IFT-2002

Informatique Théorique

H14 - cours 7

Julien Marcil - julien.marcil@ift.ulaval.ca

David Hilbert 1862-1943

David Hilbert présente une liste de **10 problèmes** qui tenaient jusqu'alors les mathématiciens en échec.

Publiée après la tenue du congrès, la liste définitive comprendra 23 problèmes, aujourd'hui appelés les problèmes de Hilbert.

Ces problèmes vont influencer le cours des mathématiques du xx^{e} siècle. Certains sont encore non résolus.

Deuxième problème de Hilbert

Peut-on prouver la *cohérence* de l'arithmétique?

En d'autres termes, peut-on démontrer que les *axiomes* de l'arithmétique ne sont pas contradictoires?

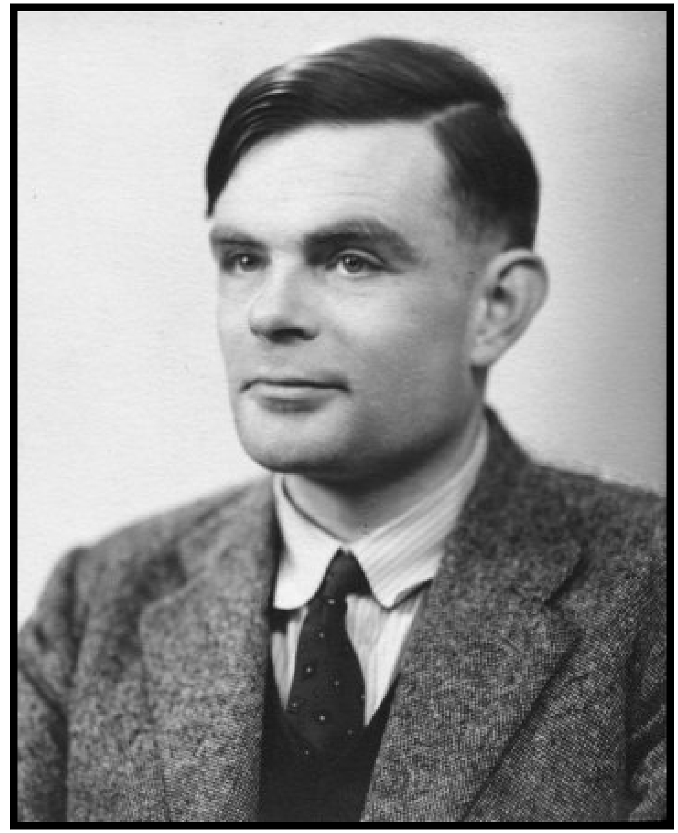
Kurt Gödel 1906-1978

En 1931, Kurt Gödel publie son théorème d'incomplétude.

Toute formalization des mathématiques contient des énoncés qui ne peut être ni *prouvé* ni *réfuté*.

Alan Turing 1912-1954

Alan Turing est l'auteur en 1936 d'un article de logique mathématique, qui présente une expérience de pensée, que l'on nommera ensuite **machine de Turing** et des concepts de programmation et de programme.



Ses travaux permettent résoudre le problème fondamental de la **décidabilité** en arithmétique.

Alonzo Church 1903-1995

Les travaux de Alonzo Church précèdent le travail d'Alan Turing sur le problème de l'arrêt.

C'est Church qui le premier a l'idée que l'on peut définir le concept de fonction calculable dans un sens très large.

Church démontre en 1936 l'existence d'un problème insoluble pen utilisant le **lambda-calcul**.

Emil Leon Post 1897-1954

Emil Leon Post introduit en 1946 le problème de correspondance de Post qui est **indécidable**.

Problème de correspondance de Post

Soit $\alpha_1, \cdots, \alpha_n$ et $\beta_1, \cdots, \beta_n$ des mots d'un alphabet Σ.

Ces mots forments des paires:

α_1	α_2	$\cdots$	α_n
β_1	β_2	$\cdots$	β_1

Exist-il une séquence de ces paires tel que

$$\alpha_{i_1}\alpha_{i_2}\cdots\alpha_{i_k} = \beta_{i_1}\beta_{i_2}\cdots\beta_{i_k}$$

Problème de correspondance de Post

Par exemple:

a	ab	bba
baa	aa	bb

Il existe la solution suivante:

bba	ab	bba	a
bb	aa	bb	baa
$i_1 = 3$	$i_2 = 3$	$i_3 = 3$	$i_4 = 3$

Dixième problème de Hilbert

Trouver un *algorithme* déterminant si une équation diophantienne a des solutions.

Par example, est-ce que

$$\begin{aligned} 3x^2y - 7y^2z^3 &= 18 \\ -7y^2 - 8z^2 &= 0 \end{aligned}$$

as des solutions entières?

Dixième problème de Hilbert

En 1970, Youri Matiiassevitch démontre qu'un tel algorithme ne peut exister : le dixième problème de Hilbert n'a pas de solution!

Conjecture de Syracuse

Soit l fonction f tel que

$$f(n) = \begin{cases} n/2 & \text{si } n \text{ est paire} \\ 3n+1 & \text{si } n \text{ est impaire} \end{cases}$$

Pour une valeur de n il est possible de produire une séquence de a_i tel que

$$a_i = \begin{cases} n & \text{si } i = 0 \\ f(a_{i-1}) & \text{si } i > 0 \end{cases}$$

Example

Pour $n = 6$ la séquence est:

6, 3, 10, 5, 16, 8, 4, 2, 1

Pour $n = 11$ la séquence est:

11, 34, 17, 52, 26, 13, 40, 20, 10, 5, 16, 8, 4, 2, 1

Example

Pour $n = 27$ la séquence est:

27, 82, 41, 124, 62, 31, 94, 47, 142, 71, 214, 107, 322, 161, 484, 242, 121, 364, 182, 91, 274, 137, 412, 206, 103, 310, 155, 466, 233, 700, 350, 175, 526, 263, 790, 395, 1186, 593, 1780, 890, 445, 1336, 668, 334, 167, 502, 251, 754, 377, 1132, 566, 283, 850, 425, 1276, 638, 319, 958, 479, 1438, 719, 2158, 1079, 3238, 1619, 4858, 2429, 7288, 3644, 1822, 911, 2734, 1367, 4102, 2051, 6154, 3077, 9232, 4616, 2308, 1154, 577, 1732, 866, 433, 1300, 650, 325, 976, 488, 244, 122, 61, 184, 92, 46, 23, 70, 35, 106, 53, 160, 80, 40, 20, 10, 5, 16, 8, 4, 2, 1

Conjecture de Syracuse

La conjecture affirme que, pour tout $n > 0$, il existe un indice k tel que $a_k = 1$.

Cours précédents

Grammaire

Définition: Une **grammaire** consiste en un quadruplet de la forme (V, Σ, S, R) où

- V est ensemble fini de *variables* (symboles non terminaux).
- Σ est *l'alphabet* (symboles terminaux).
- $S \in V$ est le *symbole de départ*.
- R est un ensemble fini de *règles de réécriture*.

Grammaire hors contexte

Définition: Soit $G = (V, \Sigma, S, R)$ une grammaire. G est **hors contexte** si les *règles de réécriture* respecte les restrictions suivantes:

- Les termes de gauche consistent en un seul symbole *non terminal*.

Langage hors contexte

Définition: Un langage est dit **hors contexte** (ou *non contextuelle*) s'il existe une grammaire hors contexte qui le génère.

Langage non hors contexte

Observation

Soit le langage $L = \{w \mid w$ contient le même nombre de a, de b et de $c\}$. Est-ce que L est hors contexte?

Lemme de pompage

Si L est un langage hors contexte, alors il existe un entier $p \geq 1$ (appelé longueur de pompage) tel que pour tout mot $w \in L$ avec $|w| \geq p$, il existe des mots u, v, x, y, z tels que $w = uvxyz$ et

1. $|vxy| \leq p$
2. $|vy| > 0$
3. pour tout entier $i \geq 0$ on a $uv^ixy^iz \in L$

Preuve qu’un langage L est non hors contexte

Pour prouver qu’un langage est non hors contexte, on fait une preuve par contradiction.

- On suppose que L est hors contexte.
- Donc il existe p la longueur de pompage de L.
- On *choisi* un mot $w \in L$, avec $|w| \geq p$ (qu'il ne sera pas possible de pomper).
- On montre qu'en pompant w, on génère des mots qui ne sont pas dans L.

Exemple

Prouver que le langage $L = \{a^n b^n c^n \mid n \geq 0\}$ n'est pas hors contexte.

Exemple

Prouver que le langage $L = \{a^i b^j c^k \mid 0 \leq i \leq j \leq k\}$ n'est pas hors contexte.

Exemple

Prouver que le langage $L = \{1^n 0^n 1^n 0^n \mid n \geq 0\}$ n'est pas hors contexte.

Exemple

Prouver que le langage

$$L = \{w\#t \mid w \text{ est un sous-chaîne de } t,\ \text{où } w,t \in \{a,b\}^*\}$$

n'est pas hors contexte.

Exemple

Soit $L_1 = \{w \mid w$ est un palindrome $\}$ et soit $L_2 = \{w \mid w$ contient le même nombre de 0 et de $1\}$.

Prouver que le langage $L_1 \cap L_2$ n'est pas hors contexte.