Mathématiques Discrétes

Dr Aminata Diop DIENE

Date

Les mathématiques discrètes

- Les cours de maths t'apprennent à **faire fonctionner ton cerveau de façon logique**. Ça t'entraîne à poser des hypothèses, à faire des démonstrations, à en tirer des conclusions
- s… bref, à penser par toi-même !

- **"Les mathématiques jouent un rôle crucial dans les télécommunications, qui impliquent la transmission de données, de signaux et d'informations à travers des réseaux de communication.**
- Les mathématiques sont importantes dans les télécommunications :

1. **Théorie de l'information** : La théorie de l'information est une branche des mathématiques qui étudie la quantité d'informations qui peut être transmise à travers un canal de communication donné. Les mathématiques sont utilisées pour modéliser la transmission de l'information, ainsi que pour déterminer les limites théoriques de la quantité d'information qui peut être transmise.
2. **Codage de canal** : technique qui permet de détecter et de corriger les erreurs de transmission qui se produisent lors de la transmission de données à travers des canaux de communication bruyants. Les mathématiques sont utilisées pour concevoir des codes qui maximisent la distance minimale entre les mots de code, ce qui permet de détecter et de corriger un plus grand nombre d'erreurs.
3. **Modulation** : technique qui permet de transmettre des signaux à travers un canal de communication en modifiant certaines caractéristiques du signal, la fréquence ou l'amplitude. Les mathématiques sont utilisées pour concevoir des modulations qui maximisent le taux de transmission tout en minimisant les erreurs de transmission.

1. **Traitement du signal** : technique qui permet d'analyser, de transformer et de synthétiser des signaux pour extraire des informations utiles. Les mathématiques sont utilisées pour concevoir des algorithmes de traitement du signal, tels que la transformée de Fourier et la transformée en ondelettes, qui permettent de représenter les signaux dans des espaces de fréquences ou de temps-fréquence.
2. **Cryptographie**: avec le chiffrement

- **En somme, les mathématiques sont essentielles pour la conception, l'optimisation et la maintenance des réseaux de télécommunications.**
- **La compréhension des mathématiques de base est donc importante pour les ingénieurs et les professionnels travaillant dans le domaine des télécommunications."**

Mathématiques discrètes

- Les **mathématiques discrètes** permettent d'étudier les structures dites discrètes, c'est à dire non continues.
- Une variable est discrète si elle ne contient que des valeurs entières (exemple : nombre d'étudiants dans une classe).
- Par ailleurs, une variable continue accepte toutes les valeurs d'un intervalle fini ou infini (exemple : diamètre de pièces,…)
- Les maths ce n'est pas que le continu. Dans la réalité le monde est plutôt discret et on utilise le continu comme approximation.

Objectifs:

- Les étudiants doivent maîtriser des structures discrètes avec les différents types de raisonnement associés :
- Théorie des ensembles: Les probas reposent sur les ensembles. les applis industrielles des probas ne manquent pas.
- Relation d'ordre : dans un ensemble est une relation binaire dans cet ensemble qui permet de comparer ses éléments de manière cohérente.
- Relation d'équivalence,
- L' arithmétique et théorie des graphes,
- Les suites et séries numériques et de fonctions: les suites servent à étudier des phénomènes discrets.

Les nombres premiers sont à la base des algorithmes de cryptage qui protègent vos données.

Domaine d’activités:

- *Un ingénieur doit possède les compétences techniques et opérationnelles lui permettant de mener des projets de modélisation mathématique, depuis la formalisation du problème posé jusqu'à sa résolution numérique et la valorisation de la solution développée.*
- *Les mathématiques discrètes sont nécessaires pour voir les structures mathématiques dans l'objet avec lequel vous travaillez, et pour comprendre leurs propriétés.*
- ***Domaine d’activités:***
- *Les ingénieurs en télécommunications, en logiciel,*
- *Les informaticiens en traitement de données,*
- *La sécurité*
- *La finance*
- *Etc…*

Utilités

- Les concepts et notations des mathématiques discrètes sont utiles pour étudier et décrire les problèmes et objets de l'informatique tels que les algorithmes, les langages de programmation, la cryptographie, etc.
- Les mathématiciens disent que c'est la branche des mathématiques qui traite des ensembles dénombrables (ensembles qui ont la même cardinalité que les sous-ensembles des nombres naturels, y compris les nombres rationnels mais pas les nombres réels).
- Cryptographie: technique d'écriture où un message chiffré est écrit à l'aide de codes secrets ou de clés de chiffrement. La cryptographie est principalement utilisée pour protéger un message considéré comme confidentiel.

PLAN

- Théorie des ensembles. union intersection, différence et complémentaire, Produit cartésien
- Relation et fonction
- Arithmétique modulaire.
- Opérateurs, classes de fonctions (injective, surjective, bijective),
- propriétés des relations (réflexive, transitive, symétrique, antisymétrique,)
- Relation d'ordre (partielle, totale)
- Relation d'équivalence
- Raisonnement (directe, par récurrence, par absurde)
- Théorie des graphes.
- Suites séries numériques
- Suites et séries de fonctions
- Transformation en Z

Bibliographie

- I André Arnold, Irène Guessarian. Mathématiques pour l’informatique.
- I Alfred Aho, Jeffrey Ullman. Concepts fondamentaux de l’informatique.
- MAT1500_pp1-20.pdf (umontreal.ca)
- Mathématiques pour l'informatique - Ensembles/Relations (univ-tln.fr)

Théories des ensembles

- *Les ensembles et leurs éléments sont une modélisation mathématique qui permettent de collectionner différents objets de la vraie vie.*
- *Un ensemble E est une collection d'objets, appelé les éléments de E. On écrit :*

$$x \in E,$$

si x est un élément de E, et $x \notin E$ sinon. Pour chaque objet x, il y a exactement deux possibilités : soit $x \in E$, soit $x \notin E$ (et donc jamais moitié-moitié).

Si un ensemble E a seulement un nombre fini n d'éléments différents, on dit que c'est un ensemble *fini* et n est la *taille* ou la *cardinalité* de E. On écrit

$$|E| = n \text{ (ou aussi comme } \#E = n).$$

Si l'ensemble E n'a pas un nombre fini d'éléments on écrit $|E| = \infty$.

Notation : Soient $e_1, e_2, \ldots, e_n$ les éléments différents de E, alors on écrit

$$E = \{e_1, e_2, \ldots, e_n\}$$

(on écrit une liste de tous les éléments entre deux accolades).

Définitions

Deux ensembles E_1 et E_2 sont considérés comme égaux si les deux ensembles ont exactement les mêmes éléments. On écrit $E_1 = E_2$.

Un ensemble sans élément s'appelle un *ensemble vide*. Peuvent-t-ils exister deux ensembles vides différents. Mais non. Voici un premier résultat avec preuve, de quelque chose fort évidente ! C'est une conséquence de la définition.

Proposition

Il existe un seul ensemble vide.

Démonstration. Définissons $V := \{\}$. C'est un ensemble avec zero elements, donc au moins un ensemble vide existe !

Supposons V_1 est aussi un ensemble vide et x un objet quelconque. Alors on n'a jamais $x \in V$ et on n'a jamais $x \in V_1$, parce que V et V_1 n'ont pas d'élément. En particulier :

L'objet x est un élément de V *si et seulement si* x est un élément de V_1. Donc par la *définition d'égalité d'ensembles* on conclut que $V = V_1$. □

Nous adoptons la *notation* suivante pour l'ensemble vide : $\emptyset := \{\}$.

Sous ensemble

Soient F et E deux ensembles. Si chaque élément de F est aussi un élément de E, on dit que F est un sous-ensemble *de E, et on écrit $F \subset E$ (ou $E \supset F$).*

Exemple

Si $E = F$ alors nécessairement $E \subset F$ (et $F \subset E$). Parce que, par définition $E = F$ veut dire que E et F ont les mêmes éléments, donc en particulier chaque élément de E est aussi un élément de F.

Remarque

Dans la vrai vie on utilise seulement *une* notion d'appartenir à une collection.

Aux mathématiques on utilise deux notions. L'un est "être élément de", et l'autre est "être sous-ensemble de". Soit $a \in A$ un élément. Alors le sous-ensemble de A qui contient seulement a, c.-a-d. $\{a\}$, est un sous-ensemble de A et n'est pas un élement de A. Nous distinguons entre $a \in A$ et $\{a\} \subset A$, mais dans la vraie vie on pense peut-être : "C'est la même chose, non ?". En effet, NON, pas en mathématiques.

On peut

Définir des sous-ensembles par des propriétés de ces éléments. Soit E un ensemble et P une propriété qu'un élément de E peut avoir ou pas. Alors

$$\{e \in E; e \text{ a propriété } P\} \quad \text{ou} \quad \{e \in E | \ e \text{ a propriété } P\}$$

est par définition le sous-ensemble de E des éléments e de E qui ont la propriété P. Il faut que ce soit claire : chaque $e \in E$ a cette propriété, ou ne l'a pas. Pas de zone grise.

Remarques

Dans la réalité pas chaque "sous-collection" est tout de suite un sous-ensemble, car la définition d'appartenance pourrait être trop vague. Par exemple, considérons la collection V de vêtements, avec la "sous-collection" R des vêtements rouges. Et prenons un T-shirt originalement rouge mais lavé trop souvent et devenu un genre de rose. Est ce qu'on le met encore dans le sous-collection de vêtements rouge R ou pas ? Il ne faut pas avoir de zone grise pour définir les (sous-)ensembles ou les éléments. Si vous voulez modéliser des (sous-)collections par la théorie mathématique des (sous-)ensembles il faut être précis dans vos définitions.

Exercices

On peut dire des choses en français courant de plusieurs façons, mais aussi en mathématiques.

Soient E et F deux ensembles. Est-ce que c'est dire la même chose :

(i) On a $F \subset E$ si pour chaque objet x c'est vrai que *si x est un élément de F alors x est nécessairement aussi un élément de E.*

(ii) On a $F \subset E$ si pour chaque objet x c'est vrai que *x est nécessairement un élément de E si x est un élément de F.* (Et si x n'est pas un élément de F ?).

(iii) On a $F \subset E$ si pour chaque objet x c'est vrai que *si x n'est pas un élément de E alors nécessairement x n'est pas un élément de F.*

(iv) On a $F \subset E$ si pour chaque objet x c'est vrai que *x est un élément de F seulement si aussi x un élément de E.* (Et si $x \in E$?)

(b) Et si pour chaque objet x c'est vrai que $x \in E$ *seulement si* $x \in F$? Et si pour chaque objet x c'est vrai que $x \in F$ *si* $x \in E$?

Egalités d'ensembles

$E = F$ alors nécessairement $E \subset F$ et $F \subset E$)

Mais aussi si $F \subset E$ et $E \subset F$ alors nécessairement $E = F$

(Le théorème du Sandwich)

Soient F et E deux ensembles. Si $F \subset E \subset F$ alors $F = E$.

Preuve

Supposons F et E sont deux ensembles tels que $F \subset E$ et $E \subset F$.

Et supposons temporairement aussi, par contre, que $F \neq E$. Par la définition d'égalité d'ensemble ça veut dire que ce n'est pas vrai que E et F ont les mêmes éléments. Donc

(i) il existe un $e \in E$ tel que $e \notin F$ ou

(ii) il existe un $f \in F$ tel que $f \notin E$.

Mais le cas (i) est impossible, parce qu'on suppose $E \subset F$ (ce qui veut dire par définition de *sous-ensemble* que pour chaque $e \in E$ on a $e \in F$). Et le cas (ii) est aussi impossible, car $F \subset E$.

Donc (sous les hypthèses que $F \subset E$ et $E \subset F$) ce n'est pas vrai que $F \neq E$.

Il suit que (sous les hypothèses que $F \subset E$ et $E \subset F$) nécessairement $F = E$. Ce qui était à montrer. $\square$

Autre démonstration

Supposons F et E sont deux ensembles, tels que (i) $F \subset E$ et (ii) $E \subset F$.

Par définition de sous-ensembles on obtient

(i) Si $x \in F$ alors aussi $x \in E$;

(ii) Si $x \in E$ alors aussi $x \in F$.

Sous ces hypothèses nous voulons montrer que $E = F$.

Il faut montrer que E et F ont les mêmes éléments. Soit x un objet. Si $x \in E$ alors par l'hypothèse (ii) on a aussi $x \in F$, et si $x \in F$ alors par l'hypothèse (i) on a aussi $x \in E$. (C'est aussi possible que x n'est ni un élément de E, ni de F : mais dans ce cas nous n'avons rien à vérifier.)

En autre mots E et F ont les mêmes éléments (ou $x \in E$ si et seulement si $x \in F$).

Il suit que $F = E$, ce qui était à montrer. □

On avoue, le théorème du sandwich est évident. Mais c'est plutôt la logique utilisée dans les preuves qu'il faut comprendre. On en discutera encore.

Propriétés sur les ensembles

L'intersection $E \cap F$ est par définition le sous-ensemble de U des éléments $u \in U$ qui sont simultanément éléments de E et de F.

On dit que deux ensembles sont *disjoints* si leur intersection est l'ensemble vide.

L'union $E \cup F$ est par définition l'ensemble des éléments $u \in U$ qui sont éléments de E ou de F (c'est permis d'être élément des deux simultanément aussi).

La *différence* de E et F, notée $E - F$ (où $E \backslash F$) est par définition l'ensemble de tous les éléments de E qui ne sont pas élément de F.

Si $E \subset F$ est un sous-ensemble, alors on définit le *complément* $\overline{E} = F - E$ (ce qui dépend de F), comme le sous-ensemble de tous les éléments de F qui ne sont pas élément de E.

Exemples

$$\{1,2,3,4,5\} \cap \{4,5,6,7\} = \{4,5\}, \{1,2,3,4,5\} - \{4,5,6,7\} = \{1,2,3\}$$

et

$$\{1,2,3,4,5\} \cup \{4,5,6,7\} = \{1,2,3,4,5,4,5,6,7\} = \{1,2,3,4,5,6,7\}.$$

Proposition

Soient A, B et C trois sous-ensembles de l'ensemble U.

(i) $A \cup \emptyset = A$; $A \cap U = A$ *("Identité")* ; *(ii)* $A \cup U = U$; $A \cap \emptyset = \emptyset$ *("Domination")* ;

(iii) $A \cup A = A = A \cap A$ *("Idempotence")* ; *(iv)* $\overline{(\overline{A})} = A$ *("Complémentarité")* ;

(v) $A \cap B = B \cap A$; $A \cup B = B \cup A$ *("Commutativité")* ;

(vi) $A \cup (B \cup C) = (A \cup B) \cup C$; $A \cap (B \cap C) = (A \cap B) \cap C$ *("Associativité")* ;

(vii) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$; $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ *("Distributivité")* ;

(viii) $\overline{(A \cap B)} = \overline{A} \cup \overline{B}$, $\overline{(A \cup B)} = \overline{A} \cap \overline{B}$ *("Lois de De Morgan")*.

Preuves

- Dans le document de bibliographie
- MAT1500_pp1-20.pdf (umontreal.ca)

Construction d'ensemble

- Avec l'intersection et l'union, on peut construire plusieurs ensembles.

Définition

Soit E un ensemble. L'ensemble des sous-ensembles (ou la puissance*) d'un ensemble E est noté $P(E)$*

Donc un *élément* de $P(E)$ est par définition un sous-ensemble de E.

On va voir que pour chaque ensemble E on a $|P(E)| = 2^{|E|}$; en particulier $|P(\emptyset)| = 1$

Exemple

Si $E = \{a, b, c\}$, alors $P(E) = \{\{\}, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$.

Il faut bien comprendre : on peut maintenant considérer $\{a, b\}$ comme sous-ensemble de E, mais aussi comme élément de $P(E)$. Et $\{\{a, b\}\}$ comme sous-ensemble de $P(E)$ et comme élément de $P(P(E))$.

La réunion $E \cup P(E)$ a 11 éléments différents :

$$E \cup P(E) = \{a, b, c, \{\}, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

Exemple

C'est comme ça ; dans la théorie d'ensembles on a décidé de voir a et $\{a\}$ comme deux éléments différents de $E \cup P(E)$. Et

$$E \cap P(E) = \emptyset.$$

En particulier :

$$E \cap P(E) \neq \{\emptyset\}$$

(vous comprenez la différence ? !).

Remarque

En pratique on voudrait peut-être de temps en temps "identifier a avec $\{a\}$".

C'est possible de faire ainsi avec une construction dans la théorie des ensembles en utilisant la notion de "relation d'équivalence" et "classe d'équivalence", ce qui viendra plus tard. La théorie d'ensembles nous force d'être précis. Si vous voulez "identifier a avec $\{a\}$" vous devez *le dire*, car ce n'est pas automatique (c.a.d. il faut définir une relation d'équivalence, et prendre les classes d'équivalence pour construire un nouveau ensemble, et tout ce tralala).

Définition

Soient E et F deux ensembles non-vides. Le produit cartésien *de E et F noté $E \times F$ est l'ensemble de tous les couples ordonnées (e, f) où $e \in E$ et $f \in F$*

$$E \times F = \{(e, f); e \in E \text{ et } f \in F\}.$$

Par exemple, si $E = \{1, 2, 3\}$ et $F = \{1, 2\}$ alors

$$E \times F = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 1), (3, 2)\}$$

a $3 \times 2 = 6$ éléments En particulier $(2, 3) \notin E \times F$.

L'exemple $\mathbb{R} \times \mathbb{R}$ est le plan ordinaire $\mathbb{R}^2$.

Remarque. Si E et F sont des ensembles finis, alors

$$|E \times F| = |E| \times |F|.$$

Définitions

Soit E un ensemble non-vide et $n > 0$ un entier. On définit E^n comme l'ensemble des suites ordonnées $(e_1, e_2, \ldots, e_n)$ *d'éléments de E de longueur n.*

Ici : l'ordre des coefficients importe, et des répétitions sont permises ! Par exemple, $(1, 2, 2) \in \mathbb{N}^3$ et $(1, 2, 2) \neq (2, 1, 2) \neq (1, 2)$.

Remarque. Si E est un ensemble fini et $n > 0$ un entier. Alors

$$|E^n| = |E|^n.$$

Notion de fonctions

- Dans les mathématiques modernes les fonctions entre les ensembles sont au moins aussi importantes que les ensembles soi-même, sinon plus importantes !
- **Définition**

$$\textit{Soient } A \textit{ et } B \textit{ deux ensembles. Une fonction } F \textit{ de } A \textit{ dans } B,$$

$$F : A \to B,$$

est l'affectation d'exactement un élément de B*, noté* $F(a) \in B$*, attribué par* F *à* $a \in A$*, et ça pour chaque* $a \in A$*.*

Une fonction est une relation mathématique qui prend une valeur et lui en associe une autre. On note souvent f la fonction et x le nombre de départ. On note f(x) le nombre d'arrivée.

Définition

Soit $F : A \to B$ une fonction.

(i) A est appelé le domaine *de F, et B le* codomaine *de F.*

Une fonction permet de définir un résultat (le plus souvent numérique) pour chaque valeur d'un ensemble appelé domaine.

(ii) Soit $a \in A$ et posons $b := F(a) \in B$. Alors b est appelé "l'image de a par F" et a est "une *préimage de b*".

(iii) Le sous-ensemble de B formé des images des éléments de A est appelé l'image (ou la portée) de F, $\operatorname{Im} F$.

Remarque

Donc F est une règle que définit pour chaque $a \in A$ une (seule!) image dans B. Mais pas chaque b a une préimage, et il peut exister plusieurs préimages pour un $b \in B$ donné ou aucune.

On peut définir une fonction par un formule. Par exemple la fonction :

$$F : \mathbb{N} \to \mathbb{N}, \ F(m) = m^2 + 1.$$

Composition de fonctions

- Si le codomaine d'une fonction est égal au domaine d'une autre fonction, on peut composer ces deux fonctions

$$Soit\ F : A \to B\ et\ G : B \to C\ deux\ fonctions.$$

$$Alors\ la\ composition\ est\ la\ fonction$$

$$G \circ F : A \to C$$

$$définie\ par$$

$$(G \circ F)(a) = G(F(a)).$$

Exemple

Soit $A = \{a, b, c\}$, $B = \{1, 2, 3, 4\}$, $C = \mathbb{N}$. Et $F : A \to B$ donnée par $F := \begin{pmatrix} a & b & c \\ 3 & 2 & 4 \end{pmatrix}$;

$G : B \to C$ donnée par $G := \begin{pmatrix} 1 & 2 & 3 & 4 \\ 13 & 23 & 33 & 4344 \end{pmatrix}$.

Alors $G \circ F : \{a, b, c\} \to \mathbb{N}$: $G \circ F = \begin{pmatrix} a & b & c \\ 33 & 23 & 4344 \end{pmatrix}$

$$(G \circ F)(c) = G(F(c)) = G(4) = 4344.$$

Fonction identité et fonction inclusion

Fonction identité

Soit A un ensemble. La *fonction identité* est la fonction $1_A : A \to A$ où

$$1_A(a) = a$$

pour chaque $a \in A$.

Fonction inclusion

Soit $A \subset B$ un sous-ensemble. La *fonction inclusion* est la fonction $\iota : A \to B$:

$$\iota(a) = a$$

pour chaque $a \in A$.

Exemple

$$A = \{a, 1, \heartsuit, \pi, \emptyset\}, \qquad B = \{a, b, c, 1, 2, 3, \heartsuit, \clubsuit, \pi, \emptyset, \}$$

alors

$$1_A = \begin{pmatrix} a & 1 & \heartsuit & \pi & \emptyset \\ a & 1 & \heartsuit & \pi & \emptyset \end{pmatrix}$$

$$\iota_A = \begin{pmatrix} a & 1 & \heartsuit & \pi & \emptyset \\ a & 1 & \heartsuit & \pi & \emptyset \end{pmatrix}.$$

La *différence* entre 1_A et ι est le codomaine (mais la portée et la formule sont les mêmes).

Injectivité, surjective, bijectivité

Soit $F : A \to B$ une fonction. On dit que

(i) F est injective si $F(a_1) = F(a_2)$ seulement si $a_1 = a_2$.

Cela revient à dire que chaque élément de l'ensemble d'arrivée a au maximum un antécédent.

(ii) F est surjective si chaque élément de B est l'image d'un élément de A.

Cela revient à dire que chaque élément de l'ensemble d'arrivée a au moins un antécédent.

(iii) F est bijective si chaque élément de B est l'image d'un seul élément de A.

F est bijective si et seulement si F est injective et surjective.

la fonction inclusion ι est injective, et la fonction identité 1_A est bijective.

Proposition

Soit la fonction $F : A \to B$ *donnée par* $F = \begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ f_1 & f_2 & f_3 & \dots & f_n \end{pmatrix}$.

Alors la fonction est

(i) injective si et seulement si chaque élément de B *se trouve au maximum une fois sur la 2-ième ligne ;*

(ii) surjective si et seulement si chaque élément de B *se trouve au minimum une fois sur la 2-ième ligne ;*

(iii) bijective si et seulement si chaque élément de B *se trouve exactement une fois sur la 2-ième ligne.*

Preuve

(i) Supposons que chaque élément de B se trouve au maximum une fois sur la deuxième ligne. Montrons par une *preuve directe* que F est injective .

Soient a et a' des éléments de A tels que $b = F(a) = F(a')$. Ces deux éléments a et a' se trouvent sur la première ligne, c'est à dire ils existent i et j tels que $a = a_i$ et $a' = a_j$ et donc $F(a) = F(a_i) = f_i$, $F(a') = f(a_j) = f_j$. Nous avons que $b = f_i = f_j$. Mais b se trouve au maximum une fois sur la 2-ième ligne. Ça veut dire $i = j$ et donc $a = a_i = a_j = a'$. Alors nous avons montré que F est injective (si chaque élément de B se trouve au maximum une fois sur la deuxième ligne).

Preuve

Supposons F est injective. Nous allons montrer par une *preuve indirecte* que chaque élément de B se trouve au maximum une fois sur la deuxième ligne.

Supposons $b \in B$ se trouve au moins deux fois sur la 2-ième ligne, disons à positions i et j $(i \neq j)$. Donc $b = f_i = f_j$. Mais $f_i = F(a_i)$ et $f_j = F(a_j)$, alors $F(a_i) = F(a_j)$ et $a_i \neq a_j$. Donc F n'est pas injective. On conclut la preuve indirecte que si F est injective alors chaque élément de B se trouve au maximum une fois sur la deuxième ligne.

Ça finit la preuve de (i).

(ii) et (iii) : exercices.

Théorème

Soit $F : A \to B$ *une fonction. Alors* F *est bijective* si et seulement si *il existe une fonction* $G : B \to A$ *telle que* $F \circ G = 1_B$ *et* $G \circ F = 1_A$.
cette fonction G est unique, appelée la *fonction inverse* et notée

$$G = F^{-1}.$$

parce que si F est bijective, pour chaque $b \in B$ il existe un *unique* $a \in A$ tel que $F(a) = b$. Alors $F^{-1}(b) = a$.

Mais si F n'est pas bijective, une fonction inverse n'existe pas et $F^{-1} : B \to A$ n'est pas définie.

Preuve

(i) Supposons $F : A \to B$ est bijective. Définition d'une fonction $G : B \to$

A : Soit $b \in B$, il existe un unique $a \in A$ tel que $F(a) = b$. Posons $G(b){:=}a$. Pour chaque $a \in A$ on a :

$$(G \circ F)(a) = G(F(a)) = G(b) = a.$$

Donc $G \circ F = 1_A$. Et pour chaque $b \in B$:

$$(F \circ G)(b) = F(G(b)) = F(a) = b.$$

Donc $F \circ G = 1_B$.

Preuve suite

(ii) De l'autre côté, supposons qu'il existe une fonction $G : B \to A$ telle que $F \circ G = 1_B$ et $G \circ F = 1_A$. Soit $b \in B$. Définissons $a := G(b) \in A$. Alors

$$F(a) = F(G(b)) = (F \circ G)(b) = 1_B(b) = b.$$

Donc a est un préimage de b pour F. Nous avons montré que F est surjective. Supposons $a_1, a_2 \in A$ tels que $F(a_1) = F(a_2)$. Donc

$$a_1 = 1_A(a_1) = (G \circ F)(a_1) = G(F(a_1)) = G(F(a_2)) = (G \circ F)(a_2) = a_2.$$

Donc F est aussi injective. On conclut la preuve, car une fonction surjective et injective est automatiquement bijective. $\square$

Preuve suite

Supposons $F : A \to B$ est injective. Supposons $G : B \to A$ et $G' : B \to A$

telles que $G \circ F = 1_A$ et aussi $G' \circ F = 1_A$. Soit $b \in B$. Parce que

F est bijective il existe un $a \in A$ tel que $F(a) = b$. Alors

$$G(b) = G(F(a)) = (G \circ F)(a) = 1_A(a) = (G' \circ F)(a) = G'(F(a)) = G'(b$$

Donc pour chaque $b \in B$ on a $G(b) = G'(b)$, c.-à-d., $G = G'$.

Relation sur un ensemble

Soit $\mathcal{R}$ une relation binaire sur un ensemble X.

Symétrique. On dira qu'une relation est symétrique si

$$\forall x, y \in X, \quad (x \mathcal{R} y) \Rightarrow (y \mathcal{R} x)$$

Transitive. On dira qu'une relation est transitive si

$$\forall x, y, z \in X, \qquad (x \mathcal{R} y) \wedge (y \mathcal{R} z) \Rightarrow (x \mathcal{R} z)$$

Antisymétrique. On dira qu'une relation est antisymétrique si

$$\forall x, y \in X, \quad (x \mathcal{R} y) \wedge (y \mathcal{R} x) \Rightarrow (x = y)$$

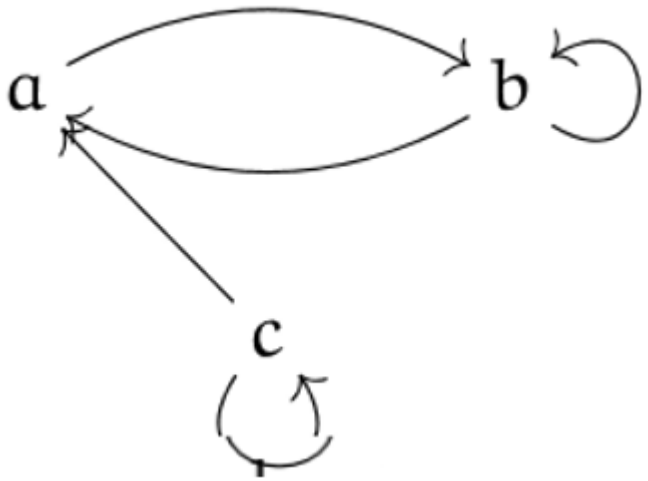
Reflexive. On dira qu'une relation est réflexive si

$$\forall x \in X, \qquad x \mathcal{R} x$$

Remarques

- Attention à ne pas assimiler l'anti symétricité à la négation de la symétricité.
- En effet la négation d'être symétrique transforme le quantificateur ∀ en ∃ ce qui n'est pas la caractérisation d'être antisymétrique.

Exemple



Cette relation n'est pas symétrique puisque cRa mais a n'est pas en relation avec c.

De même cette relation n'est pas transitive car cRa et aRb mais c n'est pas en relation avec b.

Elle n'est pas non plus antisymétrique puisque aRb, bRa et pourtant $a \neq b$.

Finalement cette relation n'est pas réflexive car a n'est pas en relation avec a.

En particulier cette relation n'est ni symétrique ni antisymétrique.

Remarque

- Soit R une relation sur un ensemble X.
    - Si R est réflexive, symétrique et transitive alors on dira que c'est une relation d'équivalence.
    - Si R est réflexive, antisymétrique et transitive alors on dira que c'est une relation d'ordre.

Par exemple sur N la relation = est une relation d'équivalence.

De même la relation $\leq$ est une relation d'ordre.

Exercice d'application

Soient $\mathcal{R}$ une relation binaire sur une ensemble X et M la matrice booléenne de $\mathcal{R}$ (il s'agit donc d'une matrice carré).

- La relation $\mathcal{R}$ est réflexive si et seulement si

$$\forall i, \qquad M_{i,i} = 1$$

  Autrement : il n'y a que des 1 sur la diagonale principale de M.

- La relation $\mathcal{R}$ est symétrique si et seulement si

$$\forall i, j, \qquad M_{i,j} = M_{j,i}$$

  Autrement : la matrice est symétrique par rapport la la diagonale principale.

- La relation $\mathcal{R}$ est antisymétrique si et seulement si

$$\forall i \neq j, \qquad , M_{i,j} \times Mj, i = 0$$

Solution

- Dire que $x_i \mathcal{R} x_i$ est strictement équivalent à dire $M_{i,i} = 1$.

- La proposition $x_i \mathcal{R} x_j$ est soit vraie soit faux. Si elle est vraie elle implique, si la relation est réflexive, que $x_j \mathcal{R} x_i$. Donc $M_{i,j} = 1$ et $M_{j,i} = 1$ soit $M_{i,j} = M_{j,i}$. Si $x_i \mathcal{R} x_j$ est faux alors $M_{i,j} = 0$. Dans ce cas peut importe que $x_j \mathcal{R} x_i$ ou non, la proposition de symétricité sera vérifiée. Mais si $x_j \mathcal{R} x_i$ est vraie alors, puisque qu'il y a le quantificateur $\forall$, il faut, par le raisonnement précédent (en inversant i et j) que $x_i \mathcal{R} x_j$ ce que nous avons supposer faux. Donc nécessairement $x_j \mathcal{R} x_i$ est faux, c'est à dire $M_{i,j} = 0 = M_{j,i}$.

- On raisonne comme précédemment en raisonnant avec des 0 et 1 dans la matrice. Si $M_{i,j} = 0$ ou $M_{j,i} = 0$ alors $x_i \mathcal{R} x_j \wedge x_j \mathcal{R} x_i$ est faux et donc l'implication est vraie. Dans ce cas $M_{i,j} \times M_{j,i} = 0$.

Ensemble d’indice

- On appelle ensemble d'indice un sous-ensemble d'un référentiel quelconque qui peut être mis en bijection avec un sous-ensemble de Z.

  Par exemple $\{-2; 6; 12\}$ est un ensemble d'indice.
- Dans la pratique les ensembles d'indices sont les sous-ensembles de Z de la forme [a; b] ou [a; b[lorsque $b = +\infty$.
- L'ensemble des entiers naturel N est un ensemble d'indice.
- L'union, l'intersection, le complémentaire et le produit cartésien (fini) d'ensembles d'indice est un ensemble d'indice.

TITRE DU COURS

FIN

Questions / Réponse

14:30 15:00 15:30 16:00	Mathématiques pour le signal discret Mme DIENE Salle:	Applications client serveur et Web Mr Doudou FALL Salle:	Environnement socio-culturel de l'entreprise M NGAGNE DIA Salle:	Réseaux mobiles Mr DIOUM Salle:	Service réseau Mr Keba Salle:
16:30 17:00 17:30 18:00	Technologie d'accés M MBAYE Salle:	Technologie IP Mr NGOM Salle:	Recherche opérationnelle Mr Oumar FALL Salle:	Programmation orientée-objet Mr KHOUSSA Salle:	Anglais:Techniques d'expression Dr: Ndour Salle: