Histoire des algorithmes
L'émergence de la notion de calculabilité

Pierre Lescanne

dernière mise à jour: *25 septembre 2008 – 17 h 40*

Plan

Le dixième problème de Hilbert

Dans son 10^{eme} problème (1900) devant le *deuxième congrès des mathématiciens*, Hilbert demandait un algorithme pour déterminer si les systèmes d'équations diophantiennes ont une solution ou non.

Le dixième problème de Hilbert

Dans son 10^{eme} problème (1900) devant le *deuxième congrès des mathématiciens*, Hilbert demandait un algorithme pour déterminer si les systèmes d'équations diophantiennes ont une solution ou non.

Sa formulation est précisément :

> 10. Détermination de la solubilité des équations diophantiennes.
>
> *Étant donnée une équation avec un nombre quelconque de quantités inconnues et avec de coefficients qui sont des nombres entiers rationnels : Trouver un procédé qui peut déterminer par un nombre fini d'opérations, si l'équation est soluble dans les entiers rationnels.*

Le dixième problème de Hilbert

En formulation moderne.

Existe-t-il une algorithme ?

DONNÉES : Un polynôme $P(X_1, ..., X_n) \in \mathbb{Z}[X_1, ..., X_n]$
(c'est-à-dire à n variables et à coefficients dans $\mathbb{Z}$).

RÉSULTATS : Un n-uple $(a_1, ..., a_n) \in \mathbb{Z}^n$
tel que $P(a_1, ..., a_n) = 0$.

Le dixième problème de Hilbert

La réponse au dixième problème de Hilbert n'a été donnée qu'en 1970 par Youri Matiyasévitch après vingt ans d'efforts

Le dixième problème de Hilbert

La réponse au dixième problème de Hilbert n'a été donnée qu'en 1970 par Youri Matiyasévitch après vingt ans d'efforts (auxquelles ont participé Julia Robinson, Martin Davis et Hilary Putnam).

Le dixième problème de Hilbert

La réponse au dixième problème de Hilbert n'a été donnée qu'en 1970 par Youri Matiyasévitch après vingt ans d'efforts (auxquelles ont participé Julia Robinson, Martin Davis et Hilary Putnam).

Elle est négative !

Le dixième problème de Hilbert

La réponse au dixième problème de Hilbert n'a été donnée qu'en 1970 par Youri Matiyasévitch après vingt ans d'efforts (auxquelles ont participé Julia Robinson, Martin Davis et Hilary Putnam).

Elle nécessite la formalisation de la calculabilité !

Un exemple parmi d'autres

Dans un article (en français) intitulé Sur les systèmes d'équations aux dérivées partielles, *Journal de mathématiques*, (Tome III), (1920), Maurice Janet traite de ce que nous appellerions aujourd'hui le calcul symbolique.

Un exemple parmi d'autres

Dans un article intitulé Sur les systèmes d'équations aux dérivées partielles, *Journal de mathématiques*, (Tome III), (1920), Maurice Janet traite de ce que nous appellerions aujourd'hui le calcul symbolique.

Il écrit

> *Nous indiquons un procédé régulier pour reconnaître au bout d'un nombre fini d'opérations si un système donné est complètement intégrable.*
>
> *Nous montrons d'ailleurs que tout système peut se ramener par un procédé régulier à une forme canonique complètement intégrable.*

Un exemple parmi d'autres

Dans un article intitulé Sur les systèmes d'équations aux dérivées partielles, *Journal de mathématiques*, (Tome III), (1920), Maurice Janet traite de ce que nous appellerions aujourd'hui le calcul symbolique.

Il écrit

> *Nous indiquons un procédé régulier pour reconnaître au bout d'un nombre fini d'opérations si un système donné est complètement intégrable.*
>
> *Nous montrons d'ailleurs que tout système peut se ramener par un procédé régulier à une forme canonique complètement intégrable.*

Plan

Der Entscheidungproblem

En 1922, Hilbert pose le problème de la décision :
der Entscheidungproblem

Tester en un nombre fini d'étapes si une expression formelle se déduit d'un système d'axiomes donné.

Der Entscheidungproblem

En 1922, Hilbert pose le problème de la décision :
der Entscheidungproblem

> *Tester en un nombre fini d'étapes si une expression formelle se déduit d'un système d'axiomes donné.*
>
> *Le problème de la décision est l'un des principaux problèmes de la logique mathématique.*
> *... en logique du premier ordre, la découverte d'une procédure de décision générale est un problème difficile non encore résolu.*

D. Hilbert, W. Ackermann, *Principes de logique théorique* (1928)

Le programme du congrès de 1928

Lors du congrès de 1928, Hilbert énonce un programme sous forme de problèmes et pose trois questions fondamentales sur les mathématiques.

Le programme du congrès de 1928

Lors du congrès de 1928, Hilbert énonce un programme sous forme de problèmes et pose trois questions fondamentales sur les mathématiques :

La complétude,

La cohérence,

La décidabilité.

Plan

La complétude

Les mathématiques sont-elles complètes ?

Tout énoncé mathématique valide peut-il être démontré ?

La cohérence

Les mathématiques sont-elles cohérentes ou consistantes ?

Est-il impossible de démontrer toutes les propositions en mathématiques ?

ou ce qui est équivalent

Est-il impossible de démontrer en mathématique une proposition et son contraire ?

La décidabilité

Existe-il une procédure qui permet de décider si un énoncé mathématique est valide ou non ?

La décidabilité

Existe-il une procédure qui permet de décider si un énoncé mathématique est valide ou non ?

Une procédure de décision d'une propriété répond oui ou non.
Une procédure de semi-décision d'une propriété

- répond oui si la propriété est satisfaite
- et boucle ou échoue si la propriété n'est pas satisfaite

Plan

L'arithmétique de Presburger

L'arithmétique de Presburger est la théorie du «premier ordre» des entiers naturels avec l'addition (mais sans la multiplication).
En 1929, Presburger a démontré que :

- elle est décidable,
- elle est cohérente,
- elle est complète.

L'arithmétique de Presburger

L'arithmétique de Presburger est la théorie du «premier ordre» des entiers naturels avec l'addition (mais sans la multiplication).
En 1929, Presburger a démontré que :

- elle est décidable,
- elle est cohérente,
- elle est complète.

Ceci est faux pour l'arithmétique de Peano, avec addition **et** multiplication.

L'arithmétique de Presburger

L'arithmétique de Presburger est la théorie du «premier ordre» des entiers naturels avec l'addition (mais sans la multiplication).
En 1929, Presburger a démontré que :

- elle est décidable,
- elle est cohérente,
- elle est complète.

Ceci est faux pour l'arithmétique de Peano, avec addition **et** multiplication.

En 1974, Fischer et Rabin ont démontré que chaque algorithme que l'on pourrait construire aurait pour certaines formules de taille n un temps de calcul de l'ordre de $2^{2^{cn}}$ pour une certaine constante n.

La géométrie élémentaire

La question qui s'est posée tout au long du 19ème est de savoir s'il existait un algorithme pour décider si un théorème de géométrie était valide ou non.

Or la théorie de la géométrie se ramène à celle des formules sur les nombres réels.

Tarski a montré que la théorie du premier ordre des nombres réels est décidable.

Complétude et incomplétude

Gödel a montré la complétude de la logique du premier ordre.

Gödel a démontré l'incomplétude l'arithmétique.

Plan

Qu'est-ce qu'une fonction calculable ?

Intuitivement, une fonction calculable est une fonction pour laquelle, il existe un procédé mécanique pour produire ses valeurs à partir de se paramètres.

Indécidabilité et calculabilité : première tentatives

Dans la démonstration de son théorème d'incomplétude, Gödel a introduit une notion de fonction calculable.

Gödel(1930) introduit une notion de fonctions calculables générales.

Sa définition ne capture pas complètement la notion de fonction calculable.

Il fait une autre tentative sur une suggestion de Herbrand introduite dans un cours a Princeton.

Indécidabilité et calculabilité

Church et Kleene donnent des définitions générales équivalentes des fonctions

Indécidabilité et calculabilité

Church et Kleene donnent des définitions générales équivalentes des fonctions calculables. Ils distinguent une première classe les

fonctions récursives primitives

et une classe plus générale les fonctions récursives.

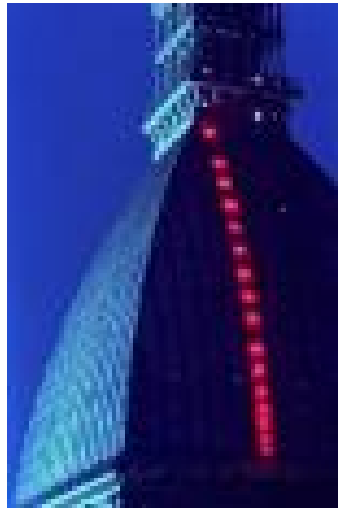
Une fonction récursive primitive

La fonction qui définit la suite de Fibonacci :

$$\begin{aligned} F_0 &= 0 \\ F_1 &= 1 \\ F_{n+2} &= F_{n+1} + F_n \end{aligned}$$

s'exprime aussi sous la forme

$$\begin{aligned} F_n &= fib(n, 1, 0) \\ fib(0, x, y) &= y \\ fib(n+1, x, y) &= fib(n, y, x+y). \end{aligned}$$



Une autre fonction récursive primitive

Le *pgcd* dans sa version avec soustraction

$$\begin{aligned} pgcd(m,n) &= pgcd(m-n,n) && \text{si } m > n \\ pgcd(m,n) &= pgcd(m,n-m) && \text{si } m < n \\ pgcd(m,n) &= m && \text{si } m|n \end{aligned}$$

et sa version avec division

$$\begin{aligned} pgcd(m,n) &= pgcd(m \bmod n,n) && \text{si } m > n \\ pgcd(m,n) &= pgcd(m,n \bmod m) && \text{si } m < n \\ pgcd(m,n) &= m && \text{si } m|n \end{aligned}$$

Une fonction non récursive primitive
la fonction d'Ackermann-Peter

La fonction Ackermann-Peter est l'archétype de la fonction récursive qui n'est pas une fonction récursive primitive.

$$\begin{aligned} Ack(0,n) &= n+1 \\ Ack(m+1,0) &= Ack(m,1) \\ Ack(m+1,n+1) &= Ack(m,Ack(m+1,n)). \end{aligned}$$

Une fonction non récursive primitive
la fonction d'Ackermann-Peter

La fonction Ackermann-Peter est l'archétype de la fonction récursive qui n'est pas une fonction récursive primitive.

$$\begin{aligned} Ack(0,n) &= n+1 \\ Ack(m+1,0) &= Ack(m,1) \\ Ack(m+1,n+1) &= Ack(m,Ack(m+1,n)). \end{aligned}$$

Wilhelm Ackermann (1896-1962)
Rózsa Peter (1905-1977).

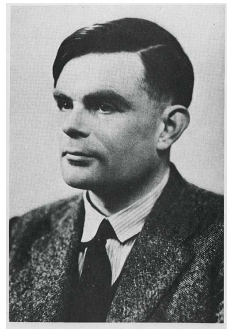
$$
\begin{aligned}
Ack(3,3) &= Ack(2, Ack(3,2)) \\
&= Ack(2, Ack(2, Ack(3,1))) \\
&= Ack(2, Ack(2, Ack(2, Ack(3,0)))) \\
&= Ack(2, Ack(2, Ack(2, Ack(2,1)))) \\
&= Ack(2, Ack(2, Ack(2, Ack(1, Ack(2,0))))) \\
&= Ack(2, Ack(2, Ack(2, Ack(1,3)))) \\
&= Ack(2, Ack(2, Ack(2, Ack(0, Ack(1,2))))) \\
&= Ack(2, Ack(2, Ack(2, Ack(0, Ack(0, Ack(1,1)))))) \\
&= Ack(2, Ack(2, Ack(2, Ack(0, Ack(0, Ack(0, Ack(1,0))))))) \\
&= Ack(2, Ack(2, Ack(2, Ack(0, Ack(0, Ack(0, Ack(0,1))))))) \\
&= Ack(2, Ack(2, Ack(2, Ack(0, Ack(0, Ack(0,2)))))) \\
&= Ack(2, Ack(2, Ack(2, Ack(0, Ack(0,3))))) \\
&= Ack(2, Ack(2, Ack(2, Ack(0,4)))) \\
&= Ack(2, Ack(2, Ack(2,5))) \\
&= Ack(2, Ack(2, Ack(1, Ack(2,4)))) \\
&= \ldots
\end{aligned}
$$

$$
\begin{aligned}
Ack(3,3) &= Ack(2, Ack(3,2)) \\
&= Ack(2, Ack(2, Ack(3,1))) \\
&= Ack(2, Ack(2, Ack(2, Ack(3,0)))) \\
&= Ack(2, Ack(2, Ack(2, Ack(2,1)))) \\
&= Ack(2, Ack(2, Ack(2, Ack(1, Ack(2,0))))) \\
&= Ack(2, Ack(2, Ack(2, Ack(1,3)))) \\
&= Ack(2, Ack(2, Ack(2, Ack(0, Ack(1,2))))) \\
&= Ack(2, Ack(2, Ack(2, Ack(0, Ack(0, Ack(1,1)))))) \\
&= Ack(2, Ack(2, Ack(2, Ack(0, Ack(0, Ack(0, Ack(1,0))))))) \\
&= Ack(2, Ack(2, Ack(2, Ack(0, Ack(0, Ack(0, Ack(0,1))))))) \\
&= Ack(2, Ack(2, Ack(2, Ack(0, Ack(0, Ack(0,2)))))) \\
&= Ack(2, Ack(2, Ack(2, Ack(0, Ack(0,3))))) \\
&= Ack(2, Ack(2, Ack(2, Ack(0,4)))) \\
&= Ack(2, Ack(2, Ack(2,5))) \\
&= Ack(2, Ack(2, Ack(1, Ack(2,4)))) \\
&= \ldots
\end{aligned}
$$

Elle croit extrêmement vite !

Plan

Turing



Turing (1936) propose un modèle calculatoire des processus de décision fondé sur des machines abstraites : les machines de Turing.

Il démontre l'indécidabilité de l'arrêt des machines de Turing. Il démontre l'indécidabilité de la logique du premier ordre.

Turing

Après avoir envoyé son article *On Computable Numbers, with an application to the Entscheidungsproblem* pour publication, Turing écrit à sa mère

> *Dans le même temps, un article est paru en Amérique, par Alonzo Church, qui fait la même chose mais de façon différente. Monsieur Newman et moi avons décidé que cependant la méthode est suffisamment différente pour permettre aussi la publication de mon article. Alonzo Church vit à Princeton, je suis par conséquent tout-à-fait décidé à aller là-bas.*

La machine de Turing universelle

Turing montre qu'il existe une machine universelle,
c'est-à-dire une machine

- qui prend en entrée le codage $\overline{M}$ d'une machine M et le codage $\overline{P}$ de nombres $(p_1, ..., p_n)$
- et qui simule le comportement de la machine M sur les entrées $(p_1, ..., p_n)$.

L'indécidabilité de l'arrêt

Supposons qu'il existe une machine qui décide si une machine M s'arrête sur une entrée E ou non.
On construit une machine D comme suit

$D(\overline{M})$

Si M s'arrête sur $\overline{M}$ *alors* boucler

sinon s'arrêter.

L'indécidabilité de l'arrêt

$D(\overline{D})$ conduit à une **contradiction**.
Si D s'arrête sur $\overline{D}$ alors D boucle.
Si D ne s'arrête pas sur $\overline{D}$ alors D s'arrête.

Post

En même temps que Turing, Post propose un autre modèle calculatoire pour démontrer l'indécidabilité de l'arrêt.

Markov

En URSS, Markov propose aussi un modèle de la calculabilité.

Tarski

Tarski est le premier a exhiber une théorie indécidable[1].

Dans son livre *Undecidable theories* (1953), avec Mostowski et Robinson, il montre que

- la théorie des groupes,
- la théorie des treillis,
- la géométrie projective

sont indécidables. Il a en revanche montré (1948) que la théorie des nombres réels et donc que la géométrie élémentaire sont décidables.

[1] Avant Post et Turing

La thèse de Church

Les notions de fonctions calculables qui ont été formalisées

1. sont équivalentes,
2. capturent la notion intuitive de fonctions calculables (ou de procédure de calcul).

La thèse de Church

Les notions de fonctions calculables qui ont été formalisées

1. sont équivalentes,
2. capturent la notion intuitive de fonctions calculables (ou de procédure de calcul).

La thèse de Church n'est pas un résultat mathématique.
C'est une affirmation de nature philosophique.

Le procédé diagonal

Les preuves d'indécidabilité et d'incomplétude sont fondés sur le même principe diagonal.

Une citation de Tarski

Dans une conférence donnée à Harvard en 1940, Tarski a dit :

> *La solution du problème de la décision dans sa forme la plus générale est négative. Il est certain qu'à l'écoute de cette information beaucoup de mathématiciens ont exprimé un profond soulagement. Probablement certains dans leurs nuits d'insomnie ont pensé avec horreur au moment où un mathématicien sournois trouverait une solution positive et construirait une machine qui résoudrait n'importe quel problème mathématique complètement mécaniquement ... Le danger est écarté, les mathématiciens peuvent dormir tranquillement.*

Plan

Le problème de correspondance de Post

Un des premiers problèmes indécidables simple

Superbe terrain, superbes tes reins ;
Amerindien, amer Indien

MC Solar

Louise de Vilmorin

Elle sort là-bas des menthes,
La belle Ève à l'âme hantée
Et le sort l'abat démente.
L'abbé laid va lamenter.

Alphonse Allais

Alphonse Allais, de l'âme erre et se f... à l'eau.
Ah ! L'fond salé de la mer ! Hé ! ce fou ! Allo !

Aidé, j'adhère au quai. Lâche et rond, je m'ébats,
Et déjà des roquets lâchés rongent mes bas.

Entrée de mon éléphant, Séraphine, et du rat bleu,
Entre Edmond et les faons, c'est raffiné, durable.

Si, mon fils, ton tutu raccommodé part.
Simon, fiston, tu tueras comme au départ.

Problème de correspondance de Post

Un ensemble $(\alpha_1, \beta_1), ..., (\alpha_n, \beta_n)$

où α_i et β_i sont des suites de lettres sur un alphabet A

est appelé un problème de correspondance de Post.

Une holorime est formée

- d'un mot w
- et d'une suite $(i_1, ..., i_p)$ d'entiers

tels que

$$w = \alpha_{i_1} ... \alpha_{i_p} = \beta_{i_1} ... \beta_{i_p}.$$

A la Alphonse Allais

L'art efface. Olé l'ami !
La Ré Fa Sol et La Mi.

issu du problème de correspondance suivant :

(ar,	ami,	é,	fas,	l,	olé)
(ré,	mi,	fa,	sol,	la,	é)

Deux correspondances proviennent des listes de rang

- (5, 1, 3, 4, 6)
- et (5, 1, 3, 4, 6, 5, 2).

A la Alphonse Allais

L'art efface. Olé l'ami !
La Ré Fa Sol et La Mi.

issu du problème de correspondance suivant :

(ar,	ami,	é,	fas,	l,	olé)
(ré,	mi,	fa,	sol,	la,	é)

Deux correspondances proviennent des listes de rang

- (5, 1, 3, 4, 6)
- et (5, 1, 3, 4, 6, 5, 2).

Il y a aussi une correspondance beaucoup plus simple !

A la Victor Hugo

1. (ala, tour)
2. (aman, dela)
3. (dela, rène)
4. (gal, galaman)
5. (magnanime, anime)
6. (rène, ala)
7. (tour, magn)

Une holorime est galamandelarènealatourmagnanime avec la suite (4,2,3,6,1,7,5).

Gal, amant de la reine, alla, tour magnanime,
Galamment de l'arène, à la tour Magne, à Nîmes.
Victor Hugo

Des exemples

Les problèmes de correspondance ci-dessous :

i	α_i	β_i
1	010	101
2	00	000
3	101	10

1

i	α_i	β_i
1	101	10
2	11	011
3	011	101

2

ont-ils une holorime ?

Des exemples (encore)

Et ceux là ?

i	α_i	β_i
1	011	1
2	1	0
3	0	011
4	10	001

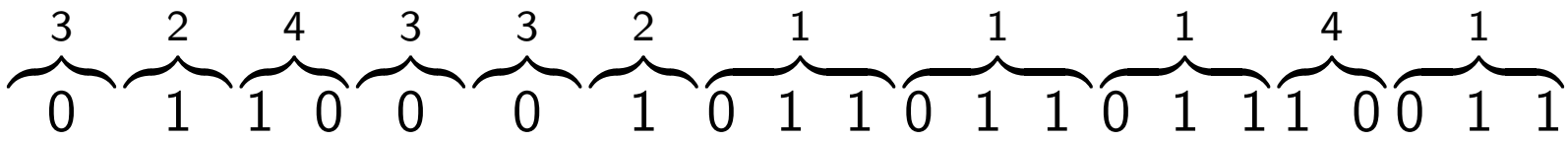
3

i	α_i	β_i
1	000	0
2	0	111
3	11	0
4	10	100

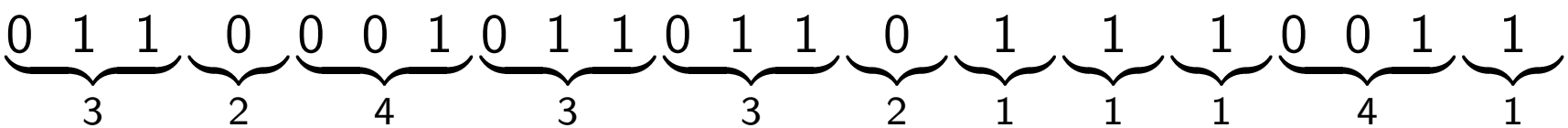
4

ont-ils une holorime ?

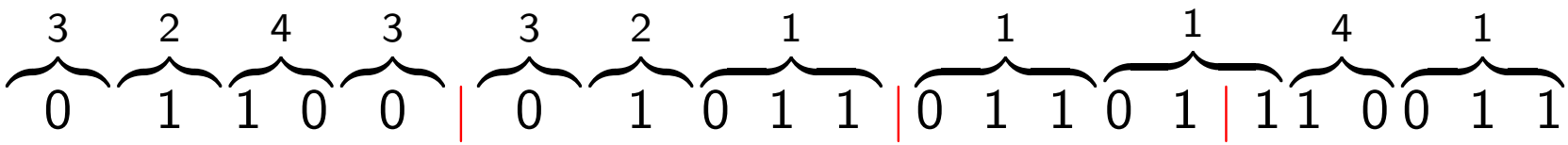
Le problème 3 a pour solution



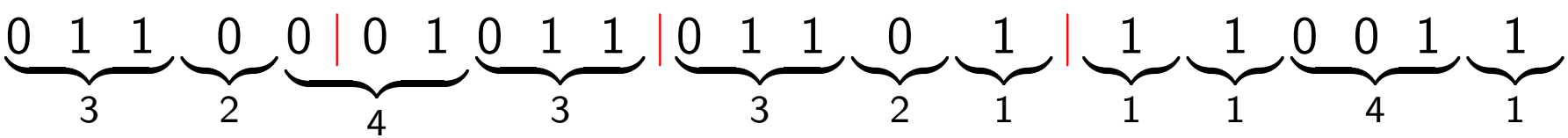
et



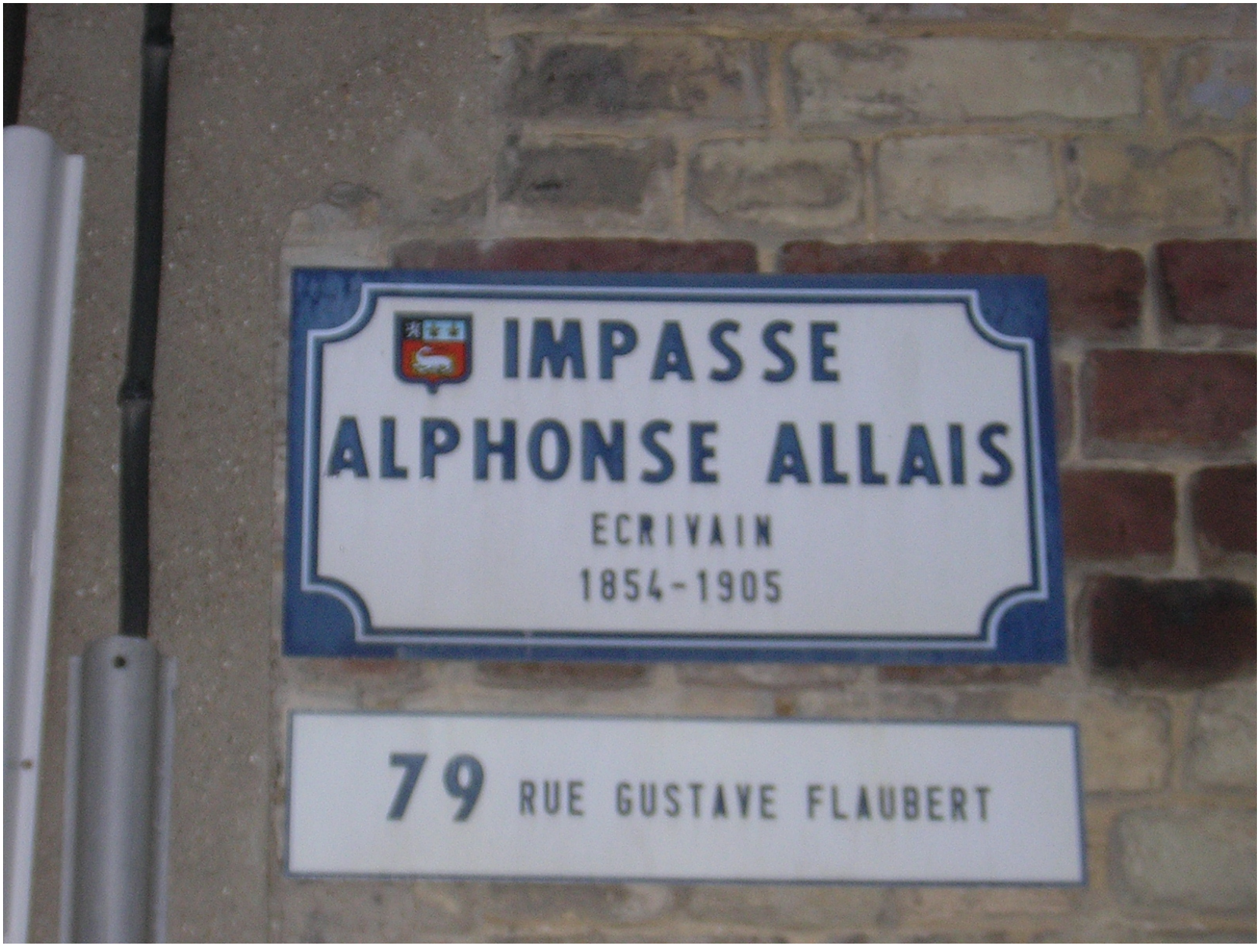
Le problème 3 a pour solution



et



La plus petite solution du problème 4 est de taille 204.


IMPASSE
ALPHONSE ALLAIS
ECRIVAIN
1854-1905
79 RUE GUSTAVE FLAUBERT

Le problème de correspondance de Post (ou PCP) est indécidable, à partir de deux éléments dans A.

Autrement dit, il n'y a pas d'algorithme avec

- entrée : un PCP sur deux lettres
- sortie : le problème a une holorime ou le problème n'a pas d'holorime .

Plan

Problèmes polynomiaux ou $\mathcal{P}$

Les problèmes pour lesquels il existe un algorithme qui s'exécute en un temps de l'ordre de n^p

- où n est la taille des données
- et p et un entier quelconque

sont dit polynomiaux et forment la classe $\mathcal{P}$

Problèmes $\mathcal{NP}$

Un problème est dans la classe $\mathcal{NP}$ si ses solutions sont vérifiables en temps polynomial.

$\mathcal{P} = \mathcal{NP}$ ou $\mathcal{P} \neq \mathcal{NP}$?

La conjecture $\mathcal{P} = NP?$ a été posée en même temps (1970) et indépendamment par Levin et Cook.

Karp a popularisé le problème en donnant une liste d'une cinquantaine de problèmes $\mathcal{NP}$-complets
c'est-à-dire de problèmes se ramenant les uns aux autres tels que si ces problèmes sont vérifiables en temps polynomial alors $\mathcal{P} = NP$.

$\mathcal{P} = \mathcal{NP}$ ou $\mathcal{P} \neq \mathcal{NP}$?

La conjecture $\mathcal{P} = NP?$ a été posée en même temps (1970) et indépendamment par Levin et Cook.

Karp a popularisé le problème en donnant une liste d'une cinquantaine de problèmes $\mathcal{NP}$-complets
c'est-à-dire de problèmes se ramenant les uns aux autres tels que si ces problèmes sont vérifiables en temps polynomial alors $\mathcal{P} = NP$.

Considéré comme l'un des problèmes de mathématiques les plus difficiles avec la conjecture de Riemmann et la conjecture de Poincaré.

Il est le 3ème dans une liste de 18 problèmes dressée par le mathématicien Steven Smale.

Plan

Bibliographie générale

Cette bibliographie ne cherche pas à être exhaustive.

- Jean-Luc Chabert et. al. Histoire d'algorithmes, Belin, (1993)[2],
- A Hodges, Alan Turing : The Enigma (1983). *en français* Alan Turing ou l'énigme de l'intelligence, Payot (1988).
- Gianbruno Guerrerio Gödel, Pour la Science, les génies de la science, Trimestriel août 2004 - novembre 2004.
- Anita Burdman Feferman, Solomon Feferman Alfred Tarski : Life and Logic Cambridge University Press, 2004.
- `http://www-groups.dcs.st-and.ac.uk/~history/` Pages web sur la vie des mathématiciens.

[2] Comporte des erreurs.

Films et vidéoconférences

- Ron Howard, Un homme d'exception, (2001), film, Un film décrivant la vie à Princeton à cette époque
- Le rôle des erreurs dans le développement des mathématiques par Étienne Ghys, Chercheur en Mathématiques, ENS Lyon jeudi 3 mai 2001,
  `http://www.ens-lyon.fr/asso/groupe-seminaires/`
  Une conférence sur l'histoire du 16ème problème de Hilbert.

Bibliographie scientifique

Des livres scientifiques qui présentent les concepts.

- D. van Dalen. Logic and Structure. Springer Verlag, (1994).
- Lewis, H. R. et Papadimitriou, Ch. H., Elements of the theory of computation, Prentice Hall, (1981).
- Y. Matiyasevich, Hilbert's tenth problem, MIT Press, (1993)
  Le dixième problème de Hilbert, Dunod.
- Nicolas Hermann et Pierre Lescanne Est-ce que «P = NP» ?
  Les dossiers de La Recherche, N°20, Août-Octobre 2005.