PREUVES SANS MOTS

Hasna BENSADEK, Robin MAZE, Médéric NIOT
Avec le regard bienveillant de Cécile Armana

Projet de Licence 3 Mathématiques
Université de Franche-Comté

UNIVERSITÉ DE FRANCHE-COMTÉ

2024

Table des matières

I Positionnement du sujet **4**

1 Définitions **5**
1.1 Qu'est-ce qu'un mot ? . . . 5
1.2 Qu'est ce qu'une preuve ? . . . 5
1.3 Qu'est ce qu'une preuve sans mots ? . . . 5

2 Point de vue épistémologique **7**
2.1 Épistémologie culturelle . . . 7
2.2 Épistémologie formaliste . . . 7
2.3 Épistémologie quasi-naturaliste . . . 7
2.4 Épistémologie réaliste logique . . . 8
2.5 Épistémologie éducative . . . 8

II Preuves par illustration **9**

3 Analyse de preuves par illustration **10**
3.1 Un carré dans un carré . . . 10
3.2 Le théorème de Pythagore . . . 11
3.3 Complété d'un carré . . . 12
3.4 Inégalité des carrés * . . . 13
3.5 Somme des cubes . . . 14
3.6 Cardinal de l'ensemble des parties * . . . 15
3.7 Évaluation géométrique d'une limite . . . 16
3.8 Somme des termes d'une suite géométrique particulière . . . 17
3.9 Nombres carrés . . . 18
3.10 Nombres triangulaires * . . . 19
3.11 Bilan . . . 19

4 Limites des illustrations **20**
4.1 Inégalité arithmético-géométrique . . . 20
4.2 Les polynômes caractéristiques des matrices AB et BA sont égaux . . . 21
4.3 Paradoxe du carré manquant . . . 22
4.4 La quadrisection de l'hypercube . . . 22
4.5 Conclusion . . . 23

III Preuves formelles **24**

5 Arbres de preuves **25**
5.1 Pré-requis . . . 25
5.1.1 Théorie des langages . . . 25
5.1.2 Règles d'inférence . . . 26
5.1.3 Axiomes . . . 27
5.2 Arbre de preuve de la non-contradiction . . . 29
5.3 Arbre de preuve de l'involution de la disjonction . . . 29
5.4 Arbre de preuve de "la symétrie de l'égalité" . . . 30
5.5 Arbre de preuve de "2 est un entier naturel" . . . 30
5.6 Arbre de preuve de "l'absence de contre-exemple" . . . 31
5.7 Conclusion . . . 31

6 L'informatique et le binaire **32**
6.1 Pré-requis . . . 32
6.1.1 Codage binaire . . . 32
6.1.2 ASCII . . . 32
6.2 Application . . . 32
6.3 Intérêt mathématique . . . 33
6.3.1 Assistants de preuves . . . 33
6.3.2 Codage de Gödel . . . 34
6.4 Application aux preuves par illustration . . . 34
6.5 Limites . . . 34

IV Conclusion **35**

Annexes **38**

A Sémantique des formules propositionnelles **38**
A.1 Symboles de séquent . . . 38
A.2 Connecteurs logiques . . . 38
A.3 Règles d'inférence . . . 38
A.3.1 Règles générales . . . 38
A.3.2 Antilogie . . . 39
A.3.3 Négation . . . 39
A.3.4 Conjonction . . . 39
A.3.5 Disjonction . . . 39
A.3.6 Implication . . . 39
A.3.7 Équivalence . . . 40
A.3.8 Quantificateur universel . . . 40
A.3.9 Quantificateur existentiel . . . 40
A.4 Axiomes de la logique . . . 40
A.5 Axiomes de Peano . . . 41
A.6 Modèle . . . 41
A.7 Représentation . . . 41

B Grammaires non-contextuelles **42**
B.1 Définitions . . . 42
B.1.1 Grammaire non-contextuelle . . . 42
B.1.2 Dérivée directe . . . 42
B.1.3 Dérivée multiple . . . 42
B.1.4 Langage reconnu . . . 42
B.1.5 Exemples de grammaires . . . 43
B.2 Application . . . 43
B.2.1 Lien potentiel avec les preuves sans mots . . . 43
B.2.2 Limites . . . 43

C Un système d'élaboration de preuves constructivistes **44**
C.1 Définitions . . . 44
C.1.1 Système grammatical de preuves constructives (SGPC) . . . 44
C.1.2 Facteur . . . 44
C.1.3 Remplacement . . . 44
C.1.4 Preuve . . . 45
C.2 Exemple de preuve . . . 45
C.3 Limites . . . 45

D Table de caractères ASCII **46**

Bibliographie **46**

Introduction

L'objectif de ce mémoire est d'étudier et d'analyser la notion de preuves sans mots qui contraste souvent avec les démonstrations dites classiques correspondantes.

La compréhension du sujet "Preuves sans mots" par les auteurs ont poussé ce document à explorer l'universalité du langage mathématique, et à étendre le formalisme des définitions et des propositions, aux démonstrations, souvent dépendantes d'un langage. Nous aborderons dans un premier le temps le sujet d'un point de vue philosophique et épistémologique, avant de proposer des preuves par illustration, et une discussion sur la pertinence de celles-ci en fonction de différents points de vue épistémologiques.

Nous poursuivrons ensuite par proposer des systèmes de construction de preuves plus formelles, en abordant une autre vision ce que peut être un mot ou un langage. On découvrira que l'on peut aussi démontrer des assertions mathématiques de façon formelle et rigoureuse, sans user de mots.

Ce document se veut accessible et compréhensible du plus grand nombre, et ne nécessite pas de connaissances mathématiques avancées préalables à sa lecture. Bien que le sujet tend à se rapprocher d'autres domaines plus avancés tels que l'implémentation informatique ou les preuves axiomatiques, les connaissances nécessaires à la compréhension de ces passages seront explicitées en amont.

Certaines des démonstrations présentées dans ce document ont été pensées par les auteurs. Elles seront marquées d'un signe * .

Première partie

Positionnement du sujet

Chapitre 1

Définitions

1.1 Qu'est-ce qu'un mot ?

On peut ici adopter deux points de vue principaux : celui de la sémantique et celui de la théorie des langages.

Du point de vue de la sémantique, un mot peut être défini de la manière "usuelle", soit comme une unité de langage propre à chaque langue et à chaque culture. Il peut aussi bien être écrit que parlé. Cette définition nécessite toute la subtilité d'un cerveau humain pour être intelligible.

Du point de vue de l'informatique et de la théorie des langages, un mot peut être défini comme une succession de caractères (souvent appelés "symboles"), traités d'un seul bloc.

Pour éviter toute ambiguïté, nous appellerons un mot au sens sémantique, un **"mot informel"**, et un mot au sens de la théorie des langages, un **"mot formel"**.

Par exemple la succession de symboles $\sqrt{2}$ n'est pas un mot informel, mais il s'agit bien d'un mot formel dès que l'on considère le symbole du radical et le chiffre 2 comme des éléments constitutifs de l'alphabet sur lequel est construit notre langage. Nous définirons "alphabet" et "langage" plus tard dans ce mémoire (5.1.1).

Cette distinction désormais effectuée, il est donc évident que la famille des preuves sans mots est divisée en au moins deux catégories, et il peut sembler plus intuitif pour des personnes non initiées aux mathématiques formelles de conduire une preuve sans utiliser de mots informels.

1.2 Qu'est ce qu'une preuve ?

Nous passerons outre les définitions juridique et législative d'une preuve ici. Nous considérerons qu'une preuve est un synonyme de "démonstration mathématique". À ce titre, elle peut être vue comme un raisonnement qui permet d'établir la véracité d'une proposition/assertion donnée, ou d'une hypothèse/conjecture que l'on cherche à vérifier.

1.3 Qu'est ce qu'une preuve sans mots ?

Au vu des considérations précédentes, nous appellerons dans ce mémoire **preuve sans mots**, tout procédé, dessin, formule, animation... permettant d'établir la véracité d'une ou plusieurs assertion(s) mathématique(s) sans user de mots.

Par rapport à une preuve "classique", une différence peut être l'absence de hiérarchie temporelle ; là où les preuves classiques admettent toujours un point de départ et un point d'arrivée (hypothèses, déductions, conclusion), les preuves sans mots, peuvent être constituées d'un seul bloc sans sens de lecture particulier (principalement pour les preuves par illustrations). Ainsi, pour certaines de ces preuves, les hypothèses, les procédés utilisés, et généralement le résultat nous sont exposés au même instant. Le lecteur doit donc fournir l'effort de saisir le déroulement de la démarche proposée. Mais nous verrons que cela n'est pas toujours le cas, puisque certaines preuves pourront être munies d'un sens de lecture et/ou d'une chronologie.

L'existence, ou du moins l'utilité des preuves sans mots est controversée. En effet elles ont des avantages certains : pour ce qui est des preuves par illustration, il n'est pas nécessaire d'expliciter des notions mathématiques complexes, ou d'imposer l'exigence intellectuelle que requiert la compréhension d'une démonstration "rigoureuse". Mais il est tout aussi évident qu'elles ont également de réels inconvénients. Il est plus complexe de suivre une démonstration qui n'est pas "déroulée" et explicitée d'un bout à l'autre.

Aussi, les preuves sans mots plus formelles, comme nous le verrons, permettent d'établir de façon plus certaine la véracité d'une assertion dans un système axiomatique donné. C'est un avantage certain, mais qui se couple avec l'inconvénient de la difficulté de leur lecture.

Chapitre 2

Point de vue épistémologique

Ce chapitre a été inspiré par les réflexions d'Olivier FOUQUET sur le sujet (voir la référence (2).)

L'épistémologie, au sens large du terme, est l'étude de la connaissance scientifique. Une épistémologie, dans un sens plus étroit, est un courant de pensée définissant l'ensemble des opinions d'un scientifique sur l'ensemble des sujets pouvant être philosophiquement traités, et des arguments qu'il utilise pour démontrer son point de vue ou convaincre ses pairs.

Il existe plusieurs épistémologies mathématiques portant des principes divergents. Ainsi, selon chacune d'entre elles, la définition de ce qu'est une *démonstration mathématique* diffère également. Voici une liste non-exhaustives de positions épistémologiques, que nous utiliserons pour analyser des preuves :

2.1 Épistémologie culturelle

Principe : Épistémologie selon laquelle les mathématiques sont influencées par la culture.

Définition de "démonstration" : Explication logique et structurée d'une proposition mathématique, reconnue comme valide au sein d'une communauté culturelle spécifique.

Lien avec le sujet : Du point de vue de cette épistémologie, la notion même de preuve est très variable puisqu'elle dépend de la culture, de la région géographique et de la temporalité. Toutes les preuves sans mots que nous présenterons dans ce document seront donc considérées comme tel par certaines cultures, mais pas par d'autres.

2.2 Épistémologie formaliste

Principe : Épistémologie selon laquelle faire des mathématiques est avant tout porter essentiellement son attention sur le formalisme et la rigueur des propositions et preuves associées. Les mathématiques peuvent être réduites à une manipulation de symboles selon des règles formelles.

Définition de "démonstration" : Séquence finie de symboles, dont les manipulations sont basées sur des règles formelles, ou à partir d'axiomes (eux aussi exprimés sous forme symbolique), visant à établir la véracité d'une ou plusieurs proposition(s) mathématique(s).

Lien avec le sujet : Du point de vue de cette épistémologie, il est inconcevable de conduire une preuve sans mots formels. En effet, sans mots formels, il est impossible de construire une séquence finie de symboles. En revanche il peut être envisageable de construire une preuve sans utiliser de mots informels, par exemple avec le codage de Gödel, les arbres de preuves... De plus, toute preuve formaliste peut être implémentée informatiquement.

2.3 Épistémologie quasi-naturaliste

Principe : Épistémologie selon laquelle les propriétés mathématiques découlent de l'observation approfondie du monde physique exprimées grâce aux facultés cognitives humaines.

Définition de "démonstration" : Raisonnement rendant compte des relations logiques entre les entités mathématiques, en les reliant de manière cohérente aux aspects observables ou déductibles du monde physique.

Lien avec le sujet : Selon ce point de vue, le concept de preuve sans mots est cohérent avec la conception des mathématiques. En effet, elles permettent de relier directement un concept mathématique abstrait avec un support physique ou visuel. Contrairement à la formaliste, cette épistémologie s'autorise la construction de preuves sans mots formels ; un dessin peut justifier d'une assertion mathématique. D'un point de vue plus extrême, les supports physiques/visuels auxquels sont reliées les mathématiques sont des approximations imparfaites dont l'image perceptible n'est qu'une illusion de la réalité. En effet, par exemple, un cube dans le monde physique, ne correspond jamais exactement à sa définition mathématique, puisqu'il n'est constitué discontinument que d'une quantité finie d'atomes.

2.4 Épistémologie réaliste logique

Principe : Épistémologie selon laquelle les propositions et objets mathématiques existent indépendamment de l'esprit humain, soutenant ainsi une notion de vérité absolue des mathématiques et le rôle du mathématicien est de les découvrir. C'est un courant de pensée proche du platonisme, qui soutient l'existence d'un monde des idées.

Définition de "démonstration" : Processus logique visant à établir la vérité d'une proposition mathématique en justifiant la cohérence objective et absolue de ses relations avec les entités mathématiques déjà existantes.

Lien avec le sujet : Ce point de vue considère les preuves sans mots comme équivalentes à tout autre type de preuves. En effet, que l'on considère que les preuves sont des entités du monde mathématique, auquel cas on pourrait les visualiser comme des chemins permettant d'accéder à un objet mathématique ; ou que l'on pense les preuves comme un procédé humain permettant de découvrir et de décrire le monde mathématique. Il est évident que le chemin ou procédé n'a que peu d'importance en comparaison avec le résultat mathématique qu'ils mettent en avant.

2.5 Épistémologie éducative

Principe : Épistémologie selon laquelle les mathématiques ne sont qu'une matière scolaire ayant pour but principal d'être transmises.

Définition de "démonstration" : Procédé pédagogique permettant d'expliciter un résultat mathématique adapté au niveau du public visé.

Lien avec le sujet : Selon cette épistémologie, l'efficacité pédagogique d'une preuve sans mots dépend à la fois de son contenu et du public visé. En effet, un résultat mathématique "simple" est destiné à priori à un public peu averti, et peut donc être pertinent à démontrer par une preuve sans mots. Au contraire un résultat "complexe" est plutôt destiné à un public averti voire expert et il semble donc peu pertinent de le présenter par ce type de preuve.

Deuxième partie

Preuves par illustration

Chapitre 3

Analyse de preuves par illustration

Rappel : Certaines des démonstrations présentées dans cette partie ont été pensées par les auteurs. Elles seront marquées d'un signe * . Les autres illustrations sont de nouvelles versions des illustrations proposées par le livre "*Preuves sans mots*" de Roger B. NELSEN.

3.1 Un carré dans un carré

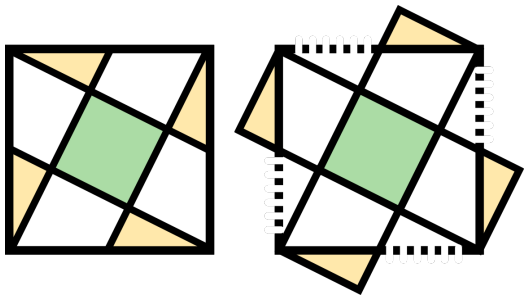


Illustration 3.1 –

Énoncé : Dans un carré quelconque, si l'on joint chaque sommet au milieu de l'un de ces côtés opposés (en respectant la même logique d'un sommet à l'autre), alors l'aire du carré ainsi formé vaut un cinquième de l'aire du carré initial.

Explication : La figure de gauche est une simple représentation des consignes de l'énoncé avec en vert, le carré formé. En redisposant les triangles jaunes, comme indiqué sur la figure de droite, on peut construire quatre nouveaux carrés **d'aire identique** au vert. Ainsi, on voit que l'aire du carré initial est égal à **cinq fois** celle du carré vert.

Commentaires : Le principe de cette illustration consiste en un découpage puis redisposition des pièces. On note d'ailleurs que la redisposition fabrique une figure qui n'est pas contenue dans la première. Cette preuve illustre la possibilité que l'on puisse construire des objets relativement complexes en partant d'une base simple.
Par exemple, Timmy souhaite construire une cabane à oiseaux de $2000\,cm^2$, mais il ne dispose que de planches de $1\,m$ de longueur dont il connaît le milieu. Pour couper ses planches à la bonne longueur pour construire sa cabane, il peut appliquer la méthode énoncée ci-dessus.
Cette preuve met en avant l'aspect le plus intuitif des preuves sans mots tel que l'on peut se les représenter. Elle use d'une succession de constructions géométriques simples pour parvenir à un résultat non trivial. De plus, on peut souligner que cette preuve n'use d'aucun mot formel.

En quoi est-ce ou non une preuve sans mots ? Il ne fait pas sens pour les formalistes de parler de preuve sans mots tandis que cette figure d'"un carré dans un carré" pourrait être fortement considérée par les épistémologues éducatifs puisqu'elle se trouve être relativement intelligible par un humain et ce peut importe son niveau de connaissances mathématiques. N'ayant recours à aucun autre théorème et n'exposant aucun symbole ou formule mathématique en plus d'user de figures géométriques relativement communes et en petit nombre, elle ne relève quasiment que de l'entendement. C'est ainsi un outil assez puissant pour cette épistémologie.

3.2 Le théorème de Pythagore

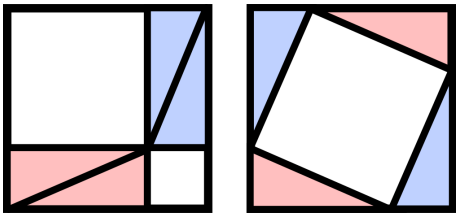
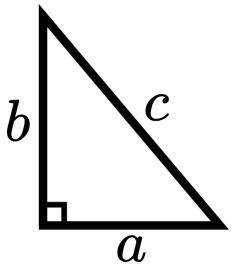


Illustration 3.2 –

Énoncé : Dans un triangle rectangle, le carré de la longueur de l'hypoténuse (côté le plus long) est égal à la somme des carrés des longueurs des deux autres côtés : $a^2 + b^2 = c^2$.



Explication : Les deux figures présentées dans l'Illustration 3.2 sont de même dimension, les quatre triangles mis en jeu sont identiques, et sont les mêmes de chaque côté. Ainsi on constate que le carré blanc de la figure de droite et les deux carrés blancs de celle de gauche sont **d'aire identique**. De plus, le carré de la figure de droite a pour côté **l'hypoténuse** de nos triangles. De l'autre côté, on remarque que les deux carrés blancs ont pour côtés, respectivement le **grand** et le **petit** côté de l'angle droit des triangles.

Commentaires : Cette preuve se base sur la représentation usuelle d'un espace à deux dimensions afin de démontrer l'égalité entre deux nombres, à première vue distincts.
L'effort est ici porté sur la simplicité des notions qui composent la preuve, cette dernière est construite de manière à être le plus accessible possible. Elle est vérifiable simplement et rapidement sans outils (intellectuels ou physiques) complexe par pratiquement n'importe qui.
Cependant, plusieurs discussions ressortent de l'analyse de cette preuve.
Premièrement, qu'est-ce que le théorème de Pythagore ? Nous savons qu'il en existe énoncés sous différentes formes. La plus célèbre est sans doute celle donnée dans l'énoncé ci-dessus, mais la réciproque est-elle donnée par le théorème ? Si oui, alors l'illustration ne semble pas montrer une équivalence, mais plutôt une seule implication. Et quid du théorème de Pythagore rédigé sous ses autres formes ?
— Dans un espace euclidien $(E, +, \cdot, \langle ., . \rangle)$, $\forall x, y \in E, x \perp y \iff \|x\|^2 + \|y\|^2 = \|x + y\|^2$
— Soient A, B, C trois points d'un espace affine euclidien, $(AB) \perp (AC) \iff AB^2 + AC^2 = BC^2$
Deuxièmement, là où la preuve précédente était un résultat sur un cas particulier, qui se suffit donc à lui-même, le théorème de Pythagore est un résultat beaucoup plus général, car il quantifie universellement sur des objets mathématiques. Ainsi on peut se demander si l'illustration tient compte de tous les cas : il est justement difficile avec cette illustration d'appréhender les cas pathologiques, comme des triangles plats ou réduits à un point.

En quoi est-ce ou non une preuve sans mots ? De la même manière que pour la démonstration sans mots d"un carré dans un carré", celle ci conviendrait parfaitement aux convictions de l'épistémologie éducative, mais aussi au quasi-naturaliste puisque, comme l'illustre bien notre exemple, on peut la déduire d'une représentation physique/matérielle/tangible. De plus, d'un point de vue culturel, ce qui précède est absolument considéré comme une preuve sans mots pour certaines ethnies, notamment sur le continent asiatique. En effet les mathématiques chinoises furent les précurseurs des preuves sans mots ; on retrouve chez Zhoubi Suanjing, l'un des plus anciens ouvrages mathématiques, une preuve sans mots du théorème de Pythagore usant aussi de figures géométriques planes pour l'expliciter, notamment de carrés.

3.3 Complété d'un carré

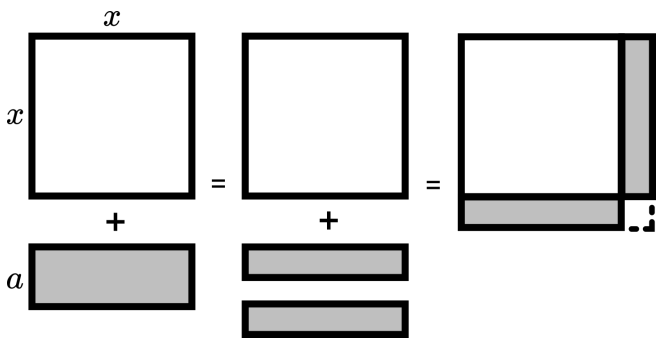


Illustration 3.3 –

Énoncé : $\forall (a,x) \in \mathbb{R}^2, x^2 + ax = \left(x + \frac{a}{2}\right)^2 - \left(\frac{a}{2}\right)^2$

Explication : À gauche nous avons un carré d'aire x^2 qu'on somme à un rectangle d'aire ax. En découpant ce rectangle en deux autres, chacun d'aire $(\frac{a}{2})$, on peut les repositionner le long des côtés du carré de côté x pour obtenir un nouveau carré de côté $x+(\frac{a}{2})$ à un carré de côté $(\frac{a}{2})$ près. Ainsi, l'aire de ce nouveau carré, dont on soustrait l'aire du petit carré manquant, est égale à la somme de l'aire du carré et celle du rectangle initial, d'où la formule énoncée.

Commentaires : Il s'agit de la première preuve qui met en évidence une certaine chronologie. Ici la preuve semble se lire uniquement de gauche à droite.
Contrairement aux preuves précédentes, on a ici un lien clair entre une preuve géométrique (dessin) et un résultat qui relève du calcul algébrique. Il s'agit à nouveau d'un découpage-redisposition.
Ce lien peut être lu dans les deux sens. On peut voir la géométrie comme un outil utilisé pour représenter les quantités algébriques mises en jeu, ou l'on peut considérer que cette preuve est avant tout une application géométrique d'un résultat qui semble n'être qu'algébrique, mettant ainsi en avant les liens qui peuvent se faire entre diverses branches des mathématiques.
Cependant, cette preuve possède une faiblesse puisqu'elle ne démontre pas tout à fait l'assertion de l'énoncé. En effet, la preuve suppose que x et a soient positifs, puisque des longueurs négatives ne semblent pas pouvoir exister. Néanmoins la formule fonctionne toujours pour des réels négatifs, voire même pour des nombres complexes, et plus généralement, elle fonctionne dans n'importe quel anneau commutatif dans lequel $2 = 1 + 1$ est inversible.
Enfin on peut se questionner sur l'utilité des lettres x et a, ainsi que des symboles $+$ dans l'illustration. Bien qu'ils d'identifier l'énoncé plus facilement, la preuve reste drastiquement identique en supprimant ces symboles. Cependant, par souci de compréhension de ce qui est démontré (à savoir une égalité), les symboles $=$ semblent nécessaires.

En quoi est-ce ou non une preuve sans mots ? Ce complété d'un carré se basant sur le même principe que les preuves précédentes (découpage et ré-agencement de figures géométriques), elle est naturellement considérée comme une preuve sans mots par les épistémologues quasi-naturalistes et encore plus par les éducatifs. En effet, cette preuve se démarque des précédentes par la présence des symboles mathématiques en plus des variables x et a et se singularise aussi par la découpe de nos figures géométriques en trois images différentes, ce qui peut tendre à la rendre plus pédagogique que les preuves sans mots en une seule image et sans symbolisme. D'ailleurs cette découpe tend à rapprocher cette démonstration des preuves par animation.

3.4 Inégalité des carrés *

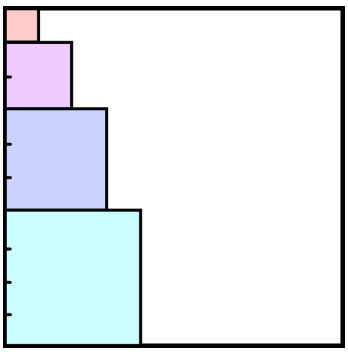


Illustration 3.4 –

Énoncé :

$$\forall n \in \mathbb{N}^*, \sum_{k=1}^{n} k^2 \leq \left(\sum_{k=1}^{n} k\right)^2$$

Explication : La figure sous-entend que le plus petit carré (en rouge) est de côté 1, et que les carrés colorés successifs sont tous de côté de longueur 1 unité plus grande que le précédent, ce qui est suggéré par la graduation.
Le côté du grand carré blanc est de $1+2+\cdots+n$ ($n=4$ dans la figure), il a donc une aire de $(\sum_{k=1}^{n} k)^2$. De plus il contient des plus petits carrés de longueur 1 pour le plus petit, 2 pour le suivant en dessous, etc. Ainsi le total de leurs aires $\left(\sum_{k=1}^{n} k^2\right)$ est inférieur à celle du grand carré, car la surface cumulée des petits carrés est contenue dans la surface du grand carré.

Commentaires : Contrairement aux preuves précédentes mettant en lumière des égalité entre des objets finis, cette figure-ci se veut de prouver une inégalité mettant en jeu une variable n pouvant prendre une valeur quelconque, ce qui implique un nombre d'objets quelconque. Ainsi, contrairement aux précédentes preuves, se convaincre de la véracité de cette inégalité implique de devoir se convaincre qu'elle reste démontrée avec cette façon d'agencer des carrés pour n'importe quelle valeur de n, et pas seulement avec $n=4$ comme l'utilise la figure démonstrative.
Il s'agit aussi de la première preuve d'une assertion contenant une inégalité et mettant en lumière une comparaison.
Un aspect notable de cette preuve est qu'elle montre que l'inégalité est loin d'être optimale : en effet, on observe que la zone blanche à droite des carrés colorés est grande, et le rapport de sa surface avec la surface colorée semble tendre vers l'infini, lorsque n tend vers l'infini. Cela prouve que l'on pourrait trouver une bien meilleure inégalité, avec peut-être, un cas d'égalité vérifié dans certaines conditions, ce qui ne semble pas être le cas ici (mis-à-part pour le cas pathologique $n=1$). Peut-être qu'une majoration dépendant de n aurait été plus optimale. Par la suite, nous allons porter notre attention à d'autres preuves sans mots voulant démontrer une égalité ou inégalité pour tout entier naturel n mais dont l'illustration ne porte que sur une valeur de n donnée.

En quoi est-ce ou non une preuve sans mots ? Le fait que cette illustration puisse être ou non une preuve sans mots peut faire débat pour les épistémologues quasi-naturalistes. En effet, rappelons que pour eux, une preuve se caractérise par un raisonnement rendant compte des relations logiques entre les entités mathématiques, en les reliant de manière cohérente aux aspects observables ou déductibles du monde physique. Or, nous sommes forcés de constater que pour démontrer l'inégalité de la somme des carrés pour n'importe quel carré de coté n, cette illustration ne prouverait de manière physique et observable que le cas d'un carré de coté 4.
D'un point de vue extrême du quasi-naturaliste, il faudrait pouvoir observer la cohérence de cette illustration avec l'inégalité dessinée pour chaque valeur de n pour se convaincre que l'on peut considérer cela comme une preuve sans mots, mais c'est bien sûr impossible.
Pour les épistémologues éducatifs, cette preuve a une utilité contestable, puisque l'on sent bien que l'on n'optimise par l'inégalité. On pourrait alors surestimer l'importance pédagogique de cette assertion, alors qu'une inégalité moins grossière serait plus adaptée. De la même façon, l'assertion semble ne rien pouvoir démontrer d'autre. On aurait alors une assertion mathématique qui se suffit à elle-même, ce qui n'a pas un intérêt pédagogique évident.

3.5 Somme des cubes

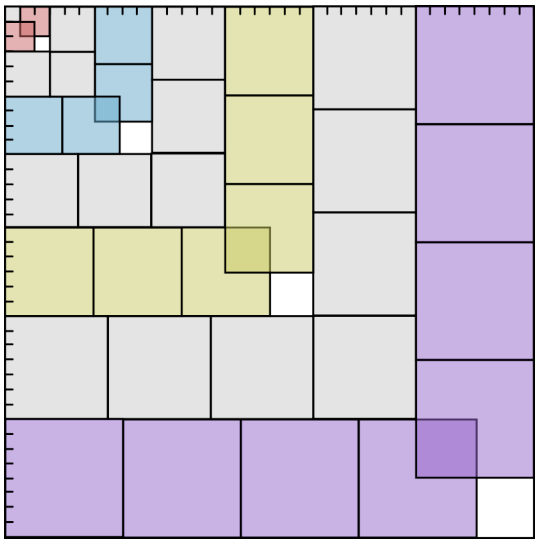


Illustration 3.5 –

Énoncé :

$$\forall n \in \mathbb{N}^*, \sum_{k=1}^{n} k^3 = \left(\sum_{k=1}^{n} k\right)^2$$

Explication : Le grand carré principal est gradué (de façon unitaire) de sorte que son côté soit de longueur égale à $1+2+3+\cdots+n$. L'aire de ce carré est donc $\left(\sum_{k=1}^{n} k\right)^2$. Par ailleurs, les carrés plus petits ont pour aires respectives 1^2, 2^2, $\cdots$, n^2. De plus, on remarque que les petits carrés sont représentés plusieurs fois : on a deux fois le carré de côté deux, trois fois celui de côté trois, etc... Ainsi, on a $1\times1^2+2\times2^2+\cdots+n\times n^2$ ce qui nous donne $\sum_{k=1}^{n} k^3$. Or, les parties blanches étant "compensées" par celles qui sont doublement recouvertes (en couleur plus foncée), on a bien l'égalité.

Commentaires : De la même manière que la preuve précédente, on doit ici se convaincre que cette manière d'agencer les carrés démontre toujours l'inégalité énoncée, peu importe la valeur de n, et pas seulement pour $n = 7$ comme l'explicite la figure. Cela peut faire débat concernant la rigueur des preuves sans mots. En effet, pour démontrer une proposition mathématique mettant en jeu une variable n de manière plus courante, hors preuves sans mots, il peut être inconcevable de se satisfaire d'une démonstration ne justifiant la propriété que pour un seul entier naturel fixé.
Le principe de cette preuve est très semblable à la preuve précédente, puisqu'il s'agit à nouveau de superposer des carrés dans un autre grand carré. Cependant, il semble plus difficile à première vue de comprendre l'assertion démontrée : conclure nécessite une étude plus approfondie de l'illustration.
De plus, cette illustration, par rapport à la preuve précédente, est dissymétrique. En effet, sur les "lignes" composées de carrés gris, aucun carré ne se superpose à un autre, tandis que sur les "lignes" composées de carrés colorés, l'intersection entre deux carrés n'est pas toujours vide. Cela peut amener à se demander si une disjonction de cas en fonction de la parité de n n'est pas à effectuer.
Cette illustration est toutefois la première à proposer de démontrer une assertion sur des objets géométriques en trois dimensions.

En quoi est-ce ou non une preuve sans mots ? Comme pour la preuve précédente, il s'agit de voir si cette démonstration s'applique à la vie réelle ou non. La "projection" d'un espace à trois dimensions sur un carré en deux dimensions n'est pas réaliste, car nous vivons dans un monde en trois dimensions.
Cependant, l'illustration peut montrer une façon de trancher des cubes, et faire un lien direct entre les aires et les volumes, ce qui est très apprécié par les épistémologues quasi-naturalistes.

3.6 Cardinal de l'ensemble des parties *

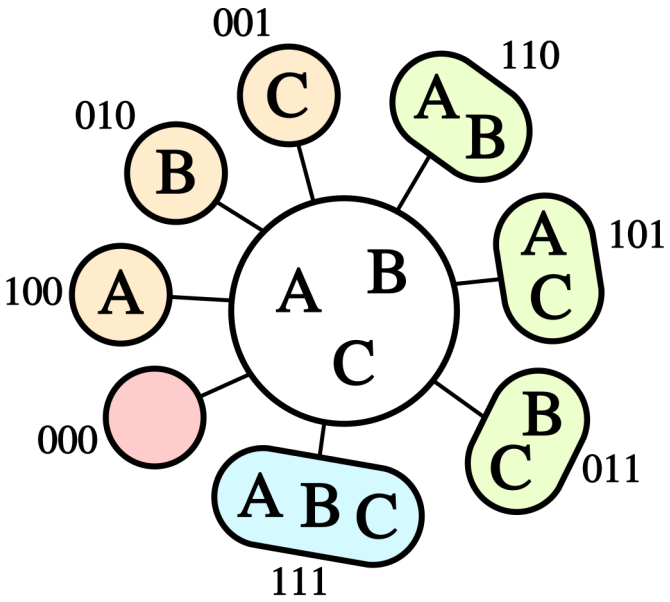


Illustration 3.6 –

Énoncé : Soit E un ensemble fini, on a $Card(\mathcal{P}(E)) = 2^{Card(E)}$.

Explication : On part de l'ensemble $E = \{A, B, C\}$ et on construit toutes les façons de sélectionner des éléments dans l'ensemble. On construit ainsi l'ensemble des parties de E.
On remarque ensuite qu'en attribuant à chaque partie une représentation en binaire en fonction de l'apparition (1) ou non (0) de chacun des ensembles A, B et C dans celle-ci, il y a le même nombre de parties de E que de nombres binaires à 3 bits. Ce passage par les nombres binaires est un codage pratique pour faire du dénombrement.
On en déduit que $\mathcal{P}(E)$ et $\{0, 1\}^3$ sont de même cardinal, et donc que $Card(\mathcal{P}(E)) = 2^3 = 8$.
Il est ensuite facile de généraliser, à partir de la suggestion de l'illustration, à un ensemble de cardinal fini quelconque, et on obtient donc l'assertion souhaitée.

Commentaires : Cette preuve sans mots se distingue des autres puisqu'elle mêle notions ensemblistes et dénombrement. De plus, on s'éloigne drastiquement de celles se reposant sur des ré-agencements de figures géométriques. En effet, son enjeu est de présenter un codage de la situation de dénombrement. Cette preuve sans mots se lit d'une traite, sans décomposition de figures en plusieurs images et sans faire appel à des objets géométriques.

En quoi est-ce ou non une preuve sans mots ? Le passage de $n = 3$ à un n quelconque est sous-entendu, ce qui pose problème en épistémologie formaliste : bien que ces derniers, comme les épistémologues éducatifs, apprécient le passage par des notions ou domaines paraissant éloignées du sujet de base (ici le codage par le binaire).
En épistémologie réaliste logique, le lien entre le cardinal des ensembles et les nombres binaires est très intéressant puisque cela fournit un guide pour explorer de nouvelles idées en théorie des ensembles et pour prouver de nouvelles assertions. C'est ce genre de preuve qui est attendu dans cette épistémologie, puisque cela permet aux mathématiciens de mieux explorer le "monde des idées", dont l'existence est prônée par celle-ci.

3.7 Évaluation géométrique d'une limite

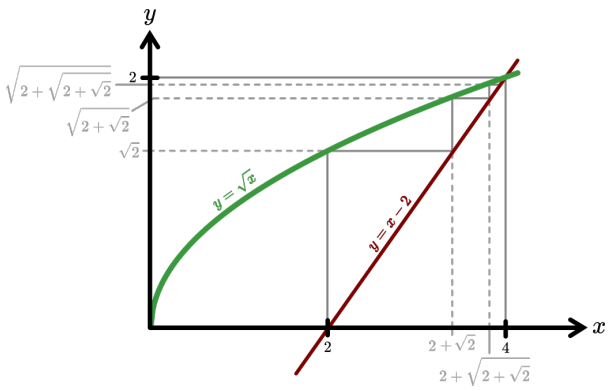


Illustration 3.7 –

Énoncé :

$$\sqrt{2+\sqrt{2+\sqrt{2+\sqrt{\cdots}}}}=2$$

Explication : On utilise ici une méthode couramment utilisée pour le calcul de point fixe. On trace une droite d'équation $y = x - 2$, de façon à ce que lorsque l'on compose avec la fonction $x \mapsto 2 + x$, on se ramène à la **fonction identité**, comme pour la recherche de point fixe. Puis l'on part de l'axe des abscisses à $x = 2$, qui est le premier terme que l'on compose dans la formule. On le projette sur la courbe de la fonction *racine carrée*, afin d'obtenir une ordonnée, que l'on projette sur la droite tracée précédemment. On reporte le point sur l'axe des abscisses, et l'on réitère le processus une infinité de fois. De cette façon, on se rapproche d'un "point limite", qui serait l'équivalent d'un **point fixe attracteur** si l'on avait décalé la courbe de 2 crans vers la gauche.
L'idée est de cette preuve est donc de déterminer la limite suivante :

$$\lim_{n\to\infty} f^n(2)$$

où $f : x \mapsto \sqrt{2+x}$ et l'exposant n signifie la composition n-ième.

Une reformulation consiste à faire intervenir une suite récurrente :

$$u_0 = 2 \quad \text{et} \quad \forall n \in \mathbb{N}, u_{n+1} = \sqrt{2+u_n}.$$

L'objectif de cette preuve est donc de calculer :

$$\lim_{x\to\infty} u_n.$$

Commentaires : Cette preuve, contrairement aux précédentes, est du domaine de l'analyse. Il s'agit de la première preuve mettant en évidence une limite, avec des calculs très implicites. C'est une preuve qui demande une maîtrise de certaines notions d'analyse (limites, points fixes, composition de fonctions, courbes représentatives...), là où les preuves précédentes étaient facilement vulgarisables à des collégiens.
Ensuite en analysant la preuve, on se rend compte de plusieurs choses.
D'abord, la raison pour laquelle la droite d'équation $y = x - 2$ est introduite n'est pas évidente.
De plus, la convergence vers 2 ne saute pas aux yeux, puisque la partie droite du graphe de la fonction est manquante, ce qui laisse penser que seules les informations "qui nous arrangent" ont été gardées.
Enfin, que se passe-t-il si l'on évalue la fonction en autre chose que 2 pour l'évaluation ? À nouveau, ce choix donne l'impression qu'il s'agit d'un particulier, alors qu'en réalité, la preuve aurait tout aussi bien fonctionné si l'on avait choisi un autre réel positif, puisque 2 est un point fixe attracteur de f.

En quoi est-ce ou non une preuve sans mots ? Cette démonstration ne fait appel à aucun mot informel, et permet d'obtenir une excellente approximation d'un résultat d'analyse, ainsi qu'une idée d'une méthode à mettre en place pour réaliser la démonstration de façon plus rigoureuse. Il s'agit cependant de la première preuve pour laquelle des mots formels semblent nécessaires à sa bonne compréhension.
Là où les démonstrations précédentes se suffisaient à elles-mêmes, pour l'épistémologie formaliste, cette illustration ne constitue pas une preuve, mais fournit une bonne inspiration à la conception d'une preuve rigoureuse de l'assertion.

3.8 Somme des termes d'une suite géométrique particulière

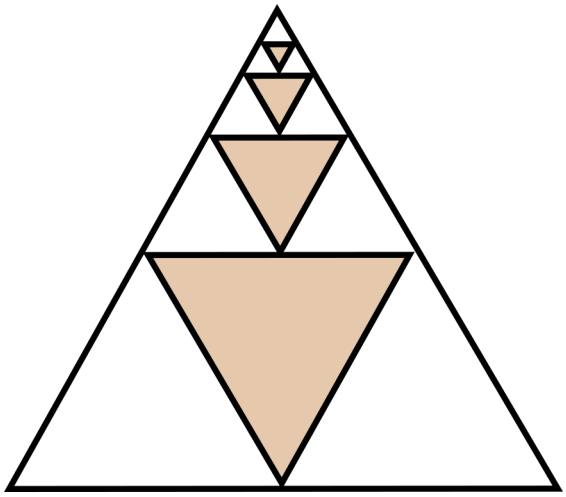


Illustration 3.8 –

Énoncé :

$$\sum_{k=1}^{+\infty} \frac{1}{4^k} = \frac{1}{3}$$

Explication : On procède à une construction par récurrence. On part d'un triangle blanc dont le côté est supposé de longueur 1 et on en colorie le triangle formé par les trois milieux de ses côtés. On sépare alors le triangle en trois parties égales en aire. On répète ainsi le processus avec le triangle blanc du dessus, dont l'aire est égale au quart ($\frac{1}{4^1}$) du triangle de base, en colorant cette fois-ci le triangle formé par les trois milieux des côtés du triangle supérieur, soit un seizième ($\frac{1}{4^2}$) du triangle de base. Et ainsi de suite... En procédant tel quel jusqu'à l'infini, l'aire colorée en orange vaut un tiers de l'aire totale du grand triangle.

La figure suggère de répéter une infinité de fois ce processus. On observe alors qu'un tiers de la surface du triangle de base est colorée. En effet, en découpant le triangle en son milieu vertical (c'est-à-dire en séparant le triangle en deux parties de hauteur égale sur l'axe vertical), un tiers de la partie inférieure est colorée, tandis que la partie supérieure n'est rien d'autre qu'une réduction du triangle précédent (le même triangle, avec la même coloration, mais à une échelle plus petite). On a alors la définition par récurrence d'une suite géométrique de raison $\frac{1}{4}$, dont la somme des n premiers termes (à partir du rang $k = 1$) vaut :

$$\frac{1-\left(\frac{1}{4}\right)^n}{1-\frac{1}{4}} - \left(\frac{1}{4}\right)^0 = \frac{1-\left(\frac{1}{4}\right)^n}{\frac{3}{4}} - 1 = \frac{4-4\times\left(\frac{1}{4}\right)^n}{3} - 1 = \frac{1}{3} - \frac{1}{3\times 4^{n-1}} \underset{n\to+\infty}{\longrightarrow} \frac{1}{3}\,.$$

Commentaires : L'utilité de l'illustration pour prouver l'assertion est discutable. En effet, il existe deux méthodes simples pour parvenir au résultat :

- Utiliser la formule de la somme des termes d'une suite géométrique pour aboutir comme ci-dessus.
- Si l'on ne connaît pas cette formule, et si l'on sait que la série converge, il suffit de multiplier la somme de la série par $\frac{1}{4}$, de sortir ensuite le premier terme, puis de résoudre une équation.

Les preuves faisant appel à l'infini sont de plus difficiles à retranscrire sur une illustration, qui doit se contenter d'un cas fini, comme c'était le cas pour la preuve précédente. Mais il reste néanmoins facile de visualiser la poursuite du processus sur l'illustration, et ainsi de se convaincre du résultat.

En quoi est-ce ou non une preuve sans mots ? Selon les épistémologues éducatifs, cette preuve, comme précédemment, est un réel outil mathématique. De plus, elle l'est aussi pour les épistémologues culturels car cette image n'utilise que des triangles, une figure universelle, pour démonter l'égalité concernant cette série. En revanche, elle n'utilise pas le symbolisme qui pourrait la rendre acceptable par les épistémologues formalistes. Par ailleurs rappelons que l'épistémologie réaliste logique porte l'idée selon laquelle les propositions et objets mathématiques existent indépendamment de l'esprit humain. Ainsi selon eux on a bien dans notre cas une preuve sans mots puisque, pour démontrer une égalité, on n'use que de simples triangles qui existent indépendamment de l'homme, en tant que figures géométriques simples.

3.9 Nombres carrés

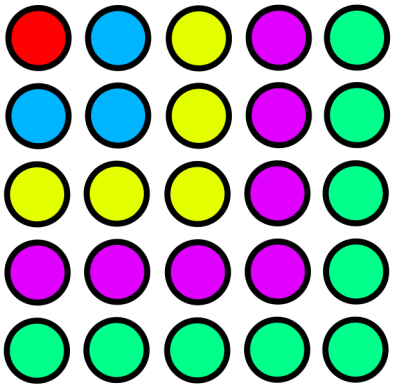


Illustration 3.9 –

Énoncé :

$$\forall n \in \mathbb{N}^*, \sum_{k=1}^{n}(2k-1) = n^2$$

Explication : Afin de construire la figure, on choisit à chaque ligne d'indice k une couleur, et on place un nombre k de boules de cette couleur (en partant de la gauche), et à chaque colonne de même indice k un nombre k de boules de cette même couleur (en partant du haut). On a donc placé $2k$ boules. En faisant cela, la dernière boule de chaque ligne et la dernière boule de chaque colonne se superposent : on en retire alors une. On a donc $2k-1$ boules de même couleur.
On procédant ainsi pour chaque ligne et pour chaque colonne, on remplit un carré dont la longueur des côtés correspond au nombre de lignes (ou au nombre de colonnes). On a alors prouvé l'assertion souhaitée, avec dans cette illustration, $n = 5$.

Commentaires : Cette preuve est convaincante pour le cas particulier $n = 5$ qu'elle présente, et il est assez intuitif de généraliser. Cependant on pourrait se demander si mettre en évidence la superposition des boules n'aurait pas clarifié la décrémentation de chaque terme de la somme. Mais ce n'est pas forcément le cas, car on pourrait aussi croire au contraire qu'il faut compter certains termes deux fois. Les deux choix sont donc acceptables.
Cette démonstration est à nouveau une preuve par découpage-redisposition, mais cette fois avec des objets discrets (boules à prendre pour des éléments unitaires), plutôt qu'avec des surfaces.

En quoi est-ce ou non une preuve sans mots ? La démonstration de cette égalité repose sur le comptage de boules de couleur. Les boules étant des figures géométriques simples mais aussi existant indépendamment des mathématiciens, cette image est véritablement une preuve sans mots du point de vue culturel et réaliste logique mais aussi éducatif.

3.10 Nombres triangulaires *

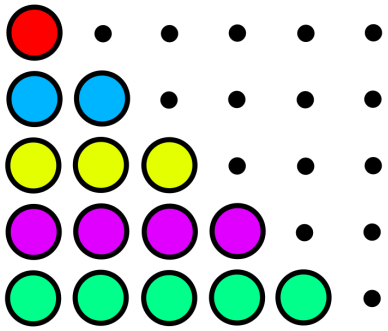


Illustration 3.10 –

Énoncé :

$$\forall n \in \mathbb{N}^*, \sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

Explication : On construit un triangle isocèle rectangle de côté 5 en posant à chaque ligne une boule de plus qu'à la ligne précédente. Le triangle forme bien la moitié d'un rectangle de côtés n et $n+1$, ce qui prouve l'égalité. Dans cette illustration, seul le cas particulier $n = 5$ est traité.

Commentaires : Encore une fois, cette illustration ne traite que le cas particulier n=5 car traiter l'infini sur un support fini à 2 dimensions reste difficile à envisager. Ainsi, il nous revient le travail personnel de se convaincre que l'on peut généraliser le principe de cette illustration pour tout entier naturel.
Par rapport à la preuve précédente, il y a une ambiguïté sur le caractère rectangulaire de la disposition des boules et des points noirs : ces derniers étant présents pour mettre en évidence le rectangle et ses dimensions. On peut se questionner sur leur utilité dans l'illustration.

En quoi est-ce ou non une preuve sans mots ? Pour les mêmes raisons que celle pour les nombres carré, cette image est véritablement une preuve sans mots du point de vue culturel et réaliste logique mais aussi éducatif.

3.11 Bilan

Ainsi nous avons mis en lumière plusieurs types de preuves par illustration provenant de divers domaines des mathématiques ; entre autres le calcul algébrique, la géométrie, le dénombrement et l'analyse. Nous avons également pu décrire les mécanismes de chacune d'entre elles et ainsi remarquer la redondance de certains procédés comme :

— Le découpage-ré-assemblage, plutôt pour démontrer une proposition géométrique. De plus, certaines de ces preuves sans mots géométriques ne reposent que sur une seule figure géométrique, d'autres sur plusieurs, parfois reliées par des symboles mathématiques élémentaires tels que l'addition et le symbole d'égalité.

— Expliciter la preuve pour une valeur particulière d'un entier naturel n pour nous laisser le soin de se convaincre mentalement de la véracité de la proposition pour toute valeur de n. Ce principe se retrouve généralement pour les propositions plutôt arithmétiques.

— L'itération successive sur schéma, plutôt pour les propositions fonctionnelles (cf Évaluation géométrique d'une limite).

Finalement nous avons pu discuter du caractère démonstratif ou non de chacune d'entre elles aux yeux des différentes épistémologies mathématiques. Bien que ces divers procédés visent à prouver des propositions mathématiques, plusieurs questions persistent :

— Est-ce que toutes les preuves sans mots par illustration conviennent à l'épistémologie éducative ? Les preuves sans mots par illustration sont-elles forcément de puissants outils pédagogiques ?

— Quelles sont les limites de la démonstration par illustration ? Peut-on tout démonter par illustration ?

Ce sont des questions auxquelles nous allons tenter de répondre dans le chapitre suivant.

Chapitre 4

Limites des illustrations

Dans ce chapitre, nous allons étudier quelques preuves par illustration ayant un aspect bien moins démonstratif que les preuves étudiées jusqu'à maintenant, ou pour lesquelles de nombreuses objections peuvent être formulés. L'objectif de cette partie est de mieux cerner ce qui peut ou ne peut pas être accepté comme une preuve sans mots.

4.1 Inégalité arithmético-géométrique

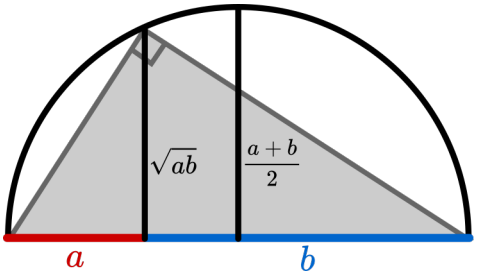


Illustration 4.1 –

Énoncé :

$$\forall a, b \in \mathbb{R}_+, \sqrt{ab} \leq \frac{a+b}{2}$$

Explication : L'objectif de cette preuve est de montrer une inégalité entre la moyenne arithmétique et la moyenne géométrique à travers une construction géométrique.
On représente ces grandeurs par des longueurs de segments. La première correspond au rayon d'un demi-cercle de diamètre $a+b$ (donc de rayon $\frac{a+b}{2}$) , tandis que la deuxième est représentée par la hauteur d'un triangle inscrit dans celui-ci. Il faut alors remarquer que le plus petit segment vertical découpe deux triangles rectangles que nous nommerons respectivement petit triangle et triangle moyen (le nom "grand triangle" étant réservé au triangle rectangle formé par les deux précédents).

Notons x la hauteur commune de nos deux triangles, y l'hypoténuse du petit et enfin z l'hypoténuse du moyen. Le théorème de Pythagore appliqué aux trois triangles nous donne alors les trois égalités :

$y^2 = a^2 + x^2$
$z^2 = b^2 + x^2$
$(a+b)^2 = y^2 + z^2$
ce qui nous donne : $2x^2 = y^2 + z^2 - a^2 - b^2 = (a+b)^2 - a^2 - b^2 = 2ab$.
Finalement, on obtient $x = \sqrt{ab}$. Puis on conclut à l'inégalité souhaitée avec le schéma.

Commentaires : La raison pour laquelle la hauteur est de longueur $\sqrt{ab}$ nécessite la résolution de plusieurs équations (les auteurs n'ont pas abouti à l'inégalité sans passer par les variables x, y et z), ce qui requiert des aptitudes mathématiques supplémentaires, et force à compléter, au moins mentalement, les données manquantes de l'illustration, avec notamment le théorème de Pythagore ou l'introduction de nouvelles variables. Cependant, une fois ces variables introduites, l'inégalité est immédiate, car l'enjeu est surtout de comprendre pourquoi la hauteur commune aux triangles petit et moyen est de longueur $\sqrt{ab}$.

En quoi est-ce ou non une preuve sans mots ? On pourrait remettre en question le caractère démonstratif de cette illustration puisqu'elle est loin de se suffire à elle-même et laisse implicite une partie conséquente de la méthode permettant de réaliser une véritable preuve de l'assertion avancée.
Ainsi les auteurs pensent qu'il ne s'agit plutôt que d'une preuve incomplète, laissant le lecteur dépourvu d'une grande partie de l'aide nécessaire à la mise en place d'un raisonnement exhaustif. Par ailleurs on peut souligner que dû à cela, cette illustration ne peut être considérée comme une véritable preuve pour les épistémologues éducatifs, contrairement à la majorité illustrations précédentes.

4.2 Les polynômes caractéristiques des matrices AB et BA sont égaux

$$-\lambda^n|AB-\lambda I| = \begin{vmatrix} A & AB-\lambda I \\ \lambda I & 0 \end{vmatrix} = \left|\begin{pmatrix} A & I \\ \lambda I & B \end{pmatrix}\begin{pmatrix} I & B \\ 0 & -\lambda I \end{pmatrix}\right| = \begin{vmatrix} A & I \\ \lambda I & B \end{vmatrix}(-\lambda)^n$$

$$-\lambda^n|BA-\lambda I| = \begin{vmatrix} 0 & \lambda I \\ BA-\lambda I & \lambda B \end{vmatrix} = \left|\begin{pmatrix} A & I \\ \lambda I & B \end{pmatrix}\begin{pmatrix} -I & 0 \\ A & \lambda I \end{pmatrix}\right| = \begin{vmatrix} A & I \\ \lambda I & B \end{vmatrix}(-\lambda)^n$$

Illustration 4.2 –

Énoncé :

$$\forall A, B \in \mathcal{M}_n(\mathbb{K}), \chi_{AB} = \chi_{BA}$$

Explication : Cette preuve consiste en un calcul de déterminants de matrices par blocs L'objectif est de montrer que ces deux déterminants sont égaux en aboutissant au même résultat dans chacune des deux suites d'égalités. On utilise alors la propriété multiplicative du déterminant, sa multilinéarité, et la formule du déterminant d'une matrice par blocs.

Commentaires : Cette preuve suppose de posséder des connaissances sur le calcul matriciel et sur les propriétés du déterminant. De plus des quantificateurs auraient été pertinents à la compréhension des objets manipulés. Par exemple, on aurait pu écrire en en-tête : $\forall n \in \mathbb{N}^*$, $\forall A, B \in \mathcal{M}_n(\mathbb{K})$. On aurait également pu préciser : I est la matrice identité I_n. Il en est de même pour le facteur λ qui n'apparaît pas dans l'assertion mais est introduit dans la preuve. Cependant il s'agit de la première preuve ne contenant aucune illustration. Elle peut donc plus facilement être retranscrite sur un ordinateur et s'adapte au langage informatique.
On peut noter le caractère dissymétrique de la preuve, avec l'apparition de deux facteurs λ dans le deuxième terme de la première ligne, tandis que la deuxième ligne en contient trois. On pourrait penser que par symétrie des rôles de A et de B, les deux suites d'égalités se conduiraient de la même façon. Un agencement différent des égalités aurait permis une compréhension bien plus efficace de la démonstration.
Une façon plus élégante et pédagogique de construire la preuve aurait été de commencer les suites d'égalités au milieu (le produit de matrices), puis de partir de chaque côté. Les calculs semblent se conduire plus intuitivement de cette manière.
Enfin on peut se questionner sur la finalité de la preuve. Démontre-t-elle réellement l'assertion souhaitée ? Peut-on facilement conclure directement à l'assertion souhaitée, étant donné qu'il reste un facteur $-\lambda^n$, qu'il fait intervenir généralement une indéterminée X, et que λ peut être nul ?
Par ailleurs cette démonstration s'apparente assez à une démonstration formelle "classique" à laquelle on aurait ôté toute rigueur mathématique, via l'absence de quantificateurs, d'ensembles de référence, etc. Mais alors est-ce que se débarrasser de la rigueur d'une preuve mathématique en fait réellement une nouvelle démonstration acceptable, une "preuve sans mots" ? Est-ce "mathématiquement licite" ? Cela dépendra évidemment du courant épistémologique.

En quoi est-ce ou non une preuve sans mots ? Cette preuve ne contient que des mots formels mais ne contient aucun mot informel, comme peut l'être toute preuve par équivalence ou suite d'égalités. Selon l'épistémologie éducative, elle pourrait manquer de clarté et de précision, ce qui peut nuire à la pédagogie. En revanche, elle s'adapte beaucoup mieux à l'épistémologie formaliste puisque seuls de simples quantificateurs sont omis. Une légère adaptation, comme explicitée plus haut, la rendrait acceptée par celle-ci. En épistémologie quasi-naturaliste, cette démonstration ne semble pas en être une, puisqu'elle ne met en évidence aucun résultat du monde physique.

4.3 Paradoxe du carré manquant

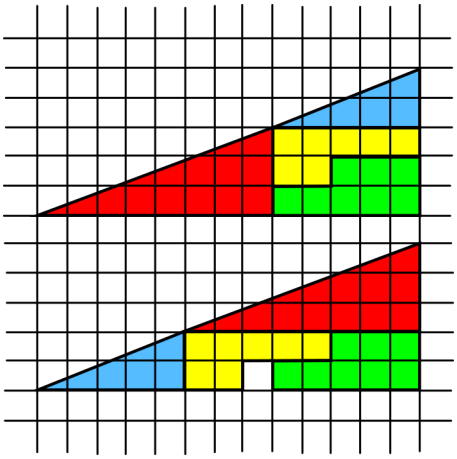


Illustration 4.3 –

Explication : Cette "démonstration" consiste à montrer qu'en réarrangeant des pièces (principe déjà rencontré plusieurs fois dans la première partie) formant un triangle rectangle pour former le même triangle rectangle, on peut créer un trou dans ce dernier. Cette illustration est souvent utilisée dans la culture populaire pour prouver l'existence de paradoxes mathématiques car l'espace laissé par le deuxième agencement des pièces semble inexplicable à première vue.
Cependant, ce paradoxe n'en est pas vraiment un (un paradoxe devrait littéralement être une assertion qui entre en contradiction avec une autre), puisqu'il les hypothèses ne sont pas vérifiées. Il s'agit en réalité plutôt d'une illusion d'optique, nous laissant croire que les pièces forment des triangles rectangles : ce qui n'est pas le cas. En effet, la pente de l'hypoténuse du triangle rouge est de $\frac{3}{8} = 0,375$, tandis que la pente de l'hypoténuse du triangle bleu est de $\frac{2}{5} = 0,4$.

Commentaires : Cette démonstration met en évidence le danger éventuel des preuves par illustrations. Cela montre clairement qu'un schéma ne suffit pas toujours pour démontrer un résultat mathématique, et que l'on peut même parfois se laisser tromper par l'absence d'arguments.
Cependant, heureusement, cette illustration ne prétend pas démontrer quoi que ce soit, puisqu'elle ne semble démontrer aucun théorème ou aucune formule mathématique. Il s'agit finalement d'une sorte de mode d'emploi pour résoudre un puzzle en partant d'une situation initiale qui semble ressembler à la situation finale attendue.

4.4 La quadrisection de l'hypercube

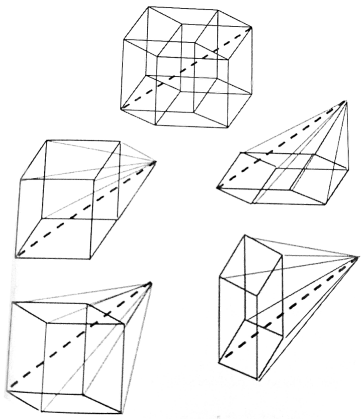


Illustration 4.4 –

Énoncé : En dimension 4, il est possible de sectionner un hypercube en quatre hyperpyramides.

Explication : L'illustration fournit directement la quadrisection de l'hypercube.

Commentaires : La dimension 4 rend trop complexe une traduction littérale de la démonstration. Il faudrait introduire des noms de points, de segments, d'angles... Et bien que cela soit possible en dimension 3, la tâche s'annonce presque impossible en dimension supérieure.
Une animation, ou une démonstration formelle en passant par un espace métrique ou un espace affine, semblent être des solutions plus pertinentes.

En quoi est-ce ou non une preuve sans mots ? Cette preuve illustre parfaitement l'un des problèmes majeurs que l'on rencontre quand on se penche sur des preuves sans mots d'une certaine complexité mathématique : la barrière dimensionnelle.
En effet pour qu'une preuve sans mots soit intéressante, on peut aisément exiger d'elle qu'elle puisse être visualisée. Or ici, le support papier en deux dimensions peine à expliciter clairement des phénomènes se déroulant sur quatre dimensions. Il semble ainsi de plus en plus complexe d'établir une preuve sans mots au fur et à mesure de l'élévation du nombre de dimensions qui régissent le résultat concerné.
On peut cependant noter qu'il est parfois possible de représenter astucieusement une dimension plus élevée que son support (cf Somme des cubes). On pourrait par exemple imaginer ici une vidéo de cube et de pyramide classique qui évolueraient au fil du temps, ce dernier représentant ici la quatrième dimension.

4.5 Conclusion

Ainsi nous avons pu prendre connaissance de différents problèmes qui limitent le principe de preuves sans mots par illustration. Parmi ces derniers, nous pouvons souligner ces quelques limites qui nuisent au fait qu'on puisse attitrer à une illustration l'appellation "preuve sans mots" :

— Lorsque les illustrations laissent au lecteur le travail écrit ou mental de concevoir plusieurs lignes de raisonnement calculatoire (cf Inégalité arithmético-géométrique). En effet dans ce cas là on peut parler de démonstration incomplète, car c'est au lecteur de raisonner pour la peaufiner alors que son travail ne devrait être que celui de suivre un raisonnement, et non pas de créer un raisonnement.

— Lorsque les illustrations sont assimilables à des démonstrations mathématiques formelles "classiques" auxquelles on aurait simplement ôté toute forme de rigueur (cf Polynômes caractéristiques). En effet, dans ce cas-là, il est difficile de trouver ce qu'apporte de plus cette preuve par rapport à sa version formelle "classique" rigoureuse. Jusqu'ici nous avons vu plusieurs preuves sans symbolisme, donc "peu rigoureuses", mais elles trouvaient souvent leurs avantages dans leurs aspects pédagogiques, tandis que si l'on enlève juste la rigueur d'une preuve formelle classique sans l'adapter plus que cela, elle n'en deviendra pas plus pédagogique.

— Lorsque les illustrations trompent notre intellect par le biais d'illusions d'optique, de manque d'étapes ou de justification (cf Paradoxe du carré manquant). En effet, il faut intelligemment et avec recul analyser une illustration se faisant appeler "preuve sans mots" pour s'assurer que l'on ne tire pas de conclusions trop hâtives.

— Lorsque les illustrations veulent démontrer une assertion mettant en jeu plusieurs variables, voire une ou plusieurs variables tendant vers l'infini. En effet il va de soi qu'il est difficile de faire entrer la notion d'infini sur une feuille de papier. De même lorsqu'il est question de démonstration à plus de trois dimensions (cf Quadrisection de l'hypercube). L'illustration n'étant qu'une projection du monde en trois dimensions sur un plan en deux dimensions, les outils visuels se voient ainsi limités.

Finalement les preuves sans mots par illustration ont bien des limites : on ne peut pas nommer n'importe quel raisonnement au titre de "preuve sans mots par illustration". Malgré cela, ce type de preuves sans mots a tout de même souvent un avantage pédagogique et indépendant de la culture ou de la région géographique. Pourtant il existe bien d'autres moyens que l'illustration pour démontrer mathématiquement sans user de mots. Nous allons voire cela dans la partie suivante avec les preuves formelles.

Troisième partie

Preuves formelles

Chapitre 5

Arbres de preuves

Dans cette partie, nous explorerons la logique propositionnelle et le calcul des prédicats. Nous ferons le lien avec le thème des preuves sans mots, qui peut être abordé au travers des arbres de preuves, une façon formelle de représenter des démonstrations mathématiques rigoureuses n'utilisant aucun mot informel. Les annexes de ce document pourront être exploitées pour approfondir les pré-requis nécessaires à la bonne compréhension de cette partie. L'annexe A pour comprendre la sémantique des arbres de preuve, l'annexe B pour découvrir un système de formalisation de langages, et l'annexe C, qui s'appuie sur l'annexe B pour créer un nouveau système de construction de preuves sans mots.

5.1 Pré-requis

5.1.1 Théorie des langages

Cette partie a été fortement alimentée et inspirée par les cours de Damien ROUHLING, retranscrits par Louis THOMAS-GIRARDET. (3)

Dans cette partie, nous introduisons des notions de théorie des langages pour pouvoir discuter de la validité des preuves usuelles utilisant des séquences d'arguments d'ordre logique (égalités, équivalences, quantificateurs...), et en s'appuyant sur la notion de mot formel, jusqu'alors peu précise.

Vocabulaire

Symbole :

Définition : Un symbole est la plus petite unité de langage.
Exemples : "a", "w", "(", "@", "5" et "Hello world !" peuvent être considérés comme des symboles.

Alphabet :

Définition : Un alphabet Σ est un ensemble fini de symboles.

Mot et taille :

Définition : Soient Σ un alphabet et $n \in \mathbb{N}$. Un mot $u \in \Sigma^n$ est un n-uplet de symboles de Σ. n est alors appelé la taille du mot u, et on note : $n = |u|$.

Mot vide :

Définition : Le mot vide, noté ε, est l'unique mot u vérifiant : $|u| = 0$.
Par convention, on posera donc $\Sigma^0 = \{\varepsilon\}$.

Fermeture de Kleene :

Définition : Soit Σ un alphabet. On note Σ^* l'ensemble suivant :

$$\Sigma^* = \bigcup_{n=0}^{+\infty} \Sigma^n$$

Σ^* est donc l'ensemble des mots de taille quelconque, formés sur l'alphabet Σ.

Langage :

Définition : Soit Σ un alphabet. Un langage sur Σ est un ensemble :

$$L \in \mathcal{P}(\Sigma^*)$$

Exemples : Les ensembles suivants sont des langages :
$\{\varepsilon\}$ sur un alphabet quelconque
$\{\varepsilon, a, b, c, ab, ac, bc, ba, cb, ca\}$ sur $\{a, b, c\}$
$\{rouge, bleu, jaune, vert, orange, violet\}$ sur l'alphabet latin
$\{\varepsilon, a, aa, aaa, aaaa, ...\} = \{a\}^*$ sur $\{a\}$

Concaténation de deux mots :

Définition : Soient $u = (u_k)_{k\in[\![1,n]\!]} \in \Sigma^n$ et $v = (v_k)_{k\in[\![1,m]\!]} \in \Sigma^m$.
On note $u \times v = uv = (w_k)_{k\in[\![1,n+m]\!]} \in \Sigma^{n+m}$ avec :

$$\forall k \in [\![1, n+m]\!], w_k = \begin{cases} u_k & \text{si } k \leq n \\ v_{k-n} & \text{sinon.} \end{cases}$$

Propriétés sur la concaténation :

1. Σ^* est la clôture de Σ pour l'opération $\times$, c'est-à-dire le plus petit ensemble stable par $\times$.
2. $(\Sigma^*, \times)$ est un monoïde commutatif d'élément neutre ε.
3. $u \mapsto |u|$ est un épimorphisme de monoïdes de $(\Sigma^*, \times)$ dans $(\mathbb{N}, +)$.

Définitions

Variable propositionnelle :

Une variable propositionnelle est un symbole qui désigne une proposition dans le calcul propositionnel, c'est-à-dire une phrase mathématique ayant une valeur de vérité (Vrai ou Faux) que l'on représentera respectivement par les entiers 1 et 0.
On notera VAR l'ensemble des variables propositionnelles.

Valuation :

Une valuation est une fonction $v : VAR \longrightarrow \{0, 1\}$.

Connecteur logique :

Un connecteur logique d'arité $n \in \mathbb{N}$ est une fonction : $f : \{0, 1\}^n \longrightarrow \{0, 1\}$.

Formule propositionnelle :

Une formule propositionnelle est une expression construite à partir de variables propositionnelles et de connecteurs logiques.

Lecture d'un arbre de preuve :

L'arbre suivant se lit : *"Pour démontrer A en sachant Γ_1 et Γ_2, il suffit de démontrer B en sachant Γ_3 et Γ_4, et de démontrer C en sachant Γ_5 et Γ_6".*

$$\frac{\Gamma_3, \Gamma_4 \vdash B \qquad \Gamma_5, \Gamma_6 \vdash C}{\Gamma_1, \Gamma_2 \vdash A}$$

5.1.2 Règles d'inférence

Règles générales (définition, représentation générale, coupure et affaiblissement) :

$$\frac{\Gamma \vdash x := y}{\Gamma \vdash x = y}\ \text{DEF} \qquad \frac{\Gamma \vdash x = y \qquad \Gamma \vdash P(y)}{\Gamma \vdash P(x)}\ \text{REPG} \qquad \frac{\Gamma \vdash A \qquad \Gamma, A \vdash B}{\Gamma \vdash B}\ \text{CP} \qquad \frac{\Gamma \vdash A}{\Gamma, \Gamma' \vdash A}\ \text{AFF}$$

Antilogie (élimination et ***Réductio Ad Absurdum***) :

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash A}\ \bot_{\mathrm{E}} \qquad \frac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}\ \mathrm{RAA}$$

Négation (introduction et élimination) :

$$\frac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}\ \neg_{\mathrm{I}} \qquad \frac{\Gamma \vdash \neg A \qquad \Gamma \vdash A}{\Gamma \vdash \bot}\ \neg_{\mathrm{E}}$$

Conjonction (introduction, élimination à gauche et élimination à droite) :

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ \wedge_{\mathrm{I}} \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\ \wedge_{\mathrm{EG}} \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\ \wedge_{\mathrm{ED}}$$

Disjonction (introduction à gauche, introduction à droite et élimination) :

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ \vee_{\mathrm{IG}} \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ \vee_{\mathrm{ID}} \qquad \frac{\Gamma \vdash A \vee B \qquad \Gamma, A \vdash C \qquad \Gamma, B \vdash C}{\Gamma \vdash C}\ \vee_{\mathrm{E}}$$

Implication (introduction et élimination) :

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}\ \to_{\mathrm{I}} \qquad \frac{\Gamma \vdash A \to B \qquad \Gamma \vdash A}{\Gamma \vdash B}\ \to_{\mathrm{E}}$$

Équivalence (introduction) :

$$\frac{\Gamma \vdash A \to B \qquad \Gamma \vdash B \to A}{\Gamma \vdash A \leftrightarrow B}\ \leftrightarrow_{\mathrm{I}}$$

Quantificateur universel (introduction et élimination) :

$$\frac{\Gamma \vdash P(t) \qquad t \notin FV(\Gamma)}{\Gamma \vdash \forall x\, P(x)}\ \forall_{\mathrm{I}} \qquad \frac{\Gamma \vdash \forall x\, P(x)}{\Gamma \vdash P([x := t])}\ \forall_{\mathrm{E}}$$

Quantificateur existentiel (introduction et élimination) :

$$\frac{\Gamma \vdash P([x := t])}{\Gamma \vdash \exists x\, P(x)}\ \exists_{\mathrm{I}} \qquad \frac{\Gamma \vdash \exists x\, P(x) \qquad \Gamma, P(t) \vdash A \qquad t \notin FV(\Gamma, A)}{\Gamma \vdash A}\ \exists_{\mathrm{E}}$$

Liberté des variables (séparation) :

$$\frac{x \notin FV(\Gamma) \qquad x \notin FV(\Gamma')}{x \notin FV(\Gamma, \Gamma')}\ \mathrm{SEP}$$

5.1.3 Axiomes

Axiomes de la logique

Thèse :

$$\frac{}{A \vdash A}\ \mathrm{TH}$$

Réflexivité de l'égalité :

$$\frac{}{\Gamma \vdash x = x}\ =_{\mathrm{REF}}$$

Indépendance des variables (antilogie et tautologie) :

$$\frac{}{x \notin FV(\bot)}\ \mathrm{IND}_{\bot} \qquad \frac{}{x \notin FV(\top)}\ \mathrm{IND}_{\top}$$

Arithmétique de Peano

Liste des axiomes

1. **Minimalité :** $\forall x, \neg(S(x) = 0)$
2. **Surjectivité :** $\forall x, (x = 0 \vee \exists y, S(y) = x)$
3. **Injectivité :** $\forall x, \forall y, S(x) = S(y) \rightarrow x = y$
4. **Neutralité :** $\forall x, (x + 0 = x)$
5. **Associativité :** $\forall x, \forall y, (x + S(y) = S(x + y))$
6. **Absorbance :** $\forall x, (x \cdot 0 = 0)$
7. **Distributivité :** $\forall x, \forall y (x \cdot S(y) = (x \cdot y) + x)$
8. **Récurrence :** $(P(0) \wedge \forall x, (P(x) \rightarrow P(S(x))) \rightarrow (\forall x, P(x))$

Modèle

$\mathbb{N}$ est un modèle de l'axiomatique de Peano. Cela signifie que, implicitement, toutes les variables introduites dans les axiomes sont quantifiées sur $\mathbb{N}$.
Mais cela ne signifie pas que $\mathbb{N}$ est l'unique ensemble vérifiant les propriétés ci-dessus. En effet, il existe d'autres constructions de $\mathbb{N}$. C'est pourquoi, pour correspondre à la définition usuelle de $\mathbb{N}$, nous utiliserons également les axiomes suivants :

1. **Existence de zéro :** $0 \in \mathbb{N}$
2. **Existence du successeur :** $\forall x, x \in \mathbb{N} \rightarrow S(x) \in \mathbb{N}$

Représentation

Il est ensuite nécessaire de définir certaines notations ; par exemple, la notation décimale, qui n'a rien d'universel. En effet, dans de nombreuses civilisations et selon les époques, le système numérique est bien différent du système occidental actuel, et fonctionne sur une base 12, 60, ou autre... En épistémologie culturelle, il faut tenir compte de ces différences. C'est pourquoi nous utiliserons également les axiomes suivants :

1. **Représentation de un :** $1 := S(0)$
2. **Représentation de deux :** $2 := S(1)$

Exemples de systèmes axiomatiques

ZF, ZFC, NGB, Euclide, Arithmétique de Peano...

Vers les arbres de preuves

Ainsi nous avons tout le bagage pour traiter quelques arbres de preuves et se rendre compte des différents intérêts de cette façon de prouver sans mots informels en mathématiques. Parmi ces différents intérêts qu'offrent les arbres de preuves, on peut en citer quelques uns :

— Une telle preuve peut être intelligible par toute personne raisonnant de manière logique, sans pour autant nécessiter des aptitudes poussées en mathématiques. En effet, la lecture d'arbres de preuves repose avant tout sur un agencement logique d'axiomes et de règles d'inférence.
— Ce type de démonstration a également un intérêt pédagogique. En effet, il suffit de se familiariser avec les quelques axiomes et règles fondamentales des arbres de preuves pour qu'une lecture d'un arbre de preuve se fasse aisément, sans se perdre dans les raisonnements alambiqués, qui passent parfois mal la barrière de l'humain faillible à la rédaction.
— Un autre intérêt des arbres de preuves est leur caractère universel. En effet, ce type de démonstration n'utilise pas de mots informel. Ainsi il peut être intelligible par n'importe quelle nationalité.
— Une telle preuve est aussi transmissible plus facilement à un ordinateur : en effet, il suffit d'expliciter l'ordre dans lequel les règles d'inférence et les axiomes sont utilisés pour aboutir à la preuve. C'est une méthode utilisée par les assistants de preuve.

Pour constater concrètement ces différents intérêts, nous donnons dans la section suivante quelques arbres de preuves, dans un ordre croissant de difficulté.

5.2 Arbre de preuve de la non-contradiction

Montrons que l'on ne peut pas à la fois prouver une assertion et son contraire.

Règles d'inférence utilisées

— Introduction de la négation ($\neg_{\mathrm{I}}$)
— Élimination de la négation ($\neg_{\mathrm{E}}$)
— Élimination de la conjonction à gauche ($\wedge_{\mathrm{EG}}$)
— Élimination de la conjonction à droite ($\wedge_{\mathrm{ED}}$)

Axiomes utilisés

— Thèse (TH)

Arbre

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \wedge \neg A \vdash A \wedge \neg A}\,\mathrm{TH}}{A \wedge \neg A \vdash \neg A}\,\wedge_{\mathrm{ED}} \quad \dfrac{\dfrac{}{A \wedge \neg A \vdash A \wedge \neg A}\,\mathrm{TH}}{A \wedge \neg A \vdash A}\,\wedge_{\mathrm{EG}}}{A \wedge \neg A \vdash \bot}\,\neg_{\mathrm{E}}}{\vdash \neg(A \wedge \neg A)}\,\neg_{\mathrm{I}}$$

5.3 Arbre de preuve de l'involution de la disjonction

Prouvons que la disjonction est involutive, c'est-à-dire que toute assertion A est équivalente à $A \vee A$.

Règles d'inférence utilisées

— Introduction de l'équivalence ($\leftrightarrow_{\mathrm{I}}$)
— Introduction de l'implication ($\rightarrow_{\mathrm{I}}$)
— Introduction de la disjonction à gauche ($\vee_{\mathrm{IG}}$)
— Élimination de la disjonction ($\vee_{\mathrm{E}}$)
— Affaiblissement (AFF)

Axiomes utilisés

— Thèse (TH)

Arbre

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A \vee A \vdash A \vee A}\,\mathrm{TH} \quad \dfrac{\dfrac{}{A \vdash A}\,\mathrm{TH}}{A \vee A, A \vdash A}\,\mathrm{AFF} \quad \dfrac{\dfrac{}{A \vdash A}\,\mathrm{TH}}{A \vee A, A \vdash A}\,\mathrm{AFF}}{A \vee A \vdash A}\,\vee_{\mathrm{E}}}{\vdash A \vee A \to A}\,\to_{\mathrm{I}} \quad \dfrac{\dfrac{\dfrac{}{A \vdash A}\,\mathrm{TH}}{A \vdash A \vee A}\,\vee_{\mathrm{IG}}}{\vdash A \to A \vee A}\,\to_{\mathrm{I}}}{\vdash A \vee A \leftrightarrow A}\,\leftrightarrow_{\mathrm{I}}$$

5.4 Arbre de preuve de "la symétrie de l'égalité"

Soient x, y deux objets fixés, prouvons l'assertion : $x = y \leftrightarrow y = x$.

Règles d'inférence utilisées

— Introduction de l'équivalence ($\leftrightarrow_{\mathrm{I}}$)
— Introduction de l'implication ($\rightarrow_{\mathrm{I}}$)
— Représentation générale (REPG)

Axiomes utilisés

— Thèse (TH)
— Réflexivité de l'égalité ($=_{\mathrm{REF}}$)

Arbre

$$\dfrac{\dfrac{\dfrac{\dfrac{}{x=y \vdash x=y}\,\mathrm{TH} \quad \dfrac{}{x=y \vdash y=y}\,=_{\mathrm{REF}}}{x=y \vdash y=x}\,\mathrm{REPG}}{\vdash x=y \rightarrow y=x}\,\rightarrow_{\mathrm{I}} \quad \dfrac{\dfrac{\dfrac{}{y=x \vdash y=x}\,\mathrm{TH} \quad \dfrac{}{y=x \vdash x=x}\,=_{\mathrm{REF}}}{y=x \vdash x=y}\,\mathrm{REPG}}{\vdash y=x \rightarrow x=y}\,\rightarrow_{\mathrm{I}}}{\vdash x=y \leftrightarrow y=x}\,\leftrightarrow_{\mathrm{I}}$$

5.5 Arbre de preuve de "2 est un entier naturel"

Prouvons l'assertion : $2 \in \mathbb{N}$ dans le cadre axiomatique de Peano, et des axiomes de représentation et du caractère "modèle" de $\mathbb{N}$.

Règles d'inférence utilisées

— Définition (DEF)
— Représentation générale (REPG)
— Élimination de l'implication ($\rightarrow_{\mathrm{E}}$)
— Élimination du quantificateur universel ($\forall_{\mathrm{E}}$)

Axiomes utilisés

— Existence de zéro (ZERO)
— Représentation de un (REP_1)
— Représentation de deux (REP_2)
— Existence du successeur (EXS)

Arbre

$$\dfrac{\dfrac{\dfrac{}{2 := S(1)}\,\mathrm{REP}_2}{2 = S(1)}\,\mathrm{DEF} \quad \dfrac{\dfrac{\dfrac{\dfrac{}{1 := S(0)}\,\mathrm{REP}_1}{1 = S(0)}\,\mathrm{DEF} \quad \dfrac{}{0 \in \mathbb{N}}\,\mathrm{ZERO} \quad \dfrac{\dfrac{}{\forall x, (x \in \mathbb{N} \rightarrow S(x) \in \mathbb{N})}\,\mathrm{EXS}}{0 \in \mathbb{N} \rightarrow S(0) \in \mathbb{N}}\,\forall_{\mathrm{E}}}{S(0) \in \mathbb{N}}\,\rightarrow_{\mathrm{E}}}{1 \in \mathbb{N}}\,\mathrm{REPG} \quad \dfrac{\dfrac{}{\forall x, (x \in \mathbb{N} \rightarrow S(x) \in \mathbb{N})}\,\mathrm{EXS}}{1 \in \mathbb{N} \rightarrow S(1) \in \mathbb{N}}\,\forall_{\mathrm{E}}}{S(1) \in \mathbb{N}}\,\rightarrow_{\mathrm{E}}}{2 \in \mathbb{N}}\,\mathrm{REPG}$$

5.6 Arbre de preuve de "l'absence de contre-exemple"

Prouvons que si l'on suppose qu'une propriété est universellement vraie, alors il n'existe aucun contre-exemple de cette propriété, c'est-à-dire prouvons le séquent suivant : $\forall x\, A(x) \vdash \neg(\exists x\, \neg A(x))$.

Règles d'inférence utilisées

— Introduction de la négation ($\neg_{\mathrm{I}}$)
— Élimination du quantificateur existentiel ($\exists_{\mathrm{E}}$)
— Élimination de la négation ($\neg_{\mathrm{E}}$)
— Élimination du quantificateur universel ($\forall_{\mathrm{E}}$)
— Séparation de la liberté des variables (SEP)

Axiomes utilisés

— Thèse (TH)
— Indépendance de l'antilogie ($\mathrm{IND}_{\perp}$)

Arbre

$$\dfrac{\dfrac{\dfrac{}{\Gamma \vdash \exists x\, \neg A(x)}\,\mathrm{TH} \quad \dfrac{\dfrac{}{\Gamma, \neg A(t) \vdash \neg A(t)}\,\mathrm{TH} \quad \dfrac{\dfrac{}{\Gamma, \neg A(t) \vdash \forall x A(x)}\,\mathrm{TH}}{\Gamma, \neg A(t) \vdash A(t)}\,\forall_{\mathrm{E}}}{\Gamma, \neg A(t) \vdash \perp}\,\neg_{\mathrm{E}} \quad \dfrac{\dfrac{}{t \notin FV(\Gamma)} \quad \dfrac{}{t \notin FV(\perp)}\,\mathrm{IND}_{\perp}}{t \notin FV(\Gamma, \perp)}\,\mathrm{SEP}}{\Gamma = (\forall x\, A(x), \exists x\, \neg A(x)) \vdash \perp}\,\exists_{\mathrm{E}}}{\forall x\, A(x) \vdash \neg(\exists x\, \neg A(x))}\,\neg_{\mathrm{I}}$$

5.7 Conclusion

On constate que les arbres de preuve peuvent être utiles pour comprendre la chronologie d'un raisonnement mathématique, et pour le décomposer en une succession d'arguments afin de former une preuve irréfutable.

Cependant, en s'éloignant du langage naturel, la sémantique contenue dans une preuve est perdue. Ainsi la démonstration perd instantanément ce qui lui permet d'être aisément intelligible.

Cette traduction vers un langage formel permet une universalisation et abstraction des écrits mathématiques. De ce fait, une preuve peut être réutilisée dans plusieurs modèles. Cette nouvelle rédaction de preuves permet une lecture systématique et qui peut donc être effectuée par un logiciel informatique. Ce type de preuve à donc un impact dans la formalisation informatique des démonstrations.

Mais dans la pratique, il semble difficile de réaliser des arbres de preuve pour des théorèmes nécessitant de nombreux lemmes pour être démontrés. En effet, puisqu'un arbre de preuve se veut se baser sur des axiomes, il faudrait beaucoup d'étapes pour démontrer ne serait-ce que le théorème de Pythagore, ou l'inégalité arithmético-géométrique. Ces assertions comme on a pu le voir dans des parties précédentes, semblent pouvoir se justifier plus aisément avec une illustration, ou dans le pire des cas, avec une rédaction plus usuelle.

Chapitre 6

L'informatique et le binaire

Quand on parle "d'absence de mot" et "d'informatique", on peut penser au mot "binaire". En effet le système binaire (quand il est couplé avec l'ASCII et ses variantes) permet de retranscrire une entité écrite par une succession de 1 et de 0. Une idée assez naturelle pour composer une preuve sans mots serait alors de transcrire une preuve écrite en code binaire.

6.1 Pré-requis

6.1.1 Codage binaire

Le codage binaire usuel est la décomposition d'un nombre en puissance de deux. Prenons les entiers naturels comme exemple car leur codage est exact et plus simple à comprendre. Un entier est codé sur un nombre de bits donné, un bit étant une valeur (0 ou 1) associée à une puissance de deux. Algébriquement, la décomposition binaire d'un entier n peut être vue comme l'unique polynôme $P \in \{0,1\}[X]$ tel que $P(2) = n$. Prenons comme exemple un vieil ordinateur en 8-bits (le bit le plus à gauche représentant alors 2^7). On a les décompositions de 0, 1 et 13 suivantes :

$$0 = 0 \times 2^0\,,$$

$$1 = 1 \times 2^0\,,$$

$$13 = 1 \times 2^3 + 1 \times 2^2 + 1 \times 2^0\,.$$

Leur codage binaire respectif est donc :

$$0 = 00000000\,,$$

$$1 = 00000001\,,$$

$$13 = 00001101\,.$$

6.1.2 ASCII

L'ASCII ou, *American Standard Code for Information Interchange*, est une convention de notation pour encoder des caractères sur sept bits (cf Table de caractères ASCII). À chacun des caractères qu'elle contient, elle associe un entier en binaire. La lettre "a", par exemple, devient ainsi 97, soit 1100001 en binaire.

6.2 Application

En utilisant la décomposition binaire et l'ASCII, on pourrait par exemple partir de la démonstration du théorème de Pythagore suivante :

Pour un triangle rectangle donné, il est possible de l'inscrire en quatre exemplaires dans les coins d'un carré dont le côté a pour longueur la somme des longueurs des côtés de l'angle droit. Les quatre hypoténuses forment alors un carré, par égalité de longueur et sachant que chacun de ses angles est supplémentaire des deux angles aigus du triangle. Avec les notations usuelles, l'aire totale du grand carré vaut donc $(a+b)^2$ et l'aire du carré intérieur vaut c^2. La différence est constituée par quatre triangles d'aire $\frac{ab}{2}$ chacun. La relation algébrique entre ces aires s'écrit alors $(a+b)^2 = 4(\frac{ab}{2}) + c^2$, c'est-à-dire $a^2 + 2ab + b^2 = 2ab + c^2$, ce qui revient à $a^2 + b^2 = c^2$.

Pour arriver au code binaire suivant :

01010000 01101111 01110101 01110010 00100000 01110101 01101110 00100000 01110100 01110010 01101001 01100001 01101110 01100111
01101100 01100101 00100000 01110010 01100101 01100011 01110100 01100001 01101110 01100111 01101100 01100101 00100000 01100100
01101111 01101110 01101110 11000011 10101001 00101100 00100000 01101001 01101100 00100000 01100101 01110011 01110100 00100000
01110000 01101111 01110011 01110011 01101001 01100010 01101100 01100101 00100000 01100100 01100101 00100000 01101100 11100010
10000000 10011001 01101001 01101110 01110011 01100011 01110010 01101001 01110010 01100101 00100000 01100101 01101110 00100000
01110001 01110101 01100001 01110100 01110010 01100101 00100000 01100101 01111000 01100101 01101101 01110000 01101100 01100001
01101001 01110010 01100101 01110011 00100000 01100100 01100001 01101110 01110011 00100000 01101100 01100101 01110011 00100000
01100011 01101111 01101001 01101110 01110011 00100000 01100100 11100010 10000000 10011001 01110101 01101110 00100000 01100011
01100001 01110010 01110010 11000011 10101001 00100000 01100100 01101111 01101110 01110100 00100000 01101100 01100101 00100000
01100011 11000011 10110100 01110100 11000011 10101001 00100000 01100001 00100000 01110000 01101111 01110101 01110010 00100000
01101100 01101111 01101110 01100111 01110101 01100101 01110101 01110010 00100000 01101100 01100001 00100000 01110011 01101111
01101101 01101101 01100101 00100000 01100100 01100101 01110011 00100000 01101100 01101111 01101110 01100111 01110101 01100101
01110101 01110010 01110011 00100000 01100100 01100101 01110011 00100000 01100011 11000011 10110100 01110100 11000011 10101001
01110011 00100000 01100100 01100101 00100000 01101100 00100111 01100001 01101110 01100111 01101100 01100101 00100000 01100100
01110010 01101111 01101001 01110100 00101110 00100000 01001100 01100101 01110011 00100000 01110001 01110101 01100001 01110100
01110010 01100101 00100000 01101000 01111001 01110000 01101111 01110100 11000011 10101001 01101110 01110101 01110011 01100101
01110011 00100000 01100110 01101111 01110010 01101101 01100101 01101110 01110100 00100000 01100001 01101100 01101111 01110010
01110011 00100000 01110101 01101110 00100000 01100011 01100001 01110010 01110010 11000011 10101001 00101100 00100000 01110000
01100001 01110010 00100000 11000011 10101001 01100111 01100001 01101100 01101001 01110100 11000011 10101001 00100000 01100100
01100101 00100000 01101100 01101111 01101110 01100111 01110101 01100101 01110101 01110010 00100000 01100101 01110100 00100000
01110011 01100001 01100011 01101000 01100001 01101110 01110100 00100000 01110001 01110101 01100101 00100000 01100011 01101000
01100001 01100011 01110101 01101110 00100000 01100100 01100101 00100000 01110011 01100101 01110011 00100000 01100001 01101110
01100111 01101100 01100101 01110011 00100000 01100101 01110011 01110100 00100000 01110011 01110101 01110000 01110000 01101100
11000011 10101001 01101101 01100101 01101110 01110100 01100001 01101001 01110010 01100101 00100000 01100100 01100101 01110011
00100000 01100100 01100101 01110101 01111000 00100000 01100001 01101110 01100111 01101100 01100101 01110011 00100000 01100001
01101001 01100111 01110101 01110011 00100000 01100100 01110101 00100000 01110100 01110010 01101001 01100001 01101110 01100111
01101100 01100101 00101110 00001101 00001010 00001101 00001010 01000001 01110110 01100101 01100011 00100000 01101100 01100101
01110011 00100000 01101110 01101111 01110100 01100001 01110100 01101001 01101111 01101110 01110011 00110000 01110100 01110011
01110101 01100101 01101100 01101100 01100101 01110011 00101100 00100000 01101100 11100010 10000000 10011001 01100001 01101001
01110010 01100101 00100000 01110100 01101111 01110100 01100001 01101100 01100101 00100000 01100100 01110101 00100000 01100111
01110010 01100001 01101110 01100100 00100000 01100011 01100001 01110010 01110010 11000011 10101001 00100000 01110110 01100001
01110101 01110100 00100000 01100100 01101111 01101110 01100011 00100000 00101000 01100001 00100000 00101011 00100000 01100010
00101001 00110010 00100000 01100101 01110100 00100000 01101100 11100010 10000000 10011001 01100001 01101001 01110010 01100101
00100000 01100100 01110101 00100000 01100011 01100001 01110010 01110010 11000011 10101001 00100000 01101001 01110110 01100100
11000011 10101001 01110010 01101001 01100101 01110101 01110010 00100000 01110110 01100001 01110101 01110100 00100000 01100011
00110010 00101110 00100000 01001100 01100001 00100000 01100100 01101001 01100110 01100110 11000011 10101001 01110010 01100101
01101110 01100011 01100101 00100000 01100101 01110011 01110100 00100000 01100011 01101111 01101110 01110011 01110100 01101001
01110100 01110101 11000011 10101001 01100101 00100000 01110000 01100001 01110010 00100000 01110001 01110101 01100001 01110100
01110010 01100101 00100000 01110100 01110010 01101001 01100001 01101110 01100111 01101100 01100101 01110011 00100000 01100100
11100010 10000000 10011001 01100001 01101001 01110010 01100101 00100000 01100001 01100010 00101111 00110010 00100000 01100011
01101000 01100001 01100011 01110101 01101110 00101110 00001101 00001010 00001101 00001010 01001100 01100001 00100000 01110010
01100101 01101100 01100001 01110100 01101001 01101111 01101110 00100000 01100001 01101100 01100111 11000011 10101001 01100010
01110010 01101001 01110001 01110101 01100101 00100000 01100101 01101110 01110100 01110010 01100101 00100000 01100011 01100101
01110011 00100000 01100001 01101001 01110010 01100101 01110011 00100000 01110011 11100010 10000000 10011001 11000011 10101001
01100011 01110010 01101001 01110100 00100000 01100001 01101100 01101111 01110010 01110011 00100000 00101000 01100001 00100000
00101011 00100000 01100010 00101001 00110010 00100000 00111101 00100000 00110100 00100000 00101000 01100001 01100010 00101111
00110010 00101001 00100000 00101011 00100000 01100011 00110010 00101100 00100000 01100011 11100010 10000000 10011001 01100101
01110011 01110100 00101101 11000011 10100000 00101101 01100100 01101001 01110010 01100101 00100000 01100001 00110010 00100000
00101011 00100000 00110010 01100001 01100010 00100000 00101011 00100000 01100010 00110010 00100000 00111101 00100000 00110010
01100001 01100010 00100000 00101011 00100000 01100011 00110010 00101100 00100000 01100011 01100101 00100000 01110001 01110101
01101001 00100000 01110010 01100101 01110110 01101001 01100101 01101110 01110100 00100000 11000011 10100000 00100000 01100001
00110010 00100000 00101011 00100000 01100010 00110010 00100000 00111101 00100000 01100011 00110010 00101110

Cette succession de bits n'a pas vraiment de valeur mathématique puisqu'il s'agit simplement d'une transcription en code binaire d'une preuve déjà rédigée. Le code binaire seul ne contient donc pas l'essence mathématique de la preuve. Cependant, lorsque la démonstration est une preuve formelle avec des symboles, comme cela peut l'être dans un arbre de preuve, le code binaire est une représentation des symboles utilisés. Il est alors parfaitement possible de redéfinir les règles d'inférence et les axiomes avec du code binaire uniquement.

6.3 Intérêt mathématique

6.3.1 Assistants de preuves

Comme vu précédemment dans les chapitres 5 et 6, les preuves formalisées peuvent être interprétées par un ordinateur. Il ne nous manque alors qu'une chose pour construire l'un des outils les plus puissants des mathématiques modernes. Prenons un peu de recul sur la philosophie de notre démarche. Jusqu'ici, nous avons simplement considéré la question "Est-ce ou non une preuve ?". Et si nous nous demandions plutôt maintenant "Est-ce que cette preuve est correcte ?". Avec ce point de vue nouveau, l'outil informatique est capable de donner une réponse. En effet, il n'est plus question de rédiger une démonstration à un problème donné. Mais, avec une démonstration bien formalisée, il est possible avec un algorithme de renvoyer un simple booléen (vrai ou faux). Or, nous l'avons dit, nous sommes capables de faire interpréter une démonstration à un ordinateur grâce à la formalisation. C'est sur ce principe qu'ont vu le jour une multitude d'assistants de preuve comme HOL ou encore Coq.

6.3.2 Codage de Gödel

En 1931, le mathématicien allemand Kurt Gödel a proposé un système de numérotation des symboles propositionnels. Il a associé de façon unique un entier naturel à chaque symbole propositionnel. Ce système a inspiré le code ASCII :

$$(x = y \Rightarrow y = x) \equiv (120, 61, 121, 32, 61, 62, 32, 121, 61, 120)$$

Par exemple ici, le nombre 120 correspond au symbole x, tandis que le nombre 121 correspond au symbole y.
Ainsi, à l'aide de la décomposition unique d'un nombre entier en produit de facteurs premiers, Gödel trouve une injection entre les assertions mathématiques et les entiers naturels. Par exemple, l'assertion $0 = 0$ a pour codage de Gödel :

$$2^6 \times 3^5 \times 5^6 = 243000000\,.$$

De fait, un entier naturel qui correspond à une assertion mathématique avec du sens (certaines suites de symboles sont dépourvues de sens) peut être naturellement utilisé dans une démonstration mathématique pour représenter une assertion. Une démonstration ne serait alors plus qu'une suite d'entiers naturels : voire mieux ! Si la barre d'inférence et les symboles de séquents des arbres de preuve sont aussi convertis, il est alors possible de transformer une démonstration en entier naturel. Entier naturel qui pourra alors être converti en binaire par la méthode explicitée plus haut. Nous n'expliciterons pas plus la méthode du codage de Gödel dans ce document, car elle est trop complexe à mettre en oeuvre. En pratique, c'est aussi difficile de la mettre en oeuvre car les entiers naturels obtenus avec le codage de Gödel peuvent devenir immenses très rapidement. C'est d'ailleurs l'idée qui se cache derrière le nombre de Rayo, qui est le plus grand entier pouvant être construit en moins de 10^{100} symboles avec les axiomes de ZFC.

6.4 Application aux preuves par illustration

Une illustration n'est rien d'autre qu'un fichier image (JPEG, PNG, SVG...). Chaque format de fichier contient un codage qui lui est propre, codage qui peut être converti en binaire. Ainsi une illustration peut être vue comme un simple code binaire, ce qui ajoute une couche supplémentaire au caractère "sans mots" d'une démonstration qui n'en contenait déjà pas.

Cependant on peut émettre quelques réserves. En effet, peut-on vraiment dire que le code binaire d'une image contient l'essence mathématique de la preuve ? Au fond, une image n'est qu'une matrice de pixels, un pixel ne contient aucune information mathématique,et n'a donc pas la valeur d'une démonstration... C'est vrai pour les images matricielles (JPEG, PNG...), mais faux pour les images vectorielles. En effet une image vectorielle est constituée d'équations de courbes de Bézier. Dans une image vectorielle, il y a donc une véritable essence mathématique qui peut parfois être différente de l'essence de la preuve que l'image se veut de démontrer, mais qui fait naturellement exister une correspondance entre les deux essences mathématiques dès lors que le tracé des courbes (à comprendre au sens vectoriel, pas au sens analytique) fait partie intégrante de la démonstration, comme c'est souvent le cas dans les deux premiers chapitres de ce document.

6.5 Limites

L'introduction de ces codes utilisés par le langage machine d'un processeur nous permet d'apercevoir le paradoxe que contient la notion de preuve sans mots. En effet en essayant de s'éloigner du langage naturel, de sa sémantique et de ses mots, nous avons fini par le traduire dans un langage machine. Mais dans ce cas, pouvons-nous vraiment considérer que notre preuve est exempte de mots puisqu'elle est basée sur un langage et un alphabet formel interprétables par un ordinateur ?

Quatrième partie

Conclusion

Conclusion

Tout au long de ce mémoire, nous avons traité de la diversité du principe de preuves sans mots à travers des démonstrations par illustration, mais aussi par des preuves sans mots plus formelles comme les arbres de preuves, pour aller jusqu'à la dimension informatique de ce sujet. Toute cette diversité peut faire sens au regard de ces quelques citations :

"*Tous les moyens sont bons quand ils sont efficaces.*" (Jean-Paul Sartre (5))

"*Pour prouver, tous les moyens sont bons.*" (Jean-Paul Delahaye (6))

Bien que le caractère démonstratif de certaines preuves par illustration ou de certains arbres de preuve peuvent être remis en question, car la simplicité des illustrations et la longueur des arbres de preuve laissent parfois muets ou dissimulés certains arguments essentiels au bon déroulement de la démonstration, les preuves sans mots gardent globalement de grands intérêts :

— Un intérêt pédagogique. En effet, accentuer l'aspect ludique et visuel d'une activité peut en faciliter l'apprentissage. Cette idée est souvent développée dans des méthodes telles que l'apprentissage par le jeu. Dans le cas des démonstrations mathématiques, cela peut permettre de rattacher un objet du monde mathématique abstrait à un contexte concret pour en faciliter l'assimilation.

— Un intérêt d'universalité des preuves. En effet, la suppression des mots des langues usuelles par la formalisation des démonstrations permet à la fois une universalisation des mathématiques mais également leur implémentation informatique, utile notamment pour certaines technologies, comme les assistants de preuves.

Il n'existe pas de consensus épistémologique pour trancher sur le caractère démonstratif d'une illustration ou d'une suite d'arguments. La définition d'une preuve mathématique est donc bien subjective mais les discussions autour d'une quelconque illustration ou d'un quelconque arbre de preuve ont toujours une grande portée pédagogique : il y a toujours des choses intéressantes à observer dans une illustration et c'est toujours intrigant de constater la difficulté de la construction de certains théorèmes mathématiques à partir des axiomes au travers des arbres de preuve.

Au-delà des mathématiques, les preuves sans mots existent dans d'autres sciences. En physique, en chimie ou encore en biologie, on prouve souvent par des expérimentations. Une expérience n'est a priori pas constituée de mots, qu'ils soient formels ou informels ! Ces domaines se distinguent tout de même des mathématiques par leur caractère réel et concret. Ce qui unit en revanche ces domaines, c'est la curiosité qu'il faut avoir pour pouvoir les pratiquer.

La curiosité est l'une des qualités des plus importantes à avoir en mathématiques car c'est cela qui permet de grandes découvertes ! Que serait l'arithmétique si Andrew Wiles n'avait pas eu la curiosité de se plonger dans la démonstration de la conjecture de Fermat ? Que seraient l'analyse et la physique théorique si Jérôme Cardan n'avait pas eu la curiosité de poser des solutions d'une équation à carré négatif ? Il y a rarement de vérités générales concernant la philosophie ou la pédagogie mais ce sont des discussions amenées sur la table qu'émergent parfois les réponses et les conséquences les plus intéressantes. C'est que nous avons souhaité conclure à travers ce mémoire.

Annexes

Annexe A

Sémantique des formules propositionnelles

Les formules propositionnelles, les connecteurs logiques, les règles d'inférence et les axiomes utilisés à partir de la section 5.1.2 n'ont pas de sémantique. Cela signifie qu'a priori, ils n'ont pas de signification logique. Seules les règles de manipulation sont introduites. Cependant, il est possible de les lier aux outils mathématiques usuels. C'est l'objet de cette annexe.

A.1 Symboles de séquent

Les symboles de séquent et leur sémantique :
— $\Gamma \vdash A$ se lit "Γ prouve syntaxiquement A" et signifie que si l'on suppose Γ dans nos hypothèses, alors cela prouve A au sens syntaxique.
— $\Gamma \vDash A$ se lit "Γ prouve sémantiquement A" et signifie que si l'on suppose Γ dans nos hypothèses, alors cela prouve A au sens sémantique. Ce symbole n'a de sens que pour signifier que l'hypothèse Γ est un modèle de la conséquence A.

A.2 Connecteurs logiques

Les connecteurs logiques et leur sémantique :
— $\neg A$ se lit "non A" et signifie que A est faux.
— $A \vee B$ se lit "A ou B" et signifie que A est vrai et/ou B est vrai.
— $A \wedge B$ se lit "A et B" et signifie que A et B sont vrais.
— $A \rightarrow B$ se lit "A implique B" et signifie que si A est vrai, alors B est vrai.
— $A \leftrightarrow B$ se lit "A est équivalent à B" et signifie que A et B ont la même valeur de vérité.
— $\bot$ se lit "antilogie" et remplace une formule propositionnelle toujours fausse.
— $\top$ se lit "tautologie" et remplace une formule propositionnelle toujours vraie.

A.3 Règles d'inférence

A.3.1 Règles générales

Définition

Pour prouver que deux objets x et y sont égaux, il suffit de prouver que x est défini comme y.

Représentation générale

Pour prouver qu'un objet x vérifie une propriété P, il suffit de montrer que x est égal à un objet y et que y vérifie la propriété P.

Coupure

Pour prouver une assertion B, il suffit de prouver qu'une assertion A est vraie, puis que si l'on suppose que A est vraie, alors B est vraie.

Affaiblissement

Pour prouver une assertion A avec plusieurs hypothèses, il suffit de généraliser en enlevant une hypothèse. Ainsi, si le cas général est vérifié, alors un cas moins général est vérifié aussi.

A.3.2 Antilogie

Élimination

L'élimination de l'antilogie signifie que si l'on parvient à démontrer une assertion fausse, on peut alors tout démontrer. Ce principe peut être vu comme la réciproque de l'un des théorèmes d'incomplétude de Gödel qui annonce qu'il n'existe pas de théorie (formalisant l'arithmétique) dans lequel tout énoncé est démontrable ou réfutable.

Réductio Ad Absurdum

Cette règle exprime la démonstration par l'absurde. En effet, si on supposant qu'une assertion A est fausse, on peut démontrer l'antilogie (qui est toujours fausse), cela permet de justifier que cette assertion n'est pas fausse et donc qu'elle est vraie. Cette règle n'est acceptée qu'en logique classique, et non en logique intuitionniste, car elle utilise ici le fait qu'un énoncé non-faux est vrai, ce qui est équivalent à l'involutivité de la négation ou au principe du tiers exclu.

A.3.3 Négation

Introduction

Cette règle ressemble beaucoup à une démonstration par l'absurde, mais il n'en est rien. Ici, on suppose qu'une assertion est vraie, on aboutit à une absurdité, ce qui permet de conclure que l'assertion est fausse.

Élimination

Pour prouver quelque chose de faux, il suffit de prouver n'importe quelle assertion et son contraire.

A.3.4 Conjonction

Introduction

Pour prouver que deux assertions sont vraies, il suffit de montrer que l'une et l'autre sont indépendamment vraies.

Élimination

Pour prouver qu'une assertion est vraie, il suffit de prouver que deux assertions, donc celle-ci, sont vraies.

A.3.5 Disjonction

Introduction

Pour prouver qu'une première assertion est vraie ou qu'une deuxième assertion est vraie, il suffit de prouver que l'une des deux est vraie.

Élimination

Pour prouver qu'une assertion C est vraie, on peut faire une disjonction des cas. On sépare d'abord l'assertion C en deux cas A et B, et prouve que $A \vee B$ est vraie. Puis on prouve que si A est vraie, alors C est vraie, puis que si B est vraie, alors C est vraie. Ainsi tous les cas ont été traités et cela permet de conclure que C est vrai.

A.3.6 Implication

Introduction

Pour prouver qu'une assertion A implique une assertion B, il suffit de prouver que si l'on suppose que A est vraie, alors B est nécessairement vraie.

Élimination

Pour prouver qu'une assertion B est vraie, il suffit de prouver qu'elle est impliquée par une assertion A, puis de prouver que A est vraie. On retrouve parfois cette règle sous le nom de *"modus ponens"*.

A.3.7 Équivalence

Introduction

Pour prouver que A est équivalent à B, on raisonne par double-implication. On prouve que A implique B et que B implique A.

A.3.8 Quantificateur universel

Introduction

Pour prouver qu'une propriété P est universellement vraie, c'est-à-dire vraie sur tout objet de la théorie, il suffit de poser un objet t quelconque, c'est-à-dire indépendant de toute hypothèse, et de prouver que cet objet t vérifie la propriété P.

Élimination

Pour prouver qu'un objet t vérifie une propriété P, il suffit de prouver que P est vrai pour tout x. En effet, si une propriété est vraie pour tout x, alors est vraie en particulier pour un certain $x = t$.

A.3.9 Quantificateur existentiel

Introduction

Pour prouver qu'il existe un objet x qui vérifie une propriété P, il suffit de prouver qu'un objet t fixé vérifie cette propriété P.

Élimination

Pour prouver qu'une assertion A est vérifiée, il suffit de prouver qu'il existe un objet x vérifiant une propriété P, et que si cette propriété est vérifiée par un objet t fixé indépendant de toute hypothèse, alors cela prouve l'assertion A.

Liberté des variables

$t \notin FV(\Gamma, \Gamma')$ signifie que t est indépendant des hypothèses Γ et Γ'.

Séparation

Pour prouver qu'un objet x est indépendant de plusieurs hypothèses, il suffit de prouver que x est indépendant de chaque hypothèse.

A.4 Axiomes de la logique

Thèse

Supposer que l'hypothèse A est vraie permet de conclure que l'hypothèse A est vraie.

Réflexivité de l'égalité

Tout objet est égal à lui-même.

Indépendance des variables

Une formule propositionnelle toujours fausse (antilogie) et une autre toujours vraie (tautologie) ne dépendent d'aucune variable.

A.5 Axiomes de Peano

Minimalité

Il existe un élément minimal, c'est-à-dire qu'il n'est le successeur de personne, et on le note 0.

Surjectivité

Tout objet est soit nul, soit le successeur d'un autre. La fonction "successeur" est donc surjective.

Injectivité

Si deux objets ont le même successeur, alors ces objets sont égaux. La fonction "successeur" est donc injective.

Neutralité

0 est élément neutre de l'addition.

Associativité

L'addition s'associe avec la fonction successeur.

Absorbance

0 est élément absorbant de la multiplication.

Distributivité

La multiplication se distribue sur la fonction successeur.

Récurrence

Si une propriété est vraie au rang 0, et que celle-ci est héréditaire, alors elle est universellement vraie.

A.6 Modèle

Existence de zéro

0 est un entier naturel.

Existence du successeur

Tout entier naturel possède un successeur entier naturel.

A.7 Représentation

Représentation de un

1 est le successeur de 0.

Représentation de deux

2 est le successeur de 1.

Annexe B

Grammaires non-contextuelles

Une avancée considérable en théorie des langages a été la formalisation des constructions de mots à partir de règles simples. Dans un premier temps, les automates ont vu le jour pour représenter de façon graphique un langage, avec des règles de construction. Cependant ces constructions ont été rapidement limitées par leur complexité. On a eu notamment besoin en informatique de formaliser simplement les expressions mathématiques. Les grammaires non-contextuelles ont alors vu le jour. Dès lors, les langages peuvent être construits à partir d'un simple objet de référence et de quelques règles sur les symboles que l'on s'autorise d'utiliser. Les grammaires sont très utilisées en informatique, notamment pour vérifier la cohérence syntaxique d'un programme.

B.1 Définitions

B.1.1 Grammaire non-contextuelle

Une grammaire non-contextuelle G est un quadruplet (Σ, V, S, R) tel que :
— Σ est un alphabet de symboles appelés "terminaux",
— V est un alphabet de symboles appelés "variables",
— $S \in V$ est appelé "axiome",
— $R \subset V \times (V \cup \Sigma)^*$ est un ensemble fini de "règles de dérivation".

B.1.2 Dérivée directe

Soient $u, v \in (V \cup \Sigma)^*$. On dit que u dérive de v, et on note $u \in D_v$, lorsque :

$$\exists (w_k)_{k \in [\![1,|v|]\!]} \in ((V \cup \Sigma)^*)^{|v|} \mid u = \prod_{k=1}^{|v|} w_k \wedge \forall k \in [\![1, |v|]\!], (u_k, w_k) \in R \cup \Sigma^2 \,.$$

B.1.3 Dérivée multiple

Soit $x \in V$. On note :
— $x^{(0)} = \{x\}$,
— $\forall n \in \mathbb{N}, x^{(n+1)} = \{u \in (V \cup \Sigma)^* \mid \exists v \in x^{(n)} \mid u \in D_v\}$,
— $x^{(\infty)} = \bigcup_{n=0}^{+\infty} x^{(n)}$.

B.1.4 Langage reconnu

Soit $G = (\Sigma, V, S, R)$ une grammaire non-contextuelle. Soit $u \in (V \cup \Sigma)^*$. On dit que u est reconnu par G, lorsque $u \in S^{(\infty)}$.
On note $L(G)$ le langage reconnu par G c'est-à-dire l'ensemble des mots reconnus par G :

$$L(G) = \left\{ u \in (V \cup \Sigma)^* \mid u \in S^{(\infty)} \right\}.$$

B.1.5 Exemples de grammaires

— La grammaire $G_1 = (\{b\}, \{a\}, a, \{(a, \varepsilon), (a, ab)\})$ reconnaît le langage $\{a\}^*\{b\} = \{b, ab, aab, aaab, \cdots\}$.
— La grammaire $G_2 = (\{c, d\}, \{a, b\}, a, \{(a, bc), (b, cd)\})$ reconnaît le langage $\{a, bc, cdc\}$.

B.2 Application

B.2.1 Lien potentiel avec les preuves sans mots

On peut voir une preuve comme un mot (à comprendre au sens formel du terme et non au sens usuel). Le système axiomatique de la preuve peut être vu comme l'ensemble des symboles terminaux Σ, l'ensemble des propositions mathématiques de la logique du premier ordre (isomorphe à $\mathbb{N}$ d'après le codage de Gödel) peut être vu comme l'ensemble des variables V. Une règle d'inférence au sens des arbres de preuve peut être vu comme une règle de dérivation au sens des grammaires. L'ensemble de ces règles peut alors être noté R. Puis on peut introduire un symbole abstrait S. Ainsi une assertion démontrée serait un mot reconnu par la grammaire (Σ, V, S, R). Une preuve sans mots de ce point de vue serait une grammaire reconnaissant un certain mot, ce qui n'utilise pas de mots informels, mais bien des mots formels.

B.2.2 Limites

En réalité, il n'en est rien, puisque les arbres de preuve sont construits sur des formules propositionnelles et non des assertions. La différence majeure est qu'une formule propositionnelle contient des variables propositionnelles, qui peuvent être remplacées par d'autres formules propositionnelles, tandis qu'une grammaire est construite à partir de mots ne contenant pas de "symboles variables".

Annexe C

Un système d'élaboration de preuves constructivistes

Dans cette annexe, nous proposons de construire un système d'élaboration de preuves, qui se voudront être constructivistes, puisque les objets manipulés seront construits (leur existence ne sera pas supposée sans être explicitement palpables). L'idée est de s'inspirer des grammaires non-contextuelles mais en permettant de transformer des variables en des objets mathématiques fixés. Cela permet en quelque sorte d'avoir des "symboles variables" dans des mots, tout comme l'on peut avoir des "variables propositionnelles" dans des formules propositionnelles, ou des "variables numériques" dans des expressions mathématiques.

C.1 Définitions

C.1.1 Système grammatical de preuves constructives (SGPC)

Un système grammatical de preuves constructives (abrégé dans la suite en "SGPC"), est un quadruplet (Σ, V, B, R) tel que :
- Σ est un alphabet de symboles appelés "terminaux",
- V est un alphabet de symboles appelés "variables",
- $B \subset \Sigma^*$ est appelé "base de mots",
- $R \subset ((\Sigma \cup V)^*)^2$ est un ensemble de "règles de transformation".

C.1.2 Facteur

Soient $u, f \in \Sigma^*$. On dit que f est un facteur de u lorsqu'il existe $v, v' \in \Sigma^*$ tels que $u = vfv'$.

Exemples :
- b est un facteur de $abcdexy$
- cde est un facteur de $abcdexy$
- a est un facteur de $abcdexy$
- bd n'est pas un facteur de $abcdexy$

C.1.3 Remplacement

Soient $u, f' \in \Sigma^*$. Soit $f \neq \varepsilon$ un facteur de u. On peut donc écrire u de manière unique sous la forme :

$$u = v_0 f v_1 f \cdots f v_n = v_0 \times \prod_{k=1}^{n} f v_k$$

Avec pour tout $k \in [\![0, n]\!]$, f n'est pas un facteur de v_k.
On note $u[f := f']$ le remplacement de f par f' dans u, défini par :

$$u[f := f'] = v_0 f' v_1 f' \cdots f' v_n = v_0 \times \prod_{k=1}^{n} f' v_k$$

Exemples :
— $abc[b := d] = adc$
— $axbxcxd[x := y] = aybycyd$
— $abxyzab[ab := cde] = cdexycde$
— $abcde[bcd := \varepsilon] = ae$

C.1.4 Preuve

Une preuve est une suite de mots $(u_k)_{1 \leq k \leq n}$, avec $n \in \mathbb{N}^*$, vérifiant :
— $\forall k \leq n, u_k \in (\Sigma \cup V)^*$
— $\forall k < n, \exists (f_1, f_2) \in R, (v, v') \in ((\Sigma \cup V)^*)^2 \mid (u_k = v f_1 v' \wedge u_{k+1} = v f_2 v') \vee (\exists m \in [\![1, Card(V)]\!], \exists (a_k)_k \in B^m, \exists (x_k)_k \in V^m \mid (f_1[a_k := x_k]_{k \in [\![1,m]\!]}, f_2[a_k := x_k]_{k \in [\![1,m]\!]}) \in R)$

Une preuve est donc une suite de mots, vérifiant que le couple de tout terme avec son successeur soit une règle valide. À savoir : soit il existe un axiome pour passer du premier terme vers le second, soit il est possible de remplacer des variables du premier terme par des mots de base pour obtenir le second.

C.2 Exemple de preuve

On souhaite prouver que $2 + 2 = 4$ dans un système grammatical.
On introduit certains symboles utilisés en arithmétique de Peano, des variables, et on retranscrit certains certains axiomes de Peano dans un système grammatical.

$\Sigma = \{0, 1, 2, 3, 4, s, +, (,)\}$
$V = \{x, y, z\}$
$B = \{0, 1, 2, 3, 4\}$
$R = \{(1, s(0)), (s(0), 1), (s(1), 2), (3, s(2)), (4, s(3)), (x, x + 0), (s(x + y), x + s(y)), (x + s(y), s(x + y)), (x + 0, x)\}$

La suite suivante est une preuve que $2 + 2 = 4$ dans le système grammatical (Σ, V, B, R).
$(4, s(3), s(3+0), 3+s(0), 3+1, s(2)+1, s(2+0)+1, 2+s(0)+1, 2+1+1, 2+1+s(0), 2+s(1+0), 2+s(1), 2+2)$

En effet, nous sommes partis du mot 4, et en utilisant uniquement les règles fixées au départ, on a effectué des transformations pour aboutir au mot $2+2$. La théorie des langages et les systèmes grammaticaux sont donc une façon de formaliser la manipulation des symboles au sein d'une démonstration mathématique.

On peut donc prouver l'égalité entre deux objets mathématiques à partir de règles simples. On pourrait, en choisissant un autre système axiomatique, démontrer un tas d'autres assertions. Tout cela sans utiliser de mots informels.

C.3 Limites

Les variables (dans l'exemple précédent x, y et z) permettent de remplacer les mots de la base B, sans imposer une quantification universelle sur ces derniers. Implicitement, donc, les variables sont quantifiées universellement. Ainsi, il n'y a pas d'équivalent au quantificateur existentiel dans ce système. Cela implique que ce système permet de créer des preuves constructives uniquement.
Ensuite nous n'avons pas démontré que ce système était cohérent. Ce système peut donc contenir des faiblesses et des contradictions que nous n'aurions pas remarquées.

Annexe D

Table de caractères ASCII

Voici la table de caractères ASCII pour les entiers de 0 à 127 (il existe des tables étendues plus complètes).

Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040		Space	64	40	100	@	@	96	60	140	`	`
1	1	001	SOH (start of heading)	33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
2	2	002	STX (start of text)	34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
3	3	003	ETX (end of text)	35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
4	4	004	EOT (end of transmission)	36	24	044	$	$	68	44	104	D	D	100	64	144	d	d
5	5	005	ENQ (enquiry)	37	25	045	%	%	69	45	105	E	E	101	65	145	e	e
6	6	006	ACK (acknowledge)	38	26	046	&	&	70	46	106	F	F	102	66	146	f	f
7	7	007	BEL (bell)	39	27	047	'	'	71	47	107	G	G	103	67	147	g	g
8	8	010	BS (backspace)	40	28	050	(	(	72	48	110	H	H	104	68	150	h	h
9	9	011	TAB (horizontal tab)	41	29	051	)	)	73	49	111	I	I	105	69	151	i	i
10	A	012	LF (NL line feed, new line)	42	2A	052	*	*	74	4A	112	J	J	106	6A	152	j	j
11	B	013	VT (vertical tab)	43	2B	053	+	+	75	4B	113	K	K	107	6B	153	k	k
12	C	014	FF (NP form feed, new page)	44	2C	054	,	,	76	4C	114	L	L	108	6C	154	l	l
13	D	015	CR (carriage return)	45	2D	055	-	-	77	4D	115	M	M	109	6D	155	m	m
14	E	016	SO (shift out)	46	2E	056	.	.	78	4E	116	N	N	110	6E	156	n	n
15	F	017	SI (shift in)	47	2F	057	/	/	79	4F	117	O	O	111	6F	157	o	o
16	10	020	DLE (data link escape)	48	30	060	0	0	80	50	120	P	P	112	70	160	p	p
17	11	021	DC1 (device control 1)	49	31	061	1	1	81	51	121	Q	Q	113	71	161	q	q
18	12	022	DC2 (device control 2)	50	32	062	2	2	82	52	122	R	R	114	72	162	r	r
19	13	023	DC3 (device control 3)	51	33	063	3	3	83	53	123	S	S	115	73	163	s	s
20	14	024	DC4 (device control 4)	52	34	064	4	4	84	54	124	T	T	116	74	164	t	t
21	15	025	NAK (negative acknowledge)	53	35	065	5	5	85	55	125	U	U	117	75	165	u	u
22	16	026	SYN (synchronous idle)	54	36	066	6	6	86	56	126	V	V	118	76	166	v	v
23	17	027	ETB (end of trans. block)	55	37	067	7	7	87	57	127	W	W	119	77	167	w	w
24	18	030	CAN (cancel)	56	38	070	8	8	88	58	130	X	X	120	78	170	x	x
25	19	031	EM (end of medium)	57	39	071	9	9	89	59	131	Y	Y	121	79	171	y	y
26	1A	032	SUB (substitute)	58	3A	072	:	:	90	5A	132	Z	Z	122	7A	172	z	z
27	1B	033	ESC (escape)	59	3B	073	;	;	91	5B	133	[	[	123	7B	173	{	{
28	1C	034	FS (file separator)	60	3C	074	<	<	92	5C	134	\	\	124	7C	174			|
29	1D	035	GS (group separator)	61	3D	075	=	=	93	5D	135	]	]	125	7D	175	}	}
30	1E	036	RS (record separator)	62	3E	076	>	>	94	5E	136	^	^	126	7E	176	~	~
31	1F	037	US (unit separator)	63	3F	077	?	?	95	5F	137	_	_	127	7F	177	&#127;	DEL

Source: www.LookupTables.com

Illustration D.1 –

Bibliographie

[1] *"Preuves sans mots"* de Roger B. NELSEN

[2] *"Que sait-on quand on connaît le théorème de Pythagore ?"* d'Olivier FOUQUET, Lm^B

[3] *"Chapitre 14 : Langages formels"* de Damien ROUHLING et Louis THOMAS-GIRARDET

[4] *"Chapitre 15 : Compléments de logique"* de Damien ROUHLING et Louis THOMAS-GIRARDET

[5] *"Les Mains sales"*, de Jean-Paul SARTRE

[6] *"Pour la science n°414"*, de Jean-Paul DELAHAYE

[7] ASCII Table - ASCII Character Codes

[8] Entretien avec Michaël KLOPFENSTEIN, Lm^B

[9] **Wikipédia** (liste non-exhaustive)

- Preuve sans mots
- Langage formel
- Zhoubi Suanjing
- Démonstration (logique et mathématique)
- Algèbre de Boole (logique)
- Axiomes de Peano
- Codage de Gödel

Les preuves marquées d'un * ont été pensées par les auteurs de ce mémoire.