LICENCE Structures Discrètes – T.D. Induction

Exercice 1   Montrer que, pour $n \geq 2$,

$$\overline{A_1 \cup A_2 \cup \cdots \cup A_n} = \overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_n}$$
$$\overline{A_1 \cap A_2 \cap \cdots \cap A_n} = \overline{A_1} \cup \overline{A_2} \cup \cdots \cup \overline{A_n}$$

(Lois de Morgan généralisées) ◇

Exercice 2   La suite harmonique est définie par $H_n = 1 + 1/2 + \cdots + 1/n$ pour $n \geq 1$. Montrer que $H_{2^n} \geq 1 + n/2$ pour tout $n \geq 0$. ◇

Exercice 3   On prouve la proposition “Toutes les roses ont le même parfum.” par récurrence sur le nombre n de roses. Si $n = 1$, c'est évident. Soit un ensemble $c_1, c_2, \cdots, c_{n+1}$ de $n+1$ roses. Par hypothèse de récurrence $c_1, \cdots, c_n$ est un ensemble de n roses qui ont donc le même parfum. De même, $c_2, c_3, \cdots, c_{n+1}$ est un ensemble de n roses qui ont donc le même parfum. Puisque ces deux ensembles ont en commun $c_2, \cdots, c_n$, les $n+1$ roses ont le même parfum. Où est l'erreur ? ◇

Exercice 4   On considère le polynôme à coefficient réels $P(x) = \frac{1}{3}x^3 + ax^2 + bx$.
1)   Trouver a et b pour que $\forall x \in \mathbb{R}$, $P(x+1) - P(x) = x^2$. On suppose dans la suite que cette propriété est vérifiée.
2)   Montrer que $\forall n \in \mathbb{N}$, $P(n)$ est un entier.
3) $\forall n \geq 0$, on pose $S_n = \sum_{k=0}^{n} k^2$. Montrer que

$$\forall n \geq 0, \quad S_n = P(n+1) = \frac{n(n+1)(2n+1)}{6}.$$ ◇

Exercice 5   Soit $H_n = 1 + 1/2 + \cdots + 1/n$ pour $n \geq 2$. Montrer que H_n n'est pas entier pour $n \geq 2$. ◇

Exercice 6   On rappelle que les nombres de Fibonacci sont définis par $F_n = F_{n-1} + F_{n-2}$ pour $n > 1$ et $F_0 = 0$, $F_1 = 1$. Montrer que pour tout $n > 0$:

1) $F_1 + F_3 + \cdots + F_{2n-1} = F_{2n}$.
2) $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$.
3) $F_1^2 + F_2^2 + \cdots + F_n^2 = F_n F_{n+1}$
4) F_{3n} est pair.
5) $\varphi^{n-2} \leq F_n \leq \varphi^{n-1}$, où $\varphi = \frac{1+\sqrt{5}}{2}$ est racine du polynôme $x^2 - x - 1$. ◇

Exercice 7   Donner une définition inductive de $f(n) = a^{2^n}$.

Indication. On pourra remarquer que $a^{2^{n+1}} = \left(a^{2^n}\right)^2$. ◇

Exercice 8   1) Montrer que $\forall n \in \mathbb{N}$, $(n+1)^2 - (n+2)^2 - (n+3)^2 + (n+4)^2 = 4$.
2) En déduire que tout entier m peut s'écrire comme somme et différence des carrés $1^2, 2^2, \ldots, n^2$ pour un certain n, c'est-à-dire

$$\forall m \in \mathbb{N}, \exists n \in \mathbb{N}, \exists \varepsilon_1, \ldots, \varepsilon_n \in \{-1, 1\}, \; m = \varepsilon_1 1^2 + \varepsilon_2 2^2 + \cdots + \varepsilon_n n^2$$

(Indication: montrer d'abord le résultat pour $m \in \{0, 1, 2, 3\}$). ◇

Exercice 9   On considère le sous-ensemble D de $\mathbb{N} \times \mathbb{N}$ défini inductivement par :

T.S.V.P.

(i) $(n, 0) \in D$
(ii) si $(n, n') \in D$, alors $(n, n + n') \in D$
1) Donner quelques éléments de D.
2) Montrer par récurrence sur k que si $n' = kn$ alors $(n, n') \in D$.
3) Montrer que si $(n, n') \in D$, alors pour $k \in \mathbb{N}$, on a $n' = kn$. ♢

EXERCICE 10 On dit qu'un ensemble ordonné est un *treillis* si tout sous-ensemble fini d'éléments de E admet une borne supérieure et une borne inférieure.

Montrer qu'un ensemble ordonné $(E, \leq)$ est un treillis si et seulement si tout sous-ensemble à deux éléments de E admet une borne supérieure et une borne inférieure.

Indication: montrer par récurrence sur n que si tout sous-ensemble à deux éléments de E admet une borne supérieure et une borne inférieure, alors tout sous-ensemble fini à n éléments de E admet une borne supérieure et une borne inférieure. ♢

EXERCICE 11 Donner une définition inductive de la hauteur $h(t)$, du nombre de nœuds $n(t)$, du nombre d'arêtes $ar(t)$ et du nombre de feuilles $f(t)$ d'un arbre binaire. ♢

EXERCICE 12 Soit t un arbre, $h(t)$ sa hauteur, $n(t)$ le nombre de ses nœuds, $f(t)$ le nombre de ses feuilles. On suppose que t est un arbre binaire (0, 1 ou 2 fils par nœud). Montrer que $n(t) \leq 2^{h(t)} - 1$, et que $f(t) \leq 2^{h(t)-1}$. ♢

EXERCICE 13 Soit t un arbre binaire *strict* (c'est-à-dire que t est non vide, chaque nœud de t a exactement 0 ou 2 fils et il n'y a aucun noeud avec un seul fils non vide). Soit $n(t)$ le nombre de ses nœuds, $f(t)$ le nombre de ses feuilles et $a(t)$ le nombre de ses arêtes.

1) Donner une définition de l'ensemble ABS des arbres stricts.
2) Montrer que si t est un arbre binaire *strict* non vide $n(t) = a(t) + 1$.
3) Montrer que si t est un arbre binaire *strict* non vide $n(t) = 2f(t) - 1$. ♢

EXERCICE 14 Un arbre n-aire *complet* est un arbre où :

- chaque nœud interne a exactement n fils,
- toutes les feuilles sont à la même profondeur.

L'arbre vide est un arbre n-aire de profondeur 0.

1) Donner une définition inductive des arbres n-aires complets et étiquetés sur l'alphabet $A = \{a\}$ (toutes les nœuds sont étiquetés a).
2) Donner une définition inductive des arbres n-aires complets et étiquetés sur un alphabet A non réduit à un unique élément.
3) Donner une définition inductive du nombre de nœuds et du nombre d'arêtes d'un arbre n-aire complet de profondeur k. ♢

EXERCICE 15 Définir le parcours préfixe d'un arbre binaire. ♢

EXERCICE 16 (Fonction d'Ackerman) Soit $f: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ définie par :

$$f(0, n) = n + 1,$$
$$f(m, 0) = f(m - 1, 1),$$
$$f(m, n) = f(m - 1, f(m, n - 1)).$$

1) Montrer que $f(m, n)$ est définie pour tout couple $(m, n) \in \mathbb{N} \times \mathbb{N}$.
2) Soit $g: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ définie par :

$$g(0, n) = n + 1,$$
$$g(m, 0) = g(m - 1, 1),$$
$$g(m, n) = g(m - 1, g(m, n + 1)).$$

Pour quels couples $(m,n) \in \mathbb{N} \times \mathbb{N}$ la fonction $g(m,n)$ est-elle définie ?
3) Calculer $f(1,n)$, $f(2,n)$ et $f(3,n)$. $\diamondsuit$

EXERCICE 17 Les listes de lettres L de l'alphabet A sont définies inductivement par :
(B) $\varepsilon \in L$,
(I) $\forall l \in L$, $\forall a \in A$, $(al) \in L$.
Définissons $g(x,y)$ sur $L \times L$ par : $\forall a \in A$, $\forall l \in L$, $\forall y \in L$,

$$g(\varepsilon, y) = y \;,$$
$$g((al), y) = g(l, (ay)) \;.$$

1) Soit $Q(x)$ le prédicat '$\forall y$, $g(x,y)$ est défini'. Prouver par induction sur x que $Q(x)$ est vrai sur L.
2) Calculer $g((a_1), y)$, pour $a_1 \in A$, $y \in L$.
3) Prouver par induction sur n (pour $n \geq 1$) que

$$g\big((a_n(a_{n-1}(\ldots(a_1)\ldots))), y\big) = g\big(\varepsilon, (a_1(\ldots(a_{n-1}(a_n y))\ldots))\big).$$

4) Soit $rev(x) = g(x, \varepsilon)$. Déduire de la question 3 que, pour $a_1, \ldots, a_n \in A$,
$rev\big((a_n(a_{n-1}(\ldots(a_1)\ldots)))\big) = (a_1(\ldots(a_{n-1}(a_n))\ldots))$. $\diamondsuit$

Les notations qui suivent sont communes aux exercices 18 à 25. Un ensemble E muni d'une opération $*$ associative est un semi-groupe. Si de plus E possède un élément neutre e pour $*$ on dit que $(E, *, e)$ est un monoïde. Etant donné un ensemble A, le monoïde libre sur A, noté A^*, est l'ensemble des suites finies d'éléments de A (dont la suite vide, notée ε). Dans ce cas, l'opération qui fait de A^* un monoïde est la concaténation, notée . ("point"), qui admet la suite vide ε, pour élément neutre.

EXERCICE 18 On considère le monoïde libre A^* sur un alphabet fini A. On note u^p le mot $u \ldots u$, où p exemplaires de u ont été concaténés. On dit que mot u est un *facteur gauche* d'un mot v, s'il existe un mot w tel que $v = uw$, (de même, u est facteur droit de v si on peut écrire $v = wu$). Soit α et β deux mots.
1) Montrer qu'une condition nécessaire et suffisante pour que l'un d'entre eux soit facteur gauche de l'autre est qu'il existe deux mots u et v tels que $\alpha u = \beta v$.
2) On suppose que $\alpha\beta = \beta\alpha$. Montrer que cela équivaut à : $\exists \gamma \in A^*, \exists (p,q) \in N \times N, \alpha = \gamma^p, \beta = \gamma^q$. $\diamondsuit$

On appelle *langage* (sur l'alphabet A) un sous-ensemble de A^*. Si L_1 et L_2 sont deux langages de A^*, on définit leur concaténation par :

$$L_1.L_2 = \{u.v \mid u \in L_1,\ v \in L_2\}$$

La concaténation de langages est une opération associative admettant $\{\varepsilon\}$ comme élément neutre. On peut alors définir les puissances d'un langage L par : $L^0 = \{\varepsilon\}$ et $L^{n+1} = L^n.L = L.L^n$. Enfin, l'étoile d'un langage L est le sous-monoïde de A^* engendré par L c'est à dire :

$$L^* = \bigcup_{n \in \mathbb{N}} L^n$$

Exercice 19 Les notations sont les mêmes que dans l'Exercice 18. On définit inductivement les langages *rationnels* (on dit aussi *réguliers*) par :

(i) Un langage fini est rationnel,
(ii) Si L_1 et L_2 sont rationnels alors $L_1 \cup L_2$ est rationnel,
(iii) Si L_1 et L_2 sont rationnels alors $L_1.L_2 = \{uv, u \in L_1, v \in L_2\}$ est rationnel,
(iv) Si L est rationnel alors $L^* = \bigcup_{n \geq 0} L^n$ est rationnel ($L^0 = \{\epsilon\}$).

On appelle *miroir* du mot $u = a_1 \cdots a_n$, le mot $\tilde{u} = a_n \cdots a_1$. Si L est un langage, on définit $\tilde{L} = \{\tilde{u}, u \in L\}$. Montrer que si L est un langage rationnel, alors $\tilde{L}$ est également rationnel. ♢

Exercice 20 [Lemme d'Arden] Soient L et M deux langages de A^* tels que $\varepsilon \notin L$, montrer que l'équation $X = L.X \cup M$ admet pour unique solution le langage $L^*.M$. ♢

Exercice 21
1) Définir la relation “est un préfixe de” sur A^*. S'agit-il d'une relation d'ordre ? si oui, s'agit-il d'un ordre total ou d'un ordre partiel ?
2) En supposant que A est muni d'un ordre total $\preceq_A$, définir l'ordre lexicographique sur A^*. S'agit-il d'un ordre total ou d'un ordre partiel ?
3) Soit $A = \{a, b\}$ tel que $a \preceq_A b$. Montrer que l'ordre lexicographique défini à la question précédente n'est pas un ordre bien fondé. ♢

Exercice 22 Soient $(A, \leq_1)$ et $(B, \leq_2)$ deux ordres bien fondés. Les ordres suivants sont-ils bien fondés ?
1. sur $A \times B$, l'ordre produit ($(a, b) \leq (a', b') \Longleftrightarrow (a \leq_1 a') \wedge (b \leq_2 b')$).
2. sur $A \times B$, l'ordre lexicographique. ♢

Exercice 23 Les ordres suivants sont-ils bien fondés ?
1. sur A^2, l'ordre lexicographique (A alphabet totalement ordonné).
2. sur $\mathbb{N}$ $m \leq n$ ssi m divise n.
3. sur l'ensemble des diviseurs d'un entier donné, la relation du 2.
4. sur A^*, l'ordre préfixe.
5. sur A^*, l'ordre $u \leq v$ ssi u est un sous-mot de v.
6. sur A^*, l'ordre lexicographique (A alphabet totalement ordonné).
7. sur $A^*/\equiv$, l'ordre des longueurs $u \leq v$ ssi $|u| \leq |v|$ (où $\equiv$ est défini par $u \equiv v$ si et seulement si $|u| = |v|$). ♢

Exercice 24 L'ordre préfixe sur A^* peut être défini de deux manières différentes :
(1) $\forall m_1, m_2 \in A^* \quad m_1 \preceq^1_{pref} m_2$ si et seulement si $\exists m_3 \in A^* \quad m_1 m_3 = m_2$
(2) Définition inductive :
(B) $\forall m \in A^* \quad \varepsilon \preceq^2_{pref} m$
(I) Si $m_1, m_2 \in A^*$ sont tels que $m_1 \preceq^2_{pref} m_2$, alors pour tout $a \in A$, $am_1 \preceq^2_{pref} am_2$

Montrer que ces deux définitions sont équivalentes. ♢

Exercice 25 Soit A^* le monoïde libre engendré par l'alphabet A.
Le miroir d'un mot $u = a_1 a_2 \cdots a_n$ est le mot $\tilde{u} = a_n \cdots a_2 a_1$. Donner une définition inductive du miroir. ♢

Exercice 26 Soit $F_0 = \{a\}$, $F_1 = \{s\}$, $F = F_0 \bigcup F_1$. L'ensemble T des termes construits sur F est $T = \{a, s\big(a\big), s\big(s\big(a\big)\big), \ldots\}$.
Posons $V = \mathbb{N}$. Soit $h\colon F_0 \longrightarrow V$, et $h_s\colon V \longrightarrow V$; il existe une et une seule fonction h^* de T dans V telle que:
(B') Si $t \in F_0$, $h^*(t) = h(t)$,
(I') Si $t = f\big(t_1, \ldots, t_n\big)$, $h^*(t) = h_f(h^*(t_1), \ldots, h^*(t_n))$.

Calculer h^* dans les cas suivants :
1) $h_1(a) = 0$, $h_{1s}(n) = n + 1$.
2) $h_2(a) = 1$, $h_{2s}(n) = 2n$.
3) $h_3(a) = 1$, $h_{3s}(n) = n + 2$. $\diamondsuit$

EXERCICE 27 Soit X un ensemble de symboles de variable et F un ensemble de symboles de fonction, on définit inductivement l'ensemble $T(F, X)$ des termes sur F et X de la façon suivante :

(B) Si $x \in X$ alors $x \in T(F, X)$; si $f \in F_0$, alors $f \in T(F, X)$;
(I) Si $t_1, \ldots, t_n \in T(F, X), n \geq 1$ et $f \in F_n$, alors $f(t_1, \ldots t_n) \in T(F, X)$. ($F_n$ est l'ensemble des symboles de fonction d'arité n.

1) Une application φ de $T(F, X)$ dans $T(F, X)$ est un *morphisme* si elle vérifie $\varphi(f_0) = f_0$ pour $f_0 \in F_0$ et $\varphi(f(t_1, \ldots, t_n)) = f(\varphi(t_1), \ldots, \varphi(t_n))$ pour $f \in F_n, n > 0$. Soit une application h de X dans $T(F, X)$, montrer qu'il existe un morphisme unique h^* de $T(F, X)$ dans $T(F, X)$ qui prolonge h (c'est à dire, tel que $\forall x \in X,\ h^*(x) = h(x)$).
2) Une substitution est une opération sur les termes permettant de remplacer certaines variables d'un terme par un terme. Plus formellement, l'ensemble Θ des substitutions est l'ensemble des fonctions de X dans $T(F, X)$:

$$\Theta = \{\theta : X \to T(F, X)\}$$

On notera s_{id} la substitution identité, c'est-à-dire la substitution telle que pour toute variable $x \in X$, $s_{id}(x) = x$. Une substitution θ se prolonge de façon unique en une fonction θ^* de $T(F, X)$ dans $T(F, X)$ définie par :

$$\forall x \in X \quad \theta^*(x) = \theta(x) \ \text{ et } \ \forall f_0 \in F_0 \quad \theta^*(f_0) = f_0$$

$$\forall f \in F_n\ \forall t_1, t_2, \cdots, t_n \in T(X, F) \quad \theta^*(f(t_1, t_2, \cdots, t_n)) = f(\theta^*(t_1), \theta^*(t_2), \cdots, \theta^*(t_n))$$

Appliquer une substitution à un terme c'est donc instancier certaines de ses variables par des termes et donc faire augmenter sa taille. Montrer que :

$$\forall \theta \in \Theta\ \forall t \in T(X, F) \quad \tau(\theta^*(t)) \geq \tau(t)$$

où la taille d'un terme est donnée par l'application $\tau : T(X, F) \to \mathbb{N}$ définie par :

$$\tau(t) = \begin{cases} 0 & \text{si } t = x, \\ 1 & \text{si } t = f_0 \in F_0, \\ 1 + \sum_{i=1}^{n} \tau(t_i) & \text{si } t = f(t_1, \cdots, t_n). \end{cases}$$

3) On peut définir un préordre (i.e. une relation réflexive et transitive) sur $T(X, F)$ comme suit : $t_1 \preceq t_2$ si et seulement si il existe une substitution θ telle que $\theta^*(t_1) = t_2$. Montrer que cette relation définit bien un préordre (ce préordre est appelé préordre de filtrage).
4) Pourquoi le préordre de filtrage ne définit-il pas une relation d'ordre (i.e. une relation réflexive, antisymétrique et transitive) ?
5) Dans cette question nous allons voir qu'il est possible de définir une relation d'ordre à partir d'un préordre.

Soit E un ensemble muni d'un préordre $\preceq$.

a) Montrer que la relation $\approx$ définie par $x \approx y$ ssi soit $x = y$ soit $x \preceq y$ et $y \preceq x$ est une relation d'équivalence (i.e., une relation réflexive, symétrique et transitive).
b) On note $[x]_{/\approx} = \{y \mid y \approx x\}$ la classe d'équivalence de x et $E_{/\approx}$ l'ensemble des classes d'équivalence de E pour $\approx$ (ensemble quotient). Montrer que la relation $\overline{\preceq}$ définie sur $E_{/\approx}$ par $[x]_{/\approx} \overline{\preceq} [y]_{/\approx}$ ssi $x \preceq y$ est une relation d'ordre (cet ordre est appelé ordre quotient du préordre $\preceq$).
6) D'après la question précédente, on peut définir une relation d'équivalence sur les termes comme suit :

$$t_1 \equiv t_2 \ \ ssi \ \ t_1 = t_2 \ \ ou \ \ (t_1 \preceq t_2 \ \ et \ \ t_2 \preceq t_1)$$

En fait, la relation $\equiv$ identifie les termes équivalents à un renommage près des variables. A partir de cette relation d'équivalence entre termes, il est alors possible de construire une relation d'ordre $\overline{\preceq}$ sur l'ensemble quotient $T(X,F)_{/\equiv}$ définie par :

$$[t_1]_{/\equiv} \overline{\preceq} [t_2]_{/\equiv} \ \ ssi \ \ t_1 \preceq t_2$$

On remarquera que tous les termes d'une même classe d'équivalence ont la même taille.

(i) Soit $\Lambda(t)$ le nombre de variables distinctes apparaissant dans le terme t. Montrer que $t \prec t'$ et $\tau(t) = \tau(t') \Longrightarrow \Lambda(t') < \Lambda(t)$.

(ii) Montrer que $\overline{\preceq}$ est un ordre bien fondé sur $T(X,F)_{/\equiv}$. ♢

Exercice 28 1. On suppose qu'une propriété P définie sur $\mathbb{N}$ vérifie :
(i) $P(1)$ est vraie
(ii) si $P(n)$ est vraie alors $P(2n)$ est vraie (pour $n \geq 1$)
(iii) si $P(n)$ est vraie alors $P(n-1)$ est vraie (pour $n \geq 2$).

Montrer par récurrence sur n que $P(n)$ est vraie pour tout $n \geq 1$.

2. On veut montrer que la moyenne arithmétique est supérieure à la moyenne géométrique. Soient $a_1, \ldots, a_n$ n nombres réels positifs, avec $n \geq 1$; on pose $A = (a_1 + \cdots + a_n)/n$ et $G = (a_1 \cdots a_n)^{1/n}$, montrer que $A \geq G$. ♢