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 !

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.
- Les mathématiques discrètes fournissent le langage conceptuel pour de nombreux domaines de l'informatique.

Objectifs:

l'objectif principal est de

- fournir aux futurs informaticiens une base intellectuelle solide pour penser comme un ordinateur,
- comprendre comment les algorithmes fonctionnent et prouver leur correction et leur efficacité.

A l’issue de ce cours l’étudiant doit être capable de maitriser le raisonnement formel, comprendre et manipuler les opérateurs logiques

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 : fournir un cadre mathématique pour modéliser les relations entre objets et de développer des algorithmes pour résoudre des problèmes complexes
- 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.

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.

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)

Plan

- Introduction

Chapitre I : Logique

Chapitre II : Méthodes de raisonnement

Chapitre III : Théorie des ensembles :

Chapitre IV : Relation et fonctions

Chapitre V : Arithmétique modulaire et théorie des nombres

Chapitre VI : Théorie des graphes

Chapitre 1 logique mathématique

La logique mathématique est l'épine dorsale de l'informatique. Elle fournit les règles formelles pour raisonner, prouver des théorèmes, concevoir des circuits logiques et écrire des algorithmes corrects.

Logique Propositionnelle (Calcul des Propositions)

La logique propositionnelle s'intéresse aux énoncés déclaratifs simples (propositions) qui peuvent être évalués comme étant soit **Vrais** (V ou 1), soit **Faux** (F ou 0), mais jamais les deux simultanément (principe du tiers exclu).

1.1. Propositions et Valeurs de Vérité

Définition : Une proposition est un énoncé auquel on peut attribuer une valeur de vérité unique.

Exemples :

« Dakar est la capitale du Sénégal" (Vraie)

"2 + 2 = 5" (Fausse)

"Quel temps fait-il ?" (Pas une proposition, c'est une question)

Logique Propositionnelle (Calcul des Propositions)

1.2. Connecteurs Logiques (Opérateurs)

Les connecteurs logiques permettent de combiner des propositions simples pour en former de plus complexes.

Connecteur	Symbole	Nom	Signification
NON	$\neg$ (ou !)	Négation	Inverse la valeur de vérité
ET	$\wedge$ (ou &&)	Conjonction	Vrai si *les deux* sont vraies
OU	$\vee$ (ou `		`)
Implication	$\Longrightarrow$	Implication	"Si... alors..."
Équivalence	$\Longleftrightarrow$	Biconditionnel	Vrai si *les deux* ont la même valeur de vérité

Logique Propositionnelle (Calcul des Propositions)

1.3. Tables de Vérité

Les tables de vérité définissent formellement le comportement des connecteurs.

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \Longrightarrow B$	$A \Longleftrightarrow B$
V	V	F	V	V	V	V
V	F	F	F	V	F	F
F	V	V	F	V	V	F
F	F	V	F	F	V	V

Point clé sur l'implication : L'implication $A \Longrightarrow B$ est toujours vraie sauf si A est vraie et B est fausse.

Logique Propositionnelle (Calcul des Propositions)

1.4. Équivalences Logiques

Deux formules sont logiquement équivalentes si elles ont toujours la même valeur de vérité.

Lois de De Morgan :

$$\neg(A \wedge B) \Longleftrightarrow (\neg A \vee \neg B)$$

$$\neg(A \vee B) \Longleftrightarrow (\neg A \wedge \neg B)$$

Équivalence de l'implication :

$$(A \Longrightarrow B) \Longleftrightarrow (\neg A \vee B)$$

Logique des Prédicats

La logique propositionnelle a des limites : elle ne permet pas d'analyser la structure interne des propositions. La logique des prédicats introduit les variables, les prédicats et les quantificateurs pour un raisonnement plus fin.

2.1. Prédicats et Variables

Un prédicat est un énoncé contenant une ou plusieurs variables, dont la valeur de vérité dépend de la valeur attribuée à ces variables.

Exemple : Soit $P(x)$ le prédicat "x est un nombre pair".

$P(4)$ est Vrai.

$P(3)$ est Faux.

Logique des Prédicats

2.2. Quantificateurs

Les quantificateurs permettent de faire des déclarations sur des collections entières d'objets.

Quantificateur Universel ($\forall$) : "Pour tout" / "Pour chaque"

$\forall x, P(x)$ signifie "Pour tout x, la propriété $P(x)$ est vraie".

Exemple : $\forall n \in \mathbb{N}, n + 1 > n$ (Vrai)

Quantificateur Existentiel ($\exists$) : "Il existe" / "Au moins un"

$\exists x, P(x)$ signifie "Il existe au moins un x pour lequel la propriété $P(x)$ est vraie".

Exemple : $\exists n \in \mathbb{N}, n \times n = 25$ (Vrai, pour $n = 5$)

Logique des Prédicats

2.3. Négation des Quantificateurs

La négation des quantificateurs suit des règles précises, similaires aux lois de De Morgan.

$\neg(\forall x, P(x)) \Longleftrightarrow (\exists x, \neg P(x))$ (Nier "Tout le monde est parfait" équivaut à dire "Il existe quelqu'un qui n'est pas parfait").

$\neg(\exists x, P(x)) \Longleftrightarrow (\forall x, \neg P(x))$ (Nier "Il existe un chat noir" équivaut à dire "Tous les chats ne sont pas noirs").

Chapitre II méthodes de raisonnement

Preuve Directe

Partir des hypothèses (prémisses) et utiliser les règles logiques pour arriver directement à la conclusion.

La preuve directe est une méthode de démonstration qui part des hypothèses données (prémisses) et utilise une série d'implications logiques, de définitions et d'axiomes connus pour arriver directement à la conclusion souhaitée.

Exemple de preuve par raisonnement directe

Prouver que si n est un entier pair, alors n^2est également un entier pair.

Définition d'un nombre pair : Un entier n est pair s'il existe un autre entier k tel que $n = 2k$

Hypothèse de départ (Prémisse A) : "n est un entier pair".

Conclusion visée (Prémisse B) : " n^2 est un entier pair".

Preuve

Étape 1 : On suppose que l'hypothèse est vraie. Supposons que n est un entier pair.

Étape 2 : On applique la définition d'un nombre pair. Par définition, s'il est pair, il existe un entier k

tel que $n = 2k$

Étape 3 : On manipule l'expression pour se rapprocher de la conclusion n^2. Nous cherchons à déterminer la parité de n^2. On élève au carré les deux côtés de l'équation $n = 2k$. n^2= $(2k)^2$.

Étape 4 : On effectue les simplifications algébriques nécessaires. $n^2 = 4k^2$

Étape 5: On réécrit l'expression pour qu'elle corresponde à la définition d'un nombre pair. On peut factoriser par 2. n^2 =2* 2 k^2.

Étape 6 : On identifie un nouvel entier. Posons m= 2 k^2. Puisque k est un entier, k^2 est un entier, et 2 k^2(donc m) est aussi un entier. L'équation devient $n^2 = 2m$.

Étape 7 : On conclut en utilisant la définition (on a atteint la forme 2*entier).Puisque n^2 peut s'écrire sous la forme 2m avec m un entier, par définition, n^2 est un entier pair.

Preuve par Contraposition

Pour prouver $A \Longrightarrow B$, on prouve $\neg B \Longrightarrow \neg A$ (qui est logiquement équivalent).

Exemple de Preuve par Contraposée Énoncé à prouver :Si n^2 est un entier pair, alors n est un entier pair.

Note : Cet énoncé est la réciproque de l'exemple précédent, et il est plus difficile à prouver directement.

Nous allons prouver la contraposée : $\neg B \Longrightarrow \neg A$.

$\neg B$ (Négation de B) : n n'est pas un entier pair", c'est-à-dire, " n est un entier impair.

$\neg A$ (Négation de A) : "n^2 n'est pas un entier pair", c'est-à-dire, n^2 est un entier impair."

L'énoncé à prouver par preuve directe devient : Si n est un entier impair, alors n^2 est un entier impair.

Preuve par Contraposée (Preuve Directe de $\neg B \Longrightarrow \neg A$)

Étape 1 : On suppose que l'hypothèse de la contraposée est vraie. Supposons que n est un entier impair.

Étape 2 : On applique la définition d'un nombre impair. Par définition, un nombre impair n peut s'écrire sous la forme $n = 2k$ où k est un entier. $\neg A$,

Étape 3 : On manipule l'expression pour se rapprocher de la conclusion , soit n^2 impair). On élève au carré les deux côtés de l'équation $n = 2(k+1)$: $n^2 = (2k+1)^2$

Étape 4 : On effectue le développement algébrique. $n^2 = 4k^2 + 4k + 1$

Étape 5 : On réécrit l'expression pour qu'elle corresponde à la définition d'un nombre impair (forme 2m+1. On factorise les deux premiers termes par 2 : $n^2 = 2(2k^2 + 2k) + 1$.

Étape 6 : On identifie un nouvel entier m. Posons m= $(2k^2 + 2k)$Puisque k est un entier, m est aussi un entier. L'équation devient : $n^2 = 2m+1$.

Étape 7 : On conclut. Puisque n^2 s'écrit sous la forme 2m+1 avec m un entier, n^2 est un entier impair.

Preuve par l'Absurde (ou Contradiction)

Supposer que la conclusion est fausse, puis montrer que cela mène à une contradiction logique.

Cette méthode de preuve repose sur le principe logique selon lequel une proposition est vraie si sa négation mène à une contradiction logique (quelque chose qui est manifestement faux ou impossible).

Exemple de Preuve par l'Absurde

- Énoncé à prouver :Le nombre $\sqrt{2}$ est irrationnel.
- Un nombre rationnel peut s'écrire comme une fraction $\frac{p}{q}$ où p et q sont des entiers et $q \neq 0$. Un nombre irrationnel ne peut pas l'être.

Preuve par l'Absurde

Pour prouver une proposition P, on suppose le contraire ¬ P et on montre que cette supposition mène à une contradiction. Si la négation est impossible, alors la proposition originale \(P\) doit être vraie.

P (Proposition à prouver) : $\sqrt{2}$ est irrationnel. ¬ P (Négation supposée) : $\sqrt{2}$ est rationnel."

Etapes logiques

- **Étape 1 :** On suppose la négation de l'énoncé. Supposons par l'absurde que $\sqrt{2}$ est un nombre rationnel.
- **Étape 2 :** On utilise la définition d'un nombre rationnel. S'il est rationnel, il peut s'écrire comme une fraction de deux entiers p et q (où $q \neq 0$) .

$$\sqrt{2} = \frac{p}{q}$$

- De plus, nous supposons que cette fraction est irréductible, c'est-à-dire que p et q n'ont aucun facteur commun autre que 1.

On peut toujours simplifier une fraction jusqu'à ce point.

- **Étape 3** : On manipule l'équation algébriquement.

On élève au carré les deux côtés : $(\sqrt{2})^2 = (\frac{p}{q})^2$ $2=\frac{p^2}{q^2}$

Étape 4 : On réarrange l'équation pour analyser la parité des nombres. $2\ q^2 = p^2$

Étape 5 : On tire une première conclusion logique.

L'équation p^2 =2 q^2 signifie que p^2 est un nombre pair (il est le double d'un entier q^2 D'après l'exemple de preuve par contraposée précédent : si p^2 est pair, alors p doit aussi être pair. Donc, p est pair.

Étape 6 : On utilise le fait que p est pair pour le réécrire. Si p est pair, il existe un entier k tel que p=2k.

Suite de la démonstration

Étape 7 : On substitue cette nouvelle expression de p dans l'équation de l'Étape 4.

$$2q^2 = (2\,k)^2 \qquad\qquad 2q^2 = 4\,k^2$$

Étape 8 : On simplifie l'équation pour analyser q. On divise les deux côtés par:

$$2\,q^2 = 2\,k^2$$

Étape 9 : On tire une deuxième conclusion logique.

L'équation $q^2 = 2\,k^2$ signifie que q^2 est un nombre pair.

De la même manière : si q^2 est pair, alors q doit aussi être pair. Donc, q est pair.

Étape 10 : On identifie la contradiction. Nous avons conclu à l'Étape 5 que p est pair.

Nous avons conclu à l'Étape 9 que q est pair. Cela signifie que p et q ont tous les deux un facteur commun de 2.

Étape 11 : On met en évidence l'absurdité. Or, à l'Étape 2, nous avions explicitement supposé que la fraction $\frac{p}{q}$ était irréductible et que p et q n'avaient aucun facteur commun autre que 1.Nous avons atteint une contradiction : p et q sont à la fois sans facteur commun (sauf 1) et pairs (donc divisibles par 2).

Conclusion

La supposition initiale $\neg$ P selon laquelle $\sqrt{2}$ est un nombre rationnel mène à une contradiction logique.

Par conséquent, cette supposition est fausse.

L'énoncé original P est donc vrai : Le nombre $\sqrt{2}$ est irrationnel.

Preuve par Récurrence

Méthode fondamentale pour prouver qu'une propriété est vraie pour tous les nombres naturels, en montrant qu'elle est vraie pour le premier élément (cas de base) et que si elle est vraie pour un certain n, elle l'est aussi pour n+1.

Propriété à démontrer : Pour tout entier naturel non nul n ≥ 1 la somme des entiers de 1 à n est donnée par la formule

$$S_n = 1 + 2 + 3 + \cdots n = \frac{n(n+1)}{2}.$$

On note P(n) la propriété : " $1 + 2 + 3 + \cdots n = \frac{n(n+1)}{2}$ ".

Une preuve par récurrence se déroule en trois étapes principales : l'initialisation, l'hérédité, et la conclusion.

Initialisation

- **Étape 1 :** On vérifie que la propriété P(n) est vraie pour le premier rang possible, ici n=1.
- Pour n=1, la somme est simplement 1.
- En utilisant la formule, on obtient $\frac{1(1+1)}{2} = \frac{1*(2)}{2}$ =1.
- Les deux résultats sont égaux 1=1.
- Donc, la propriété P(1) est vraie.

Hérédité

- On suppose que la propriété P(n) est vraie pour un certain rang n (appelée hypothèse de récurrence), et on démontre qu'elle est alors nécessairement vraie pour le rang suivant, n+1.
- **Hypothèse de récurrence :** Supposons que P(n) soit vraie pour un entier n ≥ 1 fixé,

c'est-à-dire $1+2+3+\cdots n=\frac{n(n+1)}{2}$

- Démonstration pour le rang n+1 : On veut montrer que P(n+1) est vraie, c'est-à-dire :1+2+3+…n+1= $1+2+3+\cdots n+(n+1)=\frac{(n+1)\big((n+1)+1\big)}{2}=\frac{(n+1)(n+2)}{2}$.
- Partons de la somme pour n+1 et utilisons l'hypothèse de récurrence : $1+2+3+\cdots n+(n+1)=(1+2+3+\cdots n)+(n+1)$. D'après l'hypothèse de récurrence, on peut remplacer la somme des n premiers termes $\frac{n(n+1)}{2}$ =(n+1)
- Maintenant, on met au même dénominateur pour simplifier l'expression $\frac{n(n+1)}{2}+\frac{2(n+1)}{2}$
- On factorise par n+1 : $\frac{(n+1)(n+2)}{2}$
- On a bien obtenu la formule souhaitée pour le rang n+1.
- La propriété P(n) est donc héréditaire.

Conclusion

Étape 3 : Puisque la propriété P(n) est vraie au premier rang (n=1) et qu'elle est héréditaire, alors, par le principe de récurrence, elle est vraie pour tout entier naturel n ≥ 1 .

On peut donc conclure que, pour tout n ≥ 1

$$1 + 2 + 3 + \cdots n = \frac{n(n+1)}{2}$$

Fin du cours