PB: $A \subseteq \mathbb{N}^p$. Est-ce qu'il existe un algo., qui prend $x \in \mathbb{N}^p$ en entrée et répond "oui" ou "non" suivant si $x \in A$?

I) Définitions

1) Les fonctions récursives

Notations :

- $\mathcal{F}_p = \mathbb{N}^{\mathbb{N}^p}$, $\mathcal{F} = \bigcup_{p \in \mathbb{N}} \mathcal{F}_p$;
- $\sigma \in \mathcal{F}_1$, $\sigma(n) = n+1$;
- $0() \in \mathcal{F}_0$, $0() = 0$;
- $\Pi_p^i \in \mathcal{F}_p$, $\Pi_p^i(x_1, \dots, x_p) = x_i$.

Déf-prop. Soient $g \in \mathcal{F}_p$, $h \in \mathcal{F}_{p+2}$. $\exists ! f \in \mathcal{F}_{p+1}$

(i) $f(x_1, \dots, x_p, 0) = g(x_1, \dots, x_p)$

(ii) $f(x_1, \dots, x_p, n+1) = h(x_1, \dots, x_p, n, f(x_1, \dots, x_p, n))$

On dit que f est définie par récursion primitive à partir de g et h.

Déf : on appelle prédicat une fonction qui ne prenne que les valeurs 0 ou 1.

Déf la minimisation non bornée d'un prédicat $q \in \mathcal{F}_{p+1}$, notée $\mu_q \in \mathcal{F}_p$ est :

$$\mu_q(x) = \begin{cases} \inf\{i : q(x,i) = 1\} & \text{si un tel } i \text{ existe} \\ 0 & \text{sinon} \end{cases}$$

Définition : l'ensemble des fonctions μ-récursives (resp. μ-récursives partielles) est le plus petit sous-ens. E de $\mathcal{F}$ vérifiant :

(i) E contient $0()$, σ, Π_p^i $\forall p \in \mathbb{N}, \forall i \in \{1, \dots, p\}$

(ii) E est clos par composition

(iii) E est clos par récursion primitive

(iv) E est clos par minimisation non bornée (de prédicats sûrs, i.e vérifiant : $\forall x \in \mathbb{N}^p, \exists i \in \mathbb{N} : q(x,n) = 1$) (resp. quelconques).

2) Les ensembles récursifs, RE

Déf : Une partie $A \subseteq \mathbb{N}^p$ est dite :

(i) récursive si χ_A est μ-récursive

(ii) récursivement énumérable si χ_A est μ-récursive partielle.

Exemple : l'ensemble $\mathcal{P} \subseteq \mathbb{N}$ des nombres premiers est récursifs

122

3) Ensembles récursifs et machines de Turing

On se fixe un alphabet Σ, $|\Sigma| \geq 2$

Prop. Il existe une représentation effective de $\mathbb{N}^p$ par des mots de Σ^* et réciproquement.

Soient alors $f : \Sigma^* \to \mathbb{N}^p$ et $g : \mathbb{N}^p \to \Sigma^*$ des bijections effectives.

Thm. Soit $A \subseteq \mathbb{N}$. A est récursif ssi $g(A)$ est décidé par machine de Turing.
A est récursivement énumérable ssi $g(A)$ est accepté par MT.

Déf : Soit $L \subseteq \Sigma^*$. L est dit
- Récursif s'il est décidé par une MT
- Récursivement énumérable s'il est accepté par une MT.

On note R (resp. RE) l'ens. des langages récursifs (resp. récursivement énumérables). Si $L \notin R$, L est indécidable.

Prop : $L \subseteq \Sigma^*$, $L \in R \iff L \in RE$ et $\overline{L} \in RE$.

Soient $(M_i)_{i \in \mathbb{N}}$ et $(w_i)_{i \in \mathbb{N}}$ des énumérations des MT sur Σ et bien de Σ^*.

Thm : $L_0 = \{w_i : M_i \text{ n'accepte pas } w_i\}$ n'est pas dans RE.

II) Exemples de langages non récursifs

1) La technique de la réduction

Pour montrer l'indécidabilité d'un langage L, on effectue une réduction à partir d'un langage L' qui a déjà été indécidable :

Thm : Soient L_1, L_2 deux langages tq L_1 soit indécidable. Si il existe $f : L_1 \to L_2$ calculable par MT tq $x \in L_1 \iff f(x) \in L_2$ alors L_2 est indécidable.

2) Premiers exemples de réduction

- $LU = \{(M, w) \text{ tq } M \text{ accepte } w\} \notin R$ par réduction à partir de L_0
- $HALT = \{(M, w) \text{ tq } M \text{ s'arrête sur } w\} \notin R$ (à partir de LU)

3) Le pb de correspondance de Post

Présentation du PB : étant donné un ens. de paires de mots S, existe-t-il une suite non vide $((x_1, y_1), \dots, (x_k, y_k))$ de S tq

$$x_1 \cdots x_k = y_1 \cdots y_k$$

Ex : on considère l'instance

$$\{(a, \varepsilon), (na, an), (s, as)\}$$

dont une solution est par exemple

a	na	na	s
ε	an	an	as

Théorème : le PB de correspondance de Post est indécidable. DEV

4) Le thm de Rice

Déf : une propriété P des langages RE est non triviale s'il existe au moins un langage qui vérifie P et un qui ne vérifie pas P

Thm : toute propriété non triviale de RE est ~~non décidable~~ indécidable. DEV

III) Autres caractérisations de RE

1) Ensembles calculés par MT

Déf : le langage calculé par une MT M est l'ensemble des mots se trouvant sur la bande à la fin d'une exécution de M.

Thm : Un langage est calculé par une MT ssi il est RE.

2) Langages engendrés par une grammaire

Thm : un langage est généré par une grammaire ssi il est RE.

3) Langages énumérés par une MT

On peut énumérer tous les mots d'un langage RE, en considérant un ensemble de paires (w, n), $w \in \Sigma^*$ et $n \in \mathbb{N}$, et pour chaque couple, on simule l'exécution de M sur w au plus à n étapes.

PCP

Kef : signer pour confirmance
Canton pour refaire

On va montrer que le problème de correspondance de Post (PCP) est indécidable.

Une instance du PCP :
n dominos $\left[\frac{u_1}{v_1}\right], \dots, \left[\frac{u_n}{v_n}\right]$ où $u_i, v_i \in \Sigma^*$ (ie. des él^{ts} de $\Sigma^* \times \Sigma^*$)

Une solut^{o} :
un arrangement des dominos (ac répétition)
ie. une suite $i_1, i_2, \dots, i_m$ de $\{1..n\}$ tq $u_{i_1} u_{i_2} \dots u_{i_m} = v_{i_1} v_{i_2} \dots v_{i_m}$.
(une sol^{o} est minimale si elle n'est pas de la forme uv où u, v sont deux sol^{o}).

Dans le problème du PCP modifié, on requiert que l'arrang^{t} commence par le premier domino : $i_1 = 1$ (PCPM).

On va montrer deux réductions : ① $A_{MT} \leq$ PCPM
② PCPM $\leq$ PCP

($A_{MT} = \{\langle M, w\rangle \mid M \text{ accepte } w\}$)

Ce qui montrera que **PCP est indécidable.**

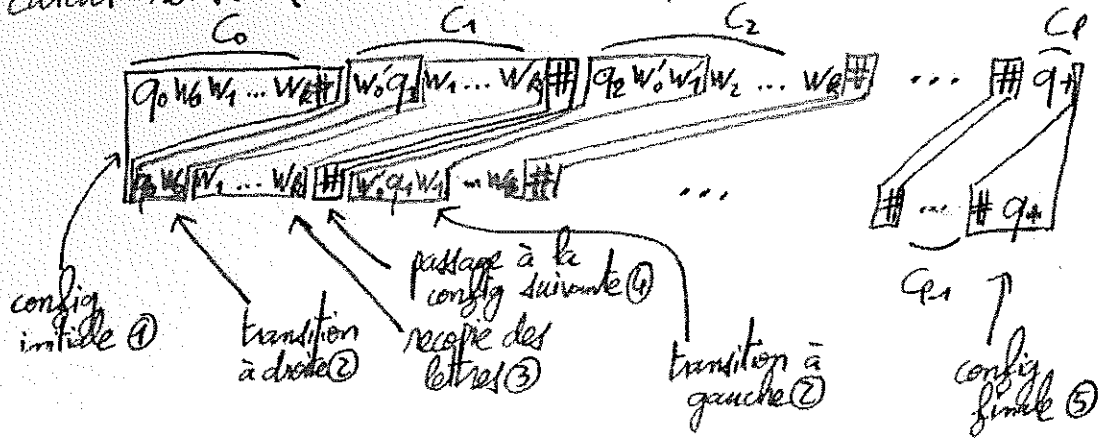
$A_{MT} \leq$ PCPM Soit M une MT et $w \in \Sigma^*$.
On cherche à construire une instance $\mathcal{I}'$ de PCPM telle que $\mathcal{I}'$ a une solution $\Leftrightarrow \langle M, w\rangle \in A_{MT} \Leftrightarrow M$ accepte w.
Quitte à ajouter des états et des symboles, on peut supposer que
- M est normalisée : $M = (Q, \Gamma, \Sigma, \Delta, q_0, q_+, q_-)$,
M ne bloque qu'en q_+ et q_-, q_+ est l'unique état acceptant,
- que M efface son ruban et repositionne sa tête à gauche avant d'accepter un mot.
- M n'écrit pas de blancs au milieu

On représente une configuration (q, w_1, w_2) par $w_1 q w_2$ (ou $w_1 q w_2 \sqcup$, ...).

Un calcul réussit dans M est de la forme :

$$q_0 w = C_0 \vdash C_1 \vdash C_2 \cdots \vdash C_\ell = q_+$$

On va construire $\mathcal{P}$ tel que les solutions minimales de $\mathcal{P}$ soient de la forme $C_0 \# C_1 \# C_2 \cdots \# C_\ell$ où $C_0 \vdash \cdots \vdash C_\ell$ est un calcul réussi ($\#$ est un nouveau symbole).



$\mathcal{P}$ est constituée des dominos suivants :

① $\left[\frac{q_0 w}{\varepsilon}\right]$ config initiale

② si $q_i, a \to q_j, b, \triangleright$ alors $\left[\frac{q_i a}{b q_j}\right]$ transition à droite

si $q_j, a \to q_j, b, \triangleleft$ alors $\left[\frac{c q_j a}{q_j c b}\right]$ $\forall c \in \Sigma$ à gauche

③ $\left[\frac{a}{a}\right]$ $\forall a \in \Sigma$ (dont le blanc $\sqcup$)

④ $\left[\frac{\#}{\#}\right]$ pour passer à la config suivante

$\left[\frac{\sqcup\#}{\#}\right]$ ——— en ajoutant un blanc final

$\left[\frac{\#}{\sqcup\#}\right]$ ——— suppr ———

⑤ $\frac{\varepsilon}{\#q_f}$ pour finir

Si $\langle M, w\rangle$ a un calcul réussit, $\mathcal{P}$ a clairement une solution

Réciproquement, si on a une solution (minimale), alors elle provient d'un calcul réussi. En effet :

* une solution commence nécessairement par ① et donc par "$C_0 \#$" (PCPM)
* le premier domino induit un décalage dans le nb de # en haut et en bas qui ne peut être rattrapé que par ⑤ $\Rightarrow$ une solution finit nécessairement par une configuration acceptante
* les dominos ② forcent la solution $C_0 \# C_1 \dots C_f$ à vérifier $C_i \vdash C_{i+1}$ $\rightarrow$ c'est bien un calcul !

PCPM $\preceq$ PCP

On transforme une instance $\mathcal{P}$ de PCPM en une instance $\mathcal{P}'$ de PCP équivalente :

$\mathcal{P}$: $\frac{u}{v}$ $\frac{u'}{v'}$ … $\frac{u^{(n)}}{v^{(n)}}$

$\mathcal{P}'$: $\frac{*u_0*u_1*\dots*u_k}{*v_0*v_1\dots*v_p*}$ $\frac{*u'_0*u'_1\dots*u'_{p'}}{v'_0*v'_1\dots v'_{p'}*}$ … $\frac{*u_0^{(n)}*\dots*u_k^{(n)}}{v_0^{(n)}*\dots*v_l^{(n)}*}$ $\frac{*\diamond}{\diamond}$

où $*$ et $\diamond$ sont deux nouveaux symboles.

On a même une bij° entre les sol° de $\mathcal{P}$ et celles de $\mathcal{P}'$:

$w_0 w_1 - w_n \longmapsto *w_0*w_1*\dots*w_n*\diamond$ (elle respecte les sol° min !)

Rice

On considère une propriété P des langages des MT (et non des MT elles-mêmes) : $P : \{\text{ens des MT}\} \longrightarrow \{\text{vrai, faux}\}$ telle que $L(M) = L(M') \Rightarrow P(M) = P(M')$.

On suppose P non triviale : $\exists M_1$ et M_2 tq $P(M_1)$ et $\neg P(M_2)$

le langage associé à P est $L_P = \{\langle M \rangle \mid M \text{ est une MT tq } P(M)\}$.

Thm : L_P est indécidable

Preuve

Quitte à changer P en $\overline{P}$, on peut supposer que $\neg P(\emptyset)$.

Soit M_1 une MT telle que $P(M_1)$.

On procède par réduction à partir de $A_{MT} = \{\langle M, w \rangle \mid M \text{ acc } w\}$

$A_{MT} \leq L_P$

Soit $\langle M, w \rangle$. On considère la MT M' suivante :

entrée : u
- * simuler M sur w, si M rejette w alors rejetter
- * si M accepte w, simuler M_1 sur u

Alors, si $w \in L(M)$, $L(M') = L(M_1)$ donc $P(M')$.

Et si $w \notin L(M)$, $L(M') = \emptyset$ donc $\neg P(M')$.

Donc $M \mapsto M'$ est bien une réduction de A_{MT} à L_P.

d'où L_P indécidable (et plus précisément : $L_P \notin coRE$).