

Mathématiques pour l'informatique ?

Mathématiques pour l'Informatique

Calcul des Ensembles

David Teller

09/02/2007

Q L'informatique, au juste, c'est quoi ?**A** L'informatique, c'est :

- ▶ de l'électronique
- ▶ de la théorie des processus
- ▶ de la linguistique
- ▶ du design
- ▶ de la logique
- ▶ de l'algorithmique
- ▶ de la calculabilité
- ▶ de l'analyse numérique
- ▶ ...

Objectif du semestre

Étudier

- ▶ les fondements mathématiques sur lesquels est construite l'informatique
- ▶ les outils mathématiques indispensables pour avancer en informatique
- ▶ la rédaction rigoureuse de preuves mathématiques.

Au programme

Calculs ensemblistes Ensembles, relations, fonctions.**Ensembles ordonnés** Ordres, préordres, treillis.**Logique** Algèbres de Boole, calcul propositionnel, calcul des prédicats.**Graphes** Arbres, graphes, chemins.**Langages rationnels** Expressions régulières, automates finis, éléments de compilation.

Modalités de notation

- ▶ quelques exercices par semaine, à rendre systématiquement, sur feuille
- ▶ un examen à mi-semestre
- ▶ un examen en fin de semestre

Vous êtes invités à vous servir de ce que vous apprenez dans ce cours aussi bien en informatique qu'en projet et dans les autres cours de mathématiques.

Comme d'habitude...

Si vous avez des questions, n'hésitez pas à les poser !



Introduction

Chapitre 1 : Calculs ensemblistes

- Notations
- Lois ensemblistes
- Fonctions

Au programme du chapitre

Ensembles Notations, définitions, lois de De Morgan

Fonctions Définitions, propriétés

Beaucoup de définitions et de notations !



Ensembles

Definition (Appartenance)

Si e est un élément et E un ensemble, la notation $e \in E$ signifie que e est un élément qui est dans l'ensemble E . On dira " e appartient à E ".

Definition (Non-appartenance)

Si e est un élément et E un ensemble, la notation $e \notin E$ est la négation de $e \in E$. On dira " e n'appartient pas à E ".



Ensemble vide

On postule l'existence d'un ensemble dit "vide", noté \emptyset .

Exercice Comment définir \emptyset ?

A

Definition (Ensemble vide)

L'ensemble vide \emptyset est défini par le fait qu'il n'existe aucun e tel que $e \in \emptyset$.



Sous-ensembles

Definition (Inclusion)

Si A et B sont deux ensembles, A est un *sous-ensemble* de B (ou A est une *partie* de B ou encore A est *inclus* dans B) si pour tout e tel que $e \in A$, on a $e \in B$. On note alors $A \subseteq B$.

Definition (Non-inclusion)

La négation de $A \subseteq B$ se note $A \not\subseteq B$.

Q La proposition $A \not\subseteq B$ implique-t-elle $B \subseteq A$? La proposition $B \subseteq A$ implique-t-elle $A \not\subseteq B$?

Exercice Prouvez-le !



Un premier théorème

Proposition

La proposition $A \not\subseteq B$ n'implique pas $B \subseteq A$.

Q Comment prouve-t-on ce genre d'affirmation ?

A À l'aide d'un contre-exemple.

Preuve Contre-exemple : $A = \{1\}$, $B = \{2\}$. On a $A \not\subseteq B$ et $B \not\subseteq A$. A et B sont dits "non-comparables".

Proposition

La proposition $B \subseteq A$ n'implique pas $A \not\subseteq B$.

Preuve Même contre-exemple.



Encore des sous-ensembles

Proposition

Si $A \subseteq B$ et $B \subseteq A$, alors $A = B$.

Définition (Inclusion stricte)

Si A est inclus dans B sans être égal à B , on dira que A est "strictement inclus" dans B , noté $A \subsetneq B$.



Produits

Définition (Produit)

Si A et B sont deux ensembles, le produit cartésien de A et B , noté $A \times B$, est l'ensemble $\{(a, b)/a \in A, b \in B\}$.

On généralise le produit cartésien à toute famille finie d'ensembles.

On notera E^n le produit cartésien de $\underbrace{E \times E \times \dots \times E}_n$.

Q Comment peut-on définir la suite des E^n pour n dans \mathbb{N}^* . Dédouisez-en une définition possible de E^0 .

A On définira $E^1 = E$ et pour tout $n \geq 1$, $E^{n+1} = E^n \times E$.

A On pourrait utiliser, par exemple, $E^0 = \{1\}$. Cela dit, on ne le fera généralement pas.



Parties

Définition (Parties)

Si E est un ensemble, $\mathcal{P}(E)$, l'ensemble des parties de E (ou *power set*), est un ensemble qui contient exactement tous les sous-ensembles de E .

Q Quels ensembles appartiennent toujours à $\mathcal{P}(E)$?

A L'ensemble vide et E lui-même.



Union, intersection, complémentaire

Exercice Définissez l'union, l'intersection, le complémentaire. (on se placera toujours dans un ensemble E)

Définition (Union)

Si A et B sont deux sous-ensembles de E , l'union de A et B , notée $A \cup B$, est l'ensemble défini comme $\{e \in E / e \in A \vee e \in B\}$.

Définition (Intersection)

Si A et B sont deux sous-ensembles de E , l'intersection de A et B , notée $A \cap B$, est l'ensemble défini comme $\{e \in E / e \in A \wedge e \in B\}$.

Définition (Complémentaire)

Si A est un sous-ensemble de E , le complémentaire de A dans E , noté A^c ou \bar{A} , est l'ensemble défini comme $\{e \in E / e \notin A\}$.



Différence, différence symétrique

Exercice Définissez la différence, la différence symétrique.

Definition (Différence)

Si A et B sont deux sous-ensembles de E , la différence de A et B , notée $A \setminus B$, est l'ensemble défini comme $\{e \in E / e \in A \wedge e \notin B\}$.

Definition (Différence symétrique)

Si A et B sont deux sous-ensembles de E , la différence symétrique de A et B , notée $A \Delta B$, est l'ensemble défini comme $\{e \in E / (e \in A \wedge e \notin B) \vee (e \in B \wedge e \notin A)\}$.

Proposition (Reformulation de la différence symétrique)

Si A et B sont deux sous-ensembles de E , alors $A \Delta B = (A \setminus B) \cup (B \setminus A)$.

Exemples

$$E^c = \emptyset$$

$$\emptyset^c = E$$

$$A \cap \emptyset = \emptyset$$

$$A \cup E = A$$

$$A \Delta E = A^c$$

$$A \cap A = A$$

Lois de Morgan

Introduction

Chapitre 1 : Calculs ensemblistes

Notations

Lois ensemblistes

Fonctions

Les lois de Morgan sont deux axiomes fort utiles pour prouver proprement des égalités entre ensembles.

Théorème (Première loi de Morgan)

Si A et B sont deux parties de E , $\overline{A \cup B} = \overline{A} \cap \overline{B}$

Théorème (Deuxième loi de Morgan)

Si A et B sont deux parties de E , $\overline{A \cap B} = \overline{A} \cup \overline{B}$

Exercice Prouvez ces lois.

Lois de distribution

Proposition (Intersection sur union)

L'intersection est distributive sur l'union. En d'autres termes, Si A , B et C sont trois parties de E , $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Proposition (Union sur intersection)

L'union est distributive sur l'intersection. En d'autres termes, Si A , B et C sont trois parties de E , $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Exercice Prouvez ces lois.



Partition

Définition (Partition)

Une famille $(A_i)_{i \in I}$ de parties de E est une partition de E si elle vérifie

- ▶ aucun des A_i n'est l'ensemble vide
- ▶ pour tout i et j de I distincts, $A_i \cap A_j = \emptyset$
- ▶ $\bigcup_{i \in I} A_i = E$.

Exemple L'ensemble \mathbf{N} peut se partitionner en A_0 , ensemble des nombres pairs et A_1 , ensemble des nombres impairs.

Exercice Si A est une partie de E et $(B_i)_{i \in I}$ est une famille de parties de E , montrer que

- ▶ $A \cup (\bigcap_{i \in I} B_i) = \bigcap_{i \in I} (A \cup B_i)$
- ▶ $A \cap (\bigcup_{i \in I} B_i) = \bigcup_{i \in I} (A \cap B_i)$.

N'oubliez pas que l'ensemble I est fini !



Généralisations

Union et intersection se généralisent à des familles (ou "suites finies") de parties de E .

Ainsi, si $(A_i)_{i \in I}$ est une famille de parties de E , on aura

$$\bigcup_{i \in I} A_i = \{e \in E / \exists i \in I, e \in A_i\}$$

$$\bigcap_{i \in I} A_i = \{e \in E / \forall i \in I, e \in A_i\}.$$

Q Comment définir $\bigcup_{i \in I} A_i$ lorsque $I = \emptyset$?

Q Comment définir $\bigcap_{i \in I} A_i$ lorsque $I = \emptyset$?

A L'union de rien est vide : $\bigcup_{i \in \emptyset} A_i = \emptyset$. L'intersection de rien est complète : $\bigcap_{i \in \emptyset} A_i = E$.



Introduction

Chapitre 1 : Calculs ensemblistes

- Notations
- Lois ensemblistes
- Fonctions

Conclusions



Correspondances

Definition (Correspondance)

Soient E et F deux ensembles. Une *correspondance* est un triplet $f = (E, F, \Gamma)$, où Γ est un sous-ensemble de $E \times F$. On appelle E l'ensemble de départ, F l'ensemble d'arrivée et Γ le graphe de f .

Q Quelle est la différence avec une fonction ?

A f peut mettre en correspondance un point de E avec plusieurs points de F , i.e. donner plusieurs images à un même point de départ.

Definition (Domaine de définition)

Si $f = (E, F, \Gamma)$ est une correspondance, son *domaine de définition*, noté $Dom(f)$, est défini comme $\{x \in E / \exists y \in F, (x, y) \in \Gamma\}$.

Definition (Image)

Si $f = (E, F, \Gamma)$ est une correspondance, son *ensemble image*, noté $Im(f)$, est défini comme $\{y \in F / \exists x \in E, (x, y) \in \Gamma\}$.



Image et antécédent

Definition (Image (généralisée))

Si $f = (E, F, \Gamma)$ est une correspondance, si X est un sous-ensemble de E , l'*image* de X par f , noté $f(X)$, est défini comme $\{y \in F / \exists x \in X, (x, y) \in \Gamma\}$.

Definition (Réciproque)

Si $f = (E, F, \Gamma)$ est une correspondance, la correspondance réciproque f^{-1} est définie comme $(F, E, \{(y, x) / (x, y) \in \Gamma\})$.

Definition (Antécédent)

Si $f = (E, F, \Gamma)$ est une correspondance, si Y est un sous-ensemble de F , l'*antécédent* de Y par f est $f^{-1}(Y)$.

Q Quels sont les liens entre image, image généralisée, domaine et antécédent ?



Fonctions

Definition (Fonction)

Si $f = (E, F, \Gamma)$ est une correspondance, f est une *fonction* si et seulement si, pour tout e de E , soit $f(\{e\}) = \emptyset$, soit $f(\{e\})$ est un singleton.

Si f est une fonction et si e appartient au domaine de définition de f , on note $f(e)$ l'unique image par f de $\{e\}$. On note de plus $f : E \rightarrow F$.

Definition (Application)

Si $f : E \rightarrow F$ est une fonction, f est une *application* si et seulement si $Dom(f) = E$.

Exemple L'application identité sur E se note $id_E : E \rightarrow E$, définie par $\forall e \in E, id_E(e) = e$.

Exemple L'application caractéristique d'une partie A de E est une fonction $\chi_A : E \rightarrow \{\text{ff}, \text{tt}\}$ définie par

- ▶ $\forall x \in A, \chi_A(x) = \text{tt}$
- ▶ $\forall x \in \bar{A}, \chi_A(x) = \text{ff}$.



Composition, restriction

Definition (Composition)

Si $f : E \rightarrow F$ est une application et $g : F \rightarrow G$ est une application, l'*application composée* est une application $h : E \rightarrow G$ définie par $\forall e \in E, h(e) = g(f(e))$.

Definition (Restriction)

Si $f : E \rightarrow F$ est une fonction et A est une partie de E , la *restriction* de f à A , notée $f|_A$, est définie comme $(E, F, \{(x, y) / x \in A, f(x) = y\})$.



Injections, surjections, bijections

Definition (Injectivité)

Une fonction $f : E \rightarrow F$ est injective si $\forall x, y \in E, f(x) = f(y) \Rightarrow x = y$.

Definition (Surjectivité)

Une fonction $f : E \rightarrow F$ est surjective si $Im(f) = F$.

Definition (Bijective)

Une fonction $f : E \rightarrow F$ est bijective si elle est injective et surjective.

Q Exemples de fonctions non-injectives ? Non-surjectives ?

A

- ▶ Injective non-surjective : $f : \mathbb{N} \rightarrow \mathbb{N}$
 $n \mapsto n + 1$
- ▶ Surjective non-injective : $g : \mathbb{N} \rightarrow \mathbb{N}$
 $n \mapsto |n - 1|$
- ▶ Ni injective, ni surjective : $h : \mathbb{N} \rightarrow \mathbb{N}$
 $n \mapsto n \bmod 2$

◀ ▶ ↻ 🔍

Propriétés de l'inversion

Proposition ([Semi-]

inverses] Soit $f : E \rightarrow F$ une application.

- ▶ Si $E \neq \emptyset$, alors f est injective si et seulement si f a un inverse à gauche, c'est-à-dire s'il existe une application $r : F \rightarrow E$ telle que $r \circ f = Id_E$.
- ▶ f est surjective si et seulement si f a un inverse à droite, c'est-à-dire s'il existe une application $s : F \rightarrow E$ telle que $f \circ s = Id_F$.
- ▶ f est bijective si et seulement si f a un inverse, c'est-à-dire s'il existe une application $f^{-1} : E \rightarrow F$ telle que $f \circ f^{-1} = Id_F$ et $f^{-1} \circ f = Id_E$.

Exercice

Prouvez cette proposition.

◀ ▶ ↻ 🔍

Exercices (maison)

Exercice (Associativité)

Soient $f : E \rightarrow F, g : F \rightarrow G$ et $h : G \rightarrow H$ trois applications.

Prouver que $(f \circ g) \circ h = f \circ (g \circ h)$.

Exercice (Bijection et réciprocity (bis))

Soit $f : E \rightarrow F$ une application. f est bijective si et seulement si f^{-1} est une application et $f \circ f^{-1} = Id_F$.

Exercice (Réciprocity et composition)

Soient $f : E \rightarrow F$ et $g : F \rightarrow G$ deux applications bijectives. Alors

- ▶ $f \circ g$ est une application bijective
- ▶ $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$

Exercice (Unicité)

Soit $f : E \rightarrow F$ une application bijective. Alors sa correspondance réciproque est unique.

◀ ▶ ↻ 🔍

Tiens, puisqu'on y est

Considérons la fonction

```
# let f x = x + 1;;
val f : int -> int = <fun>
```

Q Que fait cette fonction ?

Q Quel est le domaine de f ? Quelle est l'image de f ? f est-elle injective ? surjective ? bijective ?

A Cette fonction OCaml implante la fonction mathématique

$$f : \begin{matrix} \text{int} & \longrightarrow & \text{int} \\ x & \longmapsto & \begin{cases} x + 1 & \text{si } x < \text{max_int} \\ \text{min_int} & \text{sinon} \end{cases} \end{matrix}$$

Son domaine est l'intégralité de l'ensemble int (l'ensemble des entiers OCaml, c'est-à-dire $[\text{min_int}, \text{max_int}]$). Son image est aussi l'intégralité de l'ensemble int . Elle est bijective.

◀ ▶ ↻ 🔍

Prouvons cela

Proposition (Bijektivité de f)

La fonction f est bijective.

$f : \text{int} \rightarrow \text{int}$ est une application. Il nous suffit donc de fournir f^{-1} , de vérifier que $f^{-1} \circ f = \text{Id}_{\text{int}}$ et d'utiliser le théorème de bijection et réciprocity.

Nous utiliserons $f^{-1} : \text{int} \rightarrow \text{int}$:

$$x \mapsto \begin{cases} x - 1 & \text{si } x > \text{min_int} \\ \text{max_int} & \text{sinon} \end{cases}$$

Le reste de la preuve est trivial.

Quelques propriétés des fonctions

Si $f : E \rightarrow F$ est une fonction, si A et B sont deux parties de E et si C et D sont deux parties de F ,

$$f(A \cup B) = f(A) \cup f(B) \quad f(A \cap B) \subseteq f(A) \cap f(B)$$

$$f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D) \quad f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$$

si f est injective, $f(A \cap B) = f(A) \cap f(B)$

Pour réviser

Prouvez tout cela.

Ce que nous avons vu

- ▶ Une définition formelle des ensembles, des correspondances, des fonctions, de leurs propriétés.
- ▶ Beaucoup de notations.
- ▶ Un certain nombre de théorèmes, qui vous serviront pour la suite.
- ▶ Un tout début de correspondance avec l'informatique.

Réviser vos théorèmes régulièrement, vous vous en servirez !
 Attendez-vous à un cours à la française, c'est-à-dire très formel !

La semaine prochaine

- Cardinalité : Ensembles finis, ensembles dénombrables.
- Relations : Opérations, alphabets, ordres, équivalences, congruences.