Mathématiques Discrètes

ESSI 1

2001-2002

Corrigé de l'examen du Vendredi 16 Novembre 2001

Exercice 1 [Ce type d'exercice a été vu plusieurs fois en TD et devoir, une rédaction particulièrement soignée est donc requise]

Soit Var et Op deux ensembles finis disjoints ne contenant pas les parenthèses.
Soit E l'ensemble défini inductivement par

Base : Var Ì E
*Règle E_1 , E_2 Î E, w Î Op Þ E_1w **(** E_2 **)** Î E*

1) Montrer que tous les mots de E vérifient les deux propriétés suivantes

*i) m contient autant de **(** que **)***
*ii) tout préfixe propre de m contient au moins autant de **(** que de **)***

2) Montrer que le schéma définissant E est libre .

1) Pour ne pas changer, posons A=Var∪ Op et introduisons δ, la fonction de A* dans Z qui a tout mot associe son nombre de (moins son nombre de).
La propriété i) se récrit δ(m)=0
La propriété ii) se récrit tout p préfixe propre de m est tel que δ(p)≥0

Montrons par induction structurelle sur E que tout mot de E vérifie les propriétés i) et ii)
Base : toute variable v est bien telle que δ(v)=0, et de plus un mot réduit à une variable n'a pas de préfixe propre

Supposons que E1 et E2 mots de E vérifient les propriétés i) et ii).
Soit m=E1ω(E2)
δ(m)= δ(E1)+ δ(ω)+ 1+δ(E2) -1 =0
Donc m vérifie la propriété i)
Soit p un préfixe propre de m, Les formes possible pour p sont :

- p_{E1} où p_{E1} est un préfixe (pas nécessairement propre) de E1 donc δ(p_{E1}) ≥0

- E1ω or δ(E1ω) =0

- E1ω(p_{E2} où p_{E2} est un préfixe (pas nécessairement propre) de E2 or δ((E1ω(p_{E2})=1+ δ(p_{E2}) >0

Donc m vérifie bien la propriété ii)

Remarque : ceux qui ont utilisé une décomposition avec des préfixes propres ont souvent oublier des cas.
2) Preuve de la liberté

- il ne peut pas y avoir une variable égale à un mot contenant un opérateur

- il y a une seule règle
- cette règle est injective : Supposons qu'il existe 4 éléments de E : E1 E2 E'1 E'2 ; 2 opérateurs ω, ω' tels que E1 ω (E2)=E'1 ω'(E'2).
    - Si E1 et E'1 sont de la même longueur on a nécessairement E1=E2 et donc ω = ω ' et donc E2=E'2.
    - Mais si E1 est plus court que E'1, alors E1 est un préfixe propre de E'1 et E'1 =E1s. On doit avoir δ (s) =0, (puisque E1 et E'1 vérifient i)) . Puisque E1 ω (E2)=E'1 ω' (E'2) =E1s ω' (E'2), on a ω (E2)=s ω' (E'2), donc s est un prefixe propre de ω (E2)
        - s ne peut pas être égal à ω , car alors on aurait E'1=E1ω et aucun mot de E ne peut se terminer par un opérateur
        - s = ω (est impossible car on doit avoir δ (s) =0
        - de même s=ω (p_{E2} ,avec p_{E2} préfixe de E2, contredit δ (s) =0
    - dans tous ces cas on aboutit à une contradiction donc E1 ne peut être plus court que E'1, le cas symétrique est analogue.
-
    - mais par ailleurs E1 est dans E donc δ (E1)=0, une contradiction. La même contradiction apparaît, si on suppose que E'1 est plus court que E1.

Autre rédaction possible pour l'injectivité : montrer que si E=E1ω (E2), alors ω est le dernier opérateur sous lequel le compteur s'annule. En effet, δ(E1ω)=0, de plus quelque soit un préfixe p_{E2} de E2, δ(E1ω(p_{E2})>0.On a bien δ(E1ω(E2))=0. , mais) n'est pas un opérateur. Donc la position de ω est unique, et un seul découpage est possible.

Remarque :écrire "Mais si E1 est plus court que E'1, alors E1 est un préfixe propre de E'1 et donc δ(E1)≥0 or δ(E1)=0 , contradiction" mais incorrect il n'y a aucune contradiction là dedans.

Exercice 2

*1)Montrer que les polynômes **P** non nuls en x à coefficients dans **R** peuvent être définis inductivement par*

*Base c Î R -{0} Þ p(x)=c Î **P***

*Règle p(x) Î **P**, c Î R Þ q(x)=xp(x)+c Î **P***

*2) Montrer que le schéma définissant **P** est libre*

*3) Définir inductivement la fonction **Degré : P** ® **N** , qui associe à tout polynôme son degré*

*4) Définir inductivement la fonction **X2 : P** ® **P** , telle que X2(p(x)) = p(x^2)*

*5) Définir inductivement la fonction **Calcul : P** x R ® R , qui calcule la valeur de p(x) pour un x dans **R** donné.*

1) Appelons **P** l'ensemble défini inductivement et **Poly** l'ensemble des polynômes en x non nuls à coefficients dans ***R***

   Montrons **P** inclus dans **Poly** : la preuve se fait par induction structurelle:
   Base : un réel non nul est dans **Poly**
   Propagation si p(x) est dans **Poly**, xp(x)+c est aussi dans **Poly**

   Montrons **Poly** inclus dans **P** : la preuve se fait sur les degrés des polynômes de **Poly**
   Base : un polynome non nul de degré zéro est une constante réelle non nulle, il est donc dans **P**.
   Hypothèse d'induction : tous les polynômes non nul de degré inférieur ou égal à n sont dans **P**.

   Soit p(x) un polynôme de degré k+1, il existe k+2 réels a_i tels que $p(x) = \sum_{i=0}^{k+1} a_i x^i$ et a_{k+1} est

non nul. Soit le polynôme $q(x) = \sum_{i=1}^{k+1} a_i x^{i-1}$, q(x) est un polynôme non nul de degré k, par hypothèse de récurrence il est dans **P,** donc p(x) est dans **P ,** par définition de **P.**

2) Le schéma est libre, en effet un polynôme de la base est de degré 0 tandis qu'un polynôme créé par une règle est de degré au moins un. De plus xp(x)+c=xq(x)+c' avec p et q polynôme non nuls implique c=c' (terme de degré zéro) et par suite p(x)=q(x).

3) **Degré :** $\mathbf{P} \to \mathbb{N}$, peut être définie inductivement par

$c \in \mathbb{R}-\{0\}$, **degré**(c)=0

degré(xp(x)+c)=1+**degré**(p(x)).

Preuve : on vérifie que le degré d'une constante non nulle est bien 0 et que si le degré de q(x) est k, alors le degré de xq(x)+c' est k+1 (c'est vrai car q(x) est un polynôme non nul.

4) **X2 : P** $\to$ **P** , peut être définie inductivement par

$c \in \mathbb{R}-\{0\}$, **X2**(c)=c

X2(xp(x)+c)=c+x^2.**X2**(p(x)).

En effet, le changement de variable x donne x^2 ne modifie pas les constantes. Et pour remplacer x par x^2 dans q(x)=xp(x)+c il suffit de remplacer x par x^2 dans p(x) et le facteur x par un facteur x^2

telle que X2(p(x)) = p(x^2)

5) **Calcul :** **P** x $\mathbb{R} \to \mathbb{R}$, peut être définie inductivement par

$c \in \mathbb{R}-\{0\}$, **Calcul(**c,x_0)=c

Calcul(xp(x)+c, x_0)=c+ x_0. **Calcul**(p(x), x_0)

Remarques

1) Un polynôme est une fonction de ***R*** dans ***R*** !!!
2) Le polynôme nul vaut 0 pour tout x de ***R*** ! !!!!!!
3) Le degré de $P_1(x).P_2(x)+c$ (où c est une constante) est égal au degré de P_1 (x) plus le degré de P_2 (x)

Exercice 3

Donnez et prouvez une définition inductive pour l'ensemble des mots binaires comportant un nombre pair de zéro. Votre schéma est -il libre ?

Solution 3.1

Base $\{\varepsilon\} \in E$

Règles R1 :m $\in$ E, 1m $\in$ E

R2 : m, m' $\in$ E, 0m 0m'$\in$ E

Notons MBP les mots binaires comportant un nombre pair de zéros

Montrons E inclus dans MBP

Evident par induction structurelle, car R1 conserve le nombre de « 0 » et R2 en ajoute 2

Montrons MBP inclus dans E

Par récurrence sur la longueur des mots de MBP

Base : tout mot de MBP de longueur zéro est dans E
Hypothèse de récurrence : les mots de MBP de longueur inférieure ou égale à k sont tous dans E
Soit m un mot de MBP de longueur k+1.

- Si la première lettre de m est un 1, alors m=1m' avec m' dans MBP, or m' est de longueur k donc HR m' est dans E, par définition de E (règle 1), m est aussi dans E
- Si la première lettre de m est un zéro alors m contient au moins un nombre zéro (car un est impair). Le mot m s'écrit donc 0p0s où p est un mot (éventuellement vide) ne comportant aucun zéro. P et s sont de longueur inférieur à k et contiennent tous les deux un nombre pair de zéro. On a donc p et s dans E par HR. Mais alors par la règle R2, m est dans E.

Ce schéma n'est pas libre, il y a plusieurs façons de produire le mot 0000, règle R2 avec m=m'=0 ou règle R2 avec m=00 et m' vide;

Solution 3.2

Base $\{\varepsilon\} \in E$

Règles R1 :m $\in$ E, 1 m $\in$ E

R2 : m, m' $\in$ E, 0 m 0$\in$ E

R3 :m $\in$ E, m 1 $\in$ E

Notons MBP les mots binaires comportant un nombre pair de zéros

Montrons E inclus dans MBP

Evident par induction structurelle, car R1 et R3 conservent le nombre de « 0 » et R2 en ajoute 2

Montrons MBP inclus dans E

Par récurrence sur la longueur des mots de MBP

Base : tout mot de MBP de longueur zéro est dans E

Hypothèse de récurrence : les mots de MBP de longueur inférieure ou égale à k sont tous dans E

Soit m un mot de MBP de longueur k+1, de trois choses, l'une :

- la première lettre de m est un 1, alors m=1m' avec m' dans MBP, or m' est de longueur k donc HR m' est dans E, par définition de E (règle 1), m est aussi dans E
- la dernière lettre de m est un 1, alors m=m' 1avec m' dans MBP, or m' est de longueur k donc HR m' est dans E, par définition de E (règle 3), m est aussi dans E
- la première et la dernière lettre de m sont des 0. Le mot m s'écrit donc 0p0 où p est un mot (éventuellement vide) de longueur inférieur à k et contient un nombre pair de zéro. On a donc p dans E par HR. Mais alors par la règle R2, m est dans E.

Ce schéma n'est pas libre, il y a plusieurs façons de produire le mot 11= 1ε = ε1

Les erreurs les plus graves

- Oublier de nommer les deux ensembles et ne pas rédiger la preuve en deux parties d'inclusion réciproque : « E inclus dans MBP » et « MBP inclus dans E »
- Donner une preuve(?) de « MBP inclus dans E » alors que le système inductif est incomplet
- Dans la preuve « MBP inclus dans E » , séparer les mots m suivant des cas issus des règles de E
- Ne pas s'apercevoir dans la preuve « MBP inclus dans E » que des règles ne servent pas.