Théorie des Ensembles et Arithmétique

Florent Michel

,

Résumé

Ce document présente quelques bases de logique mathématique, théorie des ensembles, et arithmétique. Nous nous baserons essentiellement sur la logique du premier ordre et la théorie de Zermelo–Fraenkel avec axiome du choix (ZFC). L'objectif principal est de montrer une construction possible de certains objets mathématiques courants, notamments les nombres entiers, et l'obtention de quelques-unes de leur propriétés, à partir d'idées simples.

Table des matières

Chapitre 1 : Théorie des Ensembles

> Cette partie présente quelques bases de logique mathématique et de théorie des ensembles.

1.1 Logique du premier ordre

La *logique du premier ordre*, aussi appelée *logique des prédicats* ou *calcul des prédicats du premier ordre*, est un cadre semi-formel[1] permettant de définir des théories. On peut la voir comme un langage, ou comme un ensemble d'éléments de langage. Elle est utilisée tant en mathématiques qu'en philosophie, linguistique et informatique. Nous l'aborderons ici principalement d'un point de vue mathématique. On considère ici une notion très basique du terme *langage*, que l'on considère formé de deux éléments :

- Un ensemble (au sens intuitif du terme) de *symboles*.
- Des règles de formations de *phrases* à partir des symboles.

Dans cette vision, les symboles constituent les fondations du langage, premettant de contruire les phrases, porteuses de sens.[2] On sépare parfois les symboles en deux catégories : *fondamentaux* s'ils forment un ensemble unsécable, ou *composites* s'ils sont formés d'autres symboles.

Intuitivement, la logique du premier ordre a pour symboles des variables (décrivant un domaine d'objets non logiques, c'est-à-dire non définis par la logique du premier ordre elle-même) quantifiées (par les quantificateurs « pour tout » et « il existe ») ou non, des symboles non logiques, ainsi que des connecteurs, utilisés pour construire des phrases, appelées *formules*. Ces dernières sont aussi appelées *propositions*, *énoncés* ou *prédicats*.

Elle est une extension de la *logique propositionelle*, qui exprime des énoncés, ou *propositions*, aussi appelés *prédicats*, auxquels on attribue une valeur dite de *vérité* : vrai ou faux. Chaque proposition est soit vraie soit fausse, et ne peut être les deux simultanément. Ces énoncés peuvent être liés par conjonction, disjonction, implication, équivalence, ou modifés par négation. La logique du premier ordre contient, en outre, des variables et quantificateurs, ce qui la rend plus expressive. On peut dire qu'elle contient la logique propositionelle, au sens où cette dernière est équivalente à la logique du premier ordre élaguée des variables et quantificateurs.

Une théorie définie dans le cadre de la logique du premier ordre porte sur un domaine de discours spécifié que les variables quantifiées décrivent, permettant de définir des prédicats sur ce domaine, auxquels un ensemble d'axiomes tenus pour vrais permet d'associer une valeur de vérité. Un prédicat ne peut avoir pour arguments que des variables sur ce domaine, et seules

[1] On adopte ici le point de vue que la logique du premier ordre ne repose pas sur une théorie vue comme plus fondamentale. Ses concepts fondamentaux sont ainsi définis intuitivement (puisque nous n'avons aucun concept plus fondamental qui permettrait de les définir formellement), d'où le qualificatif de « semi-formel », et non « formel ».

[2] Ce sens étant défini, *in fine*, par un élément extérieur au langage, par exemple l'intuition de qui l'utilise.

les variables peuvent être quantifiés. Cela distingue la logique du premier ordre des logiques d'ordre supérieur, où un prédicat peut avoir un prédicat plus général comme argument ou des quantificateurs de prédicats peuvent être autorisés.

Plus formellement, une théorie définie dans le cadre de la logique du premier ordre se compose des éléments suivants :

- Un *alphabet*, c'est-à-dire un ensemble (au sens intuitif du terme) de symboles, dont certaines chaînes forment des *termes*. On divise généralement les symboles et deux catégories : les *symboles logiques*, dont la signification est fixée, et les *symboles non logiques*, dont le sens n'est pas univoquement défini par la théorie et doit être défini au cas par cas. Certains de ces symboles sont définis par la logique du premier ordre ; d'autres peuvent être propres à la théorie.
- Un *domaine de discours* non vide que les variables décrivent (si x désigne une variable, la formule $\exists x \mathsf{V}$ est toujours vraie (voir ci-dessous pour la signification de cette formule)).
- Des *règles de formation*, exprimant comment construire les termes et formules. Là encore, certaines sont définies par la logique du premier ordre et d'autres peuvent être propres à la théorie.
- Des *formules* (aussi appelées *propositions*) obtenues à partir de ces règles, exprimant des prédicats. (Le terme *prédicat* est aussi utilisé pour désigner une formule elle-même.) Une proposition est toujours vraie ou fausse[3], et ne peut être simultanément vraie et fausse. Deux formules seront dites *équivalentes* si elles prennent toujours la même valeur de vérité.
  - Si f et g sont deux formules équivalentes, g et f sont équivalentes.
  - Si f et g sont trois formules telles que f et g sont équivalentes et g et h sont équivalentes, alors f et h sont équivalentes.
- Un ensemble d'*axiomes*, ou propositions tenues pour vraies. Ces axiomes permettent en général de déterminer la valeur de vérité d'autres prédicats.

1.1.1 Symboles logiques

Les symboles logiques incluent :

- Le symbole de quantification universelle $\forall$ (« pour tout »).
- Le symbole de quantification existentielle $\exists$ (« il existe »).
- Le connecteur de conjonction $\wedge$ (« et ») : si P et Q sont deux formules, $P \wedge Q$ est vraie si P et Q sont vraies et fausse sinon.
- Le connecteur de disjonction $\vee$ (« ou ») : si P et Q sont deux formules, $P \vee Q$ est vraie si P est vraie ou si Q est vraie et fausse sinon.
- Le connecteur de négation $\neg$ (« non ») : si P est une formule, $\neg P$ est vraie si P est fausse et fausse si P est vraie.
- Le connecteur d'implication $\Rightarrow$ (« implique ») : si P et Q sont deux formules, $P \Rightarrow Q$ est fausse si P est vraie et Q est fausse et vraie sinon. La formule $P \Rightarrow Q$ est ainsi équivalente à $Q \vee \neg P$ (voir ci-dessous pour la signification des parenthèses et les règles d'évaluation).
- Le connecteur $\Leftarrow$: si P et Q sont deux formules, $P \Leftarrow Q$ est fausse si P est fausse et Q est vraie et vraie sinon. La formule $P \Leftarrow Q$ est ainsi équivalente à $P \vee \neg Q$.
- Le connecteur biconditionnel $\Leftrightarrow$ (« est équivalent à ») : si P et Q sont deux formules, $P \Leftrightarrow Q$ est vraie si P et Q sont soit toutes deux vraies soit toutes deux fausses, et fausse sinon. La formule $P \Leftrightarrow Q$ est ainsi équivalente à $(P \wedge Q) \vee (\neg P \wedge \neg Q)$. Notons que, si P et Q sont deux prédicats, si $P \Leftrightarrow Q$ est vrai, alors $(\neg P) \Leftrightarrow (\neg Q)$ est vrai aussi.
- Un ensemble infini de *variables*, souvent notées par des lettres grecques ou latines, éventuellement avec des indices ou exposants. Les variables sont interprétées comme décrivant un domaine d'objets de base, qui ne peut être vide. Elles sont aussi parfois appelées *paramètres*.

On définit également les constantes de vérité V pour « vraie » et F pour « fausse ». Elles sont deux formules, et F est équivalente à $\neg \mathsf{V}$.` Si f est une formule, ces deux constantes de vérité sont équivalentes, respectivements, aux formules $f \vee (\neg f)$ et $f \wedge (\neg f)$.

Enfin, on peut définir le connecteur (non standard) de vérité $\sharp$: si f est une formule, $\sharp f$ est vraie si f est vraie et fausse sinon. (Avec ces notations, $\sharp f$ a toujours la même valeur de vérité que f. On introduit ce nouveau connecteur uniquement pour pouvoir exprimer la véracité d'une formule dans le cadre de la théorie ; il sera très peu employé dans la suite.) Ce dernier connecteur ne rendant pas la théorie plus expressive, on l'omettra dans la suite sauf mention contraire.

[3] À moins d'inclure la valeur de vérité indéfinie, voir section ??.

Pour être plus formel, on peut ne définir dans un premiers temps que les variables et constantes de vérité, puis les symboles non logiques, les termes, et enfin les autres symboles logiques avec les formules qu'ils permettent de construire et l'égalité (voir ci-dessous). On adoptera ce point de vue dans la suite. Pour le moment, les symboles logiques (y compris l'égalité définie ci-dessous) ne sont donnés que comme une liste de symboles utilisés, qui prendront leur sens lorsque les formules et la sémantique seront définies.

Si P est un prédicat à un ou plusieurs paramètres libres $a_1 a_2 \ldots$ et si $b_1 b_2 \ldots$ sont un même nombre de variables, on notera $P b_1 b_2 \ldots$, ou $P(b_1, b_2, \ldots)$ la formule obtenue en remplaçant dans P les paramètres $a_1 a_2 \ldots$ par $b_1 b_2 \ldots$.

1.1.2 Égalité

La *logique du premier ordre avec égalité* inclut un autre symbole logique, $=$, définissant une relation binaire, dite *égalité*, satisfaisant les axiomes suivants :

- Axiome de réciprocité : $\forall x\,(x = x)$.
- Réflexivité : $\forall x\,\forall y\,[(x = y) \Rightarrow (y = x)]$.
- Transitivité : $\forall x\,\forall y\,\forall z\,[((x = y) \wedge (y = z)) \Rightarrow (x = z)]$.
- Schéma d'axiomes de Leibniz : Soit P un prédicat à une variable. On a : $\forall x\,\forall y\,[(x = y) \Rightarrow (P(x) \Leftrightarrow P(y))]$.

Deux objets x et y définis par une théorie sont dits *égaux* si $x = y$. On considèrera alors qu'il s'agit du même objet. En particulier, changer l'un pour l'autre dans une formule ne modifie pas sa valeur de vérité.

Si x, y et z sont trois objets, on notera parfois par $x = y = z$ la formule $(x = y) \wedge (y = z)$.

En présence de l'égalité, on définit aussi le symbole d'*inégalité* $\neq$ définissant une relation binaire comme suit : la formule $x \neq y$ est équivalente à $\neg(x = y)$.

1.1.3 Symboles non logiques

Un symbole non logique est un symbole n'ayant pas de signification donnée par la logique du premier ordre. Il représentent généralement un prédicat, pouvant dépendre de variables placées à sa droite, éventuellement entre parenthèses.

1.1.4 Parenthèses, symboles (,), [,]

Si f est une formule, alors (f) et $[f]$ sont deux formule équivalentes à f. Nous omettrons parfois les parenthèses lorsque qu'il n'y a pas d'ambiguité sur la manière dont elles peuvent être incluses, ou lorsque les différentes manières de les inclure donnent des formules équivalentes.

L'écriture d'une formule en terme de sous-formules contient toujours des arenthèses implicites. Ainsi, si les symboles f et g désignent deux formules, si $\mathrm{C_u}$ est un connecteur unaire et $\mathrm{C_b}$ un connecteur binaire, alors la notation $\mathrm{C_u}\, f$ désigne $\mathrm{C_u}(f)$ et $f\, \mathrm{C_b}\, g$ désigne $(f)\, \mathrm{C_b}(g)$.

1.1.5 Termes

Les termes sont définis comme suit :

- Si P est un prédicat ne dépendant d'aucune variable, alors P est un terme.
- Si P est un prédicat dépendant des variables $a_1 \ldots a_N$, alors $P a_1 \ldots a_N$, aussi noté $P(a_1 \ldots a_N)$, est un terme.
- En présence de l'égalité, si x et y sont deux variables, alors $x = y$ est un terme.

Une théorie formulée dans le cadre de la logique du premier ordre peut définir de règles spécifiques de construction de prédicats, par exemple *via* des relations binaires (*cf* section 1.1.10).

1.1.6 Formules

Les formules sont définies de la manière suivante :

- Tout terme est une formule.
- Si x est une variable et f une formule dans laquelle x n'est pas quantifiée, alors $\exists x\,(f)$ et $\forall x\,(f)$ sont des formules. On les notera parfois respectivement $\exists x,\ f$ et $\forall x,\ f$ pour plus de lisibilité.
- D'autres formules sont construites à l'aide des autres symboles logiques :
  - Si f est une formule, alors $\neg(f)$ (et $\sharp(f)$, si on l'admet dans la théorie) sont des formules.

– Si f et g sont deux formules telles qu'aucune variable quantifiée dans l'une n'apparaît dans l'autre, alors $(f) \vee (g)$, $(f) \wedge (g)$, $(f) \Rightarrow (g)$, $(f) \Leftarrow (g)$ et $(f) \Leftrightarrow (g)$ sont des formules.

Une variable apparaissant dans une formule (aussi dite *paramètre* de la formule) est dite *liée* si elle est quantifiée (*i.e.*, si l'une de ses occurrences est immédiatement précédée d'un quantificateur) et *libre* si elle ne l'est pas.[4] On impose parfois (et on le fera par la suite sauf mention contraire) qu'une même variable ne puisse être quantfiée plus d'une fois dans une même formule. Si une formule F contient des variables libres $a_1 a_2 \ldots$, et si $\alpha_1 \alpha_2 \ldots$ sont autant d'éléments définis par une théorie, on note parfois $F\alpha_1\alpha_2 \ldots$ ou $F(\alpha_1\alpha_2 \ldots)$ la formule obtenue à partir de F en remplaçant $a_1 a_2 \ldots$ par $\alpha_1 \alpha_2 \ldots$. Comme annoncé ci-dessus, à chaque formule correspond une unique valeur de vérité, vraie ou fausse. Ainsi, une formule non vraie est fausse, une formule vraie est non fausse, une formule fausse est non vraie et une formule non fausse est vraie.

Une formule peut être représentée par un symbole non logique. Ce lien peut être noté par le dit symbole suivi de « : » puis de la dite formule ; on dira de ce lien qu'il *définit* le symbole non logique, qui peut alors être employé comme un terme, avec la valeur de vérité associée à la formule qui lui est liée. Une formule ne peut contenir de symbole non logique qui ne soit précédemment défini.

Parfois, une virgule « , » est utilisée pour séparer deux parties d'une formule et la rendre plus lisible, sans en modifier le sens. Chaque partie d'une formule ainsi définie doit être une formule à part entière.

Une formule faisant partie d'une autre formule est dite *sous-formule*.

NB : Un prédicat ne peut référer à un prédicat que si ce dernier est déjà défini. En particulier, il ne peut référer à lui-même, sans quoi on arrive vite à des paradoxes. (Par exemple, si on pouvait definir in prédicat P par $P : \neg P$, alors il serait vrai s'il est faux et faux s'il est vrai.)

1.1.7 Formule à nombre non spécifié de paramètres

Il est parfois utile de considérer des formules avec un nombre non spécifié de variables. Celles-ci peuvent alors être collectivement désignés par une suite de symboles séparés de points de suspensions, par exemple $a_1 \cdots a_p$. Notons formellement S cette séquence. Les notations $\forall S$ et $\exists S$ désignent, respectivement, les séquences de quantification universelles et existentielles pour chacune des variables. Ainsi,

- Si la séquence S est vide, *i.e.* ne contient aucune variable, alors $\forall S$ et $\exists S$ ne représentent rien : si f est une formule, $\forall S\ f$ et $\exists\ f$ représentent simplement f.
- Si $S = a$ où a est une variable, $\forall S$ représente $\forall a$ et $\exists S$ représente $\exists a$.
- Si $S = ab$ où a et b sont deux variables, $\forall S$ représente $\forall a \forall b$ et $\exists S$ représente $\exists a \exists b$.
- Si $S = a_1 a_2 \cdots a_p$ où a_1, a_2, ..., a_p sont des variables, $\forall S$ représente $\forall a_1 \forall a_2 \ldots \forall a_p$ et $\exists S$ représente $\exists a_1 \exists a_2 \ldots \exists a_p$.

1.1.8 Quantificateur d'unicité

En logique du premier ordre avec égalité, on définit le quantificateur $\exists!$ de la manière suivante : si P est un prédicat à un paramètre libre x et d'éventuels autres paramètres dénotés par $a_1 \ldots a_p$, la formule $\exists!\ x\ Pxa_1 \ldots a_p$ est équivalente à $(\exists x\ Pxa_1 \ldots a_p) \wedge (\forall x \forall y\,(Pxa_1 \ldots a_p \wedge Pya_1 \ldots a_p) \Rightarrow (x = y))$.

Moins formellement, on définit l'unicité de la manière suivante : dans le cadre d'une théorie définie en logique du premier ordre avec égalité, si P est un prédicat à un paramètre libre, on dira qu'*il existe au plus un unique objet satisfaisant P* si et seulement si le prédicat suivant est vrai :

$$\forall x\, \forall y\, (P(x) \wedge P(y)) \Rightarrow (x = y)\,.$$

On dira qu'*il existe exactement un objet satisfaisant P* si et seulement si le prédicat suivant est vrai :

$$(\forall x\, \forall y\, (P(x) \wedge P(y)) \Rightarrow (x = y)) \wedge (\exists x\ P(x))\,.$$

Ce dernier pourra être abrégé en :

$$\exists!\ x\ P(x)\,.$$

[4] Afin de simplifier les tournures de phrases, on parlera parfois, quand il n'y a pas de confusion possible, simplement de « variables » ou « paramètres » d'une formule pour désigner ses variables libres.

1.1.9 Sémantique

Les règles énoncées ci-dessus, complétées par des règles propres à chaque théorie, permettent (au moins dans certains cas) d'attribuer une *valeur de vérité* à une formule. Les parenthèses (et) (ou [et]), indiquent que, pour évaluer la valeur d'une formule (vraie ou fausse), la formule délimitée par la premiere (à gauche) et la seconde (à droite) est évaluée en tant que formule indépendante. Si une formule est construite à partir d'autres formules, sa valeur peut dépendre des leurs, et peut être explicitée par une table de vérité (voir ci-dessous).

Cinq autres règles sont :

- Les variables n'ont pas de sens intrinsèque. Ainsi, si f est une formule faisant intervenir une variable x, et si y est une variable n'apparaissant pas dans f, alors remplacer toutes les occurrences de x par y dans f ne peut modifier sa valeur de vérité : la formule ainsi obtenue est équivalente à f. On considèrera parfois que la formule obtenue est la même (ou que les deux séquences de symboles représentent la même formule).
- Si f est une formule et x et y deux variables qui ne sont pas quantifiées dans f, alors les formules $\forall x\, \forall y\, f$ et $\forall y \forall x\, f$ sont équivalentes.
- La valeur de vérité d'une formule est inchangée par le remplacement d'une sous-formule par une formule équivalente.
- Si une formule peut s'écrire comme une séquence de sous-formules et de connecteurs telle qu'elle prend toujours la même valeur de vérité lorsque ces sous-formules sont remplacées indépendamment par V ou par F, alors elle prend cette valeur de vérité, et est équivalente à V si vraie ou à F si fausse.

On omet parois les parenthèses dans une formule lorsque celles-ci ne modifie pas sa valeur de vérité ; l'ordre d'évaluation des differents termes d'une formule est alors déterminé par les règles suivantes :

- L'évaluation s'effectue de gauche à droite sauf si cela est contraire à une des règles ci-dessous.
- Les prédicats sont évalués en premier.
- Lorsqu'une parenthèse ouvrante est atteinte, la formule se trouvant entre elle et la parenthèse fermante correspondante est évaluée en priorité.
- Ordre d'évaluation des connecteurs et quantificateurs : d'abords les quantificateurs $\exists$ et $\forall$, puis $\neg$, puis (en présence de l'égalité) $=$, puis $\wedge$ et $\vee$ (avec la même priorité), puis $\Rightarrow$, $\Leftarrow$ et $\Leftrightarrow$ (avec la même priorité).

Un connecteur binaire C est dit *transitif* si, pour toutes formules f, g et h, les formules $(f \,\mathrm{C}\, g) \,\mathrm{C}\, h$ et $\mathrm{C}(g \,\mathrm{C}\, h)$ sont équivalentes. Un connecteur binaire C est dit *symmétrique* si, pour toutes formules f et g, les formules $f \,\mathrm{C}\, g$ et $g \,\mathrm{C}\, f$ sont équivalentes.

Dans la suite, si C désigne un connecteur transitif et si f, g et h sont trois formules, on omettra parfois les parenthèses dans des formules de la forme $(f \,\mathrm{C}\, g) \,\mathrm{C}\, h$ ou $f\, \mathrm{C}(g \,\mathrm{C}\, h)$. Plus généralement, on omettra parfois les parenthèses lorsque toutes les manières d'ajouter des parenthèses pour obtenir une formule correctement formée donnent des formules équivalentes.

Si f est une formule et x une variable n'apparaissant pas comme variable liée dans f, la formule $\exists x f$ est vraie s'il existe au moins une valeur possible pour x telle que la formule obtenue en remplaçant x par cette valeur dans f est vraie, et fausse si toutes les formules obtenues en remplaçant x par chacune de ses valeurs possible sont fausses. Sous les mêmes conditions, la formule $\forall x f$ est fausse s'il existe au moins une valeur possible pour x telle que la formule obtenue en remplaçant x par cette valeur dans f est fausse, et vraie si toutes les formules obtenues en remplaçant x par chacune de ses valeurs possible sont vraies. On formalise cela par les règles suivantes :

- si x est une variable et f une formule dans laquelle x n'apparait pas, $\forall x\, f$ est équivalente à f ;
- pour toute variable x et toute formule f, la formule $\forall x\, f$ est équivalente à $\neg(\exists x\ \neg f)$;
- soit f une formule admettant exactement $a_1 a_2 \ldots a_n$ pour paramètres libres ; si $\forall a_1\, \forall a_2 \cdots \forall a_n\, f$ est vraie, alors f est équivalente à V ;
- en présence de l'égalité, si $f(x)$ est une formule à un paramètre libre éventuel x et a un objet, alors $\exists x\,(x = a) \wedge f(x)$ est équivalente à $f(a)$.

Ainsi, par exemple, si f est une formule et x une variable, la formule $\forall x\,(f \Leftrightarrow f)$ est vraie. En effet,

- la formule $f \Leftrightarrow f$ est vraie que f soit vraie ou fausse, donc elle est équivalente à V,
- la formule $\forall x\,(f \Leftrightarrow f)$ est donc éuivalente à $\forall x\, \mathsf{V}$, donc à V, et donc vraie.

Quelques conséquences immédiates sont (en remplaçant f par $\neg f$ et en notant que $\neg(\neg f))$ est équivalente à f pour toute formule f) :

- Si f est une formule et x et y deux variables qui ne sont pas quantifiées dans f, alors les formules $\exists x\, \exists y\, f$ et $\exists y\, \exists x\, f$ sont équivalentes.
- si x est une variable, alors $\exists x\, \mathsf{F}$ est fausse (en effet, sa négation est $\forall x\, \mathsf{V}$, qui est vraie) et $\exists x\, \mathsf{V}$ est vraie (en effet, sa négation est $\forall x\, \mathsf{F}$, qui est fausse) ;
- soit f une formule admettant exactement $a_1 a_2 \ldots a_n$ pour paramètres libres ; si $\exists a_1\, \exists a_2 \cdots \exists a_n\, f$ est fausse, alors f est équivalente à F ;
- soit f et g deux formules à un paramètre libre ; les formules $(\forall x\, f(x)) \wedge (\forall y\, g(y))$ et $\forall x\, (f(x) \wedge g(x))$ sont équivalentes [5] ; em soit f et g deux formules à un paramètre libre ; si $\forall x\, f(x)$ est vraie, alors les formules $\forall x\, (f(x) \wedge g(x))$ et $\forall x\, g(x)$ sont équivalentes ;
- soit f et g deux formules à un paramètre libre ; si $\exists x\, f(x)$ est fausse, alors les formules $\forall x\, (f(x) \vee g(x))$ et $\forall x\, g(x)$ sont équivalentes (en effet, $\forall x\, \neg f(x)$ est alors vraie, donc f est équivalente à F, et donc $f(x) \vee g(x)$ à $g(x)$) ;
- soit f et g deux formules à un paramètre libre ; si $\exists x\, f(x)$ est fausse, alors la formule $\forall x\, (f(x) \wedge g(x))$ est fausse ;
- soit f et g deux formules à un paramètre libre ; si $\forall x\, f(x)$ est vraie, alors la formule $\forall x\, (f(x) \vee g(x))$ est vraie ;
- soit f une formule à un paramètre libre ; si $\forall x\, f(x)$ est vraie, alors la formule $\exists x\, f(x)$ est vraie ;
- si x est une variable et f une formule dans laquelle x n'apparait pas, $\exists x\, f$ est équivalente à f (en effet, x n'apparait pas dans f, donc $\forall x\, \neg f$ est équivalente à $\neg f$, donc $\neg(\forall x\, \neg f)$ est équivalente à f, et donc $\exists x\, f$ à f) ;
- pour toute variable x et toute formule f dans laquelle x n'est pas une variable quantifiée, la formule $\exists x\, f$ est équivalente à $\neg(\forall x\, \neg f)$.
- soit f et g deux formules à un paramètre libre ; les formules $(\exists x\, f(x)) \vee (\exists y\, g(y))$ et $\exists x\, (f(x) \vee g(x))$ sont équivalentes ;
- soit f et g deux formules et x une variable ; si $\forall x\, f$ et $\forall x\, (f \Rightarrow g)$ sont vraies, alors $\forall x\, g$ est vraie (puisqu'alors $\forall x\, (f \wedge (f \Rightarrow g))$ est vraie) ;
- soit x une variable et f et g deux formules (faisant ou non intervenir x) ; si $\forall x\, f$ et $\exists x\, (f \Rightarrow g)$ sont vraies, alors $\exists x\, g$ est vraie (en effet, $\forall x\, \neg(f \Rightarrow g)$ est fausse, donc $\forall x\, (f \wedge \neg g)$ est fausse, donc $(\forall y\, f) \wedge (\forall x\, \neg g)$ est fausse ; puisque $\forall y\, f$ est vraie, on en déduit que $\forall x\, \neg g$ est fausse, et donc que $\exists x\, g$ est vraie) ;
- soit x une variable et f et g deux formules (faisant ou non intervenir x) ; si $\exists x\, f$ et $\forall x\, (f \Rightarrow g)$ sont vraies, alors $\exists x\, g$ est vraie (en effet, $\forall x\, (g \vee \neg f)$ est vraie, donc, si $\exists x\, g$ était fausse, on aurait $\forall x\, ((g \vee \neg f) \wedge (\neg g))$, donc $\forall x\, \neg f$, ce qui n'est pas le cas puisque $\exists x\, f(x)$ est vraie).

Stricto sensu, il est donc possible de se passer d'un de ces deux quantificateurs, ou de voir l'un d'eux comme fondamental et l'autre comme dérivé. Par exemple, on peut voir le quantificateur $\exists$ comme le seul quantificateur fondamental, et définir $\forall$ *via* l'équivalence de $\forall x\, f$ et $\neg(\exists x\, \neg f)$ pour toute variable x et toute formule f.

Attention : Une formule vraie (au sens où sa valeur de vérité est « vrai ») n'est pas nécessairement équivalente à V. De même, une formule faussee (au sens où sa valeur de vérité est « faux ») n'est pas nécessairement équivalente à F. Par contre, une formule équivalente à V est nécessairement vraie et une formule équivalente à F nécessairement fausse.

1.1.10 Relations binaires

Une théorie définie dans le cadre de la logique du premier ordre peut inclure des relations binaires entre les objets de son domaine de discours, chacune étant représentée par un symbole. Si x et y sont deux variables, et $\boldsymbol{R}$ le symbole dénotant une relation binaire, alors $x\ \boldsymbol{R}\ y$ est un terme. L'égalité est un exemple de reation binaire, avec pour symbole $=$.

Soit $\boldsymbol{P}$ un prédicat dépendant de deux variables. On peut définir une relation binaire $\boldsymbol{R}$ par la formule

$$\forall x \forall y\, ((x\ \boldsymbol{R}\ y) \Leftrightarrow \boldsymbol{P}xy),$$

[5] En effet,

- Si $(\forall x\, f(x)) \wedge (\forall y\, g(y))$ est vraie, alors $\forall x\, f(x)$ et $\forall y\, g(y)$ sont vraies, donc f et g sont équivalentes à V, donc $f(x) \wedge g(x)$ également, donc $\forall x\, f(x) \wedge g(x)$ est vraie.
- Si $(\forall x\, f(x)) \wedge (\forall y\, g(y))$ est fausse, alors $\forall x\, f(x) \wedge g(x)$ doit être fausse. En effet, si elle était vraie, alors $f(x) \wedge g(x)$ serait équivalente à V, donc f et g également, et donc $(\forall x\, f(x)) \wedge (\forall y\, g(y))$ serait vraie.

ignifiant que, pour chaque x et chaque y, $x \; R \; y$ est vrai si et seulement si Pxy est vrai. Autrement dit, cette formule signiie que les prédicats Pxy et $x \; R \; y$ sont équivalents.

Lors de l'évaluation d'une formule, et sauf mention contraire, les relations binaires autres que l'égalité sont prioritaires sur cette dernière, mais pas sur le connecteur $\neq$.

1.1.11 Réciproque

Soit f et g deux formules n'ayant pas de quantificateur et $P : f \Rightarrow g$. On suppose que le connecteur reliant f et g peut être évalué en dernier. La *réciproque* de P est la formule $g \Rightarrow f$.

Plus généralement, on définit la réciproque d'une formule formée de variables quantifiées et d'une formule de cette forme par celle obtenue en prenant la contraposée de cette dernière : si Q est une séquence de variables quantifiées (de la forme $\forall a_1 \ldots \forall a_n \exists b_1 \ldots \exists b_m \ldots$, où les formules $\forall a_1 \ldots \forall a_n$ et $\forall b_1 \ldots \forall b_m$ sont comprises comme pouvant contenir chacune, et indépendamment, aucune, une seule, ou plusieurs variables quantifiées), la réciproque de la formule $Q\, f \to q$ est $Q\, g \Rightarrow f$.

1.1.12 Contraposée

Soit f et g deux formules n'ayant pas de quantificateur et $P : f \Rightarrow g$. On suppose que le connecteur reliant f et g peut être évalué en dernier. La *contraposée* de P est la formule $\neg\, g \Rightarrow \neg\, f$. La formule P et sa contraposée ont toujours la même valeur de vérité (elles sont vraies si f est fausse ou g est vraie et fausses sinon).

Plus généralement, on définit la contraposée d'une formule formée de variables quantifiées et d'une formule de cette forme par celle obtenue en prenant la contraposée de cette dernière : si Q est une séquence de variables quantifiées (de la forme $\forall a_1 \ldots \forall a_n \exists b_1 \ldots \exists b_m \ldots$, où les formules $\forall a_1 \ldots \forall a_n$ et $\forall b_1 \ldots \forall b_m$ sont comprises comme pouvant contenir chacune, et indépendamment, aucune, une seule, ou plusieurs variables quantifiées), la contraposée de la formule $Qf \to q$ est $Q(\neg\, g \Rightarrow \neg\, f)$. La contraposée d'une formule a toujours la même valeur de vérité que la formule initiale.

1.1.13 NAND et NOR

Notons que chacun des connecteurs peut être construit à l'aide d'un unique connecteur, que l'on note ici $\circ$, appelé *NAND*, définit de la manière suivante : si f et g sont deux formules, alors $f \circ g$ est une formule, vraie si et seulement si f et g ne sont pas toutes deux vraies. En effet, si f et g sont deux formules, et en considérant que deux formules sont équivalentes si elles prennent toujours la même valeur,

- $\neg\, f$ est équivalente à $f \circ f$,
- $f \wedge g$ est équivalente à $\neg(f \circ g)$,
- $f \vee g$ est équivalente à $(\neg\, f) \circ (\neg\, g)$,
- $f \Rightarrow g$ est équivalente à $(\neg\, f) \vee g$,
- $f \Leftarrow g$ est équivalente à $f \vee (\neg\, g)$,
- $f \Leftrightarrow g$ est équivalente à $(f \wedge g) \vee ((\neg\, f) \wedge (\neg\, g))$.

Un tel connecteur, permettant de construire tous les autres, est dit *universel*.

Il existe un autre connecteur universel, appelé *NOR*, que l'on note dans ce paragraphe $\times$, défini par : si f et g sont deux formules, alors $f \circ g$ est une formule, vraie si et seulement si f et g sont toutes deux fausses. En effet, si f et g sont deux formules, $\neg\, f$ est équivalente à $f \times f$ et $f \wedge g$ à $(\neg\, f) \times (\neg\, g)$, donc $f \circ g$ est équivalente à $[(f \times f) \times (g \times g)] \times [(f \times f) \times (g \times g)]$. Puisque le connecteur $\circ$ est universel, le connecteur $\times$ l'est donc aussi.

1.1.14 XOR

On définit le connecteur *XOR*, noté $\oplus$, de la manière suivante : si f et g sont deux formules, alors $f \oplus g$ est une formule vraie si f est vraie et g est fausse ou si f est fausse et g est vraie, et fausse sinon. Si f et g sont deux formules, alors $f \oplus g$ est équivalente à $f \Leftrightarrow (\neg\, g)$.

L'utilité du connecteur XOR découle des trois propriétés suivantes :

- Il est *symétrique* : si f et g sont deux formules, $f \oplus g$ est équivalente à $g \oplus f$ (en effet, toutes deux sont vraies si une des formules f et g est vraie et l'autre est fausse, et fausse sinon).
- Il est *transitif* : si f, g et h sont trois formules, $(f \oplus g) \oplus h$ est équivalente à $f \oplus (g \oplus h)$ (en effet, toutes deux sont vraies soit si les trois formules f, g et h sont vraies ou si une d'entre elles est vraie et les deux autres sont fausses, et fausses sinon).
- Soit f une formule, $f \oplus f$ est toujours fausse.

Notons aussi que, si f est une formule, $f \oplus \mathsf{F}$ est équivalente à f et $f \oplus \mathsf{V}$ à $\neg f$.

1.1.15 Tables de vérité

Les valeurs de formules construites à partir d'autres formules peuvent être consignées dans des tableaux appelés *tables de vérité*, contenant sur la première ligne plusieurs formules et sur les autres leurs valeurs (un tiret indiquant qu'elle peut prendre la valeur vraie ou fausse). En voici un exemple, pour deux formules f et g :

f	g	$\neg f$	$f \wedge g$	$f \vee g$	$f \Rightarrow g$	$f \Leftarrow g$	$f \Leftrightarrow g$
F	F	V	F	F	V	V	V
F	V	V	F	V	V	F	F
V	F	F	F	V	F	V	F
V	V	F	V	V	V	V	V

On peut utiliser des tables de vérités pour montrer l'équivalence entre plusieurs formules. Montrons par exemple les trois propriétés énoncées Section 1.1.14. Pour trois formules f, g et h, on a :

f	g	h	$f \oplus g$	$g \oplus f$	$(f \oplus g) \oplus h$	$f \oplus (g \oplus h)$	$f \oplus f$
F	F	F	F	F	F	F	F
F	F	V	F	F	V	V	F
F	V	F	V	V	V	V	F
F	V	V	V	V	F	F	F
V	F	F	V	V	V	V	F
V	F	V	V	V	F	F	F
V	V	F	F	F	F	F	F
V	V	V	F	F	V	V	F

On remarque, comme attendu, que

- Les formules $f \oplus g$ et $g \oplus f$ prennent toujours la même valeur.
- Les formules $(f \oplus g) \oplus h$ et $f \oplus (g \oplus h)$ prennent toujours la même valeur.
- La formule $f \oplus f$ est toujours fausse.

Chapitre 2 : Introduction

2.1 Welcome

This is the first section of the introduction. We are demonstrating various ConTeXt features. We can refer to specific words like ConTeXt, document, and features. Let's include some mathematics: $E = mc^2$. This uses the $E = mc^2$Einstein's mass-energy equivalence XITS Math font. Another equation: $a^2 + b^2 = c^2$.

2.1.1 Getting Started

Here's a subsection.

2.1.1.1 Installation

Details about installation.

2.2 Overview

This section provides an overview.

2.2.1 Structure

The document structure.

Chapitre 3 : Advanced Topics

3.1 Font Handling

ConTeXt's font handling is very powerful. We're using XITS for text and math.

3.1.1 Font Features

Exploring OpenType features. Some more math: $\int_{-\infty}^{\infty} e^{-x^2} dx = \sqrt{\pi}$. We can also index symbols like $\int$ integral sign.

$$e = \frac{mc^2}{\sqrt{1 - v^2/c^2}}$$

3.2 Indexing

This section is about creating indices. We can index more words, like LuaTeX and OpenType.

Chapitre 4 : Conclusion

4.1 Summary

A brief summary of the document.

4.2 Next Steps

What to do next.

Appendice A : Some C++ code

```cpp
void negacyclic_ntt_pow2_bit_reversed(
    const uint64_t* const input,
    uint64_t* const output,
    const uint64_t* const powers_root_unity,
    const uint64_t modulus,
    const size_t ntt_size,
    const size_t batch_size = 1);
```

Appendice B : Jeux avec les entiers

B.1 Liste des premiers nombres premiers

2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107 109 113 127 131 137 139 149 151 157 163 167 173 179 181 191 193 197 199 211 223 227 229 233 239 241 251 257 263 269 271 277 281 283 293 307 311 313 317 331 337 347 349 353 359 367 373 379 383 389 397 401 409 419 421 431 433 439 443 449 457 461 463 467 479 487 491 499 503 509 521 523 541 547 557 563 569 571 577 587 593 599 601 607 613 617 619 631 641 643 647 653 659 661 673 677 683 691 701 709 719 727 733 739 743 751 757 761 769 773 787 797 809 811 821 823 827 829 839 853 857 859 863 877 881 883 887 907 911 919 929 937 941 947 953 967 971 977 983 991 997 1009 1013 1019 1021 1031 1033 1039 1049 1051 1061 1063 1069 1087 1091 1093 1097 1103 1109 1117 1123 1129 1151 1153 1163 1171 1181 1187 1193 1201 1213 1217 1223 1229 1231 1237 1249 1259 1277 1279 1283 1289 1291 1297 1301 1303 1307 1319 1321 1327 1361 1367 1373 1381 1399 1409 1423 1427 1429 1433 1439 1447 1451 1453 1459 1471 1481 1483 1487 1489 1493 1499 1511 1523 1531 1543 1549 1553 1559 1567 1571 1579 1583 1597 1601 1607 1609 1613 1619 1621 1627 1637 1657 1663 1667 1669 1693 1697 1699 1709 1721 1723 1733 1741 1747 1753 1759 1777 1783 1787 1789 1801 1811 1823 1831 1847 1861 1867 1871 1873 1877 1879 1889 1901 1907 1913 1931 1933 1949 1951 1973 1979 1987 1993 1997 1999 2003 2011 2017 2027 2029 2039 2053 2063 2069 2081 2083 2087 2089 2099 2111 2113 2129 2131 2137 2141 2143 2153 2161 2179 2203 2207 2213 2221 2237 2239 2243 2251 2267 2269 2273 2281 2287 2293 2297 2309 2311 2333 2339 2341 2347 2351 2357 2371 2377 2381 2383 2389 2393 2399 2411 2417 2423 2437 2441 2447 2459 2467 2473 2477 2503 2521 2531 2539 2543 2549 2551 2557 2579 2591 2593 2609 2617 2621 2633 2647 2657 2659 2663 2671 2677 2683 2687 2689 2693 2699 2707 2711 2713 2719 2729 2731 2741 2749 2753 2767 2777 2789 2791 2797 2801 2803 2819 2833 2837 2843 2851 2857 2861 2879 2887 2897 2903 2909 2917 2927 2939 2953 2957 2963 2969 2971 2999 3001 3011 3019 3023 3037 3041 3049 3061 3067 3079 3083 3089 3109 3119 3121 3137 3163 3167 3169 3181 3187 3191 3203 3209 3217 3221 3229 3251 3253 3257 3259 3271 3299 3301 3307 3313 3319 3323 3329 3331 3343 3347 3359 3361 3371 3373 3389 3391 3407 3413 3433 3449 3457 3461 3463 3467 3469 3491 3499 3511 3517 3527 3529 3533 3539 3541 3547 3557 3559 3571 3581 3583 3593 3607 3613 3617 3623 3631 3637 3643 3659 3671 3673 3677 3691 3697 3701 3709 3719 3727 3733 3739 3761 3767 3769 3779 3793 3797 3803 3821 3823 3833 3847 3851 3853 3863 3877 3881 3889 3907 3911 3917 3919 3923 3929 3931 3943 3947 3967 3989 4001 4003 4007 4013 4019 4021 4027 4049 4051 4057 4073 4079 4091 4093 4099 4111 4127 4129 4133 4139 4153 4157 4159 4177 4201 4211 4217 4219 4229 4231 4241 4243 4253 4259 4261 4271 4273 4283 4289 4297 4327 4337 4339 4349 4357 4363 4373 4391 4397 4409 4421 4423 4441 4447 4451 4457 4463 4481 4483 4493 4507 4513 4517 4519 4523 4547 4549 4561 4567 4583 4591 4597 4603 4621 4637 4639 4643 4649 4651 4657 4663 4673 4679 4691 4703 4721 4723 4729 4733 4751 4759 4783 4787 4789 4793 4799 4801 4813 4817 4831 4861 4871 4877 4889 4903 4909 4919 4931 4933 4937 4943 4951 4957 4967 4969 4973 4987 4993 4999 5003 5009 5011 5021 5023 5039 5051 5059 5077 5081 5087 5099 5101 5107 5113 5119 5147 5153 5167 5171 5179 5189 5197 5209 5227 5231 5233 5237 5261 5273 5279 5281 5297 5303 5309 5323 5333 5347 5351 5381 5387 5393 5399 5407 5413 5417 5419 5431 5437 5441 5443 5449 5471 5477 5479 5483 5501 5503 5507 5519 5521 5527 5531 5557 5563 5569 5573 5581 5591 5623 5639 5641 5647 5651 5653 5657 5659 5669 5683 5689 5693 5701 5711 5717 5737 5741 5743 5749 5779 5783 5791 5801 5807 5813 5821 5827 5839 5843 5849 5851 5857 5861 5867 5869 5879 5881 5897 5903 5923 5927 5939 5953 5981 5987 6007 6011 6029 6037 6043 6047 6053 6067 6073 6079 6089 6091 6101 6113 6121 6131 6133 6143 6151 6163 6173 6197 6199 6203 6211 6217 6221 6229 6247 6257 6263 6269 6271 6277 6287 6299 6301 6311 6317 6323 6329 6337 6343 6353 6359 6361 6367 6373 6379 6389 6397 6421 6427 6449 6451 6469 6473 6481 6491 6521 6529 6547 6551 6553 6563 6569 6571 6577 6581 6599 6607 6619 6637 6653 6659 6661 6673 6679 6689 6691 6701 6703 6709 6719 6733 6737 6761 6763 6779 6781 6791 6793 6803 6823 6827 6829 6833 6841 6857 6863 6869 6871 6883 6899 6907 6911 6917 6947 6949 6959 6961 6967 6971 6977 6983 6991 6997 7001 7013 7019 7027 7039 7043 7057 7069 7079 7103 7109 7121 7127 7129 7151 7159 7177 7187 7193 7207 7211 7213 7219 7229 7237 7243 7247 7253 7283 7297 7307 7309 7321 7331 7333 7349 7351 7369 7393 7411 7417 7433 7451 7457 7459 7477 7481 7487 7489 7499 7507 7517 7523 7529 7537 7541 7547 7549 7559 7561 7573 7577 7583 7589 7591 7603 7607 7621 7639 7643 7649 7669 7673 7681 7687 7691 7699 7703 7717 7723 7727 7741 7753 7757 7759 7789 7793 7817 7823 7829 7841 7853 7867 7873 7877 7879 7883 7901 7907 7919 7927 7933 7937 7949 7951 7963 7993 8009 8011 8017 8039 8053 8059 8069 8081 8087 8089 8093 8101 8111 8117 8123 8147 8161 8167 8171 8179 8191 8209 8219 8221 8231 8233 8237 8243 8263 8269 8273 8287 8291 8293 8297 8311 8317 8329 8353 8363 8369 8377 8387 8389 8419 8423 8429 8431 8443 8447 8461 8467 8501 8513 8521 8527 8537 8539 8543 8563 8573 8581 8597 8599 8609 8623 8627 8629 8641 8647 8663 8669 8677 8681 8689 8693 8699 8707 8713 8719 8731 8737 8741 8747 8753 8761 8779 8783 8803 8807 8819 8821 8831 8837 8839 8849 8861 8863 8867 8887 8893 8923 8929 8933 8941 8951 8963 8969 8971 8999 9001 9007 9011 9013 9029 9041 9043 9049 9059 9067 9091 9103 9109 9127 9133 9137 9151 9157 9161 9173 9181 9187 9199 9203 9209 9221 9227 9239 9241 9257 9277 9281 9283 9293 9311 9319 9323 9337 9341 9343 9349 9371 9377 9391 9397 9403 9413 9419 9421 9431 9433 9437

B.2 Décomposition des premiers entiers en produits de facteurs premiers

$2 = 2^1$
$3 = 3^1$
$4 = 2^2$
$5 = 5^1$
$6 = 2^1 \times 3^1$
$7 = 7^1$
$8 = 2^3$
$9 = 3^2$
$10 = 2^1 \times 5^1$
$11 = 11^1$
$12 = 2^2 \times 3^1$
$13 = 13^1$
$14 = 2^1 \times 7^1$
$15 = 3^1 \times 5^1$
$16 = 2^4$
$17 = 17^1$
$18 = 2^1 \times 3^2$
$19 = 19^1$
$20 = 2^2 \times 5^1$
$21 = 3^1 \times 7^1$
$22 = 2^1 \times 11^1$
$23 = 23^1$
$24 = 2^3 \times 3^1$
$25 = 5^2$
$26 = 2^1 \times 13^1$
$27 = 3^3$
$28 = 2^2 \times 7^1$
$29 = 29^1$
$30 = 2^1 \times 3^1 \times 5^1$
$31 = 31^1$
$32 = 2^5$
$33 = 3^1 \times 11^1$
$34 = 2^1 \times 17^1$
$35 = 5^1 \times 7^1$
$36 = 2^2 \times 3^2$
$37 = 37^1$
$38 = 2^1 \times 19^1$
$39 = 3^1 \times 13^1$
$40 = 2^3 \times 5^1$
$41 = 41^1$
$42 = 2^1 \times 3^1 \times 7^1$
$43 = 43^1$
$44 = 2^2 \times 11^1$
$45 = 3^2 \times 5^1$
$46 = 2^1 \times 23^1$
$47 = 47^1$
$48 = 2^4 \times 3^1$
$49 = 7^2$
$50 = 2^1 \times 5^2$
$51 = 3^1 \times 17^1$
$52 = 2^2 \times 13^1$
$53 = 53^1$
$54 = 2^1 \times 3^3$
$55 = 5^1 \times 11^1$
$56 = 2^3 \times 7^1$
$57 = 3^1 \times 19^1$
$58 = 2^1 \times 29^1$
$59 = 59^1$
$60 = 2^2 \times 3^1 \times 5^1$
$61 = 61^1$
$62 = 2^1 \times 31^1$
$63 = 3^2 \times 7^1$
$64 = 2^6$
$65 = 5^1 \times 13^1$
$66 = 2^1 \times 3^1 \times 11^1$
$67 = 67^1$
$68 = 2^2 \times 17^1$
$69 = 3^1 \times 23^1$
$70 = 2^1 \times 5^1 \times 7^1$
$71 = 71^1$
$72 = 2^3 \times 3^2$
$73 = 73^1$
$74 = 2^1 \times 37^1$
$75 = 3^1 \times 5^2$
$76 = 2^2 \times 19^1$
$77 = 7^1 \times 11^1$
$78 = 2^1 \times 3^1 \times 13^1$
$79 = 79^1$
$80 = 2^4 \times 5^1$
$81 = 3^4$
$82 = 2^1 \times 41^1$
$83 = 83^1$
$84 = 2^2 \times 3^1 \times 7^1$
$85 = 5^1 \times 17^1$
$86 = 2^1 \times 43^1$
$87 = 3^1 \times 29^1$
$88 = 2^3 \times 11^1$
$89 = 89^1$
$90 = 2^1 \times 3^2 \times 5^1$
$91 = 7^1 \times 13^1$
$92 = 2^2 \times 23^1$
$93 = 3^1 \times 31^1$
$94 = 2^1 \times 47^1$
$95 = 5^1 \times 19^1$
$96 = 2^5 \times 3^1$
$97 = 97^1$
$98 = 2^1 \times 7^2$
$99 = 3^2 \times 11^1$
$100 = 2^2 \times 5^2$
$101 = 101^1$
$102 = 2^1 \times 3^1 \times 17^1$
$103 = 103^1$
$104 = 2^3 \times 13^1$
$105 = 3^1 \times 5^1 \times 7^1$
$106 = 2^1 \times 53^1$
$107 = 107^1$
$108 = 2^2 \times 3^3$
$109 = 109^1$
$110 = 2^1 \times 5^1 \times 11^1$
$111 = 3^1 \times 37^1$
$112 = 2^4 \times 7^1$
$113 = 113^1$
$114 = 2^1 \times 3^1 \times 19^1$
$115 = 5^1 \times 23^1$
$116 = 2^2 \times 29^1$
$117 = 3^2 \times 13^1$
$118 = 2^1 \times 59^1$
$119 = 7^1 \times 17^1$
$120 = 2^3 \times 3^1 \times 5^1$
$121 = 11^2$
$122 = 2^1 \times 61^1$
$123 = 3^1 \times 41^1$
$124 = 2^2 \times 31^1$
$125 = 5^3$
$126 = 2^1 \times 3^2 \times 7^1$
$127 = 127^1$
$128 = 2^7$
$129 = 3^1 \times 43^1$
$130 = 2^1 \times 5^1 \times 13^1$
$131 = 131^1$
$132 = 2^2 \times 3^1 \times 11^1$
$133 = 7^1 \times 19^1$
$134 = 2^1 \times 67^1$
$135 = 3^3 \times 5^1$
$136 = 2^3 \times 17^1$
$137 = 137^1$
$138 = 2^1 \times 3^1 \times 23^1$
$139 = 139^1$
$140 = 2^2 \times 5^1 \times 7^1$
$141 = 3^1 \times 47^1$
$142 = 2^1 \times 71^1$
$143 = 11^1 \times 13^1$
$144 = 2^4 \times 3^2$
$145 = 5^1 \times 29^1$
$146 = 2^1 \times 73^1$
$147 = 3^1 \times 7^2$
$148 = 2^2 \times 37^1$
$149 = 149^1$
$150 = 2^1 \times 3^1 \times 5^2$
$151 = 151^1$
$152 = 2^3 \times 19^1$
$153 = 3^2 \times 17^1$
$154 = 2^1 \times 7^1 \times 11^1$
$155 = 5^1 \times 31^1$
$156 = 2^2 \times 3^1 \times 13^1$
$157 = 157^1$
$158 = 2^1 \times 79^1$
$159 = 3^1 \times 53^1$
$160 = 2^5 \times 5^1$
$161 = 7^1 \times 23^1$
$162 = 2^1 \times 3^4$
$163 = 163^1$
$164 = 2^2 \times 41^1$
$165 = 3^1 \times 5^1 \times 11^1$
$166 = 2^1 \times 83^1$
$167 = 167^1$
$168 = 2^3 \times 3^1 \times 7^1$
$169 = 13^2$
$170 = 2^1 \times 5^1 \times 17^1$
$171 = 3^2 \times 19^1$
$172 = 2^2 \times 43^1$
$173 = 173^1$
$174 = 2^1 \times 3^1 \times 29^1$
$175 = 5^2 \times 7^1$
$176 = 2^4 \times 11^1$
$177 = 3^1 \times 59^1$
$178 = 2^1 \times 89^1$
$179 = 179^1$
$180 = 2^2 \times 3^2 \times 5^1$
$181 = 181^1$
$182 = 2^1 \times 7^1 \times 13^1$
$183 = 3^1 \times 61^1$
$184 = 2^3 \times 23^1$
$185 = 5^1 \times 37^1$
$186 = 2^1 \times 3^1 \times 31^1$
$187 = 11^1 \times 17^1$
$188 = 2^2 \times 47^1$
$189 = 3^3 \times 7^1$
$190 = 2^1 \times 5^1 \times 19^1$
$191 = 191^1$
$192 = 2^6 \times 3^1$
$193 = 193^1$
$194 = 2^1 \times 97^1$
$195 = 3^1 \times 5^1 \times 13^1$
$196 = 2^2 \times 7^2$
$197 = 197^1$
$198 = 2^1 \times 3^2 \times 11^1$
$199 = 199^1$
$200 = 2^3 \times 5^2$
$201 = 3^1 \times 67^1$
$202 = 2^1 \times 101^1$
$203 = 7^1 \times 29^1$
$204 = 2^2 \times 3^1 \times 17^1$
$205 = 5^1 \times 41^1$
$206 = 2^1 \times 103^1$
$207 = 3^2 \times 23^1$
$208 = 2^4 \times 13^1$
$209 = 11^1 \times 19^1$
$210 = 2^1 \times 3^1 \times 5^1 \times 7^1$
$211 = 211^1$
$212 = 2^2 \times 53^1$
$213 = 3^1 \times 71^1$
$214 = 2^1 \times 107^1$
$215 = 5^1 \times 43^1$
$216 = 2^3 \times 3^3$
$217 = 7^1 \times 31^1$
$218 = 2^1 \times 109^1$
$219 = 3^1 \times 73^1$
$220 = 2^2 \times 5^1 \times 11^1$
$221 = 13^1 \times 17^1$
$222 = 2^1 \times 3^1 \times 37^1$
$223 = 223^1$
$224 = 2^5 \times 7^1$
$225 = 3^2 \times 5^2$
$226 = 2^1 \times 113^1$
$227 = 227^1$
$228 = 2^2 \times 3^1 \times 19^1$
$229 = 229^1$
$230 = 2^1 \times 5^1 \times 23^1$
$231 = 3^1 \times 7^1 \times 11^1$
$232 = 2^3 \times 29^1$
$233 = 233^1$
$234 = 2^1 \times 3^2 \times 13^1$
$235 = 5^1 \times 47^1$
$236 = 2^2 \times 59^1$
$237 = 3^1 \times 79^1$
$238 = 2^1 \times 7^1 \times 17^1$
$239 = 239^1$
$240 = 2^4 \times 3^1 \times 5^1$
$241 = 241^1$
$242 = 2^1 \times 11^2$
$243 = 3^5$
$244 = 2^2 \times 61^1$
$245 = 5^1 \times 7^2$
$246 = 2^1 \times 3^1 \times 41^1$
$247 = 13^1 \times 19^1$
$248 = 2^3 \times 31^1$
$249 = 3^1 \times 83^1$
$250 = 2^1 \times 5^3$
$251 = 251^1$

Cette décomposition est utile pour calculer le nombre de diviseurs $\varphi(n)$ d'un entier naturel non nul n : $\varphi(1) = 1$ et, pour tour entier naturel n strictement supérieur à 1, $\varphi(n)$ est égal au produit des puissances apparaissant dans la décomposition de n augmentées de 1. Cela est représenté figure B.1 et figure B.2. (Le code utilisé dans cette section se trouve dans le fichier **decomposition_prime_factors.rs**.)

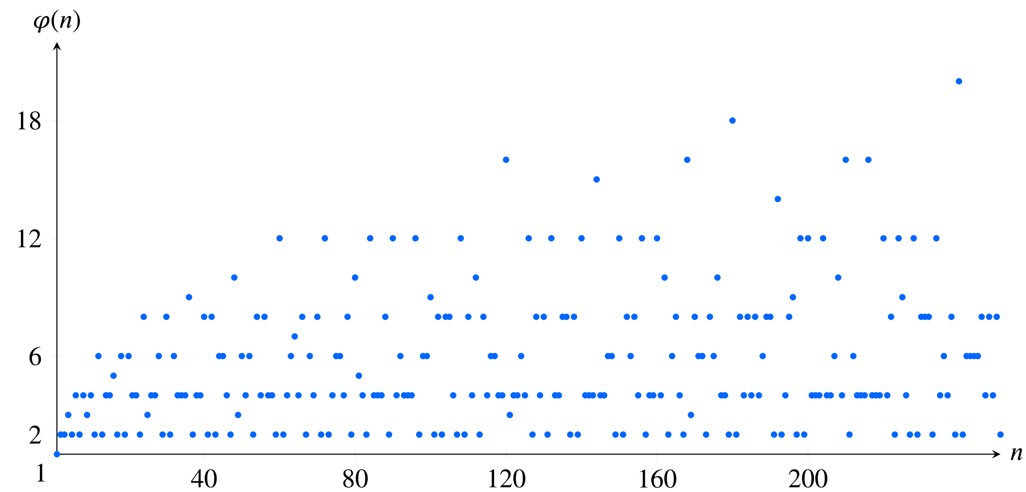

Figure B.1 Nombre de diviseurs d'un entier naturel non nul n, noté $\varphi(n)$, en fonction de n pour n allant de 1 à 251. Notons que $\varphi(1) = 1$ et, pour tout entier naturel non nul n, $\varphi(n) = 2$ si et seulement si n est premier.

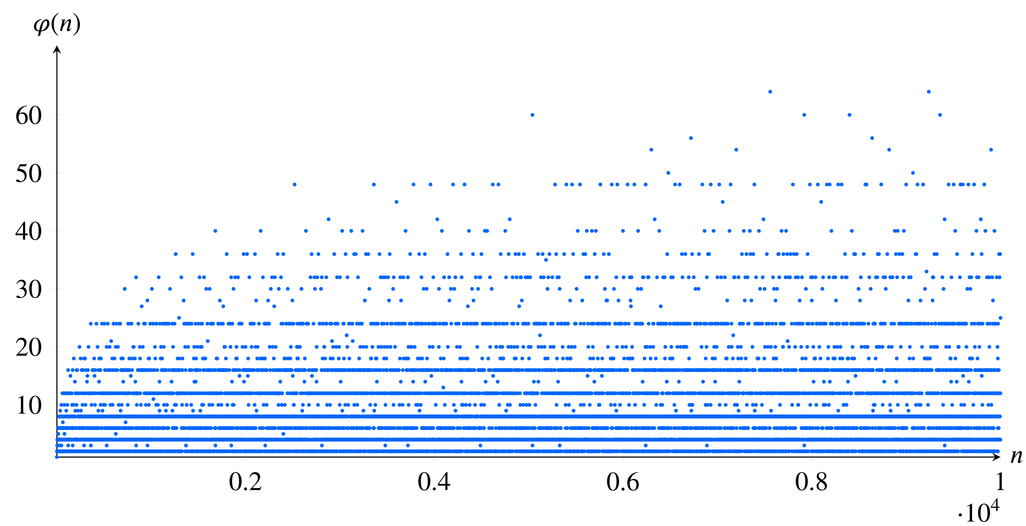

Figure B.2 Même plot que sur la figure B.1 pour n allant de 1 à 10000.

B.3 Une séquence de nombres pseudo-aléatoire

La séquence de nombres suivante sera (avec une très haute probabilité) différent à chaque compilation de ce document. (Il y a 10^{4278} possibilités différentes.)

3499361295118712461212728208230182383960454635059317518867723639864839667388864897360365139540
0986230273313736537867525536433232333418142268316526085067354146901869627000996108027259137086
4021181509014975463412004379504850159278851223277093670505776429414435890041138962356377393612
4116851598019241243170814776310413050373209009479628958155172953516445309560591073884649346500
7421959841411803220428724538475081007819072135469147635619148656092011987247705325215591348977
0069632467909001983376074733233295213220302157815853072358514184169389846714133540120279116124
0040296105907323990731934593685423832917110367155682060316637934343964389311117271640064666509
2193689381321502257617057246301975850636129299482257792372235541381536136193351182571234007030
7700896846320913420056754239325446120956401953377079023168324255398267465621208413748032997169
8971123337235913082894279817865905683219067051779225986617959497328294856217525936269397510808
8199455896072346450505624472597581234840067831795300624436184088643796969295713949156449644027
1602676981447175899672530087365066614463196750783306589172505691698708268901463044039327271937
6005727280893888419563500918764468346886701771803831983787951128552418039958924076664627510971
3280456511656369851825012452207195738590670499799843857108379188865945195166832090293553426928
6187226093319366485946222897560684473840718717632729542578265460000621044422941213164990578014
6225481746373569163059331852763284008443638974163632834700088660437183584786377986044089098674
4381157149354581794593191307386087948395911575558960108887816816223813052665491348272522636508
8275870832410426370606944917634480958759715872870520942814709364435149611684437120363816763983
2057271957286263449110097152573428352176284067056900248599688355898240801725192395632508128149
2959749576402048321692889149913115252826510798840317651553071969328789148363806057894469502712
6208678983296657700682649286597541968572199727276607841446911546729218993126765704990315926302
3424598751517550654478226214928885260492650597528674362117025439124476893160611922703742712639
6365454110795027218342613146013482165721431732503684256902283303059603412920358325392831265282
4880628834599547010327223267214720326780166197987327720235122021754405494634346363286003032815
4790739316774842548569696991807934229871398922981306347489275203220488155731954764825025387872
6677633760819623506865877176121031906237253279019963110820644266101143231021514025088738192263
6391313982039229406591342059521774633137420989977452480844670491335708501522130754326524903950
1018400536654247254633144292708572764318610160564034488982233857266575121332723328500929375606
5717477242246814327740273915554932965413906782828906835509399732897190829334600893954395121220
3123822299806530601763418925259147966482526204656796800677816719032426719765156850665120188254
7151021415047100557985213604817981782361080052517503966645004540459679929776269041903210084388
3153583351624727186715434624560512984704167704968240531781482620264937635362098055155976726553
9551358010575689987965221983994909874256363278845687142099600251208923592129691121042914269169
1960003264833947985418285008287139041284065638882763986493829357949978778878128175323988901504
2201578896311241272561429762615110157749390019484134184844520514993735074413130871383080664340
8235481970236908655567364853468832908293638416616772868835069968391820522875084318591024886260
0979467084615555939223451638175058176193251002656975725867086622386611007421212411035910858214
1114844893467243636226342788306132178488149999974196813966620993404955156181955539774517311306
6901733579632502001704127702557425729827450557648473436863295161202372549121735232666397149344
5452107097251280414532240764685569890135810864915329867413330495544059540065628269878476544491
2071698196323714549007598957006583491308584749426887984416867766168961733767664999636657066322
8711573826668139263097176858641793794828653256083395653180654062442573895634709530313904271217
5452548406843951396101076970693344983456792635722836173365938376668556205012555452662844483104
6860819318018155841025275742569121127217509637403449329313220003560100946367036423388616186581
9235255183529114984451385372861121542402987729445999596384803755131727857885304591885937030039
8860085864809055242728472778191389600943295885026652266573729310632764807923767087147783863886
4230672918729480188910078063467700028778057385164550203413279160185345164988151789245532925348

Index

Index des symboles