## Fonctions récursives





Université de Mons-Hainaut Institut de Mathématique

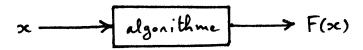
Tél: +32 65 37 35 07 — Fax: +32 65 37 33 18

Web:http://www.umh.ac.be/math/institut

# LES FONCTIONS RÉCURSIVES

La théorie des fonctions récursives s'est développée dans les années 30, suite au fameux théorème d'incomplétude de Gödel. Elle est rapidement devenue l'un des grands chapitres de la logique mathématique, mais aujound'hui elle a aussi sa place en informatique théorique. Les articles originaux des pionniers (Gödel, Church, Turing, Rosser, Kleene et Post) sont repris dans l'anthologie de M. Davis: The Undecidable (Raven Press, NY).

Les fonctions récursives sont (par définition) les fonctions calculables par un algorithme:



Une définition précise des fonctions récursives nécessite donc une définition précise de la notion d'algorithme. Un algorithme est un ensemble fini de règles de calcul, ces dernières dépendant de la méthode de calcul choisie, p. ex:

méthode de calcul	algorithme		
papier + crayon	rigles de Calcul en Français		
machine	règles de fonctionnement		
ordinateur	programme		

Une définition précise de la notion d'algorithme dépend donc du choix d'une méthode de calcul et d'une description précise de celle-ci. Différentes méthodes de calcul ont été projosées: machines de Turing, systèmes de Post, h-calcul de Church, algorithmes de Markov, .... On a pu montrer que toutes ces méthodes sont équivalentes: elles fournissent les mêmes fonctions récursives. Celles-ci doivent donc avoir des propriétés indépendantes de la méthode de calcul. Ce sont ces propriétés qui font l'objet de la théorie des fonctions récursives. En ce qui concerne les méthodes de calcul elles-mêmes, principalement les machines de Turing et les machines à registres, je conseille les livres suivants:

M. Minsky: Computation: Finite and infinite machines (Prentice-Hall); N. Cutland: Computatility: An introduction to recursive function the-

ony (Cambridge University Press).

### 1. Notions de base.

Supposons que nous disposons d'une notion précise d'algonithme.

Avec J. Shoenfield: Degrees of Umsolvability (North-Holland),

nous appellerons espace tout ensemble X tel que:

(1) XCA\* pour un certain alphabet fini (ensemble fini de signes) A, où A\* désigne l'ensemble des mots (suites finies de signes) sur A;

(2) X est infini;

(3) on peut décider par un algorithme si un mot de A\* appartient on non à X.

Voici quelques exemples:

- (1) |N| (frensemble des nombres maturels) est un espace:  $|N| = A^*$  pour  $A = \{1\}$ .
- (2) si X, Y soul des espaces, alon XxY est un espace:

  soil X c A\*, Y c B\*, \* & AUB,

  alon XxY = {xxy | x \in X, y \in Y} c (AUBU \{\pm \}).
- (3) si X of un espace, alons  $X^*$  of un espace:

  soil  $X \subset A^*$ ,  $* \notin A$ ,

  alons  $X^* = \{x_1 \times x_2 \times ... \times x_n \mid n \in \mathbb{N}, x_i \in X\} \subset (A \cup \{*\})^*$ .

Une fonction  $X \xrightarrow{F} Y$  (où X, Y sont des espaces) est dite récursive s'il existe un algorithme qui calcule F(x) jour chaque  $x \in X$ .

Exemples: IN × IN  $\stackrel{+}{\longrightarrow}$  IN, IN × IN  $\stackrel{\circ}{\longrightarrow}$  IN, ×  $\stackrel{id}{\longrightarrow}$  × , × ×  $\stackrel{proj}{\longrightarrow}$  × , × ×  $\stackrel{proj}{\longrightarrow}$  × , ×  $\stackrel{+}{\longrightarrow}$  IN (où l'associe à chaque snite finie sa longueux), la composition de deux fonctions récursives.

Une bijection X => Y telle que F et F<sup>-1</sup> sont récursives est applée isomorphisme.

Théorème d'isomorphisme: tous les espaces sont isomorphes.

Cela résulte des lemmes suivants:

Lemme 1: toute bijection réansire IN => X est un isomorphisme.

En effet, voici un algorithme pour  $F^{-1}$ : étant donné  $x \in X$ , calculer successivement F(0), F(1), ... jusqu'à ce qu'on obtienne F(n)=x.

Lemme 2: pour tout alphabet (non vide) A, A\* est isomosphe à IN.

En effet, il existe un algorithme qui énumère les mots de A\* suivant leurs longueurs, ceux de même longueur étant classés lexicographiquement. Ceci donne une bijection récursive de IN sur A\*, qui est un isomorphisme par le Lemme 1.

Lemme 3: tout sous-espace de IN est isomorphe à IN.

En effet, soit X un sous-espace de N. Il existe un algorithme qui énumère les éléments de X suivant bondre maturel, ce qui

donne une bijection récursive de IN sur X.

<u>Preuve du théorème d'isomorphisme</u>: montrons qu'un espace quelconque XCA\* est isomorphe à IN. Par le Lemme 2, A\* est isomorphe à IN, donc X est isomorphe à un sous-espace de IN, donc à IN par le Lemme 3.

Exercice: toute bijection récursive X => Y est un isomorphisme.

La fonction caractéristique d'un sous-ensemble E d'un espace X est la fonction X => IN définie comme suit :

 $F(x) = \{0 \text{ si } x \notin E, \\ 1 \text{ si } x \in E.$ 

Un sous-ensemble d'un espace est dit <u>récursif</u> lorsque sa fonction caractéristique est récursive.

Tout sous-ensemble fini d'un espace est récursif.

Les sous-ensembles récursifs infinis d'un espace coincident avec les sous-espaces de cet espace.

Enfin, la réunion, l'intersection on la différence ensembliste de deux ensembles récursifs (dans un même espace) est encore un ensemble récursif. En particulier, ECX est récursif soi son complément X-E l'est.

#### 2. L'espace des algorithmes.

Soit Alg(X,Y) l'ensemble des algorithmes qui s'appliquent aux éléments de X et fournissent un résultat dans Y on un résultat indéfensiné (ce qui arrive lorsque le calcul se poursuit indéfiniment). On note [I](x) le résultat du calcul effectué par l'algorithme I lorsqu'en l'applique à x. Pour  $I \in Alg(X,Y)$  et  $x \in X$ , on a donc  $[I](x) \in Y$  on [I](x) = ? (c-à-d [I](x) indéterminé).

Nous sommes ainsi amenés à utiliser la notion de fonction partielle X—F> Y où F n'est supposée déterminée que sur un sous-ensemble de X noté dom (F) (le domaine de F). Pour éviter boute confusion, l'usage de cette notion sera toujours mentionné explicitement. Et lossque dom (F) = X, nous utiliserons le terme de fonction on de fonction totale.

Nous pouvous maintenant élendre la notion de fonction récursive aux fonctions partielles  $X \xrightarrow{F} Y$ :

For récursive  $\iff F = [I]$  pour un  $I \in Alg(X,Y)$ .

Quelle que soit la notion d'algorithme satilisée, Alg(X,Y) vérifie les propriétés suivantes:

(1) Alz(X,Y) est un espace;

(2) la fonction partielle de Alg(X,Y) x X dens Y envoyant (I,>c) sur [I](x) est récursive.

(es propriétés impliquent immédiatement l'existence d'une fonction partielle récursive universelle  $IN \times X \longrightarrow Y$ , c-à-d telle que chaque fonction partielle récursive  $X \stackrel{F}{\Longrightarrow} Y$  prisse se mettre sous la forme F(x) = U(n,x) jour au moins une valeur de n. Il suffit en effet de poser  $U(n,x) = [I_n](x)$ , où  $n \mapsto I_n$  est un isomorphisme de IN sur Alg(X,Y).

On il n'existe pas de fonction totale récursive universelle. En effet, sullosons que T(n,x) en soit une et que X=Y=IN (ce cas suffit, grâce ou théorème d'isomorphisme). Il fout alors que T(x,x)+1=T(n,x) jour un certain n, d'on la combradiction : T(n,n)+1=T(n,n).

Ce résultat négatif implique les deux suivants (qui expliquent pourquoi on ne peut pas se limiter aux fonctions totales):

- (1)  $\{I \in Alg(X,Y) \mid [I] \text{ est totale }\}$  m'est pas un espace. (sinon il existencit un isomonthisme  $m \mapsto I_m$  de IN sur cet espace et alon  $T(n,x) = [I_m](x)$  serait une fonction totale récursive universelle)
- (2) Si U est une fonction partielle récursive universelle, alors dom (U) m'est par récursif.

  (sinon la fonction suivante  $T(n,x) = \int U(n,x) \qquad \text{Si } (n,x) \in \text{dom}(U),$ un élément fixe de Y sinon,

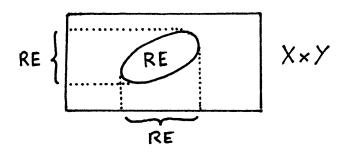
  serait une fonction totale récursive universelle)

#### 3. Ensembles récursivement énumérables.

Un ensemble ECX est dit <u>réconsivement énumérable</u> (<u>RE</u>) s'il est vide on s'il existe une fonction totale réconsive IN <del>F</del> X telle que E = im (F) (l'image de F, c-à-d {F(n)|nEIN}), auquel cas on dit que F énumère réconsivement E. Tout ensemble réconsif est RE.

En effet, si E est un sous-ensemble récursif non vide de  $\mathbb{N}$ , alors il est l'image de la fonction tohale récursive  $\mathbb{N} \xrightarrow{F} \mathbb{N}$  suivante:  $F(n) = \{n \quad \text{si } m \in E, \}$ 

Il est clair que si X => Y est totale récursive, alors l'image par F d'un sous-ensemble RE de X est un sous-ensemble RE de Y. En particulier, la projection d'un ensemble RE est RE:



Le graphe d'une fonction partielle  $X \xrightarrow{F} Y$  est le sous-ensemble Gr(F) de  $X \times Y$  formé des comples (x,y) tels que F(x) = y. Nous allons montres qu'une fonction partielle est récursive ssi son graphe est RE:

(1) si Génumère récursivement GR(F), alors le calcul successif de G(0), G(1), ... fournit un algorithme pour F.

(2) si F=[I], alons Gr(F) est une projection de l'ensemble récursif {(x,y,n) | [I](x)=y et I calcule y à partir de x en moins de n élapses}.

Comme le domaine et l'image d'une fonction partielle sont les projections de son graphe, on voit que <u>le domaine et</u> <u>l'image</u> d'une fonction partielle récursive sont RE.

En particulier, pour Unécursive universelle, dom(U) est un ensemble RE mon nécursif.

De plus:

Les sous-ensembles RE de X coincident avec les domaines des fonctions partielles récursives de X dans IN.

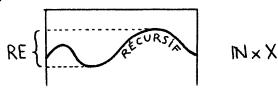
En effet, si E est un sous-ensemble RE de X, alors il est le domaine de la fonction partielle récursive  $X \xrightarrow{F} IN$  définie comme suit :  $F(x) = \{1 \text{ si } x \in E,$ 

(si on appelle cette fonction la fonction semi-carachéristique de E, on voit qu'un ensemble est RE ssi sa fonction semi-carachéristique est récursive).

El encore:

Les sous-ensembles RE de X coincident avec les projections sur X des sous-ensembles récursifs de INXX.

Cela résulte de la définition des ensembles RE et du fait que le graphe d'une fonction totale récursive est récursif:



La réunion on l'intersection de deux ensembles RE est encore RE, mais le complément X-E d'un ensemble RE ECX n'est RE que si E est récursif. En effet:

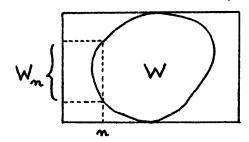
(1) si F<sub>1</sub>, F<sub>2</sub> sont respectivement des énumérations récursives de E<sub>1</sub>, E<sub>2</sub>, alors la fonction F suivante est une énumération récursive de E<sub>1</sub>UE<sub>2</sub>:

 $F(n) = \begin{cases} F_1\left(\frac{M}{2}\right) & \text{sin ost pair,} \\ F_2\left(\frac{M-1}{2}\right) & \text{sin ost impair.} \end{cases}$ 

- (2) si E1, E2 sont respectivement les domaines des fonctions partielles récursives F1, F2, alors E1 N E2 est le domaine de la fonction partielle récursive F(m) = (F1(m), F2(m)).
- (3) si F, G sont respectivement des énumérations récussives de E et X-E, alors le calcul successif de F(0), G(0), F(1), G(1), ... fournit un algorithme pour la fonction caracléristique de E.

Exercices: • si  $E_1$ ,  $E_2$  somt récursifs (resp. RE), alons  $E_1 \times E_2$  est récursif (resp. RE).

esi U est nécursive universelle, alons W = dom(U) est RE universel (chaque RE est de la forme  $W_n = \{x \mid (n,x) \in W\}$ ):



• il n'existe pas d'ensemble récursif universel.

#### 4. Indices.

Supposons fixé un isomorphisme  $m \mapsto I_m$  de IN sur Alg(IN\*, IN). Par définition:

 $[m]^{(k)} = la restriction de [Im] a IN<sup>k</sup> (m, k \in IN, k > 1);$   $[m] = [m]^{(1)}.$ (b) (k) (k)

Il est clair que la suite [0]<sup>(k)</sup>, [1]<sup>(k)</sup>,..., [n]<sup>(k)</sup>,... est une énumération de toutes les fonctions partielles récursives de IN<sup>k</sup> dans IN. Lorsque F= [n]<sup>(k)</sup> on dit que n est un <u>indice</u> de F (qui a nécessairement une infinité d'indices, puisqu'il y a une infinité d'algorithmes qui calculent F).

Théonème de paramétrisation: il existe une fonction totale récursive S telle que pour tout  $m, x, y \in IN$ :  $[m]^{(2)}(x,y) = [S(n,x)](y).$ 

Cela résulte de l'existence d'une fonction totale récursive T telle que T(I,x) est un algorithme qui calcule la fonction partielle  $y \mapsto [I](x,y)$ . (le théorème de paramétrisation se généralise facilement, par exemple:  $[n]^{(4)}(x,y,z,t) = [S(n,x,y)]^{(2)}(z,t)$ ).

Conollaine: pour toute fonction partielle récursive F(x,y) (de  $IN^2$  dans IN) il existe une fonction totale récursive T(x) (de IN dans IN) telle que (pour tout  $x,y \in IN$ ) F(x,y) = [T(x)](y).

Théorème du point fixe (Kleene): pour toute fonction totale récursive T(x) (de IN dans IN) il existe un n tel que [n] = [T(n)].

En effet, par le conollaire précédent il existe une fonction

totale récursive [m] telle que [T([x](x))](y) = [[m](x)](y) et il suffit de prendre n = [m](m).

Corollaire: pour toute fonction partielle récursive F(x,y) (de  $IN^2$  dans IN) il existe un n tel que (pour tout  $y \in IN$ ) F(n,y) = [n](y).

En effet, F(x,y) = [T(x)](y) (Conollaine précédent) et il suffit de prendre n tel que [n] = [T(n)].

Théorème de Rice: si E={neIN|[n] EE} (où E est un ensemble quelconque) et si E est distinct de \$\phi\$ et de IN, alons E m'est pas récursif.

Sinon, en choisissant a EIN-E et b E E, la fonction totale nécursive

 $T(x) = \{a \text{ si } x \in E, \\ b \text{ si } x \in \mathbb{N} \cdot E, \}$ 

vérifierait  $x \in E \leftrightarrow T(x) \notin E$ , c-à-d [50]  $\in E \leftrightarrow [T(x)] \notin E$ , ce qui est absurde pour [n] = [T(n)].

Ce théorème fournit un grand nombre d'exemples d'ensembles mon récursifs: {n | [n] est totale} (déjà envisagé fin \$2), l'ensemble de tous les indices d'une même fonction partielle récursive (p. ex. l'ensemble de tous les indices de la fonction constante nulle), {n | [n](0) = 0},...

Exercice: étendre le théorème de Rice au cas où  $E = \{(m,n) \in \mathbb{N}^2 \mid ([m],[n]) \in E\}.$ 

Remarque: puisque chaque partie RE de IN est de la forme  $W_n = dom([n])$ , on voit que  $\{n \mid n \notin W_n\}$  n'est pas RE, donc que  $\{n \mid n \in W_n\}$  (qui est RE) n'est pas récuesif.

#### 5. Fonctions récursives primitives.

à parlir de F,G.

Historiquement, les premières fonctions récursives qui apparanent sont les fonctions récursives primitives (RP), définies comme suit; ce sont les fonctions totales récursives (de INR dans IN) qu'on peut obtenir à partir des fonctions de base  $x\mapsto 0$ ,  $x\mapsto x+1$  et  $(x_1,...,x_k)\mapsto x_\ell$  (les projections) à l'aide des principes de composition et de récursion suivants; le principe de composition qui permet d'obtenir la fonction  $H(x_1,...,x_k)=F(F_1(x_1,...,x_k),...,F_\ell(x_1,...,x_k))$  à partir des fonctions  $F,F_1,...,F_\ell$ ; le principe de récursion qui permet d'obtenir la fonction  $H(x_1,...,x_k,0)=F(x_1,...,x_k)$ ,  $H(x_1,...,x_k,0)=F(x_1,...,x_k)$ ,  $H(x_1,...,x_k,0)=F(x_1,...,x_k)$ ,

A titre d'exemple, montrons que la fonction H(x,y) = x + y est RP:

les fonctions de base S(x) = x+1 et P(x,y,z) = z sont RP, donc la fonction G(x,y,z) = S(P(x,y,z)) = z+1 l'est anssi (par composition); et comme la projection F(x) = x est RP, H l'est anssi (par récursion):

$$\{H(x,0) = F(x), H(x,y+1) = G(x,y,H(x,y)).$$

Exercices: monther que la fonction  $H(x,y) = x \cdot y$  est RP; montrer que dans chacun des cas suivants G est RP si F l'est:

G(x,y)=F(x), G(x,y)=F(y,x), G(x)=F(x,x); • disons qu'une fonction  $F(x)=(F_1(x),F_2(x))$  de IN dans  $N^2$  of RP si  $F_1$  de sont; montrer que  $IN^2$  of RP-isomorphe à IN; généraliser à  $IN^k$ . La définition des fonctions RP montre qu'il existe un sous-espace de Alg(IN\*,IN) dont les éléments calculent les fonctions RP. Donc il existe une fonction totale récursive R(n,x) qui est universelle pour les fonctions RP en x. Mais alors R(x,x)+1 m'est pas RP, donc les fonctions totales récursives me sont pas toutes RP. Il y a des contre-exemples plus explicites, comme la fonction d'Ackermann (voir §6).

Lonsqu'on utilise une notion précise d'algorithme, on peut montrer que la fonction suivante est RP:

 $S_{k}(n,x_{1},...,x_{k},y,t) = 0$  si l'algorithme  $I_{n} \in Alg(IN^{*},IN)$ appliqué à  $x_{1},...,x_{k}$  calcule yon moins de t étapes,

1 sinon.

Si on pose  $T_k(n,x_1,...,x_k,z) = S_k(n,x_1,...,x_k,F_{(z)},F_{(z)})$ , où  $z \mapsto (F_1(z),F_2(z))$  est un RP-isomorphisme de IN sur IN², alors on oblient immédiatement le

Théorème de la forme normale de Kleene: xl y a des fonctions  $F_1$ ,  $T_k$  qui sont RP et telles que  $[n]^{(k)}(x_1,...,x_k) = F_1((\mu z)(T_k(n,x_1,...,x_k,z)=0))$ , où  $\mu z$  signifie "le plus petit entier z tel que".

<u>Conollaine</u>: les fonctions partielles nécussives (de IN<sup>k</sup> dans IN) sont celles qu'on peut obtenir à partir des fonctions de base à l'aide des principes de composition, de récursion et de minimalisation.

Le <u>principe de minimalisation</u> étant celui qui permet d'obtenir la fonction partielle  $H(x_1,...,x_k) = (\mu z)(F(x_1,...,x_k,z) = 0)$  à partir de la fonction partielle F. (lorsque F n'est pas totale,  $(\mu z)(F(x,z)=0)$  signifie  $(\mu z)(F(x,z)=0)$  et  $(\forall y < z)(F(x,y) \neq ?))$ .

<u>Exercice</u>: montrer que tont sous-ensemble RE de IN est la projection d'un sous-ensemble RP de IN k+1 (un ensemble est dit RP lossque sa fonction caractéristique l'est).

#### 6. Opérateurs.

Notons  $F_R$  l'ensemble de <u>boules</u> les fonctions partielles de  $IN^R$  dans IN. Parmi les éléments de  $F_R$  (notés F,G,H,...) figurent les fonctions partielles <u>finies</u> qui seront notées f,g,h,.... Par définition, un <u>opérateur</u> est une fonction (botale)  $F_R \xrightarrow{P} F_R$ , et il est dit <u>comtinu</u> lonsque pour bout  $F \in F_R$ :

 $\Phi(\mathsf{F}) = \bigcup_{\mathsf{f} \leq \mathsf{F}} \Phi(\mathsf{f}) \ .$ 

On vérifie facilement que si \$\P\$ est combinu, alon:

1) 中 or monotone: Fof implique 中(Fo) s 車(Fo);

2) plus généralement: F<sub>0</sub> ⊆ F<sub>1</sub> ⊆ ... ⊆ F<sub>2</sub> ⊆ ... (i ∈ IN) implique Φ(ŲF<sub>1</sub>) = ŲΦ(F<sub>1</sub>). Il en résulte le

Théonème du plus petit point fixe: si  $\Phi$  est un opérateur continu de  $F_k$  dans  $F_k$ , alons  $Fix(\Phi) = \bigcup_{i \in IN} \Phi^i(\emptyset)$  est son plus petit (pour  $\subseteq$ ) point fixe.

Par exemple, considérons l'opérateur & snivant (de F2 dans F2):

$$\begin{cases}
\Phi(F)(0,y) = y+1, \\
\Phi(F)(x+1,0) = F(x,1), \\
\Phi(F)(x+1,y+1) = F(x,F(x+1,y)).
\end{cases}$$

Il est combinu. Soit  $A = Fix(\Phi)$ . C'est la plus petite fonction de  $F_2$  vérifient:

$$\begin{cases} A(o,y) = y+1, \\ A(x+1,o) = A(x,1), \\ A(x+1,y+1) = A(x,A(x+1,y)), \text{ (une double récursion)} \end{cases}$$

C'est même la seule, car elle est totale (vu que le domaine de  $\Phi^i(\phi)$ 

tend vers IN2). On l'appelle la fonction d'Ackermann.

Remarque: le terme "continu" coincide avec son sens topologique si on munit chaque  $F_k$  de la topologie dont les ouverts de base sont les  $O_f = \{F | f \subseteq F\}$ .

Définition: un opérateur  $\Phi$  de  $F_k$  dans  $F_\ell$  est dit <u>récursif</u> s'il est combinu et si la fonction (partielle)  $\Phi(f)(x_1,...,x_\ell)$  en  $f,x_1,...,x_\ell$  est récursive.

Lemme: jour qu'un opérateur combinn  $\Phi$  de  $F_k$  dans  $F_\ell$  soit récursif it faut et il suffit qu'il existe une fonction totale récursive H(n) telle que  $\Phi([n]^{(k)}) = [H(n)]^{(\ell)}$ .

Cette condition est clairement suffisante; elle est nécessaire car il y a un algorithme  $I_{H(n)}$  qui, allliqué à  $x_1,...,x_\ell$ , énumère les restrictions finies f de la fonction  $[n]^{(h)}$  et les étapes de calcul de  $\Phi(f)(x_1,...,x_\ell)$ .

Théorème de récursion (Kleene): si \$\overline{\Phi}\$ est un opérateur récursif de \$F\_k\$ dans \$F\_k\$, alors Fix(\$\overline{\Phi}\$) est une fonction (partielle) récursive.

En effet, le Lemme montre que  $\Phi^{i}(\phi) = [H^{i}(n_{0})]^{(k)}$  où  $[n_{0}]^{(k)} = \phi$ .

Corollaire: la fonction d'Ackermann est (totale) récursive.

Mais (par l'exercice suivant) elle n'est pas RP.

Exercice: montrer que

- 1) A(x,y) > y (par induction sur x),
- 2) A(x,y) est strictement croissante en x et en y,

- 3) A(x+1,y) > A(x,y+1) (par induction sur y),
- 4) si  $F(x_1,...,x_k)$  est une fonction RP quelconque, alon il existe un m tel que (pour bont  $x_1,...,x_k$ ):  $F(x_1,...,x_k) < A(m, \max(x_1,...,x_k))$

(par induction sur F),

5) A(x,x) mind pas RP.

#### 7. Représentation arithmétique.

Appelons <u>RE-formules</u> les expressions engendrées par les règles suivantes;

- 1) pour tout polynôme  $p(x_1,...,x_k)$  à coefficients dans  $\mathbb{Z}$ , l'équation  $p(x_1,...,x_k) = 0$  est une RE-formule;
- 2) si  $\varphi_1$  et  $\varphi_2$  sont des RE-formules, alons  $\varphi_1 \wedge \varphi_2$  et  $\varphi_4 \vee \varphi_2$ sont des RE-formules (où  $\Lambda = eL$ , V = ou);
- 3) si q est une RE-formule, alons (3x) q et (4x<y) q sont des RE-formules.

Pour chaque RE-formule  $(\varphi(x_1,...,x_k))$  (dont les variables libres sont  $(x_1,...,x_k)$  on dit que  $\{(x_1,...,x_k) \in \mathbb{N}^k \mid \varphi(x_1,...,x_k)\}$  est l'ensemble représenté par celle-ci.

Théorème de représentation: les sons-ensembles RE de INR sont ceux qui sont représentables par une RE-formule  $\varphi(x_1,...,x_k)$ .

En effet, on voit diabord facilement que les ensembles représentés par les RE-formales sont RE. Pour la réciproque, il suffit (grâce au théorème de la forme normale de Kleene) de l'établir pour les graphes des fonctions RP. On procède par induction: c'est immédiat pour les fonctions de base et le principe de composition, et pour le principe de récursion il suffit diutiliser la fonction

B de Gödel définie ci-après.

Par définition, B(c,d,i) = p(c,1+(i+1)d) où p(a,b) = le reste de la division de a par b. On montre facilement que

1) le graphe de B est représentable par une RE-formule;

2) jour toute suite finie a, a,,..., an d'éléments de IN, il existe c, d ∈ IN tels que (3(c,d,i) = a; pour i=0,1,...,n. (en effet, soit s = max(n, a, a,,..., an) et posons d=s!; on voit facilement que pour i=0,1,...,n, les nombres 1+(i+1) d sont premiers deux à deux, donc c est fourni par le lemme chinois).

L'exemple simple de la fonction 2° montre comment utiliser la fonction B dans le paincipe de récursion:

 $2^{x} = y \leftrightarrow (\exists a_0 a_1 ... a_x)(a_0 = 1 \land (\forall i < x)(a_{i+1} = 2a_i) \land a_x = y)$   $\leftrightarrow (\exists cd)(\beta(c,d,o) = 1 \land (\forall i < x)(\beta(c,d,i+1) = 2\beta(c,d,i)) \land \beta(c,d,x) = y)$   $\leftrightarrow RE-formule.$ 

Le théorème de représentation conduit facilement au théorème d'incomplétude de Gödel. Disons qu'une théorie est assez forte si on peut y démontrer les formules suivantes (on une interprétation de celles-ci):

 $\begin{cases} (\forall x)(x+1 \neq 0), (\forall x \neq 0)(\exists y)(x=y+1), (\forall xy)(x+1=y+1 \rightarrow x=y), \\ (\forall x)(x+0=x), (\forall xy)(x+(y+1)=(x+y)+1), \\ (\forall x)(x.0=0), (\forall xy)(x.(y+1)=x.y+x). \end{cases}$ 

On peut montrer, par induction sur q, que si T est assez forte, alors pour toute RE-formule  $\varphi(x_1,...,x_k)$  et tout  $n_1,...,n_k \in IN$ :

 $(p(n_1,...,n_k) \rightarrow T+ (p(n_1,...,n_k))$  (où k=démontre).

De plus, on a l'implication inverse dès qu'on suppose que T possède un  $\omega$ -modèle (c-à-d un modèle dont la structure des entiers est isomorphe à IN, c-à-d un modèle dont les entiers sont standard).

Nous dirons qu'une théorie est convenable si elle est assez forte, si elle a un  $\omega$ -modèle et si l'ensemble de ses axiomes (donc aussi elle a un  $\omega$ -modèle et si l'ensemble de ses axiomes (donc aussi

l'ensemble de ses théorèmes) est RE.

Théorème d'incomplétude (Gödel): si  $\varphi(x)$  est une RE-formule qui représente un ensemble RE non récussif, alors pour toute théorie T convenable il existe un nEIN tel que

TH (m) of TH 7 (m) (on 7 = non).

Sinon {n/7\$\psi(n)\$ coincidenait avec {n/T+7\$\psi(n)} et snait donc RE, en combradiction avec l'hypothèse que {n/\$\psi(n)\$ est RE mon récursif.

Le théorème de représentation a été fortement amélioné. En 1950, M. Davis a conjecturé que toute RE-formule (\(\pi\_{\pi\_1,...,\pi\_k}\)) est équivalente à une formule diophambienne, c-à-d de la forme (\(\frac{3}{4}\)...\pi\_k)(\(\pi\_{\pi\_1,...,\pi\_k}\), \(\pi\_{\pi\_1,...,\pi\_k}\)) où p est un polynôme à coefficients dans Z. En raisonnant par induction sur (\pi\_1\) on voit facilement que cette conjecture se réduit à la suivante : toute RE-formule de la forme (\(\pi\_{\pi\_2,...,\pi\_k}\))(\(\pi\_{\pi\_1,...,\pi\_k}\))(\(\pi\_{\pi\_1,...,\pi\_k}\), \(\pi\_{\pi\_1,...,\pi\_k}\))(\(\pi\_{\pi\_1,...,\pi\_k}\), \(\pi\_{\pi\_1,...,\pi\_k}\)) est équivalente à une formule diophantienne. En 1961, M. Davis, H. Putnam et J. Robinson ramenaient cette dernière conjecture à la suivante: le graphe de la fonction \(\pi^\pi\) est représentable par une formule diophantienne. Enfin, celle-ci fut démontrée par Yu. Matigacevi\(\pi\) en 1970. On aboutit ainsi au

Théorème de représentation diophantienne (M. Davis, H. Putnam, J. Robinson, Ym. Matijacevič): les sous-ensembles RE de  $IN^k$  sont ceux qui sont représentables par une formule diophantienne  $(\exists y_1...y_\ell)(p(x_1,...,x_k,y_1,...,y_\ell)=0)$ .

(prenve: voir le chapitre VI de Yn. Manin, A course in mathematical logic, Springer).

Corollaire: le 10° problème de Hilbert a une solution négative: il n'y

a pas d'algorithme pour décider si une équation diophantienne en plusieurs variables a une solution dans IN on pas.

#### Exercices:

1) à partir du Héorème de représentation diophantienne, amélioner le Héorème d'incomplétade.

2) montrer que tont sons-ensemble RE de IN peut se meltre sons la forme  $\{p(x,y,...) \mid x,y,... \in IN\} \cap IN (où p = polynôme à coefficients dans <math>\mathbb{Z}$ ).

Maurice BOFFA Université de Mons-Hainaut Institut de Mathématique « Le Pentagone », Avenue du Champ de Mars, 6 B-7000 Mons (Belgique)

#### Cahiers pédagodiques récents

Les cahiers pédagogiques de l'*Institut de Mathématique* sont consultables et téléchargeables sur le site : http://www.umh.ac.be/math/preprints/. Si vous voulez recevoir des copies papier, veuillez écrire à l'adresse suivante :

Institut de Mathématique Université de Mons-Hainaut « Le Pentagone », 6 av. du champ de Mars 7000 Mons, Belgique