Notions mathématiques préliminaires

Ensembles

Définition : Le produit cartésien de n ensembles $\mathcal{A}_1 \ldots \mathcal{A}_n$ est l'ensemble de n-uplets $\mathcal{A}_1 \times \ldots \times \mathcal{A}_n = \{(a_1, \ldots, a_n) \mid a_i \in \mathcal{A}_i\}$. Si $\mathcal{A}_i = \mathcal{A}$ pour tout i, on note simplement par $\mathcal{A}^n$ le produit $\mathcal{A}_1 \times \ldots \times \mathcal{A}_n$.

Définition : Soient deux ensembles t.q. $\mathcal{A}, \mathcal{B} \subseteq \mathcal{E}$.

- L'intersection de $\mathcal{A}$ et $\mathcal{B}$ est $\mathcal{A} \cap \mathcal{B} = \{e \in \mathcal{E} \mid e \in \mathcal{A}$ et $e \in \mathcal{B}\}$
- L'union de $\mathcal{A}$ et $\mathcal{B}$ est $\mathcal{A} \cup \mathcal{B} = \{e \in \mathcal{E} \mid e \in \mathcal{A}$ ou $e \in \mathcal{B}\}$
- La différence $\mathcal{A}$ et $\mathcal{B}$ est $\mathcal{A} \setminus \mathcal{B} = \{e \in \mathcal{E} \mid e \in \mathcal{A}$ et $e \notin \mathcal{B}\}$
- Le complémentaire de $\mathcal{A}$ est $\overline{\mathcal{A}} = \mathcal{E} \setminus \mathcal{A} = \{e \in \mathcal{E} \mid e \notin \mathcal{A}\}$
- $\mathcal{P}(\mathcal{A})$ est l'ensemble qui contient toutes les parties de l'ensemble $\mathcal{A}$.

Relations

Définition : Une relation n-aire sur $\mathcal{A}_1 \ldots \mathcal{A}_n$ est un sous-ensemble de $\mathcal{A}_1 \times \ldots \times \mathcal{A}_n$.

Définition : Soit $R \subseteq \mathcal{A} \times \mathcal{A}$ une relation binaire.

- R est réflexive ssi pour tout $x \in \mathcal{A}$, $(x, x) \in R$. R est iréflexive ssi pour tout $x \in \mathcal{A}$, $(x, x) \notin R$.
- R est symétrique si pour tout $x, y \in \mathcal{A}$, $(x, y) \in R$ implique $(y, x) \in R$. R est anti-symétrique si pour tout $x, y \in \mathcal{A}$, $(x, y) \in R$ et $(y, x) \in R$ implique $x = y$.
- R est transitive si pour tout $x, y, z \in \mathcal{A}$, $(x, y) \in \mathcal{A}$ et $(y, z) \in R$ implique $(x, z) \in R$.

Relations d'équivalence

Une relation d'équivalence est une relation réflexive, symétrique et transitive.

La classe d'équivalence d'un élément $a \in \mathcal{A}$ par rapport à une relation déquivalence $\mathcal{R}$ est l'ensemble $[a] = \{b \in \mathcal{A} \mid a\mathcal{R}b\}$.

Congruences

Une relation d'équivalence $\mathcal{R}$ est une congruence par rapport à une fonction n-aire f ssi pour tout $n \geq 0$, pour tout $a_1, \ldots, a_n$ et pour tout $b_1, \ldots, b_n$

$$a_1 \mathcal{R} b_1 \text{ et } \ldots \text{ et } a_n \mathcal{R} b_n \text{ implique } f(a_1, \ldots, a_n) \mathcal{R} f(b_1, \ldots, b_n)$$

Composition de relations

Définition : Si $\mathcal{R} \subseteq \mathcal{A} \times \mathcal{B}$ et $\mathcal{S} \subseteq \mathcal{B} \times \mathcal{C}$, alors la composition de $\mathcal{S}$ avec $\mathcal{R}$ est une relation dans $\mathcal{A} \times \mathcal{C}$ t.q. $\mathcal{S} \circ \mathcal{R} = \{(x, y) \in \mathcal{A} \times \mathcal{C} \mid \exists z \in \mathcal{B}\ (x, z) \in \mathcal{R}$ et $(z, y) \in \mathcal{S}\}$.

Fonctions

Définition : Une fonction f entre deux ensembles $\mathcal{A}$ et $\mathcal{B}$, notée $f : \mathcal{A} \to \mathcal{B}$, est une relation sur $\mathcal{A} \times \mathcal{B}$ t.q. pour tout x, y, z si $(x, y) \in f$ et $(x, z) \in f$, alors $y = z$.

Notation : On écrit $f(x)$ pour dénoter l'unique élément y t.q. $(x, y) \in f$ et $f(\mathcal{C}) = \{y \in \mathcal{B} \mid \exists x \in \mathcal{C}, f(x) = y\}$.
On note $id_{\mathcal{A}}$ la fonction identité sur $\mathcal{A}$ donnée par $id_{\mathcal{A}}(x) = x$.

Définition : Soit $f : \mathcal{A} \to \mathcal{B}$ une fonction.
- Le domaine de f est $Dom(f) = \{x \in \mathcal{A} \mid \exists y \in \mathcal{B}, (x, y) \in f\}$
- L'image de f est $Im(f) = \{y \in \mathcal{B} \mid \exists x \in \mathcal{A}, (x, y) \in f\}$
- L'inverse de f est $f^{-1} = \{(y, x) \in \mathcal{B} \times \mathcal{A} \mid (x, y) \in f\}$

Composition de fonctions

Définition :
- La composition de $f : \mathcal{B} \to \mathcal{C}$ avec $g : \mathcal{A} \to \mathcal{B}$ est la fonction $f \circ g : \mathcal{A} \to \mathcal{C}$, où $f \circ g(x) = f(g(x))$.
- La n-composition de f avec elle-même , notée f^n, est défini par récurrence sur n :
  - Si $n = 0$, alors $f^0 = id$
  - Si $n > 0$, alors $f^n = f \circ f^{n-1}$

Exercice : Soit $n > 0$. Montrer que $f^n = f^{n-1} \circ f$.

Propriétés des fonctions

Définition : Une fonction $f : \mathcal{A} \to \mathcal{B}$ est injective ssi pour tout $x, y \in \mathcal{A}$, $f(x) = f(y)$ implique $x = y$.

Définition : Une fonction $f : \mathcal{A} \to \mathcal{B}$ est surjective ssi pour tout $y \in \mathcal{B}$ il existe $x \in \mathcal{A}$ tel que $f(x) = y$.

Définition : Une fonction est bijective ssi elle est injective et surjective.

Préordres, ordres

Définition :
- Un préordre est une relation réflexive et transitive.
- Un ordre ou ordre partiel est une relation réflexive, anti-symétrique et transitive.

Notation : $\geq$

Il existe une construction standard qui permet de construire un ordre à partir d'un préordre :

Théorème : Si $\succcurlyeq \subseteq A \times A$ est un préordre, alors :

- la relation $\sim = \{(x, y) | x \succcurlyeq y$ et $y \preccurlyeq x\}$ est une relation d'équivalence
- la relation $\geq = \{([x], [y]) | x \succcurlyeq y\}$ induite sur les classes d'équivalence de $\sim$ est un ordre

Définition : Un ordre strict est une relation iréflexive et transitive.

Notation : $>$

Définition : Un ordre strict sur $\mathcal{A}$ est bien fondé ssi il n'existe aucune chaîne de la forme $a_0 > a_1 > a_2 > \ldots$, où tout $a_i \in \mathcal{A}$.

L'ordre produit

On considère le produit cartésien de n ensembles $\mathcal{A}_1 \ldots \mathcal{A}_n$.

Si chaque $\mathcal{A}_i$ est muni d'un ordre strict $\succ_i$, alors l'ordre produit est défini par

$(a_1, \ldots, a_n) \succ_\times (b_1, \ldots, b_n)$ ssi
- $(a_i \succ_i b_i)$ ou $a_i = b_i$ pour tout $i = 1 \ldots n$,
- et $a_j \succ_j b_j$ pour au moins un indice j

Lemme : La rélation $\succ_\times$ est bien fondée ssi chaque relation $\succ_i$ est bien fondée.

L'ordre lexicographique

Soit $>_{A_i}$ un ordre strict sur l'ensemble $\mathcal{A}_i$.

Ordre lexicographique sur le produit de 2 ensembles :

$$(x, y) >_{lex} (x', y') \text{ ssi } (x >_{A_1} x') \text{ ou } (x = x' \text{ et } y >_{A_2} y')$$

Exemple :

$$(4, "s") >_{lex} (3, "s") >_{lex} (2, "q") >_{lex} (2, "h") >_{lex} (2, "e") >_{lex} (1, "b") >_{lex} (0, "a")$$

Ordre lexicographique (cas général)

Si chaque $\mathcal{A}_i$ est muni d'un ordre strict $\succ_i$, alors l'ordre lexicographique est défini par

$a_1 \succ^{lex}_{A_1} b_1$ ssi $a_1 \succ_1 b_1$

$(a_1, \ldots, a_n) \succ^{lex}_{A_1 \times \ldots \times A_n} (b_1, \ldots, b_n)$ ssi

$(a_1 \succ_1 b_1)$ ou
$a_1 = b_1$ et $(a_2, \ldots, a_n) \succ^{lex}_{A_2 \times \ldots \times A_n} (b_2, \ldots, b_n)$

Théorème : L'ordre lexicographique $\succ^{lex}_{A_1 \times \ldots \times A_n}$ est bien fondé ssi chaque ordre strict $\succ_{A_i}$ est bien fondé.

Avertissement : $\succ^{lex}_{A_1 \times \ldots \times A_n}$ n'est pas exactement l'ordre du dictionnaire : il faut etendre $\succ^{lex}$ aux séquences finies sur l'alphabet pour l'obtenir.

Une application :

	Ackerman(0,n)	=	n+1
Exemple :	Ackerman(m+1,0)	=	Ackerman(m,1)
	Ackerman(m+1,n+1)	=	Ackerman(m,Ackerman(m+1,n))

Ordres multi-ensembles

Soit $\mathcal{A}$ un ensemble. Un multi-ensemble de base $\mathcal{A}$ est une fonction $\mathcal{M} : \mathcal{A} \to \mathbb{N}$.

Le multi-ensemble $\mathcal{M}$ est fini si $\mathcal{M}(x) > 0$ seulement pour un nombre fini d'éléments de $\mathcal{A}$.

Notation : $\{\!\{a, a, b\}\!\}$.

Soient $\mathcal{M}$ et $\mathcal{N}$ deux multi-ensembles. Le multi-ensemble union est définie par $\mathcal{M} \uplus \mathcal{N}(a) = \mathcal{M}(a) + \mathcal{N}(a)$.

Ordres multi-ensembles

Soit $\succ$ un ordre strict. La relation $\succ_{mul}$ associée est donnée par la fermeture transitive de la relation $\succ^1_{mul}$:

$\mathcal{M} \uplus \{\!\{x\}\!\} \succ^1_{mul} \mathcal{M} \uplus \{\!\{y_1, \ldots, y_n\}\!\}$, où $n \geq 0$ et $\forall i, x \succ y_i$.

Exemple : $\{\!\{5, 3, 1, 1\}\!\} \succ_{mul} \{\!\{4, 3, 3, 1\}\!\}$.

Exercice : Si $\succ$ est un ordre strict, alors $\succ_{mul}$ est un ordre strict.

Théorème : Soit $\succ$ un ordre strict sur $\mathcal{A}$, alors $\succ$ est bien fondé ssi $\succ_{mul}$ est bien fondé.

Exercice : Un homme possède une somme d'argent en euros. Chaque jour il procède de la façon suivante :

- soit il jette une pièce de monnaie dans une fontaine,
- ou bien il change l'un de ses billets à la banque.

Montrer que ce processus termine, c'est à dire, que dans un temps fini l'homme reste sans argent.

Majorants/minorants et bornes supérieures/inférieures

Soit $\mathcal{E}$ un ensemble muni d'un ordre $\leq$. Soit $\mathcal{A} \subseteq \mathcal{E}$.

Définition :

Un majorant de $\mathcal{A}$ est un $x \in \mathcal{E}$ t.q. pour tout $y \in \mathcal{A}$, $y \leq x$.

Un minorant de $\mathcal{A}$ est un $x \in \mathcal{E}$ t.q. pour tout $y \in \mathcal{A}$, $x \leq y$.

La borne supérieure de $\mathcal{A}$, notée $sup(\mathcal{A})$, est le plus petit des majorants de $\mathcal{A}$ (si z est un majorant de $\mathcal{A}$ alors $sup(\mathcal{A}) \leq z$).

La borne inférieure de $\mathcal{A}$, notée $inf(\mathcal{A})$, est le plus grand des minorants de $\mathcal{A}$ (si z est un minorant de $\mathcal{A}$ alors $z \leq inf(\mathcal{A})$).

Fonctions monotones et points fixes

Définition : Soit $f : \mathcal{A} \to \mathcal{B}$ une fonction et soient $\leq_{\mathcal{A}}, \leq_{\mathcal{B}}$ deux ordres sur $\mathcal{A}$ et $\mathcal{B}$ respectivement.

La fonction f est monotone ssi $x \leq_{\mathcal{A}} y$ implique $f(x) \leq_{\mathcal{B}} f(y)$.

Définition : Soit $f : \mathcal{A} \to \mathcal{A}$ une fonction.
Un point fixe de f est un élément $x \in \mathcal{A}$ t.q. $f(x) = x$.
Le plus petit point fixe de f est $inf(\{x \in \mathcal{A} \mid f(x) = x\})$.
Le plus grand point fixe de f est $sup(\{x \in \mathcal{A} \mid f(x) = x\})$.