3 TD 3 : Technique de preuve et mathématiques discrètes

Certaines parties de ce cours sont inspirées du cours de principe de fonctionnement des machines binaires de Jean Marie Rifflet et du cours de langage Mathématique de René Cory. Pour les étudiants anglophone, un super séminaire And Logic Begat Computer Science : When Giants Roamed the Earth.

3.1 Qu'est-ce qu'une preuve ?

3.1.1 Les preuves qu'il ne faut pas faire

1. **Preuve par l'exemple** L'auteur démontre le cas n = 2 et prétend qu'il contient la plupart des idées de la preuve générale.
2. **Preuve par généralisation** "Ca marche pour 17, donc ça marche pour tout nombre réel."
3. **Preuve par intimidation** "Trivial."
4. **Preuve par épuisement** Trois copies doubles consacrées à votre preuve sont utiles.
5. **Preuve par omission** "Les 253 autres cas sont analogues", "Le lecteur règlera facilement les détails."
6. **Preuve par obscurcissement** Une suite longue et incohérente d'assertions syntaxiquement proches, toutes vraies et/ou sans signification.
7. **Preuve par calcul** "Cette preuve demandant du calcul, nous passons à la suite."
8. **Preuve par fin de l'exposé** "Vu l'heure, je laisserai la preuve de ce théorème en exercice."
9. **Preuve par dessin** "On voit bien que les trois doites sont concourantes".
10. **Preuve par consensus** "Tous d'accord ?"
11. **Preuve par démocratie** "Que ceux qui sont pour lèvent la main." A utiliser seulement si la preuve par consensus est impossible.

Exercice 9 *A vous de jouer*
Proposez votre définition de proposition mathématique, de preuve ou de démonstration. Que pensez-vous de la phrase : "Cette phrase est fausse.".

L'idée est de leur faire prendre conscience qu'ils ne savent pas précisément ce qu'est une proposition mathématique, une preuve, le vrai, le faux ...

Définition 1 (Preuve)**.** *En mathématiques, une démonstration permet d'établir une proposition (mathématique) à partir de propositions initiales, ou précédemment démontrées à partir de propositions initiales, en s'appuyant sur un ensemble de règles de déduction.*

On a donc besoin ici de rappeller la syntaxe et la sémantique du langage des mathématiques et la manière de l'utiliser c'est à dire les règles de déduction utilisables. C'est aussi un langage qu'on utilise pour parler des algorithmes en informatique.

Le langage mathématique manipule des *propositions*. Ces propositions prennent des valeurs dans les *booléens*, c'est à dire l'ensemble $\{VRAI, FAUX\}$. Ainsi

— il pleut
— il y a des embouteillages
— nous sommes dimanche soir

sont des propositions concrètes susceptibles d'être vrai ou fausse selon le contexte. On peut donc les voir comme des variables (propositionnelles). Il en est de même dans un programme de l'expression $x + y < z$ qui selon les valeurs de x, y et z peut avoir la valeur $VRAI$ ou $FAUX$. D'autres propositions ont des valeurs plus affirmées et s'apparentent donc plutôt à des constantes.

— Paris est la capitale de la France : c'est vrai
— 12 est un nombre premier : c'est faux
— la 23-ème décimale de π est 4 : c'est vrai

Remarquez que n'importe quel théorème est une proposition de valeur de vérité constante vraie. La suite du cours explique comment former des proposition mathématiques et comment les prouver.

3.2 Langage logique et technique de preuve

3.2.1 Définir des objets

Les mathématiques passent leur temps à définir des objets de plus en plus compliqués à partir d'objets simples. Pour faire une preuve sur un objet ou une propriété, il est ensuite nécessaire de le remplacer au cours de la preuve par sa définition. Le premier objet des mathématiques sont bien sûr les nombres et les opérations qu'on peut faire dessus $+, \times, -, \div, <, \ldots$.

Commençons par un exemple de définition récursive des entiers dans l'esprit du cours précédent.

Un nombre entier est $\begin{cases} \text{soit } 0 \\ \text{soit } S(x) \text{ ou } x \text{ est un entier} \end{cases}$

S est le successeur d'un entier, en langage courant $S(x)$ est le nombre $x+1$ mais nous devons encore définir l'addition. Cette définition des nombres entiers est naturelle : ils sont obtenus en comptant à partir de 0. Voici une définition récursive de l'addition qui nous donnerait un algorithme pour la calculer (dans les langages de programmation classique l'addition est directement prise en charge).

$$x + y = \begin{cases} x \text{ si } y = 0 \\ S(x) + z \text{ si } y = S(z) \end{cases}$$

Il est facile de voir que $2+2=4$. En effet $2 = S(S(0))$. Donc $2+2 = S(S(0))+S(S(0))$. On applique une fois la définition de l'addition pour obtenir $2+2 = S(S(S(0)))+S(0)$, puis une deuxième fois $2+2 = S(S(S(S(0))))+0$ et une troisième fois pour obtenir $2+2 = S(S(S(S(0))))$. Pour prouver des propriétés importants de l'addition nous aurons besoin d'utiliser le raisonnement par récurrence que nous verrons ultérieurement.

Exercice 10 *Preuve sur l'addition*
On suppose que $x+0 = 0+x$. Peut-on alors montrer que $x+1 = 1+x$ en utilisant uniquement les définitions précédentes ?

Exercice 11 *La multiplication des définitions*
Donner une définition récursive de la multiplication.

Voici la définition récursive la plus simple de la multiplication :

$$x \times y = \begin{cases} 0 \text{ si } z = 0 \\ x \times +z + x \text{ si } y = S(z) \end{cases}$$

Heureusement, vous n'avez pas besoin de manipuler les nombres entiers de manière aussi compliquée et lente que ce que nous venons de vous montrer. Pendant votre scolarité, de la primaire au lycée vous avez appris à additionner, multiplier, comparer des entiers, des fractions et même des termes avec des variables. Vous savez aussi mettre au même dénominateur, factoriser, calculer les racines d'un polynôme ... C'est ce qu'on appelle calculer et c'est souvent un ingrédient essentiel des preuves que vous allez faire. L'utilisation de toute ces méthodes de calcul n'est en fait que l'utilisation de *théorèmes* simples sur les nombres entiers ou les fractions ainsi que leurs définitions.

3.2.2 Connecteurs logiques

On peut construire à partir de deux énoncés un énoncé plus compliqué grâce à un connecteur logique. Par exemple on peut combiner l'énoncé "Ma vache est bleue" avec l'énoncé "Ma lampe est rouge" en un seul énoncé "Ma vache est bleue ET ma lampe est rouge".

Les connecteurs logiques peuvent être vus comme des fonctions sur les valeurs de vérité des propositions. Les plus connus sont la négation notée $\neg$, la conjonction notée $\wedge, \&$ (et en français) et la disjonction notée $\vee, |$ (ou en français). Une difficultée dans la manipulation de ces connecteurs est que leur sens mathématique et leur sens dans le langage courant diffère. Le OU mathématique a le sens suivant : A ou B est vrai si *au moins* une des deux propositions A et B est vraie. Ça n'est pas le même sens qu'en français dans l'expression "fromage ou dessert", on a droit à *exactement* un des deux (ce qui correspond à la fonction ou exclusif notée XOR). Les symboles $\wedge$ et $\vee$

ressemblent beaucoup aux symboles $\cup$ et $\cap$, pour une bonne raison. Nous avons $x \in E_1 \,\mathrm{OU}\, x \in E_2$ équivalent à $x \in E_1 \cup E_2$ et $x \in E_1 \,\mathrm{ET}\, x \in E_2$ équivalent à $x \in E_1 \cap E_2$.

Exercice 12 *Si vous répondez mal, gare ...*
Un père logicien dit à son fils fais tes devoirs ou je te colle une baffe. Le fils se dépêche de faire ses devoirs et retourne annoncer à son père qu'il les a fini. Celui-ci lui dit c'est très bien et lui colle une baffe. Le père est il cohérent avec ses déclarations ? Approuvez-vous ses méthodes pédagogiques ?

On représente les fonctions booléennes par des tables de vérité qui donnent leur valeur en fonction de la valeur de leurs arguments.

ET	VRAI	FAUX
VRAI	VRAI	FAUX
FAUX	FAUX	FAUX

OU	VRAI	FAUX
VRAI	VRAI	VRAI
FAUX	VRAI	FAUX

Les implications $\Rightarrow$ et équivalences $\Leftrightarrow$ que vous utilisez lors de démonstrations sont aussi des fonctions booléennes. Attention $\Rightarrow$ est souvent confondue avec *donc* ou *alors* en français. Effectivement $A \Rightarrow B$ a le même sens que A alors B quand A est vrai mais l'expression a aussi un sens quand A est faux : elle est vraie. En effet le faux implique n'importe quoi, c'est même une des définitions historiques de ce qu'est un énoncé faux. À la fin du 19ème siècle le langage mathématique était assez mal établi. Certains mathématiciens ont suggéré qu'une proposition fausse était une proposition qui impliquait n'importe quoi. Hilbert n'était d'abord pas très convaincu par cette définition puis il a du lire une thèse dans laquelle le premier théorème à la première page était faux et s'ensuivait une centaine de pages de résultats extraordinaires .... A est équivalent à B est vrai si A a la même valeur de vérité que B.

A est équivalent à B est vrai si A a la même valeur de vérité que B.

Exercice 13 *Table de vérité*
Écrire les tables de vérité de $A \Rightarrow B$ et de $\neg B \Rightarrow \neg A$. Que constatez-vous ? Ce phénomène permet de faire une *preuve par contraposée*. Utiliser cette technique de preuve pour montrer que n^2 impair $\Rightarrow$ n impair.

Expliquer brièvement la preuve par contraposée. Pour pouvoir en faire, il faut savoir nier des propositions. Il existe des formules qui permettent d'appliquer une négation à des propositions contenant les connecteurs ET et OU. Ce sont les lois de Morgan : $\neg(A \,\mathrm{ET}\, B)$ est équivalent à $(\neg A \,\mathrm{OU}\, \neg B)$ et $\neg(A \,\mathrm{OU}\, B)$ est équivalent à $(\neg A \,\mathrm{ET}\, \neg B)$.

Exercice 14 *Simplification*
Simplifiez les expressions suivantes :

1. $A \,\mathrm{ET}\, A$
2. $(A \Rightarrow B) \,\mathrm{OU} (B \Rightarrow C)$
3. $(A \,\mathrm{ET}\, B) \,\mathrm{OU}\, \neg(\neg A \,\mathrm{OU}\, C)$

On veut prouver des propositions avec des connecteurs. Il y a trois cas :
— $A \,\mathrm{ET}\, B$, il faut prouver indépendemment A et B
— $A \,\mathrm{OU}\, B$, en général il faut choisir soit A soit B et le prouver. Si on n'y arrive pas, on peut aussi montrer que A est vraie quand B est faux ou que B est vraie quand A est faux.
— $A \Rightarrow B$, il faut ajouter A aux hypothèses et prouver B.
On peut donner un exemple de preuve avec des connecteurs.

3.2.3 Variables et quantificateurs

Dans une proposition mathématique on peut utiliser une variable qui n'a pas de valeur définie. Si la variable est x on peut noter la proposition A, $A(x)$. La proposition est alors vraie ou fausse selon la valeur de la variable, comme dans l'expression $x+y \leq z$. Il est important de restreindre la variable à certaines valeurs possibles, par exemple $x \in \mathbb{N}$ signifie que x est n'importe quel *entier*. C'est la même chose que définir le type d'une variable dans un langage de programmation.

On peut ensuite lier les variables libres des ces proposition grâce à des quantificateurs ce qui donne une proposition close (qui a une valeur de vérité qui ne dépends de rien d'autre que d'elle même). Il existe deux quantificateurs qui permettent d'utiliser des variables dans les expressions mathématiques :

1. Quel-que-soit : $\forall x A(x)$ signifie que la propriété $A(x)$ est vraie pour toutes les valeurs possibles de x
2. Il existe : $\exists x A(x)$ signifie qu'il existe au moins un x qui satisfait la proposition $A(x)$.

Par exemple la proposition "tous les professeurs de méthodologie sont sévères" est fausse mais la proposition "il existe un professeur de méthodologie qui soit sévère" est vraie (devinez qui). Un autre exemple de la rigueur mathématique : Un ingénieur, un physicien et un mathématicien sont dans un train en Écosse. Ils voient un mouton noir sur le bord de la route. « Les moutons écossais sont noirs.» dit l'ingénieur. « Non, il est plus correct de dire qu'au moins un mouton écossais est noir. » corrige le physicien. « Non, tout ce que l'on peut conclure est qu'il existe en Écosse au moins un mouton dont l'un des côtés est noir ! » dit le mathématicien...

Pour prouver une proposition avec des quantifiquateurs on doit :
— pour $\forall x A(x)$ prouver la proposition $A(x)$ sans faire aucune supposition sur x. On peut utiliser un raisonnement par cas (voir ultérieurement).
— pour $\exists x A(x)$ on doit exhiber un x précis tel que $A(x)$ soit vrai. C'est le seul cas ou un exemple est une preuve !
Prouver pour l'exemple $\forall x \in \mathbb{R} x \geq 0 \,\mathrm{OU}\, x \leq 0$.

Exercice 15 *Mathématiques élémentaires*
Montrer que $\forall x \in \mathbb{R} > 1, x^2 > x$. Montrer que $\exists x \in \mathbb{R} > 0, x^2 < x$. Ces propositions sont elles encore vraies si on remplace $\mathbb{R}$ par $\mathbb{N}$.

Attention l'ordre des quantificateurs est important. Par exemple $\forall x \in \mathbb{N} \exists y \in \mathbb{N}, x \leq y$ signifie que pour tout entier x on peut trouver un entier y qui soit plus grand, ce qui est vrai. Par contre $\exists y \in \mathbb{N} \forall x \in \mathbb{N}, x \leq y$ siginifie qu'il existe une entier plus grand que tous les autres ce qui est faux. Un exemple similaire en français : pour tous les hommes il existe une personne qui est leur mère. Si on inverse les quantificateurs on obtient il existe une personne qui est la mère de tous les hommes.

Comme pour les connecteurs ET et OU la négation a un effet de dualité sur les quantificateurs :

$$\neg(\forall x A(x)) \Leftrightarrow \exists x \neg A(x)$$

$$\neg(\exists x A(x)) \Leftrightarrow \forall x \neg A(x)$$

Exercice 16 *Esprit de contradiction*
Nier les propositions :
— Je suis né en automne OU je suis né au printemps.
— Il existe un homme qui est né en automne.
— Tous les hommes ont un ami. Essayer de traduire cette proposition en langage symbolique en quantifiant sur l'ensemble des hommes H et en utilisant la relation $A(x, y)$ qui signifie que x et y sont amis.
— Pour tous les hommes, il existe une femme qui peut tomber (grave) amoureuse de lui
— Il existe des groupes de TD où tous les étudiants sont (grave) chiants

3.2.4 Utiliser des théorèmes

Pour faire une preuve on peut utiliser des faits déjà prouvé comme des hypothèses. L'utilisation d'un théorème de la forme $\forall x A(x)$ est appellé un syllogisme. C'est la méthode la plus ancienne de raisonnement connue est l'application d'un théorème qu'on donne en prémisse à un cas particulier.
Tous les hommes sont mortels.
Socrate est un homme.
Donc Socrate est mortel.

Les théorèmes sont aussi souvent de la forme $A \Rightarrow B$. Pour les utiliser, il faut avoir prouvé que A est vrai, et on peut alors ajouter B a ses hypothèses.

Exercice 17 *Fourni par Ionesco*
Que pensez vous de la démonstration suivante : Tous les chats sont mortels.
Socrate est mortel.
Donc Socrate est un chat.

3.2.5 Méthode de raisonnement par cas

C'est un raisonnement qui peut s'appliquer dès qu'on s'intéresse à un ensemble d'objets E qu'on peut séparer en une union d'ensembles $E_1, \dots E_n$. Pour prouver quelque chose sur E il suffit de le prouver séparément sur $E_1, \dots E_n$. De la même manière si on veut prouver $A \operatorname{ET} B$ il suffit de prouver indépendemment A et B.

Par exemple on veut prouver que tout carré est toujours un multiple de 4 ou un de plus qu'un multiple de 4. On considère x^2. On a deux cas possible, soit $x = 2n$ ou $x = 2n+1$ pour n un entier. Si $x = 2n$ alors $x^2 = 4n^2$ et c'est un multiple de 4. Si $x = 2n+1$ alors $x^2 = 4n^2 + 4n + 1 = 4(n^2 + n) + 1$ ce qui est un de plus qu'un multiple de 4.

Exercice 18 *C'est vrai dans l'absolu*
Prouver que $-5 \leq |x+2| - |x-3| \leq 5$.

3.2.6 Méthode de raisonnement par l'absurde

Le raisonnement par l'absurde est le raisonnement suivant : si d'une série d'hypothèses et de la proposition $\neg A$ je peux déduire le faux (une contradiction) alors de ma série d'hypothèses je peux déduire la proposition A. Ce raisonnement est correct à cause du principe du tiers exclu qui affirme que soit A soit $\neg A$ est vrai.

Imaginons que vous êtes en train de résoudre un sudoku et que vous considérez une case qui peut être remplie à priori par 1 ou un 2. Vous pouvez remplir la case avec un 1 et continuer à résoudre le sudoku. Si à un moment vous trouvez une contradiction, vous pouvez effacer tout ce que vous avez fait depuis que vous avez rempli le 1 et le remplacer par un 2 en étant sûr de ce nombre. C'est un raisonnement par l'absurde qui justifie cette méthode et elle correpond à un algorithme dit de backtracking qui permet de résoudre n'importe quel sudoku.

Exercice 19 *Un résultat irrationnel*
Montrer par l'absurde que $\sqrt{2}$ ne peut pas s'écrire sous la forme $\frac{a}{b}$ avec a et b des entiers.

3.2.7 Raisonnement par récurrence

Le raisonnement par récurrence est très lié aux programmes récursifs et aux fonctions et objets définis de manière récursives : *c'est la seule méthode de preuve qui permet d'établir des propriétés dans ces différents cas.* Le principe du raisonnement par récurrence est le suivant :

1. Énoncer une propriété que vous voulez prouver. Elle doit dépendre explicitement d'un entier qu'on va appeler n.
2. Prouver la propriété pour $n = 0$, ou la première valeur de n qui ait un sens. C'est ce qu'on appelle l'initialisation.
3. Supposer que la propriété est vraie pour un certain n et se servir de cette hypothèse de récurrence pour prouver la propriété pour n+1.

On peut imaginer une démonstration par récurrence comme un programme qui va prouver votre propriété pour tout n. A chaque étape de la boucle on utilise le point 3 pour incrémenter n et ajouter un nouvel n pour lequel la propriété est prouvée.

Exemple de raisonnement par récurrence : les tiroirs et les chaussettes.

Théoreme 1. *Soit m chaussettes rangées dans n tiroirs, si $m > n$ alors il y a un tiroir qui contient 2 chaussettes.*

Raisonnement par récurrence sur m. **Initialisation :** Si $m = 1$ et $n > m$ alors $n \geq 2$. Donc il y a au moins deux chaussettes dans l'unique tiroir. **Hérédité :** Supposons que la propriété soit vraie pour n, montrons la pour n+1. Il y a deux cas, soit tous les tiroirs sont remplis par deux chaussettes ou plus et la propriété est démontrée. Soit il existe au moins un tiroir rempli d'une chaussette ou moins. Considérons maintenant les n tiroirs restants, nous avons $m-1$ chaussettes dedans. Comme $m > n+1$, nous avons $m-1 > n$ et donc par hypothèse de récurrence il y a deux chaussettes dans un des tiroirs restants.

Exercice 20 *Preuve sur la multiplication*
Montrer que si $x = 0$ alors $x \times y = 0$ en utilisant la définition récursive de la multiplication.

Exercice 21 *Tous les crayons sont de la même couleur*
On veut prouver la propriété suivante : "Soit n crayons, ils sont tous de la même couleur". Est-ce que la preuve suivante est correcte ?

Soit un crayon, il y a bien une seule couleur. Supposons la propriété vraie pour n crayons et montrons la pour $n+1$ crayons. On considère l'ensemble A des n premiers crayons et l'ensemble B des n derniers crayons. Par hypothèse de récurrence, tous les crayons de A sont de la même couleur et tous les crayons de B sont de la même couleur. Comme A et B ont des éléments en commun, les $n+1$ crayons sont de la même couleur.

3.2.8 Limite de la formalisation

Nous n'avons pas entièrement formalisé les mathématiques, car c'est extrêmement lourd et on choisit toujours de raisonner au niveau d'abstraction qui rends une explication ou une démonstration la plus simple possible tout en restant rigoureux (c'est à dire en sachant que tout ce qu'on dit est compris de manière non ambigüe par le lecteur et le locuteur).

Comme nous n'avons pas entièrement formalisé les mathématiques, il reste quelques petits problèmes. Que pensez-vous d'un homme qui dans son village rase tous les hommes qui ne se rasent pas eux mêmes ?

3.2.9 Quelques problèmes de mathématiques discrètes

Exercice 22 *Les cheveux sur la tête*
Sachant qu'une tête normale a au plus 1.000.000 cheveux, montrez qu'il y a au moins deux personnes à Paris qui ont le même nombre de cheveux.

Exercice 23
Sur un tableau carré noir et blanc de 1 mètre de côté, montrer qu'il existe un couple (en fait une infinité) de points de même couleur à distance 50 cm l'un de l'autre.

Exercice 24 *Se serrer la pince*
Montrer que dans une réunion les gens qui serrent un nombre impair de fois la main d'autres personnes sont toujours en nombre pair.

Exercice 25 *Sudoku*
Dans un Sudoku montrer que si on a k cases de la même ligne qui peuvent prendre uniquement k mêmes valeurs alors ces valeurs ne peuvent pas être utilisée ailleurs dans la ligne.

Exercice 26 *Ramsey et ses amis*
Montrer que dans un groupe de 6 personnes il y en a toujours 3 qui ne se connaissent pas du tout ou qui se connaissent toutes entre elles.