Magistère STIC
Devoir de calculabilité

À rendre le 7 novembre 2005

On dira qu'une équation est *Diophantienne exponentielle* (DE en abrégé) si elle est de la forme

$$f(x_1, \ldots, x_n) = 0$$

où f est une expression formée à l'aide de constantes entières positives, des variables $x_1, \ldots, x_n$, du produit, de la somme, de la différence et de l'exponentiation.

Par exemple

$$(p+1)^{n+3} + (q+1)^{n+3} - (r+1)^{n+3} = 0$$

est une équation DE.

Un ensemble E de k-uples d'entiers positifs ou nuls ($k \leq n$) est *Diophantien exponentiel* (DE à nouveau en abrégé) s'il existe une équations DE $f(x_1, \ldots, x_n) = 0$ telle que

$$E = \{(u_1, \ldots, u_k) \in \mathbb{N}^k \mid \exists u_{k+1}, \ldots, u_n \in \mathbb{N}^{n-k}, f(u_1, \ldots, u_n) = 0\}$$

Une fonction $f : \mathbb{N}^k \to \mathbb{N}$ est DE ssi la relation

$$\{(n_1, \ldots, n_k, f(n_1, \ldots, n_k)) \mid (n_1, \ldots, n_k) \in \mathbb{N}^k\}$$

est DE.

L'objet du problème est de démontrer le théorème de Davis & Robinson :

Un ensemble est récursivement énumérable si et seulement si il est DE.

Y. Matjasevich a montré de plus en 1970 que $x = y^z$ est en fait un ensemble *Diophantien polynômial*, montrant ainsi qu'on peut se passer de l'exponentiation dans le théorème de Davis & Robinson. Il en résulte alors par exemple que l'existence de solutions entières à des équations polynômiales est indécidable. Ceci a apporté une réponse (par la négative) en 1970 à l'un des fameux problèmes posés par Hilbert en 1900. (Ici le *10ème problème de Hilbert*).

Question 1

Un ensemble d'entiers E est b-récursivement énumérable ($b \geq 2$), s'il existe une machine de Turing M telle que $L(M)$ est l'ensemble des représentations en base b des entiers de E. Cette définition est étendue aux n-uples de manière standard.

1. Montrer que, pour tous $b.b' \geq 2$, E est b-récursivement énumérable ssi E est b'-récursivement énumérable.

   Si bien qu'on peut parler d'ensemble d'entiers récursivement énumérable, sans préciser la base.
2. Montrer que tout ensemble DE est récursivement énumérable.

Question 2

Si n est un entier on note $n(i,b)$ (où $n(i)$ quand b est clair dans le contexte), le i ème symbole dans la décomposition de n en base b. Les symboles sont comptés en partant de la droite dans l'écriture de n. Lorsque $n < b^i$, $n(i,b) = 0$.

1. Montrer que, si E_1 et E_2 sont deux ensembles DE de n-uples d'entiers, alors $E_1 \cap E_2$ et $E_1 \cup E_2$ sont DE.
2. Montrer que la composée de fonctions DE est DE.
3. Montrer que les fonctions et ensembles suivants sont DE
   (a) $\{(x,y) \in \mathbb{N}^2 \mid x < y\}$
   (b) $f_1(i,n,a,b)$ qui vaut 1 si $n(i,b) = a$ et 0 sinon.
4. On veut montrer ici que la relation suivante est DE : $\{(x,y) \mid \forall i. x(i,2) \leq y(i,2)\}$. On notera la relation $x \preceq_2 y$.
   (a) Si $m \in \mathbb{N}$, soit $e(m)$ l'exposant de la plus grande puissance de 2 qui divise m et $\sigma(m)$ le nombre de 1 dans l'écriture binaire de m. Montrer que $e(m!) = m - \sigma(m)$. (Ind : on pourra remarquer que, quand m est impair, $e(m+1) = \sigma(m) - \sigma(m+1) + 1$)
   (b) Soit $\left(\begin{array}{c} n \\ k \end{array}\right)$ le coefficient binômial $\frac{n!}{(n-k)!k!}$ (0 si $n < k$). Montrer que $e(\left(\begin{array}{c} n \\ k \end{array}\right)) = \sigma(k) + \sigma(n-k) - \sigma(n)$ lorsque $n > k$.
   (c) Déduire des questions précédentes que $k \preceq_2 n$ si et seulement si $\left(\begin{array}{c} n \\ k \end{array}\right)$ est impair
   (d) Montrer que $\left(\begin{array}{c} n \\ k \end{array}\right)$ est DE. (Ind : utiliser 3b).
   (e) Montrer que $\preceq_2$ est DE.
5. Montrer que les fonctions et ensembles suivants sont DE
   (a) $\{(n,b) \in \mathbb{N}^2 \mid \exists k. b = 2^k, \forall i, n(i,b) \in \{0,1\}\}$. On notera alors $\mathsf{bit}(n,b)$ cette relation.
   (b) $f_2(x,y,b,k)$ est l'entier z tel que, pour tout i, $z(i,b) = x(i,b) \times y(i,b)$, si $(x, y \leq b^k$ et $\mathsf{bit}(x,b)$ et $\mathsf{bit}(y,b))$ et 0 sinon.

Question 3

Soit M une machine de Turing. On notera $b = 2^{1+\max(|\Sigma|,|Q|)}$. Si k est un entier et $\gamma = (w_1, q, w_2)$ est une configuration de longueur au plus k telle que w_2 est non vide ($w_2 = aw_2'$), on représentera γ par

- $D_\gamma = w_2'$, (vu comme la représentation d'un entier en base b),
- $G_\gamma = \widetilde{w_1}$ est l'entier représenté par l'image miroir de w_1 en base b,
- $|\Sigma|$ bits $a_{1,\gamma}, \ldots, a_{s,\gamma}$: $a_{i,\gamma} = 1$ si a est le $i$ème symbole de Σ et 0 sinon
- $|Q|$ bits $q_{1,\gamma}, \ldots, q_{r,\gamma}$: $q_{i,\gamma} = 1$ si q est le $i$ème symbole de Q et 0 sinon.

Une suite S de configurations $\gamma_1 \cdots \gamma_n$ représente alors $2+r+s$ entiers $G_S, D_S, A_{1,S}, \ldots, A_{s,S}$, $Q_{1,S}, \ldots, Q_{r,S}$ en base b^k :

- $G_S = G_{\gamma_n} \cdots G_{\gamma_1}$,
- $D_S = D_{\gamma_n} \cdots D_{\gamma_1}$,

– $A_{i,S} = a_{i,\gamma_n} \cdots a_{i,\gamma_1}$.

– $Q_{i,S} = q_{i,\gamma_n} \cdots q_{i,\gamma_1}$

Il peut être utile de considérer que les lettres de Σ (resp. les états de Q) sont codées pour satisfaire : $i < j \Rightarrow \bar{a}_i \prec_2 \bar{a}_j$ (resp. $\bar{q}_i \prec_2 \bar{q}_j$).

1. Montrer que les tuples de $2+r+s$ entiers représentant des configurations initiales (resp. finales) de la machine M forment un ensemble DE.
2. Soit $\delta(q, a) = (q', a', \rightarrow)$ une transition de M. Soient i, j, l, m tels que $q_i = q$, $a_j = a$, $q_m = q'$, $a_l = a'$.

   Montrer que l'ensemble des $2 + r + s$-uples d'entiers $G, D, A_1, \ldots, A_n, Q_1, \ldots, Q_n$ tels que, pour tout e, si $A_j(e, b^k) = 1$ et $Q_i(e, b^k) = 1$, alors $Q_m(e+1, b^k) = 1$ est un ensemble DE. (Ind : on pourra utiliser les fonctions de la question précédente, en particulier $\preceq_2$ et remarquer que $b^k \times Q(i, b^k) = Q(i+1, b^k)$).
3. Soient $G = \sum_{i=0}^{k-1} g_i(b^k)^i$ avec $g_i \in \{0, b^k - 1\}$, $A = \sum_{i=0}^{k-1} \alpha_i(b^k)^i$ avec $\alpha_i \in \{0, 1\}$ et $a_l \in \Sigma$. Montrer que :

   $$\forall i,\ \alpha_i = 1 \Rightarrow (\ \mathrm{reste}(g_i, b) = \bar{a}_l = 2^l) \wedge (\ \mathrm{reste}(g_{i-1}, b^{k-1})) =\ \mathrm{quotient}(g_i, b)$$

   est DE(G, A, a_l, b, k). On fera un schéma pour expliquer les étapes de calcul : voir la figure ci-dessous pour reste$(U_{b,k}, b^k)$ (les entiers sont représentés en base 2).

$U_{b,k}$	$0 \cdots 01$	$0 \cdots 01$	$\cdots$	$0 \cdots 01$	[k blocs de $log(b)$ bits]
reste$(U_{b,k}, b^k)$		$0 \cdots 01$	$\cdots$	$0 \cdots 01$	

   Utiliser ce qui précède pour exprimer la modification du ruban à gauche de la tête de lecture lors d'une transition : $\delta(q, a) = (q', a', \rightarrow)$.
4. Exprimer les autres propriétés des exécutions de la machine de Turing pour montrer que l'ensemble des tuples d'entiers qui représentent des calculs de M est DE. Dans chaque cas, donner une explication claire, accompagnée d'un schéma.
5. En déduire le théorème souhaité.