

IF228 - Calculabilité et Complexité

Cours #3 : indécidabilité

Frédéric Herbreteau

`frederic.herbreteau@bordeaux-inp.fr`

(d'après les supports de Corentin Travers)

8 janvier 2025

Indécidabilité

Expressivité des machines de Turing

Existe-t-il des fonctions non calculables ?

- **Automates finis** : a^*b^* ✓ $\{a^n b^n \mid n \in \mathbb{N}\}$ ✗

Expressivité des machines de Turing

Existe-t-il des fonctions non calculables ?

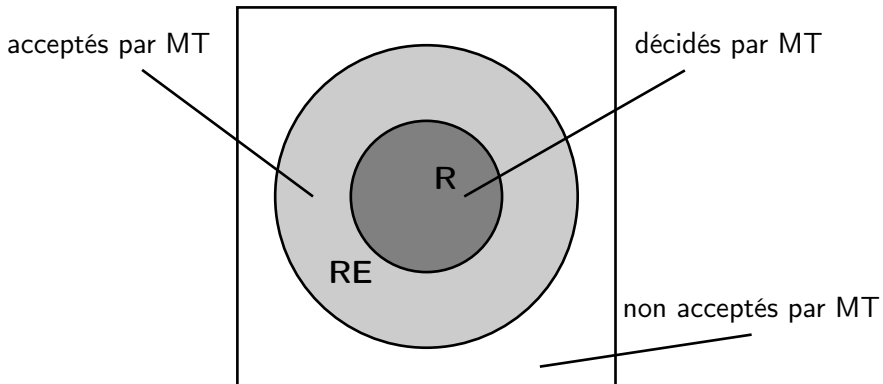
- **Automates finis** : a^*b^* ✓ $\{a^n b^n \mid n \in \mathbb{N}\}$ ✗
- **Automates à pile** : $\{a^n b^n \mid n \in \mathbb{N}\}$ ✓ $\{a^n b^n c^n \mid n \in \mathbb{N}\}$ ✗

Expressivité des machines de Turing

Existe-t-il des fonctions non calculables ?

- **Automates finis** : a^*b^* ✓ $\{a^n b^n \mid n \in \mathbb{N}\}$ ×
- **Automates à pile** : $\{a^n b^n \mid n \in \mathbb{N}\}$ ✓ $\{a^n b^n c^n \mid n \in \mathbb{N}\}$ ×
- **Machines de Turing** : $\{a^n b^n c^n \mid n \in \mathbb{N}\}$ ✓ ???

Classification des langages



Plan :

- ❶ Il existe un langage $L_{\bar{d}} \notin RE$
- ❷ Il existe un langage $L_u \in RE$ mais $L_u \notin R$

Un langage qui n'est pas RE

Théorème

*Il existe un langage $L_{\bar{d}}$ qui n'est **accepté** par **aucune** machine de Turing*

$$L_{\bar{d}} = \{\alpha \in \{0, 1\}^* \mid M_{\alpha} \text{ n'accepte pas } \alpha\}$$

Rappel : M_{α} est la machine de Turing encodée par α

Diagonalisation pour $L_{\overline{d}}$

α	ϵ	0	1	00	01	10	...
ϵ							...
0							...
1							...
00							...
01							...
10							...
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Diagonalisation pour $L_{\vec{d}}$

	α	ϵ	0	1	00	01	10	...
$\langle M_{\epsilon} \rangle =$	ϵ							...
$\langle M_0 \rangle =$	0							...
$\langle M_1 \rangle =$	1							...
$\langle M_{00} \rangle =$	00							...
$\langle M_{01} \rangle =$	01							...
$\langle M_{10} \rangle =$	10							...
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Diagonalisation pour $L_{\vec{d}}$

α	ϵ	0	1	00	01	10	...
$\langle M_{\epsilon} \rangle = \epsilon$	0	0	1	0	1	1	...
$\langle M_0 \rangle = 0$							...
$\langle M_1 \rangle = 1$							...
$\langle M_{00} \rangle = 00$							...
$\langle M_{01} \rangle = 01$							...
$\langle M_{10} \rangle = 10$							...
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

- M_{ϵ} accepte α (1) ou non (0) ?

Diagonalisation pour $L_{\vec{d}}$

	α	ϵ	0	1	00	01	10	...
$\langle M_{\epsilon} \rangle =$	ϵ	0	0	1	0	1	1	...
$\langle M_0 \rangle =$	0	1	1	0	0	1	0	...
$\langle M_1 \rangle =$	1	1	0	0	0	0	1	...
$\langle M_{00} \rangle =$	00	1	1	1	1	0	1	...
$\langle M_{01} \rangle =$	01	0	0	0	0	0	0	...
$\langle M_{10} \rangle =$	10	0	1	1	1	1	0	...
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

- M_{ϵ} accepte α (1) ou non (0) ?

Diagonalisation pour $L_{\vec{d}}$

	α	ϵ	0	1	00	01	10	...
$\langle M_{\epsilon} \rangle =$	ϵ	0	0	1	0	1	1	...
$\langle M_0 \rangle =$	0	1	1	0	0	1	0	...
$\langle M_1 \rangle =$	1	1	0	0	0	0	1	...
$\langle M_{00} \rangle =$	00	1	1	1	1	0	1	...
$\langle M_{01} \rangle =$	01	0	0	0	0	0	0	...
$\langle M_{10} \rangle =$	10	0	1	1	1	1	0	...
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

- M_{ϵ} accepte α (1) ou non (0) ?
- **Diagonale** : M_{α} accepte sa propre description α ?

Diagonalisation pour $L_{\bar{d}}$

	α	ϵ	0	1	00	01	10	...
$\langle M_{\epsilon} \rangle =$	ϵ	0	0	1	0	1	1	...
$\langle M_0 \rangle =$	0	1	1	0	0	1	0	...
$\langle M_1 \rangle =$	1	1	0	0	0	0	1	...
$\langle M_{00} \rangle =$	00	1	1	1	1	0	1	...
$\langle M_{01} \rangle =$	01	0	0	0	0	0	0	...
$\langle M_{10} \rangle =$	10	0	1	1	1	1	0	...
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

- M_{ϵ} accepte α (1) ou non (0)?
- Diagonale : M_{α} accepte sa propre description α ?
- Complément : $L_{\bar{d}} = \{\alpha \mid M_{\alpha} \text{ n'accepte pas } \alpha\}$

$L_{\bar{d}}$ n'est pas RE

Théorème

Le langage $L_{\bar{d}} = \{\alpha \mid M_{\alpha} \text{ *n'accepte pas* } \alpha\}$ *n'est pas*
récursivement énumérable

$L_{\bar{d}}$ n'est pas RE

Théorème

Le langage $L_{\bar{d}} = \{\alpha \mid M_{\alpha} \text{ *n'accepte pas* } \alpha\}$ *n'est pas*
récursivement énumérable

Preuve

Supposons $L_{\bar{d}}$ accepté par MT $M_{\bar{d}}$:

$L_{\bar{d}}$ n'est pas RE

Théorème

Le langage $L_{\bar{d}} = \{\alpha \mid M_{\alpha} \text{ n'accepte pas } \alpha\}$ n'est pas récursivement énumérable

Preuve

Supposons $L_{\bar{d}}$ accepté par MT $M_{\bar{d}}$:

	α	ϵ	$\dots$	w	$\dots$
$\langle M_{\epsilon} \rangle =$	ϵ	0	$\dots$	1	$\dots$
	$\vdots$	$\vdots$	$\dots$	$\vdots$	$\dots$
$\langle M_{\bar{d}} \rangle =$	w	0	$\dots$	?	$\dots$
	$\vdots$	$\vdots$	$\dots$	$\vdots$	$\ddots$

$L_{\bar{d}}$ n'est pas RE

Théorème

Le langage $L_{\bar{d}} = \{\alpha \mid M_{\alpha} \text{ n'accepte pas } \alpha\}$ n'est pas récursivement énumérable

Preuve

Supposons $L_{\bar{d}}$ accepté par MT $M_{\bar{d}}$:

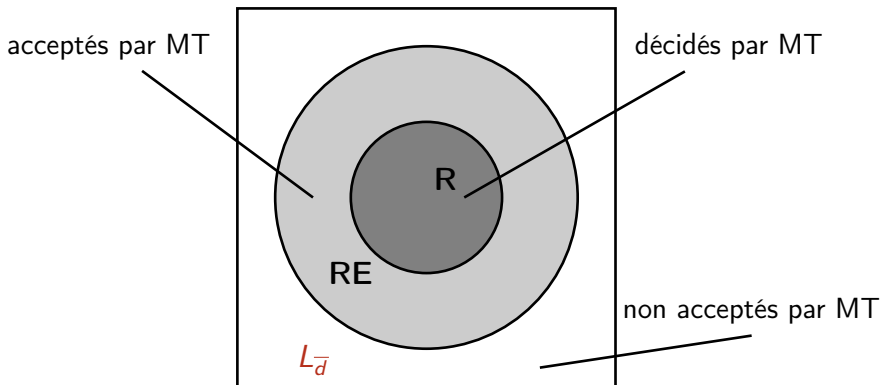
	α	ϵ	$\dots$	w	$\dots$
$\langle M_{\epsilon} \rangle =$	ϵ	0	$\dots$	1	$\dots$
	$\vdots$	$\vdots$	$\dots$	$\vdots$	$\dots$
$\langle M_{\bar{d}} \rangle =$	w	0	$\dots$	?	$\dots$
	$\vdots$	$\vdots$	$\dots$	$\vdots$	$\ddots$

Contradiction :

$M_{\bar{d}}$ accepte $w \implies w \notin L_{\bar{d}} \implies M_{\bar{d}}$ n'accepte pas $L_{\bar{d}}$

$M_{\bar{d}}$ n'accepte pas $w \implies w \in L_{\bar{d}} \implies M_{\bar{d}}$ n'accepte pas $L_{\bar{d}}$

$L_{\bar{d}}$ n'est accepté par aucune MT



Plan :

- ❶ Il existe un langage $L_{\bar{d}} \notin RE$ ✓
- ❷ Il existe un langage $L_u \in RE$ mais $L_u \notin R$

Un langage qui est RE mais pas R

Théorème

*Il existe un langage L_u qui n'est **décidé** par **aucune** machine de Turing*

$$L_u = \{ \langle M, w \rangle \mid M \text{ accepte } w \}$$

NB : $\langle M, w \rangle$ est un encodage binaire de l'entrée (M, w)

Exemple : " $\langle M \rangle 0 w$ " si $\langle M \rangle$ se termine par au moins trois 1

L_u est RE

Théorème

Le langage $L_u = \{\langle M, w \rangle \mid M \text{ accepte } w\}$ est *récursivement énumérable* (accepté par une MT)

Preuve

L_u n'est pas R

Théorème

Le langage $L_u = \{\langle M, w \rangle \mid M \text{ accepte } w\}$ n'est *pas récursif*
(décidable)

L_U n'est pas R

Théorème

Le langage $L_U = \{\langle M, w \rangle \mid M \text{ accepte } w\}$ n'est *pas récursif* (*décidable*)

Preuve

- Supposons L_U **décidé** par MT M_U

L_u n'est pas R

Théorème

Le langage $L_u = \{\langle M, w \rangle \mid M \text{ accepte } w\}$ n'est *pas récursif* (*décidable*)

Preuve

- Supposons L_u **décidé** par MT M_u
- Soit D la machine qui sur entrée $\alpha \in \{0, 1\}^*$:
 - ① exécute M_u sur $\langle M_\alpha, \alpha \rangle$ **NB : termine !**
 - ② accepte si M_u rejette, et rejette si M_u accepte

NB : D accepte $\alpha \iff M_u$ rejette $\langle M_\alpha, \alpha \rangle$

L_U n'est pas R

Théorème

Le langage $L_U = \{\langle M, w \rangle \mid M \text{ accepte } w\}$ n'est *pas récursif* (décidable)

Preuve

- Supposons L_U **décidé** par MT M_U
- Soit D la machine qui sur entrée $\alpha \in \{0, 1\}^*$:
 - ① exécute M_U sur $\langle M_\alpha, \alpha \rangle$ **NB : termine !**
 - ② accepte si M_U rejette, et rejette si M_U accepte

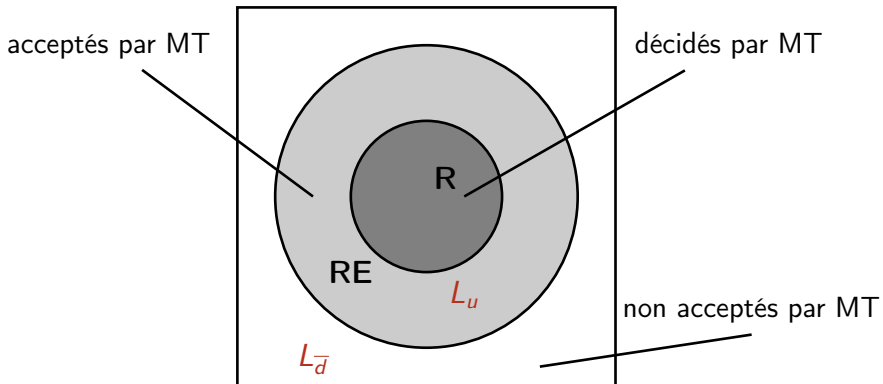
NB : D accepte $\alpha \iff M_U$ rejette $\langle M_\alpha, \alpha \rangle$

- **Contradiction :**

D accepte $\langle D \rangle \implies M_U$ rejette $\langle D, \langle D \rangle \rangle \implies D$ n'accepte pas $\langle D \rangle$

D rejette $\langle D \rangle \implies M_U$ accepte $\langle D, \langle D \rangle \rangle \implies D$ accepte $\langle D \rangle$

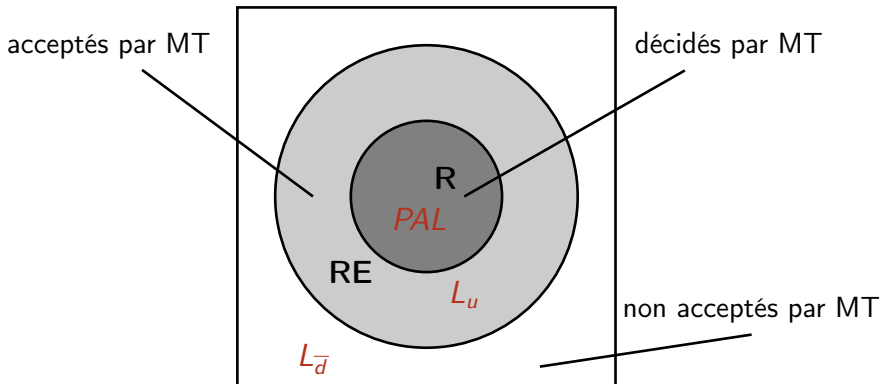
L_u n'est décidé par aucune MT



Plan :

- ❶ Il existe un langage $L_d \notin RE$ ✓
- ❷ Il existe un langage $L_u \in RE$ mais $L_u \notin R$ ✓

L_u n'est décidé par aucune MT



Plan :

- ❶ Il existe un langage $L_d^- \notin RE$ ✓
- ❷ Il existe un langage $L_u \in RE$ mais $L_u \notin R$ ✓

Quelques problèmes indécidables

Équations Diophantiennes (IIIème s.)

$$P(x_1, x_2, \dots, x_n) = 0$$

- P polynôme à **coefficients entiers**
- On cherche des **solutions entières**

Équations Diophantiennes (IIIème s.)

$$P(x_1, x_2, \dots, x_n) = 0$$

- P polynôme à **coefficients entiers**
- On cherche des **solutions entières**

Exemples :

- $aX + bY = 1$
- $W^3 + X^3 = Y^3 + Z^3$ solution $12^3 + 1^3 = 9^3 + 10^3 = 1729$
- $X^n + Y^n = Z^n$ pas de solution $X, Y, Z > 0$ pour $n \geq 3$
(Fermat)

10ème Problème de Hilbert (1900)

Problème de décision DIOPHANTE

- **ENTRÉE** : $P(X_1, \dots, X_n)$ polynôme à coefficients entiers
- **SORTIE** :
$$\begin{cases} 1 & \text{si } P(X_1, \dots, X_n) \text{ admet une solution entière} \\ 0 & \text{sinon} \end{cases}$$

10ème Problème de Hilbert (1900)

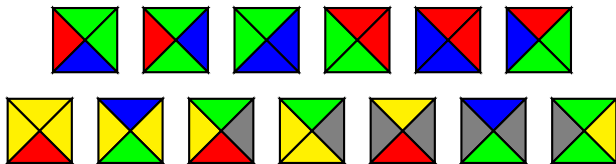
Problème de décision DIOPHANTE

- **ENTRÉE** : $P(X_1, \dots, X_n)$ polynôme à coefficients entiers
- **SORTIE** :
$$\begin{cases} 1 & \text{si } P(X_1, \dots, X_n) \text{ admet une solution entière} \\ 0 & \text{sinon} \end{cases}$$

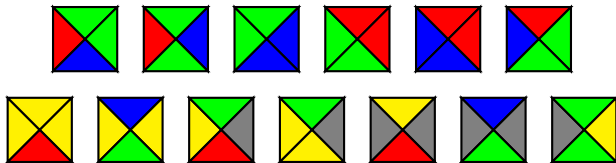
Théorème (Matiyasevich 1970)

DIOPHANTE est indécidable

Carreaux de Wang (1961)

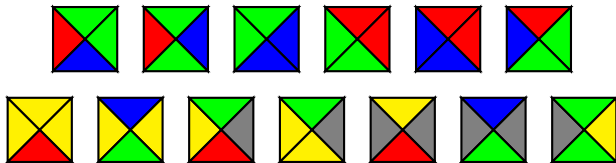


Carreaux de Wang (1961)



Pavage : rotations interdites, bords adjacents de même couleur

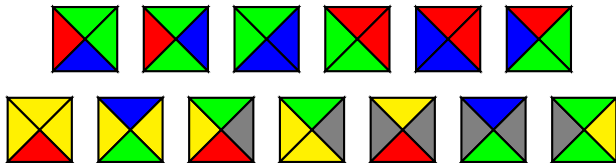
Carreaux de Wang (1961)



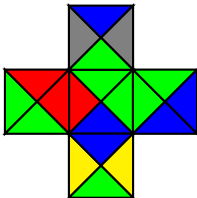
Pavage : rotations interdites, bords adjacents de même couleur



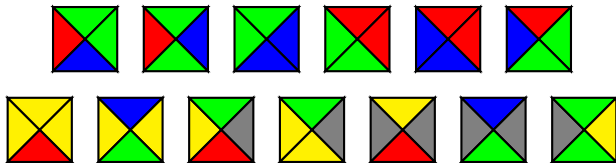
Carreaux de Wang (1961)



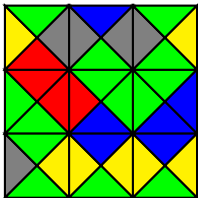
Pavage : rotations interdites, bords adjacents de même couleur



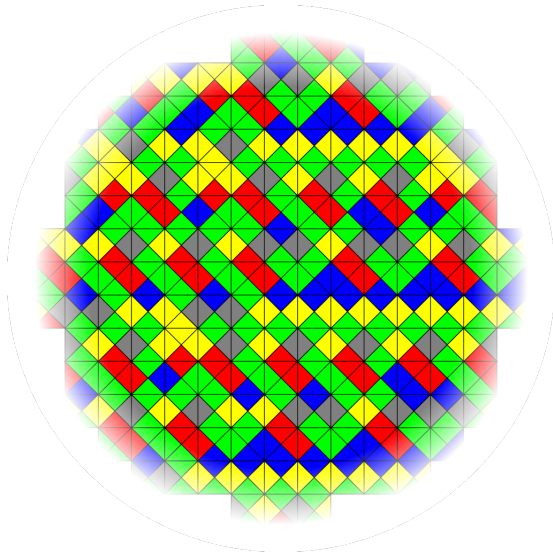
Carreaux de Wang (1961)



Pavage : rotations interdites, bords adjacents de même couleur



Carreaux de Wang



Carreaux de Wang

Problème de decision WANG

- **ENTREE** : ensemble fini S de carreaux
- **SORTIE** :
$$\begin{cases} 1 & \text{s'il existe un pavage du plan avec } S \\ 0 & \text{sinon} \end{cases}$$

Carreaux de Wang

Problème de décision WANG

- **ENTREE** : ensemble fini S de carreaux
- **SORTIE** :
$$\begin{cases} 1 & \text{s'il existe un pavage du plan avec } S \\ 0 & \text{sinon} \end{cases}$$

Théorème (Berger 1966)

Le problème WANG est indécidable

Carreaux de Wang

Problème de decision WANG

- **ENTREE** : ensemble fini S de carreaux
- **SORTIE** :
$$\begin{cases} 1 & \text{s'il existe un pavage du plan avec } S \\ 0 & \text{sinon} \end{cases}$$

Théorème (Berger 1966)

Le problème WANG est indécidable

Mais il existe des pavages **apériodiques** du plan par carreaux de Wang

Correspondance de Post (1946)

Un ensemble fini de dominos :

10	00	01
1	000	1

Problème de correspondance :

- Les mots en haut et en bas doivent correspondre
- Chaque domino peut être joué autant de fois que l'on veut

Correspondance de Post (1946)

Un ensemble fini de dominos :

10	00	01
1	000	1

Problème de correspondance :

- Les mots en haut et en bas doivent correspondre
- Chaque domino peut être joué autant de fois que l'on veut

10	00	01
1	000	1

×

Correspondance de Post (1946)

Un ensemble fini de dominos :

10
1

00
000

01
1

Problème de correspondance :

- Les mots en haut et en bas doivent correspondre
- Chaque domino peut être joué autant de fois que l'on veut

10	00	01
1	000	1

×

10	00	00	01
1	000	000	1

✓

Correspondance de Post (1946)

Un ensemble fini de dominos :

10	00	01
1	000	1

Problème de correspondance :

- Les mots en haut et en bas doivent correspondre
- Chaque domino peut être joué autant de fois que l'on veut

10	00	01
1	000	1

 ✗

10	00	00	01
1	000	000	1

 ✓

00	01
000	1

 ✓

Correspondance de Post (1946)

Problème de decision PCP

- **ENTREE** : ensemble fini D de dominos
- **SORTIE** :
$$\begin{cases} 1 & \text{s'il existe une correspondance avec } D \\ 0 & \text{sinon} \end{cases}$$

Correspondance de Post (1946)

Problème de decision PCP

- **ENTREE** : ensemble fini D de dominos
- **SORTIE** :
$$\begin{cases} 1 & \text{s'il existe une correspondance avec } D \\ 0 & \text{sinon} \end{cases}$$

Théorème (Post 1946)

Le problème POST est indécidable

Correspondance de Post (1946)

Problème de decision PCP

- **ENTREE** : ensemble fini D de dominos
- **SORTIE** :
$$\begin{cases} 1 & \text{s'il existe une correspondance avec } D \\ 0 & \text{sinon} \end{cases}$$

Théorème (Post 1946)

Le problème POST est indécidable

cf. TD