Maîtrise de Mathématiques

Logique et Complexité, TD9

Natacha Portier

Jeudi 10 avril 2003

Exercice 1 : On dit qu'un problème est "numérique" si sa solution ne dépend que de la taille de l'entrée : montrer que tout problème numérique est P au sens de la structure $(\mathbb{R}; +, -, =, <)$.

Exercice 2 : effet Shannon Montrer que quelquesoit la structure M il existe un problème qui n'est pas $\mathbb{P}$ au sens de M (distinguer le cas où M est infinie du cas où elle est finie). Montrer que si M est finie ou dénombrable il existe un problème booléen (i.e. ne contenant que des mots booléens) qui n'est pas $\mathbb{P}$ au sens de M.

Exercice 3 On considère la structure dite des dictionnaires linéaires dont l'ensemble M sous-jacent est formé d'une part des booléens 0 et 1, d'autre part de toutes les suites infinies $s = (x_0, x_1, \ldots, x_n, \ldots)$ de booléens ; on pose $t(s) = x_0$ et $q(s) = (x_1, x_2, \ldots, x_n, \ldots)$. On prolonge t et q par l'identité sur les booléens. Les seules fonctions de M sont identité, tête et queue, et sa seule relation est l'identité. Montrer que dans cette structure $P = \mathbb{P}$.

Exercice chapitre 1 4,7 p.119

Question 1,1

Donner un circuit booléen qui calcule la somme de deux entiers $y_n ... y_1$ et $x_n ... x_1$ écrits en base 2 de taille n et évaluer sa taille et sa profondeur.

Question 1,2

On améliore la profondeur du circuit précédent de la manière suivante. On suppose que n est une puissance de 2. On calcule en parallèle la somme de $y_{n/2} ... y_1$ et $x_{n/2} ... x_1$ ainsi que les sommes $y_n ... y_{n/2+1} + x_n ... x_{n/2}$ et $y_n ... y_{n/2+1} +$

$x_n ... x_{n/2} + 1$, puis on choisit le résultat en fonction de la retenue. Évaluer la taille et la profondeur du circuit.

Question 1,3

Généraliser la construction précédente (¡¡diviser pour régner¿¿), donner la taille et la profondeur du circuit obtenu.

Exercice On dit que les deux variables x et y sont apariées par la fonction booléenne $f(\ldots, x, \ldots, y, \ldots)$ si $f(\ldots, x, \ldots, y, \ldots) = f(\ldots, y, \ldots, x, \ldots)$ ou bien si $f(\ldots, x, \ldots, y, \ldots) = f(\ldots, \neg y, \ldots, \neg x, \ldots)$. Montrer que dans toute expression booléenne il y a au moins deux variables appariées. En déduire que le selecteur ne peut être calculé par une expression.

Exercice

(i) On dit qu'une fonction f de $\{0;1\}^n$ dans $\{0;1\}$ est monotone si chaque fois que $x_1 \leq y_1$ et ... $x_n \leq y_n$, où $\leq$ représente l'ordre naturel sur $\{0;1\}$, alors $f(\bar{x} \leq f(\bar{y})$; on dit qu'elle est positive si elle s'exprime par un circuit booléen sans négation. Montrer qu'il y a identité entre les fonctions positives et les fonctions monotones.

(ii) On appelle dual du circuit booléen C le circuit C^d obtenu en y remplaçant $\wedge$ par $\vee$, $\vee$ par $\wedge$, 0 par 1 et 1 par 0 ; montrer que si C calcule la fonction $f(x_1, \ldots, x_n)$ alors C^d calcule la fonction $\neg f(\neg x_1, \ldots, \neg x_n)$; montrer que tout terme booléen T est équivalent à un terme booléen T^* de taille et de profondeur inférieures sans porte d'identité et où les portes de négation ne reçoivent leur flèche que d'une entrée étiquetée par une variable.

Définition Un terme est un circuit à une seule sortie dans lequel toute autre porte émet une flèche et une seule. Le circuit a alors la forme d'un arbre. Dessiner un terme et un circuit qui ne soit pas un terme. Une expression booléenne est un

Question 5,1 : circuits booléens

Expliquer comment ajouter 1 de manière naïve (méthode de l'école primaire) à un nombre écrit en binaire. Donner la taille et la profondeur des circuits.

Question 5,2

Paralléliser l'opération précédente pour diminuer la profondeur du circuit et estimer asymptotiquement la taille et la profondeur du nouveau circuit.

Question 2,7 : Question 1,1

Combien y a-t-il de fonctions booléennes de n variables ?
Combien y a-t-il de graphes orientés avec p sommets ?
Donner un majorant du nombre de circuits booléens de taille p.

Définition

Un ensemble X de mots booléens est un problème $P/poly$ s'il existe un polynôme p et une suite de circuits booléens $(C_n(x_1, ..., x_n))_{n \in \mathbf{N}}$ tels que pour tout entier n le circuit C_n ait une seule sortie et soit de taille au plus $p(n)$, et tout n-uplet booléen $a_1, ..., a_n$ appartienne à X si et seulement si $C_n(a_1, ..., a_n)$ calcule 1.

Question 1,2

Montrer que pour tout polynôme p il existe un entier n et une fonction booléenne de n variables qui n'est calculée par aucun circuit de taille $p(n)$.

Question 1,3

En déduire qu'il existe un problème qui n'est pas P/poly.

Question 1,1

Donner un circuit booléen qui calcule la somme de deux entiers $y_n...y_1$ et $x_n...x_1$ écrits en base 2 de taille n et évaluer sa taille et sa profondeur.

Question 1,2

On améliore la profondeur du circuit précédent de la manière suivante. On suppose que n est une puissance de 2. On calcule en parallèle la somme de

$y_{n/2}...y_1$ et $x_{n/2}...x_1$ ainsi que les sommes $y_n...y_{n/2+1}+x_n...x_{n/2}$ et $y_n...y_{n/2+1}+x_n...x_{n/2}+1$, puis on choisit le résultat en fonction de la retenue. Évaluer la taille et la profondeur du circuit.

Question 1,3

Généraliser la construction précédente (¡¡diviser pour régner¿¿), donner la taille et la profondeur du circuit obtenu.

Question 2

Montrer que si C est un circuit booléen dont aucune entrée n'est une sortie, alors :

$$t(C) \leq 3(t(C) - e(C))$$

Question 3

Montrer que pour tout terme T, alors $2e(T) - 1 \leq t(T)$, et il y a égalité si toutes les portes qui ne sont pas des entrées reçoivent deux flèches.

Question 4

Montrer que si T est un terme on peut trouver un terme T' équivalent (donc en particulier avec le nombre d'entrées), de taille et de profondeur inférieure et qui satisfasse :

$$2e(T') - 1 \leq t(T') \leq 3e(T') - 1$$

Question 5

Le nombre de portes d'un circuit C est une mesure pertinente de sa taille. En effet, on montrera que le nombre de flèches est compris entre $t(C) - s(C)$ et $2(t(C) - e(C))$.

Question 6

Montrer que pour tout circuit C :

$$p(C) \leq t(C) - e(C) \ \text{ et } \ t(C) \leq s(C).(2^{p(C)+1} - 1)$$

. Montrer que pour tout terme T, $\log_2(e(T)) \leq p(T)$.

Question 7

Théorème de Hoover, Klawe et Pippenger : À tout circuit booléen C correspond un circuit équivalent C^* de degré sortant deux tel que

$$t(C^*) \leq 3t(C) \ \text{ et } \ p(C^*) \leq 2p(C) + \log_2(s(C))$$

.

Question 7,1

Montrer le résultat pour la taille. Qu'obtient on pour la profondeur ?

Question 7,2

On introduit la notion de pondération dans un arbre binaire renversé. Si toute sortie (toute feuille) est affectée d'un poids, qui est un entier positif, on définit inductivement le poids d'un noeud de l'arbre comme étant le maximum des poids de ses fils, augmenté de un. Montrer que quelle que soit la distribution de poids entiers $a_1, ..., a_n$ dont on affecte les points $p_1, ..., p_n$, il est possible de construire au dessus un arbre renversé dont le poids c de la racine satisfasse $2^c < 2.(2^{a_1} + ... + 2^{a_n})$.

Question 7,3

Soit C un circuit. On le découpe en niveaux à partir du bas. Soit N_0 l'ensemble des sorties et N_1 l'ensemble des portes qui n'émettent des flèches que vers des sorties. L'ensemble N_2 est constitué des portes qui n'émettent des flèches que vers des portes de N_0 ou N_1. On veut que le circuit soit bien étagé, c'est-à-dire que les portes de N_2 n'émettent des flèches que vers des portes de N_1. Pour cela, on ajoute éventuellement des portes d'identité au niveau N_1 entre une porte de N_2 et une sortie. On construit de même tous les niveaux du circuit. Donner un exemple de cette construction sur un circuit de votre choix.

Question 7,4

Utiliser les deux questions précédentes pour montrer le résultat sur la profondeur.

Question 8

Montrer que toute fonction booléenne en n variables peut être représentée par un terme booléen de profondeur (au plus) $n + \log_2 n + 2$ et de taille exponentielle en n. En déduire que pour tout polynôme p il existe pour n assez grand une fonction n-aire non exprimable par un terme de taille $p(n)$. C'est l'effet Shannon. Il montre l'existence de problèmes non-polynomiaux.

Question 9

Montrer que tout circuit acceptant tous les 00..010..00 et refusant 00...0 a une profondeur supérieure ou égale à $\log_2 n$. En déduire que l'expression de la fonction $Sup(x_1, ..., x_n)$ nécessite un circuit de profondeur au moins $\log_2 n$ (et donc qu'il n'est pas raisonnable d'exiger des circuits de profondeur moins que logarithmique).

Question 10

Théorème de Spira : Tout terme booléen de taille t est équivalent à un terme de profondeur inférieure à $4 \log_2 t$.

Le montrer par induction sur t, en extrayant un sous-terme minimal de taille strictement supérieure à t, puis en utilisant le sélecteur.

Question ouverte

P=NC ? C'est le problème du temps parallèle. Est-ce que les circuits sont vraiment plus puissants que les termes ? Est-il possible de transformer de manière polynomiale tout circuit en un terme équivalent ? noindent**Question 1**

Considérons le modèle des **corps différentiels**. Le corps **R** est muni d'une fonction unaire d, appelée dérivée, qui est additive et qui vérifie la formule de Leibniz : pour tous x et y nous avons $d(x+y) = dx+dy$ et $d(xy) = xdy+ydx$. Nous considérons des circuits dont les portes sont soit des entrées étiquetées par une variable ou le réel 1, soit des dérivées et reçoivent une flèche, soit des portes de calcul arithmétique $+$, $\times$ ou $-$ et reçoivent deux flèches.

Question 1,1

Donner le circuit dont les entrées sont x et y et dont l'unique sortie calcule $d(2x + d^2(xy))$, où d^2 désigne la composée $d \circ d$.

Faire ¡¡remonter¿¿ les dérivées : donner un circuit qui calcule la même chose mais dont les uniques portes de dérivées sont situées sous les entrées.

Un tel circuit est dit **réduit**. Nous allons généraliser cette méthode et trouver un polynôme p tel que tout circuit de taille n soit équivalent à un circuit réduit de taille $p(n)$. C'est un outil pour l'étude de la complexité des problèmes dans les corps différentiels.

Question 1,2

Soit C un circuit et δ le nombre maximal de portes de dérivées sur un chemin allant d'une entrée à une sortie. Montrer par induction que C est équivalent à un circuit réduit qui a au plus δ dérivées successives sous chacune de ses entrées.

Remarque : La preuve donne un algorithme de construction du circuit réduit qui fait exploser le nombre de portes...

Question 1,3

Donner un circuit réduit dont les entrées sont x, y et 1 et dont l'unique sortie calcule $d^n(xy)$. Donner sa taille, qui doit être polynomiale en n.

Question 1,4

Soit C un circuit, δ le nombre maximal de portes de dérivées sur un chemin allant d'une entrée à une sortie et N le nombre maximal de portes de calcul arithmétique sur un chemin allant d'une entrée à une sortie.

Nous définissons les niveaux (arithmétiques) du circuit de la manière suivante. Pour i compris entre 0 et N, une porte arithmétique appartient au niveau i si le nombre maximal de portes de calcul arithmétique sur un chemin allant d'une entrée à cette porte est i. Les portes de dérivées successives d'une porte arithmétique appartiennent alors au même niveau qu'elle.

Décomposer le circuit de la question 1,1 en niveaux et montrer qu'une porte arithmétique reçoit ses flèches des niveaux strictement supérieurs.

Un circuit est réduit si toutes les dérivées sont dans le niveau 0.

Question 1,5

Soit i compris entre 1 et N. Supposons que les dérivées les plus basses soient dans le niveau i, et que chaque porte arithmétique dans les niveaux $0, ..., i$ ait δ portes de dérivées successives.

Montrer commment nous pouvons construire un circuit équivalent dont les dérivées les plus basses sont dans le niveau $i-1$, en supprimant les dérivées du niveau i, en laissant inchangés les niveaux $0, ..., i-1$, en ajoutant des portes arithmétiques mais pas de porte de dérivée.

Question 1,6

En déduire une méthode de réduction d'un circuit et le polynôme p, ainsi que la profondeur du circuit obtenu.

Question 2

Soit S une fonction ternaire sur les booléens, appelée sélecteur et telle que pour tous y et z nous ayons $S(0, y, z) = y$ et $S(1, y, z) = z$. Exprimer cette fonction à l'aide des connecteurs logiques et montrer que réciproquement toute fonction booléenne peut s'exprimer avec seulement le sélecteur.

Définitions

Nous généralisons la définition de sélecteur aux entrées réelles : S est un sélecteur si pour tous y et z nous avons $S(0, y, z) = y$, $S(1, y, z) = z$ et si x n'est ni 0 ni 1 alors $S(x, y, z)$ est un polynôme quelconque.

Nous définissons un modèle de calcul sur les réels en généralisant la notion de circuit.

Un *circuit sur le corps* **R** est un graphe orienté sans cycle orienté. Les sommets sont appelés portes, et les arêtes flèches. Ce n'est pas nécessairement un arbre : une porte peut émettre plusieurs flèches. Les portes qui ne reçoivent pas de flèches sont les entrées. Elles sont étiquetées par un élément de **R** ou par une variable. Les autres portes sont étiquetées par une opération arithmétique, $+$, $\times$ ou - et reçoivent deux flèches, ou par un test ¡¡=0?¿¿ ou ¡¡$\geq$ 0?¿¿ et n'en reçoivent qu'une, ou par la fonction sélecteur S et en reçoivent trois. C'est le modèle des **corps ordonnés**.

Le calcul dans un circuit s'effectue de proche en proche de manière canonique. Un porte de test calcule 1 si la réponse est oui et 0 sinon.

Question 3

Montrer que nous pouvons nous passer des portes de sélection en multipliant par une constante le nombre de portes et la profondeur.

Question 4

Supposons qu'il existe des portes de division qui reçoivent deux flèches (nous supposons que le cas de la division par zéro ne se produit jamais). Montrer que nous pouvons nous passer des portes de division pour faire les tests en multipliant par une constante le temps séquentiel et le temps parallèle.

Question 5

Montrer que la fonction calculée par une porte d'un circuit est une fonction polynôme par morceaux, les morceaux étant définis par des systèmes d'équations et d'inéquations polynomiales et les variables des polynômes étant les entrées du circuit.

Question 6

Que calculons nous s'il n'y a pas de porte de multiplication et que seuls les tests d'égalité sont autorisés ? (circuit sur un **groupe**).

Montrer que dans ce cas nous ne pouvons pas nous passer du sélecteur.