Une petite balade dans le premier ordre

Friedrich Wehrung

Université de Caen
LMNO, CNRS UMR 6139
Département de Mathématiques
14032 Caen cedex
E-mail: friedrich.wehrung01@unicaen.fr
URL: https://wehrungf.users.lmno.cnrs.fr

Canopé Caen, le 8 mars 2023

“Premier ordre” ?

- Se réfère à “logique du premier ordre”, “structures du premier ordre”.

“Premier ordre”?

- Se réfère à “logique du premier ordre”, “structures du premier ordre”.
- “Logique”? Domaine de mathématiques qui traite les énoncés et raisonnements mathématiques comme des objets mathématiques (tels les nombres, ensembles, relations).

"Premier ordre"?

- Se réfère à "logique du premier ordre", "structures du premier ordre".
- "Logique"? Domaine de mathématiques qui traite les énoncés et raisonnements mathématiques comme des objets mathématiques (tels les nombres, ensembles, relations).
- "Premier ordre"? Quantifie sur les éléments (par opposition aux sous-ensembles).

Centaures

- *Échecs avancés*: opposent deux "centaures" homme + machine.

Centaures

- *Échecs avancés*: opposent deux "centaures" homme + machine.
- Exemples de centaures en mathématiques:

Centaures

- *Échecs avancés*: opposent deux "centaures" homme + machine.
- Exemples de centaures en mathématiques:
- *Conjecture de Guthrie / Théorème des 4 couleurs* (Appel et Haken, 1976); 1478 cas critiques, 1200 heures de calcul (*source*: Wikipedia). Beaucoup amélioré depuis, mais assistance informatique inévitable pour le moment.

Centaures

- *Échecs avancés*: opposent deux “centaures” homme + machine.
- Exemples de centaures en mathématiques:
- *Conjecture de Guthrie / Théorème des 4 couleurs* (Appel et Haken, 1976); 1478 cas critiques, 1200 heures de calcul (*source*: Wikipedia). Beaucoup amélioré depuis, mais assistance informatique inévitable pour le moment.
- *Conjecture de Kepler / Théorème de Hales* sur les empilements de sphères; prouvé en 1998, certifié en 2014.

Centaures

- *Échecs avancés*: opposent deux "centaures" homme + machine.
- Exemples de centaures en mathématiques:
- *Conjecture de Guthrie / Théorème des 4 couleurs* (Appel et Haken, 1976); 1478 cas critiques, 1200 heures de calcul (*source*: Wikipedia). Beaucoup amélioré depuis, mais assistance informatique inévitable pour le moment.
- *Conjecture de Kepler / Théorème de Hales* sur les empilements de sphères; prouvé en 1998, certifié en 2014.
- *"Unit conjecture" de Kaplansky / Théorème de Gardam* (2021).

L'outil en question ici

- **Avertissement**: ceci n'est pas un exposé d'informatique!

L'outil en question ici

- **Avertissement**: ceci n'est pas un exposé d'informatique!
- L'assistant de preuve en question ici est `Prover9-Mace4`, `https://www.cs.unm.edu/~mccune/prover9/` (MacOS, Windows, Linux), créé par William McCune (Décembre 1953–Mai 2011)

L'outil en question ici

- **Avertissement**: ceci n'est pas un exposé d'informatique!
- L'assistant de preuve en question ici est `Prover9-Mace4`, `https://www.cs.unm.edu/~mccune/prover9/` (MacOS, Windows, Linux), créé par William McCune (Décembre 1953–Mai 2011)

L'outil en question ici

- **Avertissement**: ceci n'est pas un exposé d'informatique!
- L'assistant de preuve en question ici est `Prover9-Mace4`, `https://www.cs.unm.edu/~mccune/prover9/` (MacOS, Windows, Linux), créé par William McCune (Décembre 1953–Mai 2011)

- Voir aussi le site `http://proverx.com`

Introduction

- Un exemple fondamental:

Introduction

- Un exemple fondamental:
- $2 + 2 = 4$

Introduction

- Un exemple fondamental:
- $2 + 2 = 4$
- Comment le prouver?

Introduction

- Un exemple fondamental:
- $2 + 2 = 4$
- Comment le prouver?
- . . . .

Introduction

- Un exemple fondamental:
- $2 + 2 = 4$
- Comment le prouver?
- . . . .
- GOTO assistant de preuve, `Prover9-Mace4`

Approcher le problème

$+$	0	1	2	3	4
0	0	0	0	0	0
1	0	0	0	0	0
2	0	0	0	0	0
3	0	0	0	0	0
4	0	0	0	0	0

Table: Premier contrexemple

Approcher le problème

$+$	0	1	2	3	4
0	0	0	0	0	0
1	0	0	0	0	0
2	0	0	0	0	0
3	0	0	0	0	0
4	0	0	0	0	0

Table: Premier contrexemple

Donc $2 + 2$, ça ferait en fait 0 ?!

Définir les objets

- Nombres ordinaux:

Définir les objets

- Nombres ordinaux:
- $2 = 1 + 1,\ 3 = 2 + 1,\ 4 = 3 + 1,\ \ldots$

Définir les objets

- Nombres ordinaux:
- $2 = 1 + 1,\ 3 = 2 + 1,\ 4 = 3 + 1,\ \ldots$

$+$	0	1	2	3	4
0	0	0	0	0	0
1	0	2	0	0	0
2	0	3	0	0	0
3	0	4	0	0	0
4	0	0	0	0	0

Table: Second contrexemple

Définir les objets

- Nombres ordinaux:
- $2 = 1 + 1$, $3 = 2 + 1$, $4 = 3 + 1$, ...

$+$	0	1	2	3	4
0	0	0	0	0	0
1	0	2	0	0	0
2	0	3	0	0	0
3	0	4	0	0	0
4	0	0	0	0	0

Table: Second contrexemple

Bizarre, $2 + 2$ continue de faire 0 !

Qu'avons-nous oublié?

- Nous avons bien décrit 1, 2, 3, 4 . . .

Qu'avons-nous oublié?

- Nous avons bien décrit 1, 2, 3, 4 . . .
- . . . **mais nous n'avons rien dit sur** $+$ **!**

Qu'avons-nous oublié?

- Nous avons bien décrit 1, 2, 3, 4 ...
- ... **mais nous n'avons rien dit sur + !**
- Nous avons défini $\_ + 1 \ldots$

Qu'avons-nous oublié?

- Nous avons bien décrit 1, 2, 3, 4 ...
- ... **mais nous n'avons rien dit sur $+$!**
- Nous avons défini $\_ + 1$...
- ... mais pas $\_ + 2$!

Qu'avons-nous oublié?

- Nous avons bien décrit 1, 2, 3, 4 ...
- ...**mais nous n'avons rien dit sur + !**
- Nous avons défini $\_ + 1\ldots$
- ...mais pas $\_ + 2$!
- Essayons donc $x + 2 = (x + 1) + 1$.

Qu'avons-nous oublié?

- Nous avons bien décrit 1, 2, 3, 4 ...
- ... **mais nous n'avons rien dit sur + !**
- Nous avons défini $\_ + 1$...
- ... mais pas $\_ + 2$!
- Essayons donc $x + 2 = (x + 1) + 1$.
- **Ça marche!** En plus ça donne une preuve.

Qu'avons-nous oublié?

- Nous avons bien décrit 1, 2, 3, 4 ...
- ... **mais nous n'avons rien dit sur $+$!**
- Nous avons défini $\_ + 1$...
- ... mais pas $\_ + 2$!
- Essayons donc $x + 2 = (x + 1) + 1$.
- **Ça marche!** En plus ça donne une preuve.
- **Pour résumer**: pour une bonne description du problème, il nous faut

$$
\begin{aligned}
2 &= 1 + 1. \\
3 &= 2 + 1. \\
4 &= 3 + 1. \\
x + 2 &= (x + 1) + 1.
\end{aligned}
$$

La nécessité d'axiomes

- Let "x" ci-dessus peut être n'importe quel entier naturel: lire $(\forall x)(x + 2 = (x + 1) + 1)$.

La nécessité d'axiomes

- Let "x" ci-dessus peut être n'importe quel entier naturel: lire $(\forall x)(x + 2 = (x + 1) + 1)$.
- Le signe $\forall$ se lit "Quel que soit": quantification universelle.

La nécessité d'axiomes

- Let "x" ci-dessus peut être n'importe quel entier naturel: lire $(\forall x)(x + 2 = (x + 1) + 1)$.
- Le signe $\forall$ se lit "Quel que soit": quantification universelle.
- Que doit-on présupposer (axiomes!) pour **tous** les problèmes (disons d'arithmétique; $2 + 3 = 5$ etc.)?

La nécessité d'axiomes

- Let "x" ci-dessus peut être n'importe quel entier naturel: lire $(\forall x)(x + 2 = (x + 1) + 1)$.
- Le signe $\forall$ se lit "Quel que soit": quantification universelle.
- Que doit-on présupposer (axiomes!) pour **tous** les problèmes (disons d'arithmétique; $2 + 3 = 5$ etc.)?
- Revient à demander une bonne description de l'addition (et autres) sur les entiers naturels, $\mathbb{N} = \{0, 1, 2, \dots\}$,

La nécessité d'axiomes

- Let "x" ci-dessus peut être n'importe quel entier naturel: lire $(\forall x)(x + 2 = (x + 1) + 1)$.
- Le signe $\forall$ se lit "Quel que soit": quantification universelle.
- Que doit-on présupposer (axiomes!) pour **tous** les problèmes (disons d'arithmétique; $2 + 3 = 5$ etc.)?
- Revient à demander une bonne description de l'addition (et autres) sur les entiers naturels, $\mathbb{N} = \{0, 1, 2, \dots\}$, suffisante pour $2 + 3 = 5$, ..., $x^2 \neq 2y^2$, $\dots x^n + y^n \neq z^n$, etc.

Axiomes de Peano (semi-formellement)

- Tout peut être décrit par la constante 0 et la fonction successeur s, c.à.d. $s(0) = 1$,

Axiomes de Peano (semi-formellement)

- Tout peut être décrit par la constante 0 et la fonction successeur s, c.à.d. $s(0) = 1$, $s(1) = 2$,

Axiomes de Peano (semi-formellement)

- Tout peut être décrit par la constante 0 et la fonction successeur s, c.à.d. $s(0) = 1$, $s(1) = 2$, $s(2) = 3$,

Axiomes de Peano (semi-formellement)

- Tout peut être décrit par la constante 0 et la fonction successeur s, c.à.d. $s(0) = 1$, $s(1) = 2$, $s(2) = 3$, $s(3) = 4$, etc.

Axiomes de Peano (semi-formellement)

- Tout peut être décrit par la constante 0 et la fonction successeur s, c.à.d. $s(0) = 1$, $s(1) = 2$, $s(2) = 3$, $s(3) = 4$, etc.
- La partie "du premier ordre" :

$$\begin{aligned}(\forall x)(sx \neq 0)\,;\\ (\forall x)\big(x = 0 \text{ ou } (\exists y)(x = sy)\big)\,;\\ (\forall x)(\forall y)(sx = sy \Rightarrow x = y)\,,\end{aligned}$$

Axiomes de Peano (semi-formellement)

- Tout peut être décrit par la constante 0 et la fonction successeur s, c.à.d. $s(0) = 1$, $s(1) = 2$, $s(2) = 3$, $s(3) = 4$, etc.
- La partie "du premier ordre" :

$$
\begin{aligned}
(\forall x)(sx \neq 0)\,; \\
(\forall x)\bigl(x = 0 \text{ ou } (\exists y)(x = sy)\bigr)\,; \\
(\forall x)(\forall y)(sx = sy \Rightarrow x = y)\,,
\end{aligned}
$$

où $(\exists y)(x = sy)$ se lit "il existe y tel que $x = sy$".

Axiomes de Peano (semi-formellement)

- Tout peut être décrit par la constante 0 et la fonction successeur s, c.à.d. $s(0)=1$, $s(1)=2$, $s(2)=3$, $s(3)=4$, etc.
- La partie “du premier ordre” :

$$\begin{aligned} (\forall x)(sx \neq 0)\,; \\ (\forall x)\big(x = 0 \text{ ou } (\exists y)(x = sy)\big)\,; \\ (\forall x)(\forall y)(sx = sy \Rightarrow x = y)\,, \end{aligned}$$

où $(\exists y)(x = sy)$ se lit “il existe y tel que $x = sy$”.

- La partie “du second ordre” est le schéma d'induction:

$$\Big(\big(P(0) \text{ et } (\forall x)(P(x) \Rightarrow P(sx))\big)\Big) \Rightarrow (\forall x)P(x)\,,$$

pour toute propriété P.

Débuts prometteurs. . .

- 0, s **définissent tout le reste!**

Débuts prometteurs...

- 0, s **définissent tout le reste!**
- $x + 0 = x$, $x + sy = s(x + y)$ définissent l'addition $+$.

Débuts prometteurs...

- 0, s **définissent tout le reste!**
- $x + 0 = x$, $x + sy = s(x + y)$ définissent l'addition $+$. On définit $1 = s0$, du coup $sx = x + 1$.

Débuts prometteurs...

- **0, s définissent tout le reste!**
- $x+0=x$, $x+sy=s(x+y)$ définissent l'addition $+$. On définit $1=s0$, du coup $sx=x+1$.
- $x\cdot 0=0$, $x\cdot(y+1)=x\cdot y+x$ définissent la multiplication $\cdot$.

Débuts prometteurs...

- **0, s définissent tout le reste!**
- $x + 0 = x$, $x + sy = s(x + y)$ définissent l'addition $+$. On définit $1 = s0$, du coup $sx = x + 1$.
- $x \cdot 0 = 0$, $x \cdot (y + 1) = x \cdot y + x$ définissent la multiplication $\cdot$.
- Exponentiation: $x^0 = x$, $x^{y+1} = x^y \cdot x$. Etc etc.

Débuts prometteurs...

- **0, s définissent tout le reste!**
- $x+0=x$, $x+sy=s(x+y)$ définissent l'addition $+$. On définit $1=s0$, du coup $sx=x+1$.
- $x\cdot 0=0$, $x\cdot(y+1)=x\cdot y+x$ définissent la multiplication $\cdot$.
- Exponentiation: $x^0=x$, $x^{y+1}=x^y\cdot x$. Etc etc.
- L'ordre naturel: $x\leq y$ signifie alors $(\exists z)(x+z=y)$.

Débuts prometteurs...

- **0, s définissent tout le reste!**
- $x + 0 = x$, $x + sy = s(x + y)$ définissent l'addition $+$. On définit $1 = s0$, du coup $sx = x + 1$.
- $x \cdot 0 = 0$, $x \cdot (y + 1) = x \cdot y + x$ définissent la multiplication $\cdot$.
- Exponentiation: $x^0 = x$, $x^{y+1} = x^y \cdot x$. Etc etc.
- L'ordre naturel: $x \leq y$ signifie alors $(\exists z)(x + z = y)$.
- Le Schéma d'induction se lit alors:

Débuts prometteurs...

- **0, s définissent tout le reste!**
- $x+0=x$, $x+sy=s(x+y)$ définissent l'addition $+$. On définit $1=s0$, du coup $sx=x+1$.
- $x\cdot 0=0$, $x\cdot(y+1)=x\cdot y+x$ définissent la multiplication $\cdot$.
- Exponentiation: $x^0=x$, $x^{y+1}=x^y\cdot x$. Etc etc.
- L'ordre naturel: $x\leq y$ signifie alors $(\exists z)(x+z=y)$.
- Le Schéma d'induction se lit alors:
- Si une propriété est vraie en 0, et sa véracité en n entraîne celle en $n+1$, alors elle est vraie partout (*exemple*: pair / impair).

Débuts prometteurs. . .

- **0, s définissent tout le reste!**
- $x+0=x$, $x+sy=s(x+y)$ définissent l'addition $+$. On définit $1=s0$, du coup $sx=x+1$.
- $x\cdot 0=0$, $x\cdot(y+1)=x\cdot y+x$ définissent la multiplication $\cdot$.
- Exponentiation: $x^0=x$, $x^{y+1}=x^y\cdot x$. Etc etc.
- L'ordre naturel: $x\leq y$ signifie alors $(\exists z)(x+z=y)$.
- Le Schéma d'induction se lit alors:
- Si une propriété est vraie en 0, et sa véracité en n entraîne celle en $n+1$, alors elle est vraie partout (*exemple*: pair / impair). *Variante:*

Débuts prometteurs. . .

- **0, s définissent tout le reste!**
- $x + 0 = x$, $x + sy = s(x + y)$ définissent l'addition $+$. On définit $1 = s0$, du coup $sx = x + 1$.
- $x \cdot 0 = 0$, $x \cdot (y + 1) = x \cdot y + x$ définissent la multiplication $\cdot$.
- Exponentiation: $x^0 = x$, $x^{y+1} = x^y \cdot x$. Etc etc.
- L'ordre naturel: $x \leq y$ signifie alors $(\exists z)(x + z = y)$.
- Le Schéma d'induction se lit alors:
- Si une propriété est vraie en 0, et sa véracité en n entraîne celle en $n + 1$, alors elle est vraie partout (*exemple*: pair / impair). *Variante:*
- Toute propriété satisfaisable (dans $\mathbb{N}$) admet une solution la plus petite possible.

. . . puis le crash!

Cette dernière formulation, à l'apparence inoffensive, cause de gros problèmes.

. . . puis le crash!

Cette dernière formulation, à l'apparence inoffensive, cause de gros problèmes.

Paradoxe de Berry

. . . puis le crash!

Cette dernière formulation, à l'apparence inoffensive, cause de gros problèmes.

Paradoxe de Berry

"Le plus petit entier non-définissable en moins de 100 mots."

. . . puis le crash!

Cette dernière formulation, à l'apparence inoffensive, cause de gros problèmes.

Paradoxe de Berry

"Le plus petit entier non-définissable en moins de 100 mots."

?!

. . . puis le crash!

Cette dernière formulation, à l'apparence inoffensive, cause de gros problèmes.

Paradoxe de Berry

"Le plus petit entier non-définissable en moins de 100 mots."

?!

Donc: nous en tenir au premier ordre pour le moment!

Opérations sur les ensembles (les “patates”)

- On se donne un ensemble E; “$x \in E$” se lit “x appartient à E”, “$x \notin E$” se lit “x n'appartient pas à E”.

Opérations sur les ensembles (les “patates”)

- On se donne un ensemble E; “$x \in E$” se lit “x appartient à E”, “$x \notin E$” se lit “x n'appartient pas à E”.
- Pour tous sous-ensembles A et B de E, on pose

$$
\begin{aligned}
A \cup B &= \{x \in E \mid x \in A \text{ ou } x \in B\}\,;\\
A \cap B &= \{x \in E \mid x \in A \text{ et } x \in B\}\,;\\
\complement A &= \{x \in E \mid x \notin A\}\,.
\end{aligned}
$$

Opérations sur les ensembles (les "patates")

- On se donne un ensemble E; "$x \in E$" se lit "x appartient à E", "$x \notin E$" se lit "x n'appartient pas à E".
- Pour tous sous-ensembles A et B de E, on pose

$$\begin{aligned} A \cup B &= \{x \in E \mid x \in A \text{ ou } x \in B\}\,; \\ A \cap B &= \{x \in E \mid x \in A \text{ et } x \in B\}\,; \\ \complement A &= \{x \in E \mid x \notin A\}\,. \end{aligned}$$

- On peut alors montrer des propriétés élémentaires, comme

$$\begin{aligned} A \cup (B \cup C) &= (A \cup B) \cup C\,; \\ A \cap (B \cup C) &= (A \cap B) \cup (A \cap C)\,; \\ \complement\complement A &= A\,; \\ \complement(A \cup B) &= (\complement A) \cap (\complement B)\,; \end{aligned}$$

etc.

Algèbres de Boole

Deux symboles d'opérations binaires, $\vee$ et $\wedge$, et deux symboles de constante, 0 et 1. Dans ce qui suit, quantificateurs universels $\forall$ omis. On prend donc du recul par rapport au concept de tribu (en probabilités).

Algèbres de Boole

Deux symboles d'opérations binaires, $\vee$ et $\wedge$, et deux symboles de constante, 0 et 1. Dans ce qui suit, quantificateurs universels $\forall$ omis. On prend donc du recul par rapport au concept de tribu (en probabilités).

$$
\text{(treillis)}\begin{cases}
(x \vee y) \vee z = x \vee (y \vee z)\,; \\
x \vee y = y \vee x\,; \\
x \vee x = x\,; \\
(x \wedge y) \wedge z = x \wedge (y \wedge z)\,; \\
x \wedge y = y \wedge x\,; \\
x \wedge x = x\,; \\
x \wedge (x \vee y) = x \vee (x \wedge y) = x\,.
\end{cases}
$$

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)\,;$$

$$x \wedge \neg x = 0\,;\ x \vee \neg x = 1\,.$$

Algèbres de Robbins

- Identités (*faire précéder par* $(\forall x)(\forall y)(\forall z)$):

$$\begin{aligned}(x \vee y) \vee z &= x \vee (y \vee z)\,;\\ x \vee y &= y \vee x\,;\\ \neg(\neg(x \vee y) \vee \neg(x \vee \neg y)) &= x\,.\end{aligned}$$

Algèbres de Robbins

- Identités (*faire précéder par* $(\forall x)(\forall y)(\forall z)$):

$$\begin{aligned} (x \vee y) \vee z &= x \vee (y \vee z)\,; \\ x \vee y &= y \vee x\,; \\ \neg(\neg(x \vee y) \vee \neg(x \vee \neg y)) &= x\,. \end{aligned}$$

- Toute algèbre de Boole est une algèbre de Robbins (exercice).

Algèbres de Robbins

- Identités (*faire précéder par* $(\forall x)(\forall y)(\forall z)$):

$$\begin{aligned} (x \vee y) \vee z &= x \vee (y \vee z)\,; \\ x \vee y &= y \vee x\,; \\ \neg(\neg(x \vee y) \vee \neg(x \vee \neg y)) &= x\,. \end{aligned}$$

- Toute algèbre de Boole est une algèbre de Robbins (exercice).
- Problème de la réciproque posé par Herbert Robbins en 1933.

Solution de la conjecture de Robbins

- Nombreuses tentatives infructueuses, par de nombreux mathématiciens dont Huntington, Robbins, Tarski.

Solution de la conjecture de Robbins

- Nombreuses tentatives infructueuses, par de nombreux mathématiciens dont Huntington, Robbins, Tarski.
- Problème finalement résolu (positivement!) en 1996 par William McCune, qui a pour cela développé le logiciel de preuve automatique EQP.

Solution de la conjecture de Robbins

- Nombreuses tentatives infructueuses, par de nombreux mathématiciens dont Huntington, Robbins, Tarski.
- Problème finalement résolu (positivement!) en 1996 par William McCune, qui a pour cela développé le logiciel de preuve automatique EQP.
- McCune a ensuite développé EQP, qui est devenu le système de preuve / constructeur d'exemples Prover9-Mace4.

Exemples d'utilisation (groupes)

- Un groupe consiste en un ensemble G, muni d'une opération binaire (= "loi de composition interne") $*$, une constante e ("élément neutre"), une opération unaire $\_^{-1}$, satisfaisant les lois $x * (y * z) = (x * y) * z$, $x * e = e * x = x$, et $x * x^{-1} = x^{-1} * x = e$ (pour tous x, y, z).

Exemples d'utilisation (groupes)

- Un groupe consiste en un ensemble G, muni d'une opération binaire (= "loi de composition interne") $*$, une constante e ("élément neutre"), une opération unaire $\_^{-1}$, satisfaisant les lois $x * (y * z) = (x * y) * z$, $x * e = e * x = x$, et $x * x^{-1} = x^{-1} * x = e$ (pour tous x, y, z).
- **Exemple**: $G = \{0, 1, 2\}$, $e = 0$, $x * y = x + y$ "addition modulo 3", c.à.d. $0 + 0 = 1 + 2 = 2 + 1 = 0$, $1 + 1 = 2$, etc. (les entiers modulo 3, notés $\mathbb{Z}/3\mathbb{Z}$).

Exemples d'utilisation (groupes)

- Un groupe consiste en un ensemble G, muni d'une opération binaire (= "loi de composition interne") $*$, une constante e ("élément neutre"), une opération unaire $\_^{-1}$, satisfaisant les lois $x * (y * z) = (x * y) * z$, $x * e = e * x = x$, et $x * x^{-1} = x^{-1} * x = e$ (pour tous x, y, z).
- **Exemple**: $G = \{0, 1, 2\}$, $e = 0$, $x * y = x + y$ "addition modulo 3", c.à.d. $0 + 0 = 1 + 2 = 2 + 1 = 0$, $1 + 1 = 2$, etc. (les entiers modulo 3, notés $\mathbb{Z}/3\mathbb{Z}$).
- **Exemple**: permutations d'un ensemble donné (couleurs, nombres, etc.).

Un groupe non-commutatif

Construire, avec `Mace4`, un groupe avec $a * b \neq b * a$.

Un groupe non-commutatif

Construire, avec `Mace4`, un groupe avec $a * b \neq b * a$.

a: 0 b: 1 e: 2

$^{-1}$	0	1	2	3	4	5
	0	1	2	4	3	5

$*$	0	1	2	3	4	5
0	2	3	0	1	5	4
1	4	2	1	5	0	3
2	0	1	2	3	4	5
3	5	0	3	4	2	1
4	1	5	4	2	3	0
5	3	4	5	0	1	2

Table: Un groupe non-commutatif

Une implication (presque) sans espoir à la main

- **Problème**: montrer que dans tout groupe, tous éléments a, b, c avec $aba^{-1} = b^2$, $bcb^{-1} = c^2$ et $cac^{-1} = a^2$ sont égaux à l'élément neutre du groupe.

Une implication (presque) sans espoir à la main

- **Problème**: montrer que dans tout groupe, tous éléments a, b, c avec $aba^{-1} = b^2$, $bcb^{-1} = c^2$ et $cac^{-1} = a^2$ sont égaux à l'élément neutre du groupe. (On note $ab = a * b$, $abc = (a * b) * c$, $b^2 = b * b$, etc.)

Une implication (presque) sans espoir à la main

- **Problème**: montrer que dans tout groupe, tous éléments a, b, c avec $aba^{-1} = b^2$, $bcb^{-1} = c^2$ et $cac^{-1} = a^2$ sont égaux à l'élément neutre du groupe. (On note $ab = a * b$, $abc = (a * b) * c$, $b^2 = b * b$, etc.)
- `Prover9` résout immédiatement le problème.

Une implication (presque) sans espoir à la main

- **Problème**: montrer que dans tout groupe, tous éléments a, b, c avec $aba^{-1} = b^2$, $bcb^{-1} = c^2$ et $cac^{-1} = a^2$ sont égaux à l'élément neutre du groupe. (On note $ab = a * b$, $abc = (a * b) * c$, $b^2 = b * b$, etc.)
- `Prover9` résout immédiatement le problème. (*Attention aux yeux*!)

Intermède

L'"associativité" $x * (y * z) = (x * y) * z$ généralise la loi vue précédemment (pour les entiers) $x + (1 + 1) = (x + 1) + 1$.

Intermède

L' "associativité" $x * (y * z) = (x * y) * z$ généralise la loi vue précédemment (pour les entiers) $x + (1 + 1) = (x + 1) + 1$.

Un petit exercice sous `Mace4`

Vérifier qu'aucune des lois $x * (y * z) = (x * y) * z$ et $x * (y * z) = (z * x) * y$ (associativité "tordue") n'implique l'autre.

Exemples avec monoïdes

- Un monoïde consiste en un ensemble M, muni d'une opération binaire (= "loi de composition interne") $*$ et une constante e ("élément neutre"), satisfaisant les lois $x * (y * z) = (x * y) * z$ (associativité, donc!) et $x * e = e * x = x$ (pour tous x, y, z).

Exemples avec monoïdes

- Un monoïde consiste en un ensemble M, muni d'une opération binaire (= "loi de composition interne") $*$ et une constante e ("élément neutre"), satisfaisant les lois $x * (y * z) = (x * y) * z$ (associativité, donc!) et $x * e = e * x = x$ (pour tous x, y, z).
- **Exemple**: tout groupe est un monoïde.

Exemples avec monoïdes

- Un monoïde consiste en un ensemble M, muni d'une opération binaire (= "loi de composition interne") $*$ et une constante e ("élément neutre"), satisfaisant les lois $x * (y * z) = (x * y) * z$ (associativité, donc!) et $x * e = e * x = x$ (pour tous x, y, z).
- **Exemple**: tout groupe est un monoïde.
- **Exemple**: les entiers naturels, $\mathbb{N} = \{0, 1, 2, \ldots\}$, forment un monoïde aussi bien avec l'addition (élément neutre 0) qu'avec la multiplication (élément neutre 1).

Exemples avec monoïdes

- Un monoïde consiste en un ensemble M, muni d'une opération binaire (= "loi de composition interne") $*$ et une constante e ("élément neutre"), satisfaisant les lois $x * (y * z) = (x * y) * z$ (associativité, donc!) et $x * e = e * x = x$ (pour tous x, y, z).
- **Exemple**: tout groupe est un monoïde.
- **Exemple**: les entiers naturels, $\mathbb{N} = \{0, 1, 2, \dots\}$, forment un monoïde aussi bien avec l'addition (élément neutre 0) qu'avec la multiplication (élément neutre 1). Dans aucun des deux cas ils ne forment un groupe.

Exemples avec monoïdes

- Un monoïde consiste en un ensemble M, muni d'une opération binaire (= "loi de composition interne") $*$ et une constante e ("élément neutre"), satisfaisant les lois $x * (y * z) = (x * y) * z$ (associativité, donc!) et $x * e = e * x = x$ (pour tous x, y, z).
- **Exemple**: tout groupe est un monoïde.
- **Exemple**: les entiers naturels, $\mathbb{N} = \{0, 1, 2, \dots\}$, forment un monoïde aussi bien avec l'addition (élément neutre 0) qu'avec la multiplication (élément neutre 1). Dans aucun des deux cas ils ne forment un groupe.
- **Exemple** (système de comptage primitif): $M = \{0, 1, \text{beaucoup}\}$ avec $+$, $x + 0 = x$, $1 + 1 = x + \text{beaucoup} = \text{beaucoup}$, $x + y = y + x$.

Limitations

- `Prover9-Mace4` ne considère que les formules du premier ordre.

Limitations

- `Prover9-Mace4` ne considère que les formules du premier ordre. Il ne quantifie donc ($\forall$, $\exists$) que sur des éléments, pas des sous-ensembles.

Limitations

- `Prover9-Mace4` ne considère que les formules du premier ordre. Il ne quantifie donc ($\forall$, $\exists$) que sur des éléments, pas des sous-ensembles.
- Espace / temps de calcul. En général, a du mal avec des structures à plusieurs opérations, comme les anneaux.

Limitations

- `Prover9-Mace4` ne considère que les formules du premier ordre. Il ne quantifie donc ($\forall$, $\exists$) que sur des éléments, pas des sous-ensembles.
- Espace / temps de calcul. En général, a du mal avec des structures à plusieurs opérations, comme les anneaux.
- Absence de contrexemple fini pour certaines questions: existence d'une injection non surjective, existence d'un corps non-commutatif. . .

Limitations

- `Prover9-Mace4` ne considère que les formules du premier ordre. Il ne quantifie donc ($\forall$, $\exists$) que sur des éléments, pas des sous-ensembles.
- Espace / temps de calcul. En général, a du mal avec des structures à plusieurs opérations, comme les anneaux.
- Absence de contrexemple fini pour certaines questions: existence d'une injection non surjective, existence d'un corps non-commutatif. . .
- Ne comprend pas les entiers (*raison*: la finitude ne peut pas s'exprimer au premier ordre)!

Limitations

- `Prover9-Mace4` ne considère que les formules du premier ordre. Il ne quantifie donc ($\forall$, $\exists$) que sur des éléments, pas des sous-ensembles.
- Espace / temps de calcul. En général, a du mal avec des structures à plusieurs opérations, comme les anneaux.
- Absence de contrexemple fini pour certaines questions: existence d'une injection non surjective, existence d'un corps non-commutatif...
- Ne comprend pas les entiers (*raison*: la finitude ne peut pas s'exprimer au premier ordre)!
- Indécidabilité de certaines questions (par exemple, énoncés du premier ordre en théorie des graphes...).

Monoïdes ordonnés / ordonnables

- Rappel (monoïdes): $x * (y * z) = (x * y) * z$, $x * e = e * x = x$ $(\forall x, y, z)$.

Monoïdes ordonnés / ordonnables

- Rappel (monoïdes): $x * (y * z) = (x * y) * z$, $x * e = e * x = x$ $(\forall x, y, z)$.
- Relation d'ordre (total): $x \leq x$; $(x \leq y$ et $y \leq x) \Rightarrow x = y$; $(x \leq y$ et $y \leq z) \Rightarrow x \leq z$; $x \leq y$ ou $y \leq x$.

Monoïdes ordonnés / ordonnables

- Rappel (monoïdes): $x * (y * z) = (x * y) * z$, $x * e = e * x = x$ $(\forall x, y, z)$.
- Relation d'ordre (total): $x \leq x$; $(x \leq y$ et $y \leq x) \Rightarrow x = y$; $(x \leq y$ et $y \leq z) \Rightarrow x \leq z$; $x \leq y$ ou $y \leq x$.
- Compatibilité: $x \leq y \Rightarrow x * z \leq y * z$ (à droite), $x \leq y \Rightarrow z * x \leq z * y$ (à gauche).

Monoïdes ordonnés / ordonnables

- Rappel (monoïdes): $x * (y * z) = (x * y) * z$, $x * e = e * x = x$ $(\forall x, y, z)$.
- Relation d'ordre (total): $x \leq x$; $(x \leq y$ et $y \leq x) \Rightarrow$ $x = y$; $(x \leq y$ et $y \leq z) \Rightarrow$ $x \leq z$; $x \leq y$ ou $y \leq x$.
- Compatibilité: $x \leq y \Rightarrow x * z \leq y * z$ (à droite), $x \leq y \Rightarrow z * x \leq z * y$ (à gauche).
- Monoïde muni d'une relation d'ordre (total) compatible à droite (gauche): monoïde ordonné à droite (gauche).

Monoïdes ordonnés / ordonnables

- Rappel (monoïdes): $x * (y * z) = (x * y) * z$, $x * e = e * x = x$ $(\forall x, y, z)$.
- Relation d'ordre (total): $x \leq x$; $(x \leq y$ et $y \leq x) \Rightarrow x = y$; $(x \leq y$ et $y \leq z) \Rightarrow x \leq z$; $x \leq y$ ou $y \leq x$.
- Compatibilité: $x \leq y \Rightarrow x * z \leq y * z$ (à droite), $x \leq y \Rightarrow z * x \leq z * y$ (à gauche).
- Monoïde muni d'une relation d'ordre (total) compatible à droite (gauche): monoïde ordonné à droite (gauche). Exemple: $\leq$ sur les entiers naturels ($1 \leq 2$, $24 \leq 42$, etc.).

Monoïdes ordonnés / ordonnables

- Rappel (monoïdes): $x * (y * z) = (x * y) * z$, $x * e = e * x = x$ $(\forall x, y, z)$.
- Relation d'ordre (total): $x \leq x$; $(x \leq y$ et $y \leq x) \Rightarrow x = y$; $(x \leq y$ et $y \leq z) \Rightarrow x \leq z$; $x \leq y$ ou $y \leq x$.
- Compatibilité: $x \leq y \Rightarrow x * z \leq y * z$ (à droite), $x \leq y \Rightarrow z * x \leq z * y$ (à gauche).
- Monoïde muni d'une relation d'ordre (total) compatible à droite (gauche): monoïde ordonné à droite (gauche). Exemple: $\leq$ sur les entiers naturels ($1 \leq 2$, $24 \leq 42$, etc.).
- Monoïde ordonnable: quand on peut l'ordonner.

Un exemple simple

$*$	0	1	2	3
0	0	1	2	3
1	1	1	2	3
2	2	1	2	3
3	3	1	2	3

Table: Un monoïde ordonnable à droite mais pas à gauche

Un exemple simple

$*$	0	1	2	3
0	0	1	2	3
1	1	1	2	3
2	2	1	2	3
3	3	1	2	3

Table: Un monoïde ordonnable à droite mais pas à gauche

Cependant, cet exemple est non simplifiable (on peut avoir $ac = bc$ et $a \neq b$).

Un exemple plus imposant (cf. Big Bang)

$+$	$\overline{1}$	0	1	2	3	4	5	6	∞
$\overline{1}$	$\overline{1}$	$\overline{1}$	1	2	2	4	5	5	∞
0	$\overline{1}$	0	1	2	3	4	5	6	∞
1	1	1	4	5	5	5	∞	∞	∞
2	2	2	5	5	5	∞	∞	∞	∞
3	2	3	5	5	6	∞	∞	∞	∞
4	4	4	5	∞	∞	∞	∞	∞	∞
5	5	5	∞	∞	∞	∞	∞	∞	∞
6	5	6	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	∞

Table: Un monoïde commutatif ordonnable, mais non positivement ordonnable, avec $\overline{1} < 0 < 1 < 2 < 3 < 4 < 5 < 6 < \infty$

Du fini à l'infini

Après un certain nombre d'essais (finis, Mace4) et d'erreurs, on aboutit à:

Du fini à l'infini

Après un certain nombre d'essais (finis, Mace4) et d'erreurs, on aboutit à:

Exemple (FW 2021):

Un monoïde simplifiable ($xz = yz \Rightarrow x = y$ et $zx = zy \Rightarrow x = y$), ordonnable à droite mais pas à gauche.

Du fini à l'infini

Après un certain nombre d'essais (finis, Mace4) et d'erreurs, on aboutit à:

Exemple (FW 2021):

Un monoïde simplifiable ($xz = yz \Rightarrow x = y$ et $zx = zy \Rightarrow x = y$), ordonnable à droite mais pas à gauche.

Ce monoïde est "le plus général possible" avec des éléments p_0, p_1, p_2, q_0, q_1, q_2, r_0, r_1, r_2, a_0, a_1, a_2 soumis aux relations

$$\begin{aligned}
p_0 a_0 &= r_0 a_2\,, & p_0 a_1 &= q_0 a_0\,, & q_0 a_1 &= r_0 a_0\\
p_1 a_1 &= r_1 a_0\,, & p_1 a_2 &= q_1 a_1\,, & q_1 a_2 &= r_1 a_1\\
p_2 a_2 &= r_2 a_1\,, & p_2 a_0 &= q_2 a_2\,, & q_2 a_0 &= r_2 a_2
\end{aligned}$$