STRUCTURES DISCRÈTES — CORRIGÉ DU PARTIEL DU 31 OCTOBRE 2007

EXERCICE 1

Montrons tout d'abord que f est injective. Soient n et m entiers relatifs, tels que $f(n) = f(m)$. Il se présente 4 cas, selon le signe de chacun des deux entiers :

- si n et m sont tous deux négatifs ou nuls, alors par définition $f(n) = n^2$ et $f(m) = m^2$ et n et m sont de même signe. Or la fonction $n \mapsto n^2$ est injective sur $\mathbb{Z}_-$ et on conclut que $n = m$.
- si n et m sont tous deux strictement positifs, alors par définition $f(n) = n^2 + 1$ et $f(m) = m^2 + 1$ et n et m sont de même signe. Or la fonction $n \mapsto n^2 + 1$ est injective sur $\mathbb{Z}_+^*$ et on conclut que $n = m$.
- si n est négatif et m est positif alors $f(n) = n^2$ et $f(m) = m^2+1$. De $f(n) = f(m)$, on déduit que $n^2 = m^2+1$, c'est-à-dire que $n^2 - m^2 = 1$, soit $(-n-m) \times (-n+m) = 1$ où $-n \in \mathbb{N}$ et $m \in \mathbb{N}^*$. Puisque $-n \geq 0$ et $m \geq 1$, $-n + m \geq 1$ et cette équation a pour unique solution $-n + m = 1$ et $-n - m = 1$ donc $m = 0$ et $-n = 1$. Or $m \geq 1$ ce qui contredit la conclusion que l'on vient de tirer de l'hypothèse selon laquelle il peut exister deux entiers de signes différents qui ont la même image. Cette hypothèse conduit donc à une contradiction et on en déduit que l'hypothèse était fausse : deux entiers de signes différents ne peuvent pas avoir la même image.
- le cas où n est strictement positif et m est négatif ou nul est identique au précédent.

En conclusion, si $f(n) = f(m)$ alors n et m sont nécessairement de même signe et égaux. Par conséquent f est injective.

Remarques

- *Une erreur fréquente dans les copies consiste à considérer dans le cas de deux entiers de signes différents* n^2 *et* $n^2 + 1$ *comme leurs images et déduire du fait que* $n^2 \neq n^2 + 1$ *pour tout* n *que la fonction est injective.*
- *Une autre erreur fréquente consiste à oublier le cas où* n *et* m *ne sont pas de même signe, qui est pourtant le plus intéressant.*
- *Une dernière erreur fréquente consiste à s'appuyer sur l'injectivité de l'élévation au carré pour déduire de* $n^2 = m^2$ *(resp.* $n^2 + 1 = m^2 + 1$*) que* $n = m$*, sans préciser que* n *et* m *sont de même signe. Or l'équation* $n^2 = m^2$ *admet deux couples de solutions dans* $\mathbb{Z}$ *:* $n = m$ *et* $n = -m$*. Il est donc nécessaire de préciser que* n *et* m *sont de même signe pour que* $n^2 = m^2$ *implique que* $n = m$*.*

f est surjective si et seulement si tout élément de l'ensemble d'arrivée, $\mathbb{N}$, est l'image d'un élément de l'ensemble de départ, $\mathbb{Z}$.

Soit $p \in N$, si p est l'image d'un entier relatif n, soit $n \leq 0$ et $p = n^2$, soit $n \geq 1$ et $p = n^2 + 1$, dans les deux cas $p = |n|^2$ ou $|n|^2 + 1$, c'est-à-dire qu'il existe $m = |n| \in \mathbb{N}$ tel que $p = m^2$ ou $p = m^2 + 1$.

f est donc surjective si et seulement si tout élément p de $\mathbb{N}$ est un carré m^2 ou le successeur d'un carré $m^2 + 1$.

Or c'est loin d'être toujours le cas, ces nombres sont même plutôt rares : entre 0 et 10, citons 3, 6, 7 et 8 qui ne sont ni un carré, ni le successeur d'un carré.

Par conséquent f n'est pas surjective.

Remarque *Une erreur fréquente dans les copies consiste à considérer que* f *est à image dans* $\mathbb{Z}$ *et à considérer le fait qu'il n'y ait aucun nombre négatif comme image comme une preuve du fait que* f *n'est pas surjective. Or dans la surjectivité, l'ensemble d'arrivée est primordial : à l'inverse, si je restreins l'ensemble d'arrivée d'une fonction aux images de l'ensemble de départ j'ai toujours une fonction surjective.*

Une fonction est bijective si et seulement si elle est injective et surjective. f n'est pas surjective donc elle n'est pas bijective.

EXERCICE 2

- Montrons que si $\leq$ est bien fondée sur E alors toute partie non vide de E admet au moins un élément minimal. Pour cela nous allons montrer la contraposée qui a l'avantage d'exprimer des propriétés plus constructives : nous supposons donc qu'il existe une partie non vide A de E qui n'admet pas d'élément minimal. Puisque A est non vide, A contient au moins un élément x_0. A n'admet pas d'élément minimal donc il existe $x_1 \neq x_0$ dans A tel

que $x_1 \leq x_0$, c'est-à-dire $x_1 < x_0$. De même il existe x_2 élément de A tel que $x_2 < x_1$ et ainsi de suite, on construit donc une suite infinie strictement décroissante d'éléments de A.
Nous avons donc montré que s'il existe une partie non vide A de E qui n'admet pas d'élément minimal, alors on peut construire une suite infinie strictement décroissante d'éléments de A, donc de E et donc que $\leq$ n'est pas bien fondée sur E.

– Dans l'autre sens, nous voulons montrer que si toute partie non vide de E admet au moins un élément minimal, alors $\leq$ est un ordre bien fondé sur E. Considérons là encore la contraposée : supposons qu'il existe une suite infinie strictement décroissante d'éléments de E, $\ldots < x_{n+1} < x_n < \ldots < x_1 < x_0$, soit $A = \{x_i, i \in \mathbb{N}\}$, A est une partie non vide de E qui n'admet pas d'élément minimal.
Nous venons donc de montrer que si $\leq$ n'est pas une relation bien fondée alors il existe une partie non vide de E qui n'admet pas d'élément minimal.
Nous en déduisons donc sa contraposée : si toute partie non vide de E admet au moins un élément minimal alors nécessairement $\leq$ est une relation d'ordre bien fondée.

Nous avons montré les deux sens de l'équivalence donc les deux propriétés sont équivalentes.

Remarques

– *Dans les copies il manque souvent la démonstration d'un des sens de l'équivalence, et la démonstration est souvent très insuffisante. Cet exercice, bien que relevant du cours, a été le plus mal traité.*
– *Souvent a été utilisée une « équivalence » entre le fait que $\leq$ soit bien fondée et le fait que E admette un élément minimal. Ce résultat n'est pas vrai (on s'en convaincra aisément sur $\mathbb{R}_+$ qui admet un élément minimal mais pour qui $\leq$ n'est pourtant pas bien fondé puisque je peux construire la suite $x_n = 0.\underbrace{0\ldots0}_{n}1$ strictement décroissante) et semble provenir d'un souvenir erroné du résultat que l'on s'efforce justement de démontrer.*

EXERCICE 3

Là encore il s'agit d'un résultat vu en cours : l'ordre lexicographique sur A^* est bien fondé si et seulement si A admet au plus un élément.

Si $A = \{a\}$, alors A^* muni de l'ordre lexicographique est isomorphe à $\mathbb{N}$ muni de l'ordre sur les entiers $n \mapsto a^n = \underbrace{a\ldots a}_{n}$. Or $\leq$ est un ordre bien fondé sur les entiers donc l'ordre lexicographique sur $\{a\}^*$ aussi.

Si $A = \{a, b, c\}$, alors l'ordre lexicographique sur A^* n'est pas bien fondé car la suite $x_n = a^n b$ est infinie strictement décroissante.

EXERCICE 4

1. Cette définition suit la définition inductive du langage de Dyck :
   $\mathrm{g}(\varepsilon) = 0$, $\mathrm{g}(\,(x)\,) = \mathrm{g}(x) + 1$, $\mathrm{g}(xy) = \mathrm{g}(x) + \mathrm{g}(y)$
   $\mathrm{d}(\varepsilon) = 0$, $\mathrm{d}(\,(x)\,) = \mathrm{d}(x) + 1$, $\mathrm{d}(xy) = \mathrm{d}(x) + \mathrm{d}(y)$.
   Le mot vide ne contient aucune parenthèse. Dans le mot (x), les parenthèses ouvrantes (resp. fermantes) sont soit celle avant (resp. après) x, soit celles de x. De même dans le mot xy, les parenthèses ouvrantes (resp. fermantes) sont soit dans x, soit dans y.
2. On pourrait évidemment dire que g et d ont la même définition inductive (satisfont le même système d'équations) donc que $\mathrm{g}(x) = \mathrm{d}(x)$ pour tout $x \in D$, mais il nous est demandé une démonstration par induction.
   Nous pouvons effectuer ce raisonnement de deux façons :
   – Nous pouvons raisonner directement par induction sur D en démontrant d'une part que $\mathrm{g}(\varepsilon) = \mathrm{d}(\varepsilon)$ et d'autre part que si $x \in D$ et $y \in D$ vérifient $\mathrm{g}(x) = \mathrm{d}(x)$ et $\mathrm{g}(y) = \mathrm{d}(y)$ alors $\mathrm{g}(\,(x)\,) = \mathrm{d}(\,(x)\,)$ et $\mathrm{g}(xy) = \mathrm{d}(xy)$:
     ⋆ $\mathrm{g}(\varepsilon) = 0$ et $\mathrm{d}(\varepsilon) = 0$ par définition donc $\mathrm{g}(\varepsilon) = \mathrm{d}(\varepsilon)$.
     Donc un terme de D construit selon la règle (B) vérifie l'égalité.
     ⋆ Soient $x \in D$ et $y \in D$ qui vérifient $\mathrm{g}(x) = \mathrm{d}(x)$ et $\mathrm{g}(y) = \mathrm{d}(y)$.

Par définition $\mathrm{g}(\,(x)\,) = 1 + \mathrm{g}(x)$ et $\mathrm{d}(\,(x)\,) = 1 + \mathrm{d}(x)$. D'après l'hypothèse d'induction $\mathrm{g}(x) = \mathrm{d}(x)$. En combinant ces deux égalités on obtient $\mathrm{d}(\,(x)\,) = 1 + \mathrm{d}(x) = 1 + \mathrm{g}(x) = \mathrm{g}(\,(x)\,)$.
Par définition $\mathrm{g}(xy) = \mathrm{g}(x) + \mathrm{g}(y)$ et $\mathrm{d}(xy) = \mathrm{d}(x) + \mathrm{d}(y)$. D'après l'hypothèse d'induction, $\mathrm{g}(x) = \mathrm{d}(x)$ et $\mathrm{g}(y) = \mathrm{d}(y)$. En combinant ces deux égalités on obtient $\mathrm{d}(xy) = \mathrm{d}(x) + \mathrm{d}(y) = \mathrm{g}(x) + \mathrm{g}(y) = \mathrm{g}(xy)$.
Donc un terme construit selon la règle (I) à partir de termes qui vérifient l'égalité à démontrer, vérifie lui-même cette égalité.

Par conséquent, puisque D est par construction le plus petit ensemble qui vérifie les règles (B) et (I), tout terme x de D vérifie l'égalité $\mathrm{g}(x) = \mathrm{d}(x)$.

– Nous pouvons par ailleurs prouver par récurrence forte sur le nombre d'applications de la règle (I) la propriété suivante :
$\mathcal{P}(n)$: pour tout $x \in D$, construit par n applications de la règle (I) à partir de la règle (B), $\mathrm{g}(x) = \mathrm{d}(x)$.
Tout d'abord $\mathrm{g}(\varepsilon) = 0$ et $\mathrm{d}(\varepsilon) = 0$ par définition donc $\mathrm{g}(\varepsilon) = \mathrm{d}(\varepsilon)$, l'égalité est vraie pour un terme construit sans application de la règle (I) à partir de la règle (B) et $\mathcal{P}(0)$ est vraie.

Supposons que $\mathcal{P}(i)$ soit vraie pour tout $0 \leq i \leq n$, c'est-à-dire que l'égalité soit vraie pour tout terme construit avec au plus n applications de la règle (I) à partir de la règle (B).
Soit t un terme de D construit avec $n + 1$ applications de la règle (I) à partir de la règle (B), alors :

⋆ soit il existe $x \in D$ construit avec n applications de la règle (I) à partir de la règle (B), tel que $t = (x)$.
Par définition $\mathrm{g}(t) = \mathrm{g}(\,(x)\,) = 1 + \mathrm{g}(x)$ et $\mathrm{d}(t) = \mathrm{d}(\,(x)\,) = 1 + \mathrm{d}(x)$. D'après l'hypothèse d'induction appliquée à x construit avec n applications de la règle (I) à partir de la règle (B), $\mathrm{g}(x) = \mathrm{d}(x)$. En combinant ces deux égalités on obtient $\mathrm{d}(t) = \mathrm{d}(\,(x)\,) = 1 + \mathrm{d}(x) = 1 + \mathrm{g}(x) = \mathrm{g}(\,(x)\,) = \mathrm{g}(t)$.

⋆ soit il existe x et y construits avec au total n applications de la règle (I) à partir de la règle (B), tel que $t = xy$.
Par définition $\mathrm{g}(t) = \mathrm{g}(xy) = \mathrm{g}(x) + \mathrm{g}(y)$ et $\mathrm{d}(t) = \mathrm{d}(xy) = \mathrm{d}(x) + \mathrm{d}(y)$. Or si la construction de x et y a nécessité en tout n applications de la règle (I) à partir de la règle (B), alors chacune des deux a nécessité au plus n applications de la règle (I) à partir de la règle (B) et d'après l'hypothèse d'induction appliquée à x et y , $\mathrm{g}(x) = \mathrm{d}(x)$ et $\mathrm{g}(y) = \mathrm{d}(y)$. En combinant ces deux égalités on obtient $\mathrm{d}(t) = \mathrm{d}(xy) = \mathrm{d}(x) + \mathrm{d}(y) = \mathrm{g}(x) + \mathrm{g}(y) = \mathrm{g}(xy) = \mathrm{g}(t)$.

Dans les deux cas, on a obtenu l'égalité $\mathrm{d}(t) = \mathrm{g}(t)$ et par conséquent $\mathcal{P}(n + 1)$ est vraie.

Nous avons donc démontré $\mathcal{P}(0)$ et $(\forall i, 0 \leq i \leq n, \mathcal{P}(i)) \Longrightarrow \mathcal{P}(n + 1)$ et par conséquent $\mathcal{P}(n)$ est vraie pour tout $n \in \mathbb{N}$.

Puisque D est par construction le plus petit ensemble qui vérifie les règles (B) et (I), pour tout terme x de D, il existe $n \in \mathbb{N}$ tel que x est construit par n applications de la règle (I) à partir de la règle (B). D'après $\mathcal{P}(n)$, on a $\mathrm{g}(x) = \mathrm{d}(x)$.

Par conséquent pour tout terme x de D, on a $\mathrm{g}(x) = \mathrm{d}(x)$.

EXERCICE 5

1. Les flèches du schéma indiquent les relations de division :

$$
\begin{tikzcd}
 & & 30 & & \\
 & 6 \arrow[ur] & & 15 \arrow[ul] & \\
2 \arrow[ur] & & 3 \arrow[ul] \arrow[ur] & & 5 \arrow[ul]
\end{tikzcd}
$$

2. E admet un maximum, 30, car tout élément de E divise 30, $\mathrm{ppcm}(2, 3, 5, 6, 15, 30) = 30 \in E$. En revanche E n'admet pas de minimum car $\mathrm{pgcd}(2, 3, 5, 6, 15, 30) = 1 \notin E$.

3. Les éléments en bas du graphe sont minimaux puisqu'aucun élément de E ne les divise, les éléments minimaux sont donc 2, 3 et 5.

   Seul 30 est maximal car il est le seul à n'avoir pas d'autre multiple dans E que lui-même.

4. A n'admet pas de maximum car $\mathrm{ppcm}(3,6,15) = 30 \notin A$. En revanche A admet un minimum 3 car $\mathrm{pgcd}(3,6,15) = 3 \in A$.

   La borne supérieure de A dans E est le plus petit des majorants de A s'il est présent dans E. Or $\mathrm{ppcm}(3,6,15) = 30 \in E$ donc A admet 30 comme borne supérieure.

   La borne inférieure de A dans E est le plus grand des minorants de A s'il est présent dans E. Or $\mathrm{pgcd}(3,6,15) = 3 \in E$ donc A admet 3 comme borne inférieure.

   6 et 15 sont maximaux car chacun n'a pas d'autre multiple dans A que lui-même.

   Seul 3 est minimal car c'est le seul nombre qu'aucun autre ne divise dans A.

EXERCICE 6

Il suffit de vérifier l'égalité pour les deux valeurs de x.

Pour $x = 0$, $f(x,y) = f(0,y)$, $\overline{x}\,f(0,y) + x\,f(1,y) = 1\,f(0,y) + 0\,f(1,y) = f(0,y)$ donc $f(x,y) = \overline{x}\,f(0,y) + x\,f(1,y)$ si $x = 0$.

Pour $x = 1$, $f(x,y) = f(1,y)$, $\overline{x}\,f(0,y) + x\,f(1,y) = 0\,f(0,y) + 1\,f(1,y) = f(1,y)$ donc $f(x,y) = \overline{x}\,f(0,y) + x\,f(1,y)$ si $x = 1$.

Dans les deux cas, on a $f(x,y) = \overline{x}\,f(0,y) + x\,f(1,y)$ donc quelle que soit la valeur de x cette égalité est vraie.

Remarque *Il n'y avait pas lieu de discriminer sur les deux variables dans cet exercice, c'était plutôt une source de confusion et de complication.*

EXERCICE 7

1.a `Small(a) ∨ (Large(c) ∧ Large(d))`

1.b `(Small(a) ∧ Large(c)) ∨ (Small(a) ∧ Large(d))`

1.c `(Cube(a) ∧ Cube(e)) ∨ (Cube(a) ∧ Cube(f))`

2. Pour vérifier si les formules trouvées en 1.a et 1.b sont équivalentes, nous disposons de trois méthodes :
   - nous pouvons partir de l'idée que la formule de la question 1.b ressemble à la formule de la question 1.a développée par distributivité.
     Pour s'en assurer nous allons effectivement développer la formule de la question 1.a par distributivité du $\vee$ sur le $\wedge$: on obtient `(Small(a) ∨ Large(c)) ∧ (Small(a) ∨ Large(d))`. Ce n'est pas la même formule qu'en 1.b puisque les $\vee$ et les $\wedge$ y jouent des rôles inversés.
     On peut donc penser que ces deux formules ne sont pas équivalentes mais cela ne suffit pas cependant à établir cette non-équivalence des deux formules.
     Pour cela nous allons examiner les deux formules et imaginer comment interpréter `Small(a)`, `Large(c)` et `Large(d)` pour que l'une soit vraie et l'autre fausse : dans la formule de la question 1.a il suffit que a soit petit pour que la formule soit vraie, mais à défaut si c et d sont grands la formule de la question 1.a le sera aussi. Alors que dans la seconde si c et d sont grands mais que a est petit aucune des deux alternatives `Small(a) ∧ Large(c)` et `Small(a) ∧ Large(d)` n'est vraie donc la formule de la question 1.b est fausse. Nous avons donc trouvé une interprétation des formules atomiques pour laquelle les formules des questions 1.a et 1.b n'ont pas la même valeur de vérité et ces deux formules ne sont pas équivalentes.
   - on peut évidemment tout de suite soupçonner que les deux formules ne sont pas équivalentes et chercher un contre-exemple.
   - si l'on n'est pas inspiré ou que l'on a aucune idée sur l'équivalence des deux formules, on peut toujours dresser la table de vérité des ces deux formules sans quantificateurs en tenant compte des valeurs de vérité des trois formules atomiques qui apparaissent dans les deux formules `Small(a)`, `Large(c)` et `Large(d)`.

`Small(a)`	`Large(c)`	`Large(d)`	1.a	1.b
V	V	V	V	V
V	V	F	V	V
V	F	V	V	V
V	F	F	V	F
F	V	V	V	F
F	V	F	F	F
F	F	V	F	F
F	F	F	F	F

on constate donc que si `Small(a)` est vrai et `Large(c)` et `Large(d)` sont tous deux faux ou si `Small(a)` est faux et `Large(c)` et `Large(d)` sont tous deux vrais, la valeur de vérité de ces deux formules n'est pas la même donc ces deux formules ne sont pas équivalentes.
Cette dernière approche est plus lourde mais systématique.

3. Dans ce cas-ci en revanche, il n'y a pas de problème : la formule de la question 1.c est bien équivalente à la formule proposée à la question 3 : la formule de la question 1.c est obtenue par distributivité de $\wedge$ sur $\vee$ dans la formule de la question 3.

EXERCICE 8

Il s'agit là encore d'un exercice classique vu en cours et en TD.

1. L'ensemble AB des arbres binaires étiquetés sur l'alphabet A est la partie de $A \cup \{\emptyset, (,), \, , \}$ définie inductivement par
   (B) $\emptyset \in AB$ (arbre vide)
   (I) $g,\, d \in AB \Longrightarrow \forall a \in A, (a, g, d) \in AB$ (arbre de racine a, de fils gauche g, de fils droit d).
2. Le nombre de noeuds d'un arbre binaire est défini inductivement par :
   (B) $n(\emptyset) = 0$
   (I) $g,\, d \in AB$, $a \in A$, $n((a, g, d)) = 1 + n(g) + n(d)$
   Le nombre d'arêtes d'un arbre binaire est défini inductivement par :
   (B) $ar(\emptyset) = 0$
   $(I0)$ $a \in A$, $ar((a, \emptyset, \emptyset)) = 0$
   $(Il1)$ $g \in AB$, $a \in A$, $g \neq \emptyset$ alors $ar((a, g, \emptyset)) = 1 + ar(g)$
   $(Ir1)$ $d \in AB$, $a \in A$, $d \neq \emptyset$ alors $ar((a, \emptyset, d)) = 2 + ar(d)$
   $(I2)$ $g,\, d \in AB$, $a \in A$, $g \neq \emptyset$ et $d \neq \emptyset$ alors $ar((a, g, d)) = 2 + ar(g) + ar(d)$