

6. Incalculabilité – exemples

Bruno Grenet

Université Grenoble Alpes – IM²AG
L3 Informatique
UE Modèles de calcul – Machines de Turing



<https://membres-ljk.imag.fr/Bruno.Grenet/MCAL-MT.html>

Table des matières

1. Pavage du plan

2. Problème de correspondance de Post

3. Autres problèmes indécidables

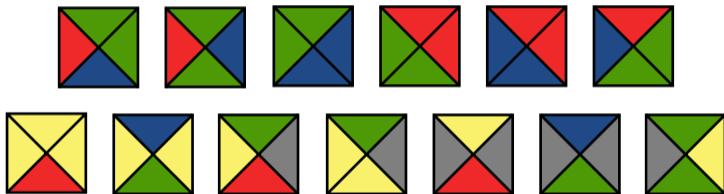
Table des matières

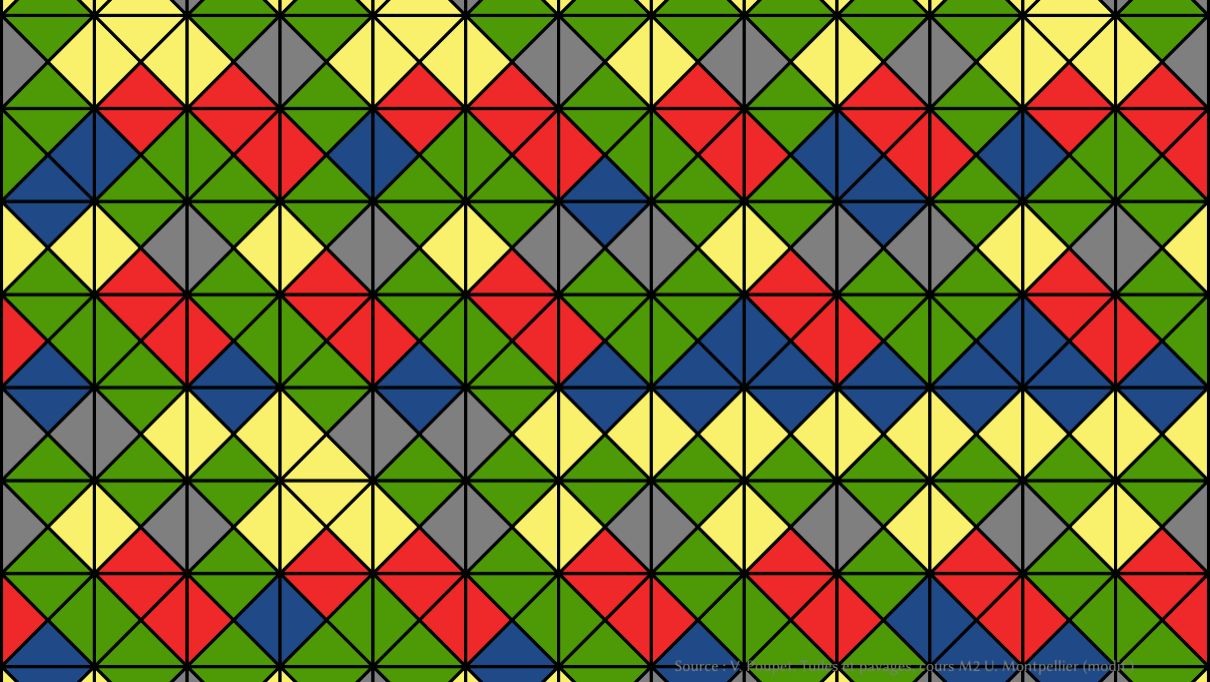
1. Pavage du plan

2. Problème de correspondance de Post

3. Autres problèmes indécidables

Peut-on paver tout le plan avec ces tuiles ?



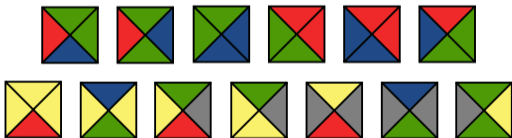


Tuiles de Wang pavage

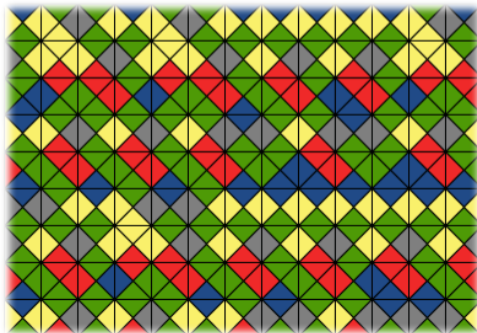
Définitions

- ▶ Une **tuile** est un carré unité dont les bords ont une couleur
- ▶ Un jeu de tuiles est un ensemble fini de tuiles
- ▶ Un **pavage** du plan est le placement de copies de tuiles, bord-à-bord, de façon à ce que les couleurs en contact coïncident

Tuiles



Pavage

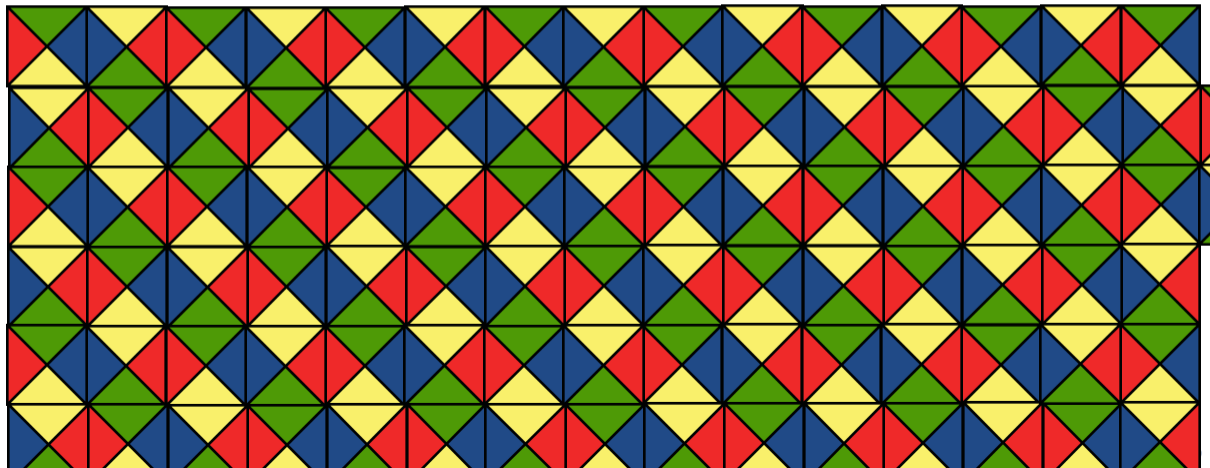


Remarque

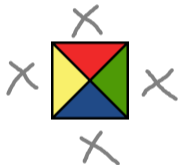
Les tuiles ne peuvent pas être tournées



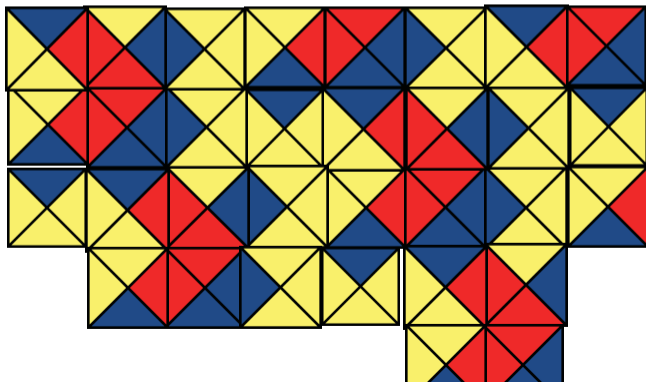
Exemple 1



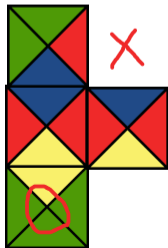
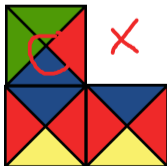
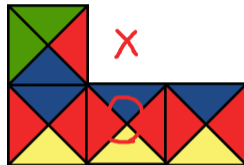
Exemple 1



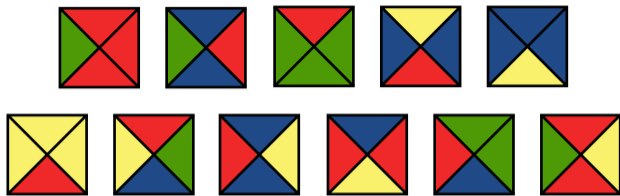
Exemple 2

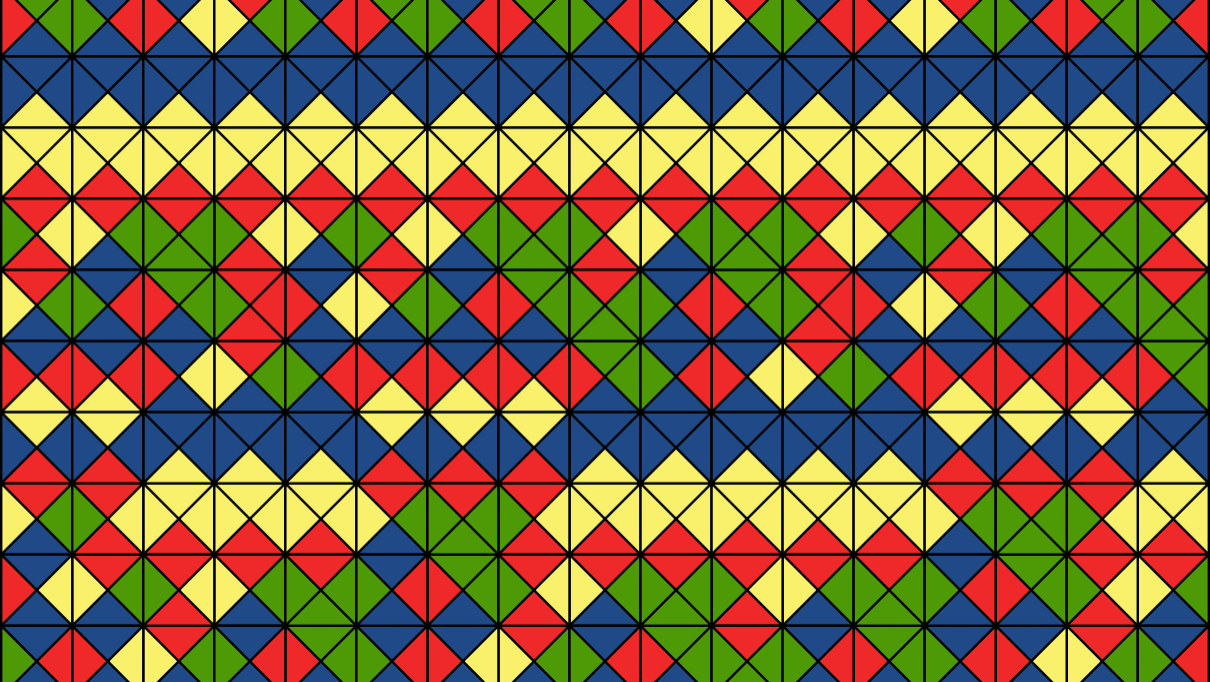


Exemple 3



Exemple 4





Le(s) problème(s)

Pavage du plan

Entrée: Un ensemble fini de tuiles de Wang

Sortie: Existe-t-il un pavage du plan avec ce jeu de tuiles ?

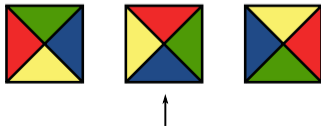


Pavage du plan *avec tuile de départ*

Entrées: Un ensemble fini T de tuiles de Wang

Une tuile de départ $t_0 \in T$

Sortie: Existe-t-il un pavage du plan avec ce jeu de tuiles qui contient t_0 ?



Indécidabilité

Théorème

- ▶ Le problème du pavage du plan est indécidable
- ▶ Le problème du pavage du plan avec tuile de départ est indécidable

Remarques

- ▶ Problèmes co-reconnaissables
 - ▶ Si le plan n'est pas pavable, il existe un carré $n \times n$ non pavable
 - ▶ Essayer toutes les possibilités \rightarrow on trouve un carré non pavable s'il existe
- ▶ Pavage du plan avec tuile de départ *plus difficile*
 - ▶ Supposons qu'on sache le résoudre avec un algorithme A
 - ▶ On applique A avec toutes les tuiles de départ possibles
 \Rightarrow résolution du pavage du plan

On démontre uniquement le 2^{ème} résultat, (beaucoup) plus simple

Point de départ : les machines de Turing

Rappel

Il n'y a pas d'algorithme pour décider si une machine de Turing s'arrête sur l'entrée vide

Choix de variante

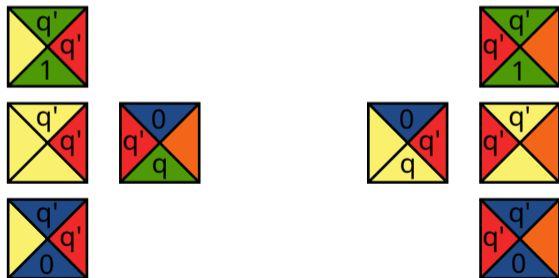
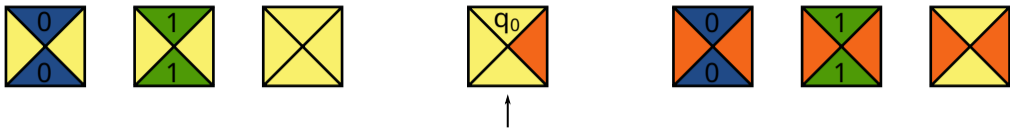
- ▶ On considère $\mathcal{M} = (Q, \Sigma, q_0, \delta)$ avec $\Sigma = \{0, 1, \square\}$

Stratégie

- ▶ Étant donné \mathcal{M} , on construit un jeu de tuiles qui *simule* \mathcal{M}
 - ▶ Une *ligne* du pavage = état du ruban à une étape donnée
 - ▶ Deux lignes consécutives = une étape de calcul
 - ▶ Une tuile de départ = état initial de la machine
 - ▶ Une tuile blanche pour compléter le plan
- ▶ \mathcal{M} termine sur l'entrée vide \iff le jeu de tuile ne pave pas le plan

\Rightarrow *réduction* du problème du *non-arrêt* sur l'entrée vide au pavage avec tuile de départ
(non-arrêt sur l'entrée vide \leq_m pavage avec tuile de départ)

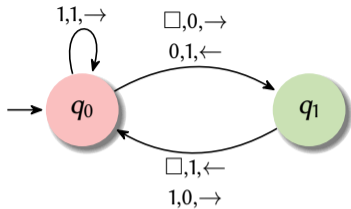
Le jeu de tuile



... etc
pour chaque
transition

$$\delta(q, 1) = (q', 0, \leftarrow)$$

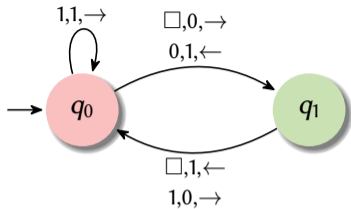
Example



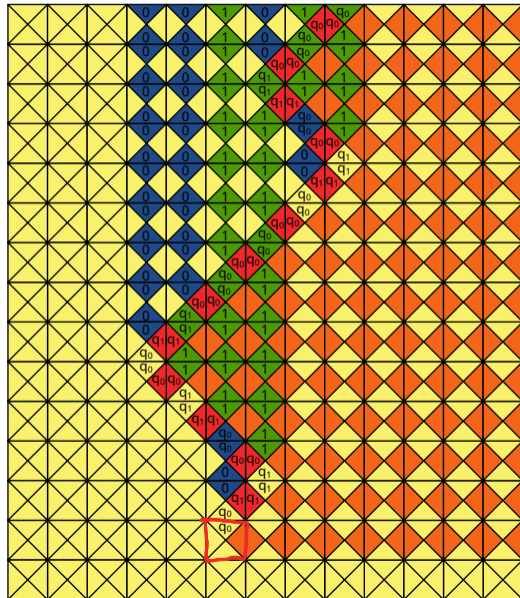
↑

		0	0	1	0	1	1		
		1	0	1	1	1	1		
		0	0	1	1	0	1		
		0	0	1	1	0	\square		
		0	0	1	1	\square			
		0	0	1	1	1			
		0	0	1	1				
		0	1	1	1				
		\square	1	1	1				
			\square	1	1				
				0	1				
				0	\square				
				\square					

Example



		0	0	1	0	1	1		
		1	0	1	1	1	1		
		0	0	1	1	0	1		
		0	0	1	1	0	□		
		0	0	1	1	□			
		0	0	1	1	1			
		0	0	1	1				
		0	1	1	1				
		□	1	1	1				
			□	1	1				
				0	1				
				0	□				
						□			



La preuve

Lemme

Il existe un pavage du plan avec la tuile initiale

- \iff Il existe une suite infinie de configurations, partant de q_0 : \square
- \iff La machine \mathcal{M} ne termine pas sur l'entrée vide



Conséquence

- ▶ Si le pavage du plan avec tuile initiale était décidable, le problème de l'arrêt sur l'entrée vide également
- ▶ Donc le pavage du plan avec tuile initiale n'est pas décidable

Remarque

- ▶ Démontre également que le problème n'est pas reconnaissable
- ▶ (On le savait car il est co-reconnaissable mais pas décidable)

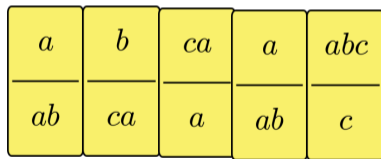
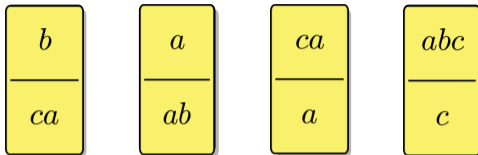
Table des matières

1. Pavage du plan

2. Problème de correspondance de Post

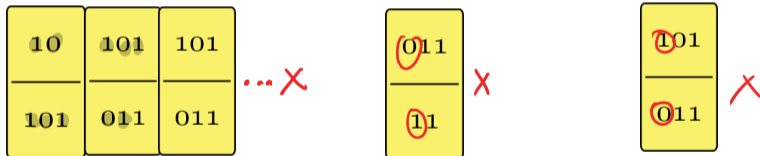
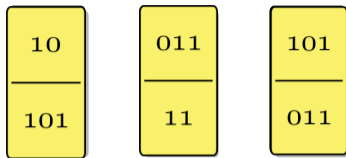
3. Autres problèmes indécidables

Des dominos un peu bizarres



$abcaabc$

Un autre jeu



Le(s) problème(s)

Problème de correspondance de Post (PCP)

Entrée : Un ensemble fini de *dominos*

Chaque domino contient un mot *en haut* et un *en bas* (sur un alphabet Σ)

Sortie : Une suite **finie** de dominos (avec répétitions possibles)

Correcte si les mots obtenus par concaténation en haut et en bas coïncident

PCP avec domino de départ (PCP*)

Entrées : Un ensemble fini de *dominos*

Un des dominos de l'ensemble

Sortie : Une suite de dominos correcte, qui commence par le domino fixé

Théorème

▶ Les deux problèmes sont indécidables : $K \leq_m \text{PCP}^* \leq_m \text{PCP}$

(K : problème de l'arrêt)

Réduction de l'arrêt à PCP*

Point de départ

- ▶ Problème de l'arrêt : entrée $\langle \mathcal{M}, w \rangle$ avec $\mathcal{M} = (Q, \Sigma, q_0, \delta)$ et $w \in (\Sigma \setminus \{\square\})^*$
- ▶ Hypothèses sur \mathcal{M} :
 - ▶ $\Sigma = \{0, 1\}$
 - ▶ Ruban semi-infini vers la droite
 - ▶ Un seul état final « \downarrow » où \mathcal{M} peut s'arrêter
- ▶ Représentation d'une configuration :
 - ▶ mot w du ruban
 - ▶ une lettre x^q : position de la tête + état q

Idée générale

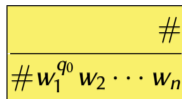
- ▶ Construction d'un ensemble de dominos :
 - ▶ Si \mathcal{M} s'arrête : suite (finie) des configurations \rightsquigarrow suite finie de dominos
 - ▶ Si \mathcal{M} ne s'arrête pas : aucune suite finie de dominos possible
- ▶ Configuration à la suite, séparées par des $\#$
- ▶ Mots du haut et du bas *passent l'information* d'une configuration à la suivante

Liste des dominos

pour tout $x, y, z \in \Sigma$

entrée $w = w_1 \cdots w_n$

- ▶ Domino de départ :



- ▶ Dominos de transition :

- ▶ $\delta(q, a) = (q', b, \rightarrow) \rightsquigarrow$



- ▶ $\delta(q, a) = (q', b, \leftarrow) \rightsquigarrow$

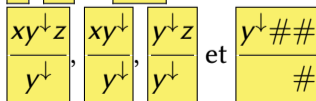


- ▶ Dominos de copie :

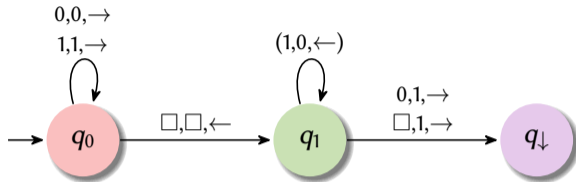


pour agrandir le ruban

- ▶ Dominos d'effacement et final :



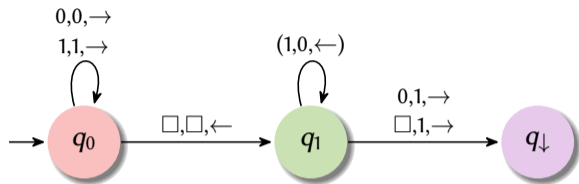
Example



A grid representing the tape configuration. The grid has 8 rows and 12 columns. The first three columns are empty. The fourth, fifth, and sixth columns contain binary digits (0 or 1). The seventh column contains square boxes. The eighth column is empty. The remaining columns are also empty. An upward-pointing arrow is on the left side of the grid.

				1	1	0	<input type="checkbox"/>					
				1	0	0	<input type="checkbox"/>					
				1	0	1	<input type="checkbox"/>					
				1	0	1	<input type="checkbox"/>					
				1	0	1	<input type="checkbox"/>					
				1	0	1						
				1	0	1						
				1	0	1						

Example

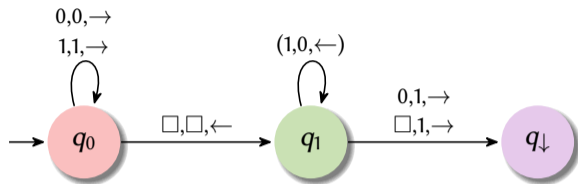


A grid representing the tape configuration. The grid has 8 rows and 12 columns. The first three columns are empty. The fourth, fifth, and sixth columns contain binary digits (0 or 1). The seventh column contains symbols: a white square, a white square, a green square, a red square, a white square, a white square, and a white square. An upward-pointing arrow is on the left side of the grid.

				1	1	0	□				
				1	0	0	□				
				1	0	1	□				
				1	0	1	□				
				1	0	1	□				
				1	0	1					
				1	0	1					
				1	0	1					

1⁰01 # 10⁰1 # 101⁰□ # 101□⁰ # 101¹□ # 10¹0□ # 110[↓]□

Example

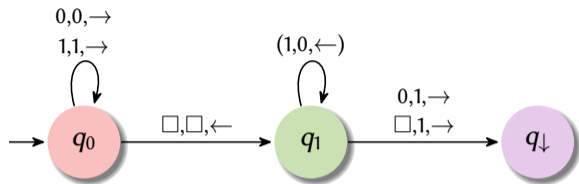


A grid representing the tape configuration. The grid has 8 rows and 12 columns. The first three columns are empty. The fourth, fifth, and sixth columns contain the sequence of symbols read from the tape. The seventh column contains the head position, represented by a square box. The eighth column is empty. The first three columns are empty. The fourth, fifth, and sixth columns contain the sequence of symbols read from the tape. The seventh column contains the head position, represented by a square box. The eighth column is empty.

					1	1	0	□			
					1	0	0	□			
					1	0	1	□			
					1	0	1	□			
					1	0	1	□			
					1	0	1				
					1	0	1				
					1	0	1				

1⁰01 # 10⁰1 # 101⁰□ # 101□⁰ # 101¹□ # 10¹0□ # 110[↓]□ # 110[↓] # 10[↓] # 0[↓]##

Example



					1	1	0	<input type="checkbox"/>				
					1	0	0	<input type="checkbox"/>				
					1	0	1	<input type="checkbox"/>				
					1	0	1	<input type="checkbox"/>				
					1	0	1	<input type="checkbox"/>				
					1	0	1					
					1	0	1					

1⁰01 # 10⁰1 # 101⁰□ # 101□⁰ # 101¹□ # 10¹0□ # 110[↓]□ # 110[↓] # 10[↓] # 0[↓]##

1⁰01 # 10⁰1 # 101⁰□ # 101□⁰ # 101¹□ # 10¹0□ # 110[↓]□ # 11 0[↓] # 1 0[↓] # 0[↓] #

La preuve (idée)

Lemme

Il existe une suite finie correcte de dominos qui commence par le domino de départ

\iff La machine \mathcal{M} s'arrête sur l'entrée w

Conséquence

- ▶ Si le problème PCP* était décidable, le problème de l'arrêt également
- ▶ Donc PCP* n'est pas décidable

Remarque

- ▶ Démontre également que le problème n'est pas co-reconnaisable
- ▶ (Exercice : démontrer que le problème est reconnaissable)

Modifier les dominos pour qu'il n'y ait qu'un seul domino de départ possible

Modification des dominos

- ▶ Étant donné un mot $w = w_1 \cdots w_n$, on définit
- $$\begin{cases} *w & = *w_1 * w_2 * \cdots * w_n \\ w* & = w_1 * w_2 * \cdots * w_n* \\ *w* & = *w_1 * w_2 * \cdots * w_n* \end{cases}$$

- ▶ Modification des dominos :

- ▶ Départ: $\frac{h_0}{b_0} \rightarrow \frac{*h_0}{*b_0*}$

- ▶ Autres dominos: $\frac{h_i}{b_i} \rightarrow \frac{*h_i}{b_i*}$

- ▶ Nouveau domino final: $\frac{* \diamond}{\diamond}$

⇒ Seule suite finie possible du nouveau ensemble de dominos: $\frac{*h_0}{*b_0*} \frac{*h_i}{b_i*} \cdots \frac{*h_j}{b_j*} \frac{* \diamond}{\diamond}$

Bilan

Deux réductions

- ▶ $K \leq_m \text{PCP}^*$: encodage du calcul d'une machine de Turing avec des dominos
- ▶ $\text{PCP}^* \leq_m \text{PCP}$: intercaler des * au milieu des mots

⇒ le problème de correspondance de Post est indécidable

Réductions inverses

- ▶ On a aussi : $\text{PCP} \leq_m K$
 - ▶ Algorithme A :
 - ▶ énumère toutes les suites finies de dominos (par longueur croissante)
 - ▶ teste si les mots du haut et du bas coïncident
 - ▶ s'arrête dès qu'une solution est trouvée
 - ▶ Un ensemble D de domino a une solution $\iff A(D)$ termine
- ▶ Donc PCP et l'arrêt sont *équivalents*

Table des matières

1. Pavage du plan

2. Problème de correspondance de Post

3. Autres problèmes indécidables

$x^{\text{ème}}$ problème de Hilbert

Énoncé

Étant donné un polynôme $P \in \mathbb{Z}[x_1, \dots, x_k]$, existe-t-il des entiers n_1, \dots, n_k tels que $P(n_1, \dots, n_k) = 0$?

Exemple

- ▶ $P(x_1, x_2, x_3) = 4x_1^2x_2x_3^5 - 2x_1x_3^6 + 6x_1x_3^5 - 4x_1x_2^4 + 2x_2^3x_3 - 6x_2^3 + 24x_1x_2 - 12x_3 + 36$
- ▶ $P(0, 0, 0) = 36, P(1, 1, 1) = 48, \dots$
- ▶ $P(1, 1, 5) = 0$

Théorème (Matiyasevich-Robinson-Davis-Putnam, 1961-70)

Le $x^{\text{ème}}$ problème de Hilbert est indécidable

Théorème de Richardson

Énoncé

Étant donné une expression mathématique constituée des symboles

- ▶ x , $\exp(\cdot)$, $\sin(\cdot)$, $|\cdot|$,
- ▶ $\ln(2)$, π , les nombres rationnels,
- ▶ $+$, $-$, \times et \circ (composition),

est-ce que la fonction $f : \mathbb{R} \rightarrow \mathbb{R}$ définie par l'expression est égale à 0 ?

Exemple

▶ $f(x) = \pi \exp\left(\frac{2}{3} |\sin(x \ln 2)|\right) + \sin(2 \exp(|x|))$

Théorème (Richardson, 1968)

La question ci-dessus est indécidable, car le $x^{\text{ème}}$ problème de Hilbert s'y réduit

Conclusion

L'indécidabilité existe de partout !

- ▶ En informatique :
 - ▶ questions sur les algorithmes (arrêt, théorème de Rice, ...)
 - ▶ questions sur le typage de certaines fonctions
 - ▶ ...
- ▶ En mathématiques : tous les domaines sont touchés !
 - ▶ Analyse, algèbre, géométrie, topologie, ...
 - ▶ *Entscheidungsproblem* : déterminer si un énoncé mathématique est correct
- ▶ Ailleurs :
 - ▶ Quel joueur va gagner dans une partie de *Magic: The Gathering*?
 - ▶ Certaines questions de planification des trajets en avion
 - ▶ Dessiner exactement une image 3D sur un ordinateur
 - ▶ Simuler idéalement un fluide

Mais elle est tout de même rare

- ▶ Ne pas croire qu'on tombe souvent *par hasard* sur un problème indécidable
- ▶ Ils existent, sont nombreux, mais il faut les chercher...