
Mathématiques pour l'informatique

Licence d'informatique (premier semestre)

Roberto Di Cosmo et Delia Kesner
PPS, Université Paris VII

Email : roberto@dicosmo.org, kesner@pps.jussieu.fr
URL : www.dicosmo.org, www.pps.jussieu.fr/~kesner

Plan du cours

1. Notions préliminaires :
ensembles, relations, ordres, fonctions, point fixe
2. Induction :
principe d'induction, preuves par induction.
3. Eléments de combinatoire :
permutations, arrangements, combinaisons, application au comptage d'ensemble finis
4. Eléments de probabilité discrète :
espace de probabilité, probabilité conditionnelle, variable aléatoire, événements indépendants
5. Induction :
définitions inductives ascendantes et descendentes, principe d'induction bien fondée, constructions sur les ordres bien fondés.
6. Calcul propositionnel :
syntaxe, sémantique, tables de vérité, définissabilité, systèmes de preuves syntaxiques.
7. Calcul des prédicats :
syntaxe, sémantique, calcul de Gentzen, unification et résolution.

Modalités du cours

- Nb cours : 13 (Lundi de 14h30 à 16h30) Amphi 43
- Nb TD : 13 (début cette semaine)
- Chargés de TD :
Alexandre Miquel, Dominique Poulhalhon
Mardi 8h30-10h30 et 10h30-12h30, Jeudi 12h30-14h30
- Examen partiel : jeudi 13 novembre, de 12h30 à 14h30, Amphi 43 et X2
- Examen final : entre le 19/01/2004 et le 07/02/2004
- Note Janvier : $\frac{1}{3}$ note partiel + $\frac{2}{3}$ exam Janvier
- Note Septembre : Max(exam Septembre, $\frac{1}{3}$ note partiel + $\frac{2}{3}$ exam Septembre)

Documents du cours

- **Transparents** (uniquement les définitions)
Tirage tous les 15 jours, mais consulter régulièrement
<http://www.dicosmo.org/CourseNotes/MathInfo/>
<http://www.pps.jussieu.fr/~kesner/enseignement/licence/math-info/>
- **Tableau** (exemples et démonstrations)

- **Feuilles de TD**

<http://www.pps.jussieu.fr/~miquel/enseignement/maths-info/>

Tout est accessible à partir de la page web du cours :

<http://www.pps.jussieu.fr/~miquel/enseignement/maths-info/>

Bibliographie

- **Mathématiques pour l'informatique.**
A. Arnold et I. Guessarian, MASSON.
- **Introduction à la logique.**
R. David, K. Nour et C. Raffalli, DUNOD.
- **Logique Mathématique I.**
R. Cori et J.-L. Krivine, MASSON.
- **Logique et fondements de l'informatique.**
R. Lassaigne et M. Rougemont, HERMES.
- **First-Order Logic and Automated Theorem Proving.**
M. Fitting, SPRINGER.
- **Concrete Mathematics.**
R. L. Graham, D. E. Knuth et O. Patashnik, ADDISON-WESLEY.
- **Logic for Computer Science.**
J. Gallier, WILEY.

Notions préliminaires

Ensembles

Définition : Soient deux ensembles \mathcal{A}, \mathcal{B} inclus dans \mathcal{U}^1 .

L'intersection de \mathcal{A} et \mathcal{B} est $\mathcal{A} \cap \mathcal{B} = \{e \in \mathcal{U} \mid e \in \mathcal{A} \text{ et } e \in \mathcal{B}\}$

L'union de \mathcal{A} et \mathcal{B} est $\mathcal{A} \cup \mathcal{B} = \{e \in \mathcal{U} \mid e \in \mathcal{A} \text{ ou } e \in \mathcal{B}\}$

La différence de \mathcal{A} et \mathcal{B} est $\mathcal{A} \setminus \mathcal{B} = \{e \in \mathcal{U} \mid e \in \mathcal{A} \text{ et } e \notin \mathcal{B}\}$

Le complémentaire de \mathcal{A} est $\overline{\mathcal{A}} = \mathcal{U} \setminus \mathcal{A} = \{e \in \mathcal{U} \mid e \notin \mathcal{A}\}$

$\mathcal{P}(\mathcal{A})$ est l'ensemble de toutes les parties de l'ensemble \mathcal{A} .

$$\text{(Lois de de Morgan)} \quad \overline{\mathcal{A} \cup \mathcal{B}} = \overline{\mathcal{A}} \cap \overline{\mathcal{B}} \quad \overline{\mathcal{A} \cap \mathcal{B}} = \overline{\mathcal{A}} \cup \overline{\mathcal{B}}$$

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

Relations

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

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

- R est réflexive² ssi pour tout $x \in \mathcal{A}$, $(x, x) \in R$. R est irréflexive³ ssi pour tout $x \in \mathcal{A}$, $(x, x) \notin R$.
- R est symétrique⁴ si pour tout $x, y \in \mathcal{A}$, $(x, y) \in R$ implique $(y, x) \in R$. R est anti-symétrique⁵ si pour tout $x, y \in \mathcal{A}$, $(x, y) \in R$ et $(y, x) \in R$ implique $x = y$.
- R est transitive⁶ si pour tout $x, y, z \in \mathcal{A}$, $(x, y) \in R$ et $(y, z) \in R$ implique $(x, z) \in R$.

¹Univers

² \geq sur les entiers

³ $>$ sur les entiers

⁴= sur les entiers

⁵être la mère de

⁶ \subseteq sur les ensembles

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. $\mathcal{S} \circ \mathcal{R} = \{(x, y) \in \mathcal{A} \times \mathcal{C} \mid \exists z \in \mathcal{B} (x, z) \in \mathcal{R} \text{ et } (z, y) \in \mathcal{S}\}$.

Définition : Soit $\mathcal{R} \subseteq \mathcal{A} \times \mathcal{A}$. On note R^n la n -composition

$$\underbrace{R \circ \dots \circ R}_{n \text{ times}}$$

Définition : Soit $\mathcal{R} \subseteq \mathcal{A} \times \mathcal{A}$. On note R^* l'union de toutes les n -compositions de R

$$R^* = \bigcup_{n=1}^{\infty} R^n$$

Fonctions

Définition : Une fonction f entre deux ensembles \mathcal{A} et \mathcal{B} , notée $f : \mathcal{A} \rightarrow \mathcal{B}$, 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 $f : \mathcal{A} \rightarrow \mathcal{B}$ 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'inverse⁷ 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 $f : \mathcal{B} \rightarrow \mathcal{C}$ avec $g : \mathcal{A} \rightarrow \mathcal{B}$ est la fonction $f \circ g : \mathcal{A} \rightarrow \mathcal{C}$, 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 $n > 0$. Montrer⁸ que $f^n = f^{n-1} \circ f$.

⁷pas toujours une fonction

⁸Par induction, voir la Section suivante

Propriétés des fonctions

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

Définition : Une fonction $f : \mathcal{A} \rightarrow \mathcal{B}$ 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.

Fonction caractéristique

Définition : Soit \mathcal{A} un ensemble inclus dans un univers \mathcal{U} . La **fonction caractéristique** de \mathcal{A} dans \mathcal{U} est la fonction $\chi : \mathcal{U} \rightarrow \{0, 1\}$ telle que

$$\forall a \in \mathcal{U}, \chi(a) = 1 \text{ ssi } a \in \mathcal{A}$$

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

Définition : Un **ordre strict** est une relation irreflexive et transitive.

Notation : $>$

Définition : Un ordre strict est **bien fondé** ssi il n'existe aucune chaîne infinie (i.e., de la forme $a_0 > a_1 > a_2 > \dots$).

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 $f : \mathcal{A} \rightarrow \mathcal{B}$ 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 $f : \mathcal{A} \rightarrow \mathcal{A}$ 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 $\sup(\{x \in \mathcal{A} \mid f(x) = x\})$.

Ordres complets et fonctions continues

Notation : Pour tout ensemble \mathcal{E} , on note \perp , s'il existe, l'élément minimum (t.q. $\perp \leq e$ pour tout $e \in \mathcal{E}$).

Définition : Un ensemble \mathcal{E} muni d'un ordre \leq est **complet** ssi toute partie de \mathcal{E} admet une borne supérieure.

En particulier, $\perp = \sup(\emptyset)$ ⁹.

Définition : Un sousensemble *non vide* D d'un ensemble ordonné E est **dirigé** si pour toute paire d'éléments x et y de D il existe un élément $z \in D$ t.q. $x \leq z$ et $y \leq z$.

Définition : Un sousensemble *non vide* C d'un ensemble ordonné E est une **chaîne** s'il est totalement ordonné.

Définition : Soient $f : \mathcal{E} \rightarrow \mathcal{E}$ une fonction et \leq un ordre sur l'ensemble complet \mathcal{E} . f est **continue** ssi pour toute chaîne C non vide de E on a $f(\sup(C)) = \sup(f(C))$.

Exercice :

- Montrer que $\sup(\{\perp\} \cup \mathcal{X}) = \sup(\mathcal{X})$.
- Montrer que toute fonction continue est monotone.

⁹tout élément de \mathcal{E} est un majorant de l'ensemble vide

Théorèmes du point fixe

Soit $f : \mathcal{A} \rightarrow \mathcal{A}$ une fonction et \leq un ordre complet sur \mathcal{A} .

Théorème : Si f est monotone, alors f a un plus grand point fixe $\sup(\{x \in \mathcal{A} \mid x \leq f(x)\})$.

Théorème : Si f est une fonction continue, alors f a un plus petit point fixe $\sup(\{f^n(\perp) \mid n \in \mathbb{N}\})$.

Induction

Définitions inductives

- Induction mathématique
- Induction complète
- Équivalence

Induction Mathématique

Théorème : Soit P une propriété sur les entiers. Supposons

IM1 $P(0)$,

IM2 $\forall n \in \mathbb{N}. P(n) \Rightarrow P(n+1)$,

alors $\forall n \in \mathbb{N}. P(n)$

Exemples

$$\sum_{i=1}^n i = \frac{n * (n + 1)}{2}$$

$$n^2 = \sum_{i=1}^n (2i - 1)$$

Mais il est bien moins évident comment prouver

"Tout entier est décomposable en produit de nombres premiers"

ou

$$fact(n) \leq 2^n$$

Induction Complète (course of values)

Théorème : Soit P une propriété sur les entiers. Supposons

$$(I) \quad \forall n \in \mathbb{N}. ((\forall k < n. P(k)) \Rightarrow P(n))$$

alors $\forall n \in \mathbb{N}. P(n)$

Équivalence des deux principes

Malgré l'apparente supériorité du deuxième principe, on prouve

Théorème : Induction mathématique et complète sont équivalentes.

On finit avec un le théorème fondamental du cours :

Théorème : Tous le monde est d'accord avec le professeur.

Preuve : On montre, par induction sur le nombre de personnes dans l'amphi, que tout groupe de n personnes contenant le professeur est d'accord avec lui.

Cas de base : il y a seulement le professeur, trivial.

Cas inductif : on suppose l'énoncé vrai pour tout groupe de n personnes, et on le prouve pour tout groupe de $n+1$.

Numérotions de 1 à $n+1$ les personnes en question, de façon que le professeur soit le numéro n , et considérons le groupe A des premières n et le groupe B des dernières n personnes.

Les deux groupes contiennent le professeur et sont de taille $n < n+1$, donc on peut appliquer l'hypothèse d'induction et en déduire qu'ils sont tous d'accord avec le professeur (qui est dans les deux), ce qui nous permet de conclure.

Corollaire : Le professeur a toujours raison.