Les théorèmes de Gödel

(ou : Introduction à la logique informatique)

Raphaël Le Bihan

27 octobre 2021

Introduction : qu'est-ce que la logique ?

La logique = étude des raisonnements

(ici au sens : démonstration mathématique)

- comment faire un raisonnement en maths ? quelles "règles" de déduction peut on appliquer ?
- peut on expliciter ces règles de déduction, les formaliser ? si oui comment ?

Introduction : qu'est-ce que la logique ?

puis...

- y a-t-il des "limites" à ce qu'on peut déduire en maths ? à cause des règles, des notations utilisées ?
- les maths sont elles cohérentes ? peut on trouver une contradiction et "casser" les maths ?
- peut on rajouter/modifier/inventer des règles de déduction pour "étendre" nos raisonnements ?
- peut on automatiser les raisonnements mathématiques ? si oui comment ?
- etc etc...

Plan de la présentation

Plan de la présentation

Construire une formule logique

$$F ::= p, q... \mid \top \mid \bot \mid \neg F \mid F \vee F \mid F \wedge F \mid F \Rightarrow F$$

Construire une formule logique

$$F ::= p, q... \mid \top \mid \bot \mid \neg F \mid F \vee F \mid F \wedge F \mid F \Rightarrow F$$

- $\top, \bot, p, q...$ sont des *propositions atomiques*
  - $\top$ (top) : vrai
  - $\bot$ (bottom) : faux
  - $p, q...$ sont indéterminés (pour l'instant)
- $\neg, \vee, \wedge, \Rightarrow$ sont des *connecteurs logiques*
  - $\neg$: non
  - $\vee$: ou (inclusif)
  - $\wedge$: et
  - $\Rightarrow$: implication

Construire une formule logique

$$F ::= p, q... \mid \top \mid \bot \mid \neg F \mid F \vee F \mid F \wedge F \mid F \Rightarrow F$$

exemples :

- $\top$
- p
- $p \vee \neg q$
- $q \Rightarrow (\neg q \wedge p)$
- $[(\top \Rightarrow q) \vee (q \wedge \neg \bot)] \wedge \neg [q \Rightarrow (r \vee \neg p)]$
- etc etc...

Construire une formule logique

- on sait construire des formules logiques...
- ... qui n'ont pas de sens :'(

  (pour l'instant)

Interpréter une formule logique

$$[\![\cdot]\!]_v : \mathcal{F} \to \{0, 1\}$$

Interpréter une formule logique

$$[\![\cdot]\!]_v : \mathcal{F} \to \{0, 1\}$$

- $[\![F]\!]_v$: interprétation d'une formule logique F (avec la valuation v)
- $v : \mathcal{P} \to \{0, 1\}$: valuation des propositions atomiques
- défini par récurrence

Interpréter une formule logique

$[\![p]\!]_v = v(p)$ (idem avec q...)

$[\![\top]\!]_v = 1$

$[\![\bot]\!]_v = 0$

$[\![\neg F]\!]_v = 1 - [\![F]\!]_v$

$[\![F_1 \vee F_2]\!]_v = 1$ ssi $[\![F_1]\!]_v = 1$ ou $[\![F_2]\!]_v = 1$

$[\![F_1 \wedge F_2]\!]_v = 1$ ssi $[\![F_1]\!]_v = 1$ et $[\![F_2]\!]_v = 1$

$[\![F_1 \Rightarrow F_2]\!]_v = 1$ ssi $[\![F_1]\!]_v = 0$ ou $[\![F_2]\!]_v = 1$

Interpréter une formule logique

valuation : $v(p) = 1$
$v(q) = 0$

exemple :

$$p \Rightarrow (\neg p \vee \neg q)$$

- $[\![p \Rightarrow (\neg p \vee \neg q)]\!]_v = 1$ ssi $[\![p]\!]_v = 0$ ou $[\![\neg p \vee \neg q]\!]_v = 1$
  - $[\![p]\!]_v = 1$
  - $[\![\neg p \vee \neg q]\!]_v = 1$ ssi $[\![\neg p]\!]_v = 1$ ou $[\![\neg q]\!]_v = 1$
    - $[\![\neg p]\!]_v = 1 - [\![p]\!]_v = 1 - 1 = 0$
    - $[\![\neg q]\!]_v = 1 - [\![q]\!]_v = 1 - 0 = 1$

    donc $[\![\neg p \vee \neg q]\!]_v = 1$

  donc $[\![p \Rightarrow (\neg p \vee \neg q)]\!]_v = 1$

Un cas particulier : les tautologies

Une *tautologie*, ou formule *valide* =
une formule dont l'interprétation est toujours 1 (quelque soit v)

Exemples :

- $\top$
- $p \vee \neg p$
- $p \Rightarrow p$
- $\bot \Rightarrow p$
- $p \Rightarrow (q \Rightarrow p)$
- etc...

Résumé

- On sait construire des formules logiques
- et les interpréter.

... on a défini la *logique d'ordre 0* :)

Maintenant, comment formaliser la notion de raisonnement ?

Plan de la présentation

En maths / dans la vie :

comment fait-on une démonstration ?

Comment fait-on une démonstration ?

une démonstration = une succession d'affirmations

- une affirmation = une formule logique
  - ce que je sais, pour l'instant
- d'une affirmation vers la suivante :
  - une transition élémentaire = une "règle"

Règles

Une *règle* :

$$\frac{\phi_1 \quad \cdots \quad \phi_n}{\psi}$$

- $\phi_1, \ldots, \phi_n$ sont les *hypothèses*
- ψ est la *conclusion*
- $\phi_1, \ldots, \phi_n$ et ψ contiennent :
  - des *symboles* : $\top, \bot, \vee, \wedge, \neg, \Rightarrow$
  - des *emplacements de formules* : $F_1, F_2, \ldots$

Règles

Un exemple de règle :

$$\frac{F_1}{F_1 \vee F_2}$$

- si on a une preuve de F_1...
- ... en appliquant cette règle, on prouve $F_1 \vee F_2$

Règles

D'autres exemples :

$$\frac{F_1 \Rightarrow F_2 \qquad F_1}{F_2} \qquad \frac{F \qquad \neg F}{\bot} \qquad \frac{}{\top} \qquad \frac{\bot}{F}$$

Construire des preuves

On prouve une formule en construisant un *arbre de preuve*.

Pour construire un arbre de preuve :

1. écrire les hypothèses
   (autant de fois qu'on aura besoin de les utiliser)

2. appliquer des règles successivement
   (chaque conclusion devient une hypothèse de la règle suivante)

3. "décharger" les hypothèses restantes
   (= recopier les hypothèses avec des symboles $\Rightarrow$)

Construire des preuves

ex : prouver $(p \wedge q) \Rightarrow (p \wedge \top)$

$$p \wedge q$$

1. écrire les hypothèses

Construire des preuves

ex : prouver $(p \wedge q) \Rightarrow (p \wedge \top)$

$$\dfrac{\dfrac{p \wedge q}{p} \qquad \dfrac{}{\top}}{p \wedge \top}$$

2. appliquer des règles successivement

Construire des preuves

ex : prouver $(p \wedge q) \Rightarrow (p \wedge \top)$

$$\dfrac{\dfrac{\dfrac{[p \wedge q]}{p} \qquad \dfrac{}{\top}}{p \wedge \top}}{(p \wedge q) \Rightarrow (p \wedge \top)}$$

3. décharger les hypothèses

Quelles règles se donne-t-on pour construire des preuves ?

Un *système de preuve* est un ensemble de règles permettant de construire des arbres de preuve

Un système de preuve : la déduction naturelle

$$\frac{}{\top}\ (\top_I) \qquad \frac{F \quad \neg F}{\bot}\ (\bot_I) \qquad \frac{\bot}{F}\ (\bot_E) \qquad \frac{\neg\neg F}{F}\ (\text{RAA})$$

$$\frac{F_1}{F_1 \vee F_2}\ (\vee_{I1}) \qquad \frac{F_2}{F_1 \vee F_2}\ (\vee_{I2})$$

$$\frac{F_1 \vee F_2 \quad F_1 \Rightarrow F_3 \quad F_2 \Rightarrow F_3}{F_3}\ (\vee_E)$$

$$\frac{F_1 \quad F_2}{F_1 \wedge F_2}\ (\wedge_I) \qquad \frac{F_1 \wedge F_2}{F_1}\ (\wedge_{E1}) \qquad \frac{F_1 \wedge F_2}{F_2}\ (\wedge_{E2})$$

$$\frac{F_2}{F_1 \Rightarrow F_2}\ (\Rightarrow_I) \qquad \frac{F_1 \Rightarrow F_2 \quad F_1}{F_2}\ (\Rightarrow_E)$$

Correction

- les règles de la déduction naturelle semblent legit...
- ... mais on aurait pu ajouter la règle

$$\frac{F_1}{F_1 \wedge F_2}\ \text{(WTF)}$$

- on peut prouver $\bot$
  puis n'importe quelle formule... :(

Correction

Un système de preuve est *correct* si les seules formules que l'on peut prouver sont des tautologies.

La déduction naturelle est correcte :)

démonstration par récurrence sur la hauteur d'un arbre de preuve

Complétude

On a réussi à prouver $(p \wedge q) \Rightarrow (p \wedge \top)$
(c'est donc une tautologie)

... mais existe-t-il des tautologies qu'on ne peut pas prouver avec la déduction naturelle ? O_o

Si oui, peut-on rajouter des règles pour prouver plus de tautologies ?

Complétude

Un système de preuve est *complet* s'il permet de prouver toute formule qui est une tautologie.

La déduction naturelle est complète :)
(pas besoin d'ajouter de règles !)

démonstration plus compliquée, par récurrences imbriquées :
d'abord sur le nombre de propositions atomiques indéterminées ($p, q \ldots$)
puis sur la taille d'une formule

Résumé

On a montré que la déduction naturelle est *correcte* et *complète* :

les formules prouvables sont exactement les tautologies (cool !)

Nos formules permettent-elles de décrire tout ce qu'on fait en maths d'habitude ?

... comment parler de choses ? de gens ? de nombres ?

Plan de la présentation

Termes et formules

$$t ::= x, y... \mid c_1, c_2... \mid f_1(\vec{t}), f_2(\vec{t})...$$

$$\begin{aligned} F ::= & P_1(\vec{t}), P_2(\vec{t})... \mid \top \mid \bot \mid \\ & \neg F \mid F \vee F \mid F \wedge F \mid F \Rightarrow F \mid \\ & \exists x F \mid \forall x F \end{aligned}$$

Termes et formules

Exemples :

- $P_1(x)$
- $P_2(c_2, y, x)$
- $\top \wedge \exists x(P_1() \Rightarrow P_2(x, y))$

Interprétation

On interprète une formule dans un *modèle* $\mathcal{M}$

- $\mathrm{dom}\mathcal{M}$ est un ensemble (non vide)
- $c_i^{\mathcal{M}} \in \mathrm{dom}\mathcal{M}$
- $f_i^{\mathcal{M}} : (\mathrm{dom}\mathcal{M})^k \to \mathrm{dom}\mathcal{M},\ k \geq 1$
- $P_i^{\mathcal{M}} \subseteq (\mathrm{dom}\mathcal{M})^k,\ k \geq 0$

avec une *valuation* $v : \mathcal{V} \to \mathrm{dom}\mathcal{M}$

D'abord interpréter des termes

$$[\![x]\!]_{\mathcal{M},v} = v(x)$$

$$[\![c_i]\!]_{\mathcal{M},v} = c_i^{\mathcal{M}}$$

$$[\![f_i(\vec{t})]\!]_{\mathcal{M},v} = f_i^{\mathcal{M}}(\vec{[\![t]\!]}_{\mathcal{M},v})$$

Puis interpréter des formules

$[\![P_i(\vec{t})]\!]_{\mathcal{M},v} = 1$ ssi $([\![t]\!]^{\vec{}}_{\mathcal{M},v}) \in P_i^{\mathcal{M}}$

$[\![\exists x F]\!]_{\mathcal{M},v} = 1$ ssi $[\![F]\!]_{\mathcal{M},v'} = 1$ pour un certain v'

$[\![\forall x F]\!]_{\mathcal{M},v} = 1$ ssi $[\![F]\!]_{\mathcal{M},v'} = 1$ pour chaque v'

où v' correspond à v sauf sur x

$+$

le reste est interprété comme à l'ordre 0

... c'est la *logique d'ordre 1* !

Un exemple

Modèle :

- $\mathrm{dom}\mathcal{M} = \mathbb{N}$
- $c_1^{\mathcal{M}} = 4$
- $f_1^{\mathcal{M}} = +$
- $P_1^{\mathcal{M}} = \{n \text{ pair}\}$

Un exemple

modèle : $c_1^{\mathcal{M}} = 4 \qquad f_1^{\mathcal{M}} = " + " \qquad P_1^{\mathcal{M}} = \{n \text{ pair } \}$

valuation : $v(x) = 6$

exemple :

$$P_1(f_1(c_1, x))$$

- $[\![P_1(f_1(c_1, x))]\!]_{\mathcal{M},v} = 1$ ssi $[\![f_1(c_1, x)]\!]_{\mathcal{M},v}$ est pair
  - $[\![f_1(c_1, x)]\!]_{\mathcal{M},v} = [\![c_1]\!]_{\mathcal{M},v} + [\![x]\!]_{\mathcal{M},v}$
    - $[\![c_1]\!]_{\mathcal{M},v} = c_1^{\mathcal{M}} = 4$
    - $[\![x]\!]_{\mathcal{M},v} = v(x) = 6$

  donc $[\![f_1(c_1, x)]\!]_{\mathcal{M},v} = 10$

donc $[\![P_1(f_1(c_1, x))]\!]_{\mathcal{M},v} = 1$

Quantificateurs

Avec $v(x) = 6$
la formule $P_1(f_1(c_1, x))$ est satisfaite dans $\mathcal{M}$.

alors en posant $v' = v$
la formule $\exists x P_1(f_1(c_1, x))$ est satisfaite dans $\mathcal{M}$.

Par contre $P_1(f_1(c_1, x))$ n'est pas satisfaite avec n'importe quelle valuation.
(par exemple $v(x) = 5$)

alors la formule $\forall x P_1(f_1(c_1, x))$ n'est pas satisfaite dans $\mathcal{M}$.

La déduction naturelle (à l'ordre 1)

règles précédentes

$+$

$$\frac{F}{\forall x F}\ (\forall_I) \qquad \frac{\forall x F}{(x \to t)F}\ (\forall_E)$$

$$\frac{(x \to t)F}{\exists x F}\ (\exists_I) \qquad \frac{\exists x F_1 \qquad F_1 \Rightarrow F_2}{F_2}\ (\exists_E)$$

Correction

La déduction naturelle à l'ordre 1 est correcte :)
comme à l'ordre 0 !

démonstration comme à l'ordre 0
par récurrence sur la hauteur d'un arbre de preuve, en ajoutant des cas supplémentaires pour les quantificateurs

... et la complétude ?

(WAIT FOR IT)

Plan de la présentation

Le théorème de complétude de Gödel

La déduction naturelle est complète ! :D

Reformulation :
Si une formule F n'est pas prouvable
Alors il existe un modèle qui satisfait $\neg F$

démonstration en construisant un modèle
où dom$\mathcal{M}$ est l'ensemble des termes
(démonstration simplifiée par Henkin)

Théorie

Une *théorie* = un ensemble de formules

Une formule est *satisfiable/valide* dans une théorie
si elle est vraie dans un/tout modèle *où la théorie est vraie*.

Une formule est *prouvable* dans une théorie
si elle est prouvable en déchargeant les hypothèses de la théorie.

Fabriquons une turbo-théorie, dans laquelle tout est
démontrable ! :D

Le 1er théorème d'incomplétude de Gödel (1931)

Une théorie cohérente permettant de prouver les théorèmes de base de l'arithmétique est incomplète.

:'(

cause : on peut encoder des formules et des preuves avec des nombres entiers

démonstration : enfer

Try again

"Fabriquons une turbo-théorie, dans laquelle tout est démontrable ! :D"
$\rightarrow$ C'est mort.

... Fabriquons une théorie suffisamment puissante :)

où on peut faire de l'arithmétique
(même si on ne peut pas tout démontrer avec)

et montrons qu'elle est cohérente !

Le 2nd théorème d'incomplétude de Gödel (1931)

Une théorie cohérente permettant d'exprimer sa propre cohérence est incomplète.

x'(

cause : "je ne suis pas prouvable"

	prouvable	non prouvable
vraie	-	incomplet
fausse	incohérent	-

démonstration : le même enfer

Peut on casser les maths ?

On ne peut pas montrer que c'est impossible.

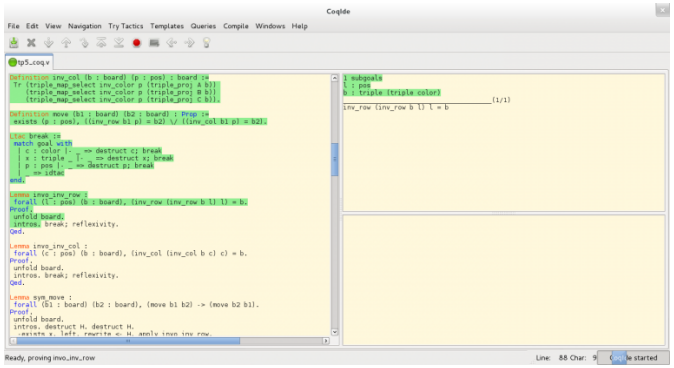
C'est déjà arrivé : "l'ensemble de tous les ensembles qui ne se contiennent pas"
(fin XIXe siècle)

dans le même style :
"La phrase suivante est vraie. La phrase précédente est fausse."

et pour les maths actuelles ?

... on verra ¯_(ツ)_/¯

Happy ending



$\Box p \rightsquigarrow q$

$\Diamond q \Rightarrow r$

- assistants de preuves (programmes, théorèmes, hardware...)
- explorer différentes logiques : intuitioniste, ordre 2, temporelle
- correspondance de Curry-Howard (preuve = programme), programmation fonctionnelle
- etc

Merci pour votre attention ! :)