Mathématiques pour l'informatique 1

Cours 4 - Quantificateurs et démonstration par récurrence

Émilie Charlier

Université de Liège

Quantificateurs

Le langage de la logique propositionnelle ne contient pas les symboles $\forall$ and $\exists$. Ces symboles sont les ingrédients de base de la logique du premier ordre.

Définition

Le symbole $\forall$ se lit “pour tout” et est appelé le quantificateur universel.
Le symbole $\exists$ se lit “il existe” et est appelé le quantificateur existentiel.

Comment nier une assertion contenant des quantificateurs ?

Considérons l'assertion

"Pour tout $x \in \mathbb{R}$, on a $x^2 \geq 0$."

La négation de cette assertion est

"Il existe $x \in \mathbb{R}$ tel que $x^2 < 0$."

Formellement, on écrira

$$\neg\big(\forall x,\ P(x)\big) \equiv \exists x,\ \neg P(x).$$

Considérons maintenant l'assertion

"Il existe $x \in \mathbb{R}$ tel que $x + 3 \geq x^3$."

Nier cette assertion revient à dire

"Pour tout $x \in \mathbb{R}$ tel que $x + 3 < x^3$.".

Formellement, on écrira

$$\neg\big(\exists x,\, P(x)\big) \equiv \forall x,\, \neg P(x).$$

Calcul des prédicats

Dans ces écritures, x n'est pas une variable propositionnelle.

On suppose que x est une variable représentant un élément du domaine D de la structure dans laquelle est définie le prédicat P, et on met ce fait en évidence en écrivant $P(x)$.

La logique du premier ordre est aussi appelée calcul des prédicats.

Définition
Un prédicat sur un domaine D est une partie de D^p pour un certain naturel p. On parle de prédicat d'arité p.

Si P est un prédicat d'arité p sur D et si $(x_1, \ldots, x_p) \in D^p$, on dit que $(x_1, \ldots, x_p)$ vérifie P lorsque $(x_1, \ldots, x_p) \in P$.

Vocabulaire

- Le terme “premier ordre” vient du fait qu’on a le droit de quantifier uniquement sur les variables et non sur les prédicats eux-mêmes.
- Lorsqu’une variable d’une formule n’est pas quantifiée, on dit qu’elle est libre.
- Les variables quantifiées sont dites liées ou muettes. On dit aussi qu’elles sont liée par un quantificateur.
- On peut renommer les variables liées (partout dans une même formule) sans en changer le sens. Ainsi, les formules

$$\forall x,\ x + y = 2 \qquad \text{et} \qquad \forall a,\ a + y = 2$$

sont équivalentes.

Une autre technique de démonstration : le contre-exemple

L'équivalence logique $\neg\big(\forall x,\ P(x)\big) \equiv \exists x,\ \neg P(x)$ conduit à la technique de démonstration par le contre-exemple.

Plus précisément, lorsque l'on souhaite prouver qu'une formule du type $\forall x,\ P(x)$ est fausse, il suffit d'exhiber un contre-exemple, c'est-à-dire un x tel que $\neg P(x)$ est vrai.

Un exemple

Pour démontrer que l'affirmation que

$$\text{"tout réel } x \text{ vérifie l'inégalité } x^2 + 3x + 1 \geq 0\text{"}$$

est fausse, il suffit de trouver un réel x tel que cette inégalité n'est pas vérifiée.

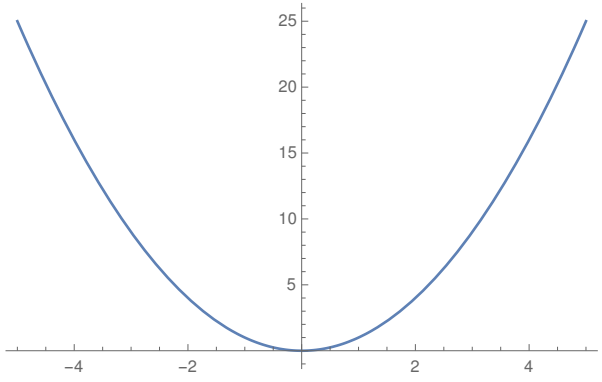
Par exemple, le réel -1 est tel que

$$(-1)^2 + 3(-1) + 1 = 1 - 3 + 1 = -1 < 0.$$

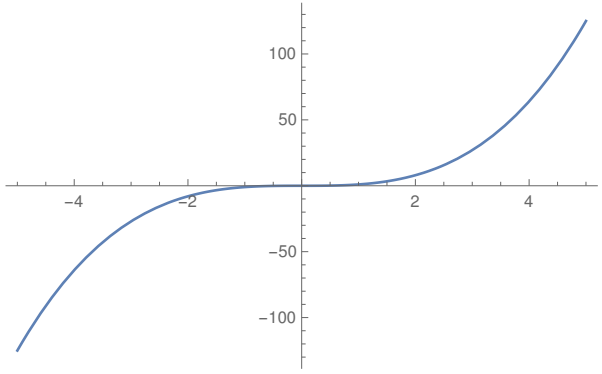
Un deuxième exemple

On dit qu'une fonction $f : \mathbb{R} \to \mathbb{R}$ est paire lorsque pour tout $x \in \mathbb{R}$, on a $f(-x) = f(x)$.

C'est par exemple le cas de la fonction $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$



mais pas de la fonction $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^3$.



Pour affirmer que la fonction $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^3$ n'est pas paire, on doit montrer que la formule

$$\text{"pour tout } x \in \mathbb{R}\text{, on a } f(-x) = f(x)\text{"}$$

est fausse pour cette fonction f particulière, c'est-à-dire que la formule

$$\text{"pour tout } x \in \mathbb{R}\text{, on a } (-x)^3 = x^3\text{"}$$

est fausse.

Un contre-exemple est donné par le réel -2 puisque

$$(-2)^3 = -8 \neq 2^3 = 8.$$

L'ordre des quantificateurs est important.

Lorsqu'on écrit

$$\forall x \, \exists y \, P(x, y)$$

ce qui se lit "pour tout x, il existe y tel que la propriété $P(x, y)$ a lieu", le choix de y dépend de celui de x.

Inversement, lorsqu'on écrit

$$\exists y \, \forall x \, P(x, y)$$

ce qui se lit "il existe y tel que pour tout x, la propriété $P(x, y)$ a lieu, le choix de y ne dépend pas de celui de x.

La propriété est plus forte dans le second cas : on a toujours

$$\exists y \, \forall x \, P(x, y) \implies \forall x \, \exists y \, P(x, y).$$

Un exemple parlant

Considérons le prédicat $P(x, y)$ signifiant y est la mère de x.

Ici, x représente une personne (homme ou femme) et y une femme.

Les deux phrases suivantes ont des sens différents :

- $\forall x \exists y\, P(x, y)$ signifie que "pour toute personne, il existe une femme qui est sa mère", autrement dit "tout le monde a une mère".
- $\exists y \forall x\, P(x, y)$ signifie que "il existe une femme telle que pour toute personne, cette femme est sa mère", autrement dit "il existe une femme qui est la mère de tout le monde".

Un exemple mathématique

Les assertions suivantes sont-elles vraies ou fausses ?

- $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x + y = 2.$
- $\exists y \in \mathbb{R}, \forall x \in \mathbb{R}, x + y = 2.$

Néanmoins, remarquons que deux quantificateurs universels successifs commutent toujours entre eux.

Il en est de même pour deux quantificateurs existentiels successifs.

Ainsi, on a

$$\forall x \, \forall y \, P(x, y) \equiv \forall y \, \forall x \, P(x, y)$$

et

$$\exists x \, \exists y \, P(x, y) \equiv \exists y \, \exists x \, P(x, y).$$

La démonstration par récurrence

Principe de récurrence

Soient P un prédicat défini sur $\mathbb{N}$ et $m \in \mathbb{N}$ tels que les deux conditions suivantes soient vérifiées.

1. L'entier m vérifie P.
2. Pour tout entier $n > m$, si $n-1$ vérifie P, alors n vérifie P.

Alors tous les entiers $n \geq m$ vérifient P.

La condition 1 est appelée le cas de base ou l'initialisation.
La condition 2 est appelée l'hérédité ou le pas de récurrence.
La partie "si $n-1$ vérifie P" de la condition 2 est appelée l'hypothèse de récurrence.

Un exemple

Montrons que pour tout entier $n \geq 1$, on a

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}.$$

Démonstration par récurrence

Nous procédons par récurrence sur n.

Démontrons d'abord le cas de base : $n = 1$. D'une part, $\sum_{i=1}^{1} i^2 = 1$ et d'autre part, $\frac{1(1+1)(2\cdot 1+1)}{6} = 1$. Le cas de base est donc vérifié.

Montrons à présent l'hérédité. Soit $n \geq 1$ et supposons que l'égalité demandée soit vérifiée en n (hypothèse de récurrence). Nous devons montrer que cette égalité est vérifiée également en $n+1$, c'est-à-dire que

$$\sum_{i=1}^{n+1} i^2 = \frac{(n+1)(n+2)(2(n+1)+1)}{6}.$$

D'une part, en développant le membre de gauche, nous obtenons

$$\begin{aligned}
\sum_{i=1}^{n+1} i^2 &= \sum_{i=1}^{n} i^2 + (n+1)^2 \\
&= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\
&= \frac{n(n+1)(2n+1) + 6(n+1)^2}{6} \\
&= \frac{(n+1)\big(n(2n+1) + 6(n+1)\big)}{6} \\
&= \frac{(n+1)(2n^2+7n+6)}{6},
\end{aligned}$$

où l'on a utilisé l'hypothèse de récurrence à la deuxième ligne.

D'autre part, en développant le membre de droite, nous avons

$$\begin{aligned}\frac{(n+1)(n+2)(2(n+1)+1)}{6} &= \frac{(n+1)(n+2)(2n+3)}{6} \\ &= \frac{(n+1)(2n^2+7n+6)}{6}.\end{aligned}$$

D'où la conclusion. □

Récurrence forte

Principe de récurrence forte

Soient P un prédicat défini sur $\mathbb{N}$ et $m \in \mathbb{N}$ tels que les deux conditions suivantes soient vérifiées.

1. L'entier m vérifie P.
2. Pour tout entier $n > m$, si tout entier $i \in \{m, m+1 \ldots, n-1\}$ vérifie P, alors n vérifie P.

Alors tous les entiers $n \geq m$ vérifient P.

Exemple de récurrence forte

Montrons que tous les entiers $n \geq 2$ se factorisent en un produit de nombres premiers.

Démonstration par récurrence (forte)

Cas de base : $n = 2$. Puisque 2 est un nombre premier, il est évidemment le produit d'un unique nombre premier, à savoir lui-même.

Hérédité. Supposons à présent que $n > 2$ et que tout nombre entier m compris entre 2 et $n - 1$ se factorise en un produit de nombres premiers.

Si n est un nombre premier, c'est évident (comme pour le cas de base).

Supposons à présent que n n'est pas un nombre premier : n est donc divisible par un entier d compris entre 2 et $n - 1$.

Le quotient $\frac{n}{d}$ est donc un entier compris entre 2 et $n - 1$ lui aussi.

Par hypothèse de récurrence appliquée à d et à $\frac{n}{d}$, on obtient que ces deux entiers se factorisent en un produit de nombres premiers.

Puisque $n = d \cdot \frac{n}{d}$, le produit de ces deux factorisations nous fournit une factorisation en nombres premiers pour n. □

Sur l'importance du cas de base

En négligeant le cas de base, on pourrait montrer (erronément, donc) que

- les nombres impairs sont pairs ;
- tous les chevaux sont de la même couleur.

Tours de Hanoï

- Données du jeu : 3 socles et n disques de tailles différentes empilés du plus grand au plus petit sur le premier socle.
- But du jeu : Déplacer les n disques du 1^{er} socle au 3^{e}.
- Règles du jeu : Un seul disque peut être déplacé à la fois et on ne peut pas placer un disque sur un disque plus petit que lui.

On voudrait justifier en combien de déplacements $H(n)$ on peut gagner le jeu pour un nombre de disques n quelconque.

Nous allons montrer que $H(n) = 2^n - 1$ pour tout $n \geq 1$.

Stratégie : On procède par récurrence sur n.

Cas de base. Si on a un seul disque, un seul déplacement du 1^{er} au 3^{e} socle est effectué : on a $H(1) = 1 = 2^1 - 1$.

Hérédité. Supposons à présent avoir $n > 1$ disques et être capables de gagner le jeu pour $n-1$ disques au moyen de $H(n-1) = 2^{n-1} - 1$ déplacements.

Pour gagner le jeu avec n disques au départ, on commence par déplacer les $n-1$ disques supérieurs du 1^{er} au 2^{e} socle (le disque restant sur le premier socle ne pose pas de problème puisqu'il est de taille maximale). Ceci nous coûte $H(n-1)$ déplacements.

On déplace ensuite le disque restant du 1^{er} au 2^{e}. Ceci nous coûte 1 déplacement.

Enfin, on déplace les $n-1$ disques du 2^{e} au 3^{e} socle, ce qui nous coûte encore $H(n-1)$ déplacements.

On en conclut que notre stratégie vérifie

$$\begin{aligned} H(n) &= 2H(n-1) + 1 \\ &= 2(2^{n-1} - 1) + 1 \quad \text{(hypothèse de récurrence)} \\ &= 2^n - 2 + 1 \\ &= 2^n - 1. \end{aligned}$$