de pas fini sa valeur pour tout argument de son domaine.*
- *Il existe une procédure algorithmique finie permettant de résoudre n'importe laquelle des questions de cette classe en un nombre fini de pas.*

Alan Turing

- Mathématicien britannique qui s'intéresse au problème de la calculabilité
- Kleene-Church (1932/1935) définissent les fonctions lambda-calculables
- Godel (1934) présente les fonctions récursivement énumérables
- Godel (1936) démontre l'équivalence des deux notions

Turing calculabilité

- Une fonction Turing calculable est une fonction dont on est capable de construire une description algorithmique de calcul pour une machine de Turing
- En 1937, Turing démontre l'équivalence avec les fonctions lambda-calculables et les fonctions récursivement énumérables.

Machine de Turing déterministe

- Un ensemble de symboles
- Un ensemble d'états
- Un programme
- Une tête de lecture
- Une bande infinie de stockage
- On peut se contenter d'une machine à 2 symboles

F(x)=x+1

- (A,1,1,A,R): si la machine est dans l'état A, que la tête lit un 1, on écrit 1, on reste dans l'état A, et on va à droite.
- (A,0,0,A,R)
- (A, , ,B,L)
- (B,0,1,Z,S)
- (B,1,0,B,L)
- (B, ,1,Z,S)

Fonction Turing-calculable

- *Une fonction f définie sur un domaine* D *est Turing-calculable si nous pouvons construire une machine M telle que M appliquée à tout élément a de D calcule f(a)*

Dénombrabilité des machines de Turing

- Un programme de machine de Turing se compose d'une suite finie composée de symboles. On peut associer à ce programme un nombre appelé index de la machine de Turing.
- Les machines de Turing sont énumérables, et donc dénombrables, et on les note M_i

Fonction non calculable

- On désigne par $f_i(a)$ la fonction qui renvoie $M_i(a)$ si $M_i(a)$ existe
- On définit $g(a)=f_a(a)+1$ si $f_a(a)$ existe et $g(a)=0$ sinon.
- Si g est calculable, il existe une machine M_j qui la calcule et on a pour tout a $g(a)=f_j(a)$
- M_j calculant g, nous savons que $f_j(j)$ est calculable et donc $g(j)=f_j(j)=f_j(j)+1$
- g n'est donc pas calculable.

Le castor frénétique (busy beaver)

- Construire une machines de Turing a 2 symboles (B et 1) et n états qui écrit un maximum de 1 sur une bande blanche en s'arrétant
- On note $\Sigma(m)$ le nombre de 1 laissé sur la bande à la fin du calcul par la machine m
- On note: $\Sigma(n)=\max\{\Sigma(m)|m \in En\}$
- Σ est la fonction « busy beaver »

Quelques propriétés

- Φ n'est pas calculable en général
- Il est possible de trouver facilement des valeurs de Φ pour n=0, n=1, n=2. On peut la calculer pour n=3 et n=4, mais on ne connait pas le résultat pour n>4

Quelques valeurs

- □(2)=4
- □(3)=6
- □(4)=13 (107 étapes)
- □(5)=?4098 (47176870 étapes)
- □(6)□4.64 E 1439 (?)

Le problème de Post

- Soit les deux listes suivantes:
  - (aabb, ab, aab)
  - (bb, abaa, b)
- Peut-on construire une liste d'indices telle que la concaténation des éléments de la première liste est égale à la concaténation des éléments de la seconde?

Le problème de Post

- Reprenons les deux listes suivantes:
  - (aabb, ab, aab)
  - (bb, abaa, b)
- La solution est (2,3,2,1)
  - abaababaabb
- Peut-on trouver un algorithme résolvant le problème de Post?
- Non

Les équations diophantiennes

- *Un ensemble E de n-uplets* $(x_1, \ldots, x_n)$ *d'entiers positifs ou nuls est dit diophantien s'il existe un polynôme* $P(x_1, \ldots, x_n, y_1, \ldots, y_m)$ *à coefficients entiers tel que :*
- $(x_1, \ldots, x_n) \in E \Leftrightarrow \exists (y_1 \geq 0, \ldots, y_m \geq 0), P(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0$

Le dixième problème de Hilbert

- Trouver un algorithme permettant de déterminer si une équation polynomiale à coefficients entiers admet une solution entière
- En 1973, Davis démontre que ce problème est indécidable
- Ce résultat a des conséquences plus profondes

Exemple: les nombres premiers

$$
\begin{aligned}
Q(a,b,\ldots,x,y,z) = \\
&(k+2)(1-(wz+h+j-q)^2 \\
&-((gk+2g+k+1)(h+j)+h-z)^2 \\
&-(2n+p+q+z-e)^2-(16(k+1)^3(k+2)(n+1)^2+1-f^2)^2 \\
&-(e^3(e+2)(a+1)^2+1-o^2)^2-((a^2-1)y^2+1-x^2)^2 \\
&-(16r^2y^4(a^2-1)+1-u^2)^2 \\
&-(((a+u^2(u^2-a))^2-1)(n+4dy)^2+1-(x+cu)^2)^2 \\
&-(n+1+v+y)^2 \\
&-((a^2-1)l^2+1-m^2)^2-(ai+k+1-l-i)^2 \\
&-(p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m)^2 \\
&-(q+y(a-p-1)+s(2ap-p^2-2p-2)-x)^2 \\
&-(z+pl(a-p)+t(2ap-p^2-1)-pm)^2)
\end{aligned}
$$

Caractère aléatoire d'une série

- *Une suite de nombres est aléatoire si e plus petit algorithme capable de la construire est d'une taille équivalente à la taille de la suite. (Chaitin 1979)*
  - 1 3 5 7 9 11 13 15 17 19
  - 7 2 9 1 19 11 14 3 5 6
- Le nombre de bits du programme minimal permettant d'engendrer une série est appelé sa « complexité »

Le nombre Ω

- Soit Ω défini par:
  - « La probabilité d'arrêt d'un programme aléatoire pour un ordinateur donné. Le programme est une suite finie de 0 et de 1 qui ont été tirés à pile ou face. »
- Ω est aléatoire, il ne peut pas être exprimé par une séquence de bits plus courte que lui-même.

Machines de Turing non déterministes

- « Non déterminisme »: terme extrêmement mal choisi
- Il vaut mieux parler d'un calculateur disposant d'un nombre de processeurs « toujours suffisant » pour exécuter un programme susceptible de « brancher » à chaque étape