# Les fausses preuves sont beaucoup plus rapides

## Un résultat de J. P Aguilera et M. Baaz

Antoine Poulin (McGill)

22-23 Mai 2021

# La logique

La logique essaie d'utiliser des méthodes mathématiques pour analyser les preuves et les manières dans lesquelles les mathématiques sont faites.

Il faut une définition de preuve !
Avant tout, il faut même une définition d'énoncés mathématiques !

# Les énoncés mathématiques

Nos **formules** auront les symboles suivants :

- Des connecteurs : $\vee, \wedge, \neg$
- Des propositions : P,Q,R,...
- Des variables : a,b,c,...
- Des quantifieurs : $\forall x, \exists y$

En exemple, on peut avoir la formule suivante :

$$(\forall x, P(x,a) \wedge Q(x,x,b)) \vee Q(b,a,b)$$

# Séquents

Le principal objet qu'on manipule sont des **séquents**

$$A_1, \ldots, A_n \vdash B_1, \ldots, B_n,$$

qu'on interprète comme

*Si tout les $A_i$ sont vrais, au moins un des $B_j$ l'est.*

Notez l'asymétrie des séquents. Souvent, on note

$$\Gamma \vdash \Delta,$$

avec $\Gamma = \{A_1, \ldots, A_n\}$ et similairement pour $\Delta$.

# Calcul des séquents

On veut manipuler les séquents en utilisant des **inférences**. On aura trois types d'inférences. Voici une inférence **structurelle**, qu'on note avec $\sigma$ :

$$\frac{\Gamma \vdash \Delta}{\Gamma, A \vdash \Delta}\, \sigma$$

On interprète en disant que rajouter une hypothèse ne peut pas changer ce qu'on sait déjà.

# Inférences logiques et de quantifieurs

On trouve aussi les inférences **logiques** :

$$\frac{\Gamma, A \vdash \Delta \qquad \Gamma, B \vdash \Delta}{\Gamma, A \vee B \vdash \Delta} \lambda$$

Notez qu'il y a deux hypothèse cette fois-ci. Voici une inférence de **quantifieurs faibles** :

$$\frac{\Gamma, \mathrm{P(a)} \vdash \Delta}{\Gamma, \forall \mathrm{x},\ \mathrm{P(x)} \vdash \Delta} q_a$$

# Preuves

Des preuves sont des arbres d'inférences

$$\dfrac{\dfrac{P(a) \vdash P(a)}{\vdash P(a) \rightarrow P(a)}\,\lambda}{\vdash \forall x, (P(x) \rightarrow P(x))}\,Q_a$$

La dernière est une inférence de **quantifieurs forts**. Avait on le droit de la faire ?

# Types d'inférences fortes

Les deux inférences fortes sont celles-ci :

$$\frac{\Gamma \vdash \mathsf{P(a)}, \Delta}{\Gamma, \vdash \forall \mathsf{x},\ \mathsf{P(x)}, \Delta}\ Q_a$$

$$\frac{\Gamma, \mathsf{P(a)} \vdash \Delta}{\Gamma, \exists \mathsf{x},\ \mathsf{P(x)} \vdash \Delta}\ Q_a$$

Classiquement, on peut faire ce type d'inférences si la variable *a* disparait complètement du séquent. C'est l'équivalent de commencer une preuve en fixant *a* un entier quelconque et de la finir en disant que puisque *a* était quelconque, notre conclusion suit de tout les entiers.

# Relaxation des conditions

La condition pour utiliser des inférences Q est donc de faire disparaitre complètement la variable. Une infèrence comme ceci est donc fausse

$$\cfrac{\cfrac{\cfrac{\mathrm{P(a)} \vdash \mathrm{P(a)}}{\mathrm{P(a)} \vdash \forall\ \mathrm{x},\ \mathrm{P(x)}}\ Q_a}{\vdash \mathrm{P(a)} \rightarrow \forall x,\ \mathrm{P(x)}}\ \lambda}{\vdash \exists\ \mathrm{y},\ ((\mathrm{P(y)} \rightarrow \forall x,\ \mathrm{P(x)})}\ q_a$$

Peut-on relaxer les conditions sur notre usage des inférences $Q$ pour que cette preuve soit valide ?

# Les trois conditions suffisantes

On dit qu'une preuve est valide si les trois conditions suivantes sont satisfaites

- Subs. Les variables fortement quantifiées ne doivent pas apparaitre dans la conclusion de la preuve.
- Rég. F. Une variable ne peut se faire fortement quantifier qu'une fois.
- Acyc. Si b apparait dans une inférence Q pour a, on note $a <_Q b$. La relation $<_Q$ doit être acyclique.

# Théorème de complétude

**Theorem (Aguilera, J.P., Baaz, M.)**

*Si un théorème se prouve avec les nouvelles règles d'inférences Q, il est prouvable classiquement*

Donc, on ne prouvera aucune contradiction ! On prouve en changeant toutes les instances de fausses inférences explicitement en un système d'inférences qui fonctionnent.

# Théorème d'accélération

Intuitivement, si $F$ est une fonction batie à l'aide de l'addition $+$, multiplication $\cdot$ et de l'exponentiation $x \mapsto 2^x$, on dit que c'est une fonction élémentaire.

**Theorem (Aguilera, J.P., Baaz, M.)**

*Si $f$ est élémentaire, il existe une formule dont la preuve "fausse" a une longueur de $n$, mais la preuve classique est plus longue que $f(n)$.*

Pour que ce théorème tienne, il faut aussi oublier l'inférence structurelle Cut. On prouve avec des "manipulations profondes de quantifieurs".

# Example d'accélération

Voici une preuve classique

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{P(a) \vdash P(a)}{P(a) \vdash P(a),\ Q}\ \sigma}{\vdash P(a),\ P(a) \to Q}\ \lambda}{\vdash P(a),\ \exists\ x,\ P(x) \to Q}\ q_a}{\vdash \exists\ x,\ P(x) \to Q,\ P(a)}\ \sigma}{\vdash \exists\ x,\ P(x) \to Q,\ \forall\ y,\ P(y)}\ {\color{red}Q_a} \qquad Q \vdash Q}{(\forall\ y,\ P(y)) \to Q \vdash \exists\ x,\ (P(x) \to Q),\ Q}\ \lambda}{\ldots}\ \sigma,\lambda,\ q_b}{(\forall\ y,\ P(y)) \to Q \vdash \exists\ x,\ (P(x) \to Q)}\ \sigma
$$

# Example d'accélération

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{P(a) \vdash P(a)}{P(a) \vdash \forall\ x,\ P(x)}\ {\color{red}Q_a} \qquad Q \vdash Q}{P(a),\ (\forall\ x,\ P(x)) \to Q \vdash Q}\ \lambda}{(\forall\ x,\ P(x)) \to Q,\ P(a) \vdash Q}\ \sigma}{(\forall\ x,\ P(x)) \to Q \vdash P(a) \to Q}\ \lambda}{(\forall\ x,\ P(x)) \to Q \vdash \exists\ y,\ (P(y) \to Q)}\ {\color{red}q_a}
$$

Nous sommes passés de 10 inférences à 5 !

# Bibliographie

Aguilera, J. P., Baaz, M (2019). Unsound Inferences Make Proofs Shorter. Journal of Symbolic Logic, vol. 84, no. 1, p. 102-122.

# Merci !