SCIENCES SORBONNE UNIVERSITÉ

Mathématiques Discrètes

LU2IN005

ANNÉE 2022-2023

Partiel du 7 novembre 2022

Durée : 1h30

Documents, calculettes et téléphones interdits. Inscrire votre numéro de groupe sur votre copie. La note (entre 0 et 60) est le minimum entre 60 et la somme des points obtenus (entre 0 et 63). **Le barême est donné à titre indicatif.** Dans chaque exercice vous pouvez utiliser les résultats des questions précédentes, même si vous n'avez pas réussi à les démontrer.

Exercice 1 (Total : 15 points)

(1) (6 points) Soit $\mathcal{R} \subseteq \mathbb{Q} \times \mathbb{Q}$ telle que $\frac{n}{m}\mathcal{R}\frac{p}{q}$ si et seulement si $n * q = m * p$. La relation $\mathcal{R}$ est-elle une relation d'équivalence ? Justifier.

> **Solution:** Il faut montrer que $\mathcal{R}$ est réflexive, symétrique, et transitive.
> Montrons que $\mathcal{R}$ est réflexive : soit $\frac{n}{m} \in \mathbb{Q}$, alors $n * m = m * n$, donc $\frac{n}{m}\mathcal{R}\frac{n}{m}$.
> Montrons que $\mathcal{R}$ est symétrique : soit $\frac{n}{m}$ et $\frac{p}{q} \in \mathbb{Q}$ tels que $\frac{n}{m}\mathcal{R}\frac{p}{q}$. Donc $n * q = m * p$. Par commutativité de la multiplication, on a aussi $p * m = q * n$, donc $\frac{p}{q}\mathcal{R}\frac{n}{m}$.
> Montrons que $\mathcal{R}$ est transitive : soient $\frac{n}{m}$, $\frac{p}{q}$ et $\frac{r}{s} \in \mathbb{Q}$ tels que $\frac{n}{m}\mathcal{R}\frac{p}{q}$ et $\frac{p}{q}\mathcal{R}\frac{r}{s}$. Alors $n * q = m * p$ et $p * s = q * r$. Donc, comme $q \neq 0$, on en déduit que $n = m * p/q$, et $r = p * s/q$. Donc $n * s = m * p/q * s = m * p * s/q = m * r$. Ainsi $\frac{n}{m}\mathcal{R}\frac{r}{s}$.
> Donc $\mathcal{R}$ est une relation d'équivalence.

(2) (6 points) Soit E un ensemble non vide. On note $\mathcal{P}(E)$ l'ensemble des parties de E. Soit $f : E \to \mathcal{P}(E)$ telle que $f(e) = \{e\}$, pour tout $e \in E$. La fonction f est-elle injective ? surjective ? bijective ? Est-ce une application ? Justifier vos réponses.

> **Solution:** Soient $e, e' \in E$ tels que $f(e) = f(e')$. Alors $\{e\} = \{e'\}$, donc $e = e'$, et f est injective. Pour tout $e \in E$, $f(e) \neq \emptyset$. Or, $\emptyset \in \mathcal{P}(E)$. Donc f n'est pas surjective, et n'est donc pas bijective. Comme f est définie sur E tout entier, f est une application.

(3) (3 points) Les fonctions suivantes sont-elles injectives ? bijectives ? surjectives ? On rappelle que $\mathbb{R}^+$ désigne les réels positifs.

$$f : \mathbb{R} \to \mathbb{R} \qquad\qquad g : \mathbb{R}^+ \to [0, 1[$$
$$x \mapsto x^2 - 2 \qquad\qquad x \mapsto \frac{x^2}{x^2+1}$$

> **Solution:**
> - — $f(2) = 2 = f(-2)$ donc f n'est pas injective.
>   - Supposons qu'il existe x tel que $x^2 - 2 = -3$, alors $x^2 = -1$ et il n'existe pas de $x \in \mathbb{R}$ tel que $f(x) = -3$ donc f n'est pas surjective.
>   - f n'est donc pas bijective.
> - — Si $\frac{x^2}{x^2+1} = \frac{y^2}{y^2+1}$ alors $x^2(y^2+1) = y^2(x^2+1)$ et $x^2y^2 + x^2 = y^2x^2 + y^2$. Dans ce cas, $x^2 = y^2$. Comme $x, y \geq 0$, on a $x = y$ et g est injective.

— Soit $y \in [0,1[$. Alors $y \geq 0$, et $1-y > 0$, donc $\frac{y}{1-y} \geq 0$ et $g(\sqrt{\frac{y}{1-y}}) = y$ et g est surjective.
— g étant injective et surjective, elle est bijective.

Exercice 2 (Total : 27 points)

(1) (3 points) Soit $\mathcal{P}$ une propriété sur les éléments d'un ensemble ordonné $(E, \preceq)$ muni d'un ordre bien fondé $\preceq$. Énoncer le principe d'induction bien fondée.

Solution:
Si (pour tout $x \in E$, (si pour tout $y \prec x, P(y)$), alors $P(x)$)) alors pour tout $e \in E, P(e)$.

(2) On définit $\leq_{\text{lex}} \subseteq \mathbb{N} \times \mathbb{N}$ par $(n, m) \leq_{\text{lex}} (n', m')$ si et seulement si $n < n'$ ou ($n = n'$ et $m \leq m'$), où $\leq$ est l'ordre usuel sur les entiers naturels.

a. (2 points) L'ordre $\leq_{\text{lex}}$ est-il un ordre total ou partiel ? Justifier.

Solution: C'est un ordre total. En effet, soient (m, n) et $(m', n') \in \mathbb{N} \times \mathbb{N}$.
Comme l'ordre usuel sur $\mathbb{N}$ est un ordre total, on a $m < m'$, $m' < m$ ou $m = m'$:
— Dans le premier cas, on a $m < m'$ donc $(m, n) \leq_{\text{lex}} (m', n')$.
— Dans le second cas, on a $m' < m$ donc $(m', n') \leq_{\text{lex}} (m, n)$.
— Dans le troisième cas $m = m'$, on doit comparer n et n'
  — Soit $n < n'$ et $(m, n) \leq_{\text{lex}} (m', n')$.
  — Soit $n > n'$ et $(m', n') \leq_{\text{lex}} (m, n)$.
  — Soit enfin $n = n'$ et alors $(m, n) = (m', n')$.
Donc pour tout (m, n) et $(m', n') \in \mathbb{N} \times \mathbb{N}$, on a soit $(m, n) \leq_{\text{lex}} (m', n')$, soit $(m', n') \leq_{\text{lex}} (m, n)$.

b. (1 point) Pour la partie $A = \{1, 2, 3\} \times \{0, 2\}$ de $\mathbb{N} \times \mathbb{N}$, représenter $(A, \leq_{\text{lex}})$ par un graphe (sans les arcs de transitivité ni de réflexivité).

Solution:

$$(1,0) \longrightarrow (1,2) \longrightarrow (2,0) \longrightarrow (2,2) \longrightarrow (3,0) \longrightarrow (3,2)$$

c. (4 points) Donner l'ensemble des minorants et des majorants de A dans $\mathbb{N} \times \mathbb{N}$. S'ils existent, donner la borne inférieure, la borne supérieure, le plus petit élément et le plus grand élément. Donner les éléments minimaux et les éléments maximaux.

Solution: L'ensemble des minorants de A est $Min(A) = \{(0, n) \mid n \in \mathbb{N}\} \cup \{(1, 0)\}$, et l'ensemble des majorants de A est $Maj(A) = \{(3, n) \mid n \geq 2\} \cup \{(m, n) \mid m > 3, n \in \mathbb{N}\}$. La borne inférieure, qui est aussi le plus petit élément est $(1, 0)$ et la borne supérieure qui est aussi le plus grand élément est $(3, 2)$. Le seul élément minimal est $(1, 0)$ et le seul élément maximal est $(3, 2)$.

(3) Soit $X \subseteq \mathbb{N} \times \mathbb{N}$ un sous-ensemble non vide de $\mathbb{N} \times \mathbb{N}$.

a. (3 points) Montrer que l'ensemble $X_1 = \{n \in \mathbb{N} \mid \text{ il existe } m \in \mathbb{N} \text{ tel que } (n, m) \in X\}$ admet un élément minimal n_1 pour l'ordre usuel $\leq$ sur les entiers naturels.

Solution: Comme X est non vide, il contient au moins un élément (n_0, m_0), donc $n_0 \in X_1$ et X_1 est non vide. Or, $X_1 \subseteq \mathbb{N}$, et l'ordre usuel sur les entiers naturels étant bien fondé, toute partie non vide de $\mathbb{N}$ admet un élément minimal. Donc X_1 admet un élément minimal n_1.

b. (3 points) Montrer que $X_{n_1} = \{m \in \mathbb{N} \mid (n_1, m) \in X\}$ admet un élément minimal m_1 pour l'ordre usuel $\leq$ sur les entiers naturels.

Solution: On sait que $n_1 \in X_1$ donc il existe $m \in \mathbb{N}$ tel que $(n_1, m) \in X$. Donc X_{n_1} est non vide, et admet donc un élément minimal m_1 car l'ordre usuel sur les entiers naturels est bien fondé.

c. (5 points) En déduire que l'ordre $\leq_{\text{lex}}$ est bien fondé.

Solution: Soit $X \subseteq \mathbb{N} \times \mathbb{N}$ un sous-ensemble non vide de $\mathbb{N} \times \mathbb{N}$. On montre que (n_1, m_1) tel que défini dans les questions précédentes est un élément minimal de X : supposons qu'il existe $(n, m) \in X$ tel que $(n, m) \leq_{\text{lex}} (n_1, m_1)$. Alors par définition de $\leq_{\text{lex}}$, on a soit $n < n_1$, soit $n = n_1$ et $m \leq m_1$. Dans le premier cas, comme $(n, m) \in X$, $n \in X_1$ et $n < n_1$ est en contradiction avec le fait que n_1 est un élément minimal de X_1. Donc $n = n_1$ et $m \leq m_1$. On observe alors que $m \in X_{n_1}$. Comme m_1 est un élément minimal de X_{n_1}, on en déduit, par définition d'un élément minimal, que $m = m_1$. Donc, pour tout $(n, m) \in X$ tel que $(n, m) \leq_{\text{lex}} (n_1, m_1)$ on a $(n, m) = (n_1, m_1)$ et (n_1, m_1) est un élément minimal de X.

On a donc montré que toute partie non vide de $\mathbb{N} \times \mathbb{N}$ admet un élément minimal pour l'ordre $\leq_{\text{lex}}$, cet ordre est donc bien fondé sur $\mathbb{N} \times \mathbb{N}$.

(4) (6 points) On définit la fonction suivante :

```
def foo(m,n):
    if (m != n):
        if (m > n):
            return foo(m-n,n)
        else:
            return foo(m,n-m)
    else:
        return (m,n)
```

On veut montrer la propriété
$\mathcal{P}(m,n)$: « L'appel à `foo(m,n)` termine. » pour tout $(m,n) \in (\mathbb{N} \setminus \{0\}) \times (\mathbb{N} \setminus \{0\})$.
Démontrer la propriété $\mathcal{P}$ par induction bien fondée avec un ordre bien choisi.

> **Solution:** On utilise l'ordre $\leq_{\text{lex}}$. Soit $(m,n) \in (\mathbb{N}\setminus\{0\})\times(\mathbb{N}\setminus\{0\})$, et supposons $\mathcal{P}(m',n')$ vraie pour tout $(m',n') \lneq_{\text{lex}} (m,n)$.
>
> Si $m = n$, alors `foo(m,n)` se termine immédiatement.
>
> Si $m > n$, alors la terminaison de `foo(m,n)` dépend de la terminaison de `foo(m-n,n)`. Comme $n > 0$, $m - n < m$, et comme $m \neq n$, alors $m - n \in \mathbb{N} \setminus \{0\}$. Donc $(m-n,n) \lneq_{\text{lex}} (m,n)$, et par hypothèse d'induction, $\mathcal{P}(m-n,n)$ est vraie et `foo(m-n,n)` termine.
>
> Enfin si $m < n$, alors la terminaison de `foo(m,n)` dépend de la terminaison de `foo(m,n-m)`. À nouveau, comme $m > 0$, $n - m < n$ et comme $m \neq n$, alors $m - n \in \mathbb{N} \setminus \{0\}$. Donc $(m,n-m) \lneq_{\text{lex}} (m,n)$ et par hypothèse d'induction, `foo(m,n-m)` termine. Donc `foo(m,n)` termine.
>
> On a montré que pour tout $(m,n) \in (\mathbb{N} \setminus \{0\}) \times (\mathbb{N} \setminus \{0\})$, si `foo(m',n')` termine pour tout $(m',n') \lneq_{\text{lex}} (m,n)$, alors `foo(m,n)` termine. Par le principe d'induction bien fondée, `foo(m,n)` termine pour tout $(m,n) \in (\mathbb{N} \setminus \{0\}) \times (\mathbb{N} \setminus \{0\})$.

Exercice 3 (Total : 18 points)

(1) On définit l'ensemble ABS des arbres binaires *stricts* étiquetés sur un alphabet A :
— pour tout $a \in A$, $(a, \emptyset, \emptyset) \in ABS$.
— pour tout arbre $g \in ABS$ et $d \in ABS$, pour toute lettre $a \in A$, $(a,g,d) \in ABS$.
On rappelle par ailleurs la définition de l'ensemble AB des arbres binaires étiquetés sur un alphabet A :
— $\emptyset \in AB$,
— pour tout arbre $g \in AB$ et $d \in AB$, pour toute lettre $a \in A$, $(a,g,d) \in AB$.

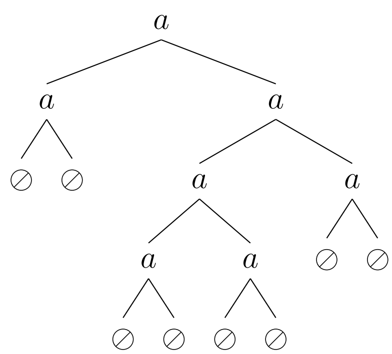
a. (2 points) Donner la fonction $n : AB \to \mathbb{N}$ qui associe à un arbre $t \in AB$ son nombre de nœuds, et la fonction $ns : ABS \to \mathbb{N}$ qui associe à un arbre $t \in ABS$ son nombre de nœuds.

> **Solution:** Par induction structurelle :
> — $n(\emptyset) = 0$
> — pour tout $a \in A$, pour tout $g, d \in AB$, $n(a,g,d) = 1 + n(g) + n(d)$.
> — $ns((a, \emptyset, \emptyset)) = 1$ pour tout $a \in A$
> — pour tout $a \in A$, pour tout $g, d \in ABS$, $ns(a,g,d) = n(g) + n(d) + 1$

On considère à présent un alphabet A réduit à une lettre : $A = \{a\}$. On définit la fonction $f : AB \to ABS$ de la façon suivante :
— $f(\oslash) = (a, \oslash, \oslash)$
— pour tout $g, d \in AB$, $f(a, g, d) = (a, f(g), f(d))$.

b. (3 points) Donner $f(t)$ si $t = (a, \oslash, (a, (a, \oslash, \oslash), \oslash))$. On pourra donner une représentation graphique de $f(t)$.

Solution:



c. (5 points) Montrer par induction structurelle que f est surjective.

Solution: On montre par induction structurelle que pour tout $t \in ABS$, il existe $t' \in AB$ tel que $f(t') = t$
— si $t = (a, \oslash, \oslash)$, alors par définition de f, $f(\oslash) = t$.
— Soient $g, d \in ABS$. Par hypothèse d'induction, il existe $t'_1 \in AB$ et $t'_2 \in AB$ tel que $f(t'_1) = g$ et $f(t'_2) = d$. Donc $f(a, t'_1, t'_2) = (a, g, d)$ par définition de f.

d. (5 points) Montrer que pour tout $t \in AB$, $ns(f(t)) = 2 * n(t) + 1$.

Solution: Si $t = \oslash$, alors $f(t) = (a, \oslash, \oslash)$. On a montré que $ns(a, \oslash, \oslash) = 1$ et $n(\oslash) = 0$. On a donc bien $ns(f(\oslash)) = 2 * n(\oslash) + 1$.
Soient à présent $a \in A$, $g, d \in AB$, et $t = (a, g, d)$. Supposons que $ns(f(g)) = 2 * n(g) + 1$ et $ns(f(d)) = 2 * n(d) + 1$. Par définition de n, f et ns, on sait que :
— $n(t) = 1 + n(g) + n(d)$
— $f(t) = (a, f(g), f(d))$
— $ns(f(t)) = 1 + ns(f(g)) + ns(f(t))$.
Par hypothèse de récurrence, on en déduit que $ns(f(t)) = 1+2*n(g)+1+2*n(d)+1 = 2(1 + n(g) + n(d)) + 1 = 2 * n(t) + 1$.
On a donc montré par induction structurelle sur t que pour tout $t \in AB$, $ns(f(t)) = 2 * n(t) + 1$.

(2) (3 points) Montrer par récurrence sur $n \in \mathbb{N}$ que $8^n - 1$ est un multiple de 7. *Rappel :* $8 = 7+1$.

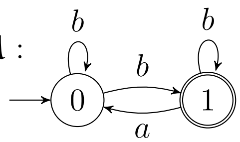
Solution: Montrons la propriété au rang 0 : $8^0 - 1 = 0$ est bien un multiple de 7.
Soit $n \in \mathbb{N}$, et supposons $8^n - 1$ multiple de 7. Alors, $8^{n+1} - 1 = 8.8^n - 1 = (7+1).8^n - 1 = 7 * 8^n + 8^n - 1$. Par hypothèse de récurrence, $8^n - 1$ est un multiple de 7, donc il existe $k \in \mathbb{N}$ tel que $8^n - 1 = 7.k$, donc $7 * 8^n + 8^n - 1 = 7 * 8^n + 7 * k = 7(8^n + k)$ et $8^{n+1} - 1$ est bien un multiple de 7.

On a montré que $8^0 - 1$ est un multiple de 7, et pour tout $n \in \mathbb{N}$, si $8^n - 1$ est un multiple de 7, alors $8^{n+1} - 1$ est un multiple de 7.

Exercice 4 (Total : 3 points)

On considère l'alphabet $A = \{a, b\}$. On note $L = \mathcal{L}(\mathcal{A})$ le langage accepté par l'automate $\mathcal{A}$ suivant :

$\mathcal{A}$:



(1) (1 point) Cet automate est-il déterministe ? complet ? Justifier.

Solution: L'automate n'est pas déterministe, car on a les transitions $(0, b, 0)$ et $(0, b, 1)$. Il n'est pas complet car il n'y a aucune transition étiquetée par a depuis l'état 0.

(2) (2 points) Le mot *baab* est-il accepté par l'automate ? Le mot *babb* ? Justifier vos réponses.

Solution: Le mot *baab* n'est pas accepté par l'automate. En effet, il n'y a aucune exécution d'étiquette *baab* dans l'automate (car il n'y a aucune transition étiquetée par a depuis l'état 0, et la seule transition étiquetée par a mène à l'état 0). Le mot *babb* est accepté par l'automate car il est étiquette de l'exécution : $0 \xrightarrow{b} 1 \xrightarrow{a} 0 \xrightarrow{b} 0 \xrightarrow{b} 1$, qui est acceptante car 1 est acceptant.