DM de Logique

Younesse Kaddar	Énoncé	Version PDF	http://younesse.net/Logique/DM_Logique/

I. De QBF à la logique intuitionniste

Le lemme suivant sera récurremment utilisé dans la suite :

> *Lemme Introductif* : Si φ est une formule QBF et $I \subseteq \mathscr{P}$:
>
> $$I \cap (fv(\varphi) \cup bv(\varphi)) \overset{QBF}{\vDash} \varphi \Longleftrightarrow I \overset{QBF}{\vDash} \varphi$$

Preuve : Par induction structurelle sur φ :

- *Si $\varphi = \bot$ (resp. $\varphi = \top$)* : cela revient à montrer l'équivalence de deux propositions fausses (resp. vraies), c'est immédiat.
- *Si $\varphi = p \in \mathscr{P}$* : Pour tout $I \subseteq \mathscr{P}$:

$$\begin{aligned} & I \cap \underbrace{(fv(\varphi) \cup bv(\varphi))}_{=\{p\}} \overset{QBF}{\vDash} p \\ \Longleftrightarrow \quad & p \in I \cap \{p\} \\ \Longleftrightarrow \quad & p \in I \\ \Longleftrightarrow \quad & I \overset{QBF}{\vDash} p \end{aligned}$$

- *Si $\varphi = \neg\psi$* : Pour tout $I \subseteq \mathscr{P}$:

$$\begin{aligned} & I \cap (fv(\varphi) \cup bv(\varphi)) \overset{QBF}{\vDash} \varphi \\ \Longleftrightarrow \quad & I \cap (fv(\varphi) \cup bv(\varphi)) \overset{QBF}{\nvDash} \psi \\ \Longleftrightarrow \quad & I \overset{QBF}{\nvDash} \psi && \text{(par hypothèse d'induction)} \\ \Longleftrightarrow \quad & I \overset{QBF}{\vDash} \neg\psi = \varphi \end{aligned}$$

- *Si $\varphi \in \{\varphi_1 \wedge \varphi_2, \varphi_1 \vee \varphi_2, \varphi_1 \longrightarrow \varphi_2\}$* : Le résultat découle directement de l'application de l'hypothèse d'induction à φ_1 et φ_2
- *Si $\varphi = \forall p.\, \psi$ (resp. $\varphi = \exists p.\, \psi$)* :

$$\begin{aligned} & & I \cap (fv(\varphi) \cup bv(\varphi)) \overset{QBF}{\vDash} \varphi & \\ \Longleftrightarrow & & \underbrace{\Big(I \cap \underbrace{(fv(\varphi) \cup bv(\varphi))}_{=\{p\} \cup fv(\psi) \cup bv(\psi)}\Big)\backslash\{p\}}_{=\left(I \backslash \{p\}\right) \cap (fv(\psi) \cup bv(\psi))} \overset{QBF}{\vDash} \psi & \\ & \text{et (resp. ou)} & I \cap (fv(\varphi) \cup bv(\varphi)) \cup \{p\} \overset{QBF}{\vDash} \psi & \\ \Longleftrightarrow & & I \backslash \{p\} \overset{QBF}{\vDash} \psi & \quad \text{(par hypothèse d'induction)} \\ & \text{et (resp. ou)} & I \cap \Big(\{p\} \cup fv(\psi) \cup bv(\psi)\Big) \cup \{p\} \overset{QBF}{\vDash} \psi & \\ \Longleftrightarrow & & I \backslash \{p\} \overset{QBF}{\vDash} \psi & \\ & \text{et (resp. ou)} & \Big(I \cap \Big(\{p\} \cup fv(\psi) \cup bv(\psi)\Big) \cup \{p\}\Big) \cap \big(fv(\psi) \cup bv(\psi)\big) \overset{QBF}{\vDash} \psi & \quad \text{(par hypothèse d'induction)} \\ \Longleftrightarrow & & I \backslash \{p\} \overset{QBF}{\vDash} \psi & \\ & \text{et (resp. ou)} & \underbrace{\Big(\Big(I \cap (fv(\psi) \cup bv(\psi))\Big) \cup \overbrace{\Big(I \cap \{p\}\Big) \cup \{p\}}^{=\{p\}}\Big) \cap \big(fv(\psi) \cup bv(\psi)\big)}_{=\left(I \cap (fv(\psi) \cup bv(\psi))\right) \cup \left(\{p\} \cap (fv(\psi) \cup bv(\psi))\right) = (I \cup \{p\}) \cap (fv(\psi) \cup bv(\psi))} \overset{QBF}{\vDash} \psi & \\ \Longleftrightarrow & & I \backslash \{p\} \overset{QBF}{\vDash} \psi & \\ & \text{et (resp. ou)} & I \cup \{p\} \overset{QBF}{\vDash} \psi & \quad \text{(par hypothèse d'induction)} \\ \Longleftrightarrow & & I \overset{QBF}{\vDash} \varphi & \end{aligned}$$

Donc le résultat est acquis.

NB :

- L'induction structurelle sur une formule QBF φ est entendue comme étant :
  - l'induction structurelle sur φ si $\varphi \in \mathcal{F}_0$ n'a pas de quantificateurs
  - l'induction sur le nombre de quantificateurs φ en a

  En d'autres termes, la syntaxe d'une formule QBF peut-être définie par la grammaire suivante (sur laquelle l'induction structurelle est faite) :

$$\begin{aligned} S &\longrightarrow p \mid \bot \mid \top && (\text{pour } p \in \mathscr{P}) \\ F_0 &\longrightarrow \neg F_0 \mid F_0 \vee F_0 \mid F_0 \wedge F_0 \mid F_0 \to F_0 \mid S \\ QBF &\longrightarrow \forall p.\, QBF \mid \exists p.\, QBF \mid \forall p.\, F_0 \mid \exists p.\, F_0 && (\text{pour } p \in \mathscr{P}) \end{aligned}$$

- Intuitivement, ce lemme signifie que si φ ne contient pas la variable p, alors rajouter ou non p à une interprétation donnée ne change rien au fait que cette interprétation statisfasse φ ou non.
- Un lemme analogue (plus simple à démontrer, puisqu'il n'y a pas à considérer les quantificateurs) peut être démontré pour la logique intuitionniste.

1.

> *Scolie* : Pour toute formule QBF φ, pour toute $p \in bv(\varphi)$, et pour toute $q \in \mathscr{P} \backslash (bv(\varphi) \cup fv(\varphi))$, φ est équivalente à la $\varphi[p \leftarrow q]$, où φ est la formule QBF obtenue à partir de φ en remplaçant p par q.

Preuve : par induction structurelle sur φ.

- **Cas de base** : si $\varphi \in \mathcal{F}_0(\mathscr{P})$:
  c'est immédiat puisque $bv(\varphi) = \emptyset$
- **Hérédité** : si $\varphi \overset{\text{def}}{=} Qp.\, \psi$ (avec les notations de l'énoncé) :
  alors
  - $\varphi[p \leftarrow q] \overset{\text{def}}{=} Qq.\, \psi[p \leftarrow q]$
  - on montre par une induction structurelle immédiate sur ψ que toute interprétation $I \subseteq \mathscr{P}$ vérifie $I \cup \{p\} \overset{QBF}{\models} \psi \left(\text{resp. } I \backslash \{p\} \overset{QBF}{\models} \psi \right)$ dès que $I \cup \{q\} \overset{QBF}{\models} \psi[p \leftarrow q] \left(\text{resp. } I \backslash \{q\} \overset{QBF}{\models} \psi[p \leftarrow q] \right)$, et la réciproque se montre de manière analogue.

  Il découle donc ainsi que :
  - *Si* $Q = \forall$: $\left(I \cup \{p\} \overset{QBF}{\models} \psi \text{ et } I \backslash \{p\} \overset{QBF}{\models} \psi \right) \text{ ssi } \left(I \cup \{q\} \overset{QBF}{\models} \psi[p \leftarrow q] \text{ et } I \backslash \{q\} \overset{QBF}{\models} \psi[p \leftarrow q] \right)$
  - *Si* $Q = \exists$: $\left(I \cup \{p\} \overset{QBF}{\models} \psi \text{ ou } I \backslash \{p\} \overset{QBF}{\models} \psi \right) \text{ ssi } \left(I \cup \{q\} \overset{QBF}{\models} \psi[p \leftarrow q] \text{ ou } I \backslash \{q\} \overset{QBF}{\models} \psi[p \leftarrow q] \right)$ Dans tous les cas : le résultat est acquis.

Soit φ une formule QBF.

Montrons que φ est équivalente à une formule QBF bien quantifiée, par induction sur le nombre de quantificateurs n de φ.

- **Cas de base** : si $n = 0$
  alors $\varphi \in \mathcal{F}_0(\mathscr{P})$, et φ est clairement bien quantifiée, puisqu'elle n'a pas de sous-formule de la forme $Qp.\, \psi$
- **Hérédité** : si $\varphi \overset{\text{def}}{=} Qp.\, \psi$ où $Q \in \{\forall, \exists\}$ a $n > 0$ quantificateurs et est bien quantifiée :
  alors
  - $p \notin bv(\psi)$ (φ est bien quantifiée)
  - ψ est une formule QBF bien quantifiée (puisque φ l'est) à $n-1$ quantificateurs, donc par hypothèse d'induction : ψ est équivalente à une formule QBF ψ' bien quantifiée.
  - Comme $\mathscr{P}$ est infini, il existe $\mathscr{P} \backslash (bv(\psi') \cup fv(\psi')) \ni q \neq p$.
    Quitte à considérer $\psi'[p \leftarrow q]$, qui reste bien quantifiée (car $q \notin bv(\psi') \cup fv(\psi')$) et est équivalente à ψ' si $p \in bv(\psi')$ (par la *scolie*), on peut supposer que $p \notin bv(\psi')$ (l'équivalence des formules QBF est une relation d'équivalence (et est donc transitive)).

  Soit $I \subseteq \mathscr{P}$. Montrons que

$$I \overset{QBF}{\models} \varphi = Qp.\, \psi \Longleftrightarrow I \overset{QBF}{\models} Qp.\, \psi' \overset{\text{def}}{=} \varphi'$$

  - $\Longrightarrow$:
    Si $I \cup \{p\} \overset{QBF}{\models} \psi \left(\text{resp. } I \backslash \{p\} \overset{QBF}{\models} \psi \right)$, alors $I \cup \{p\} \overset{QBF}{\models} \psi' \left(\text{resp. } I \backslash \{p\} \overset{QBF}{\models} \psi' \right)$ par équivalence de ψ et ψ'.
    Donc que Q vaille $\forall$ ou $\exists$, on vérifie bien que si $I \overset{QBF}{\models} Qp.\, \psi$, alors $I \overset{QBF}{\models} Qp.\, \psi'$.
  - $\Longleftarrow$: se montre de la même manière.

  Comme $\varphi' = Qp.\, \psi'$ est bien quantifiée (puisque ψ' l'est et $p \notin bv(\psi')$), le résultat est donc acquis.

On a montré que :

> Toute formule QBF est logiquement équivalente à une formule QBF bien quantifiée.

2.

Par induction sur le nombre de quantificateurs n de φ, montrons que :

> Pour tous $I \subseteq \mathscr{P}$, $\mathscr{K} \overset{\text{def}}{=} (W, \leq_{\mathscr{K}}, \alpha_{\mathscr{K}})$, φ bien quantifiée telle que $(fv(\varphi) \cup bv(\varphi)) \cap \mathscr{Q} = \emptyset$:
>
> *si* $I \overset{QBF}{\models} \varphi$ et $\mathscr{K}$ force I sur $\mathscr{P} \backslash (bv(\varphi) \cup \mathscr{Q})$ *alors* pour tout $w \in W, \mathscr{K}, w \overset{KPK}{\models} \varphi^*$

NB : Comme φ^* n'est pas définie dans le cas contraire, on fera l'hypothèse que $(fv(\varphi) \cup bv(\varphi)) \cap \mathscr{Q} = \emptyset$

Cas de base : si $n = 0, \varphi \in \mathcal{F}_0(\mathscr{P})$:

Soient $I \subseteq \mathscr{P}$, $\mathscr{K} \overset{\text{def}}{=} (W, \leq_{\mathscr{K}}, \alpha_{\mathscr{K}})$ un modèle de Kripke, φ une formule QBF de $\mathcal{F}_0(\mathscr{P})$ telle que $(fv(\varphi) \cup bv(\varphi)) \cap \mathscr{Q} = \emptyset$.

Supposons que $I \overset{QBF}{\models} \varphi$, *i.e* $I \overset{CL}{\models} \varphi$, et que $\mathscr{K}$ force I sur $\mathscr{P} \backslash (\underbrace{bv(\varphi)}_{=\emptyset} \cup \mathscr{Q}) = \mathscr{P} \backslash \mathscr{Q}$.

Soit $w \in W$.

Pour toute $p \in \mathscr{P} \backslash \mathscr{Q}$,

- $p \in I \Longrightarrow \mathscr{K}, w \overset{KPK}{\models} p$
- $p \notin I \Longrightarrow \forall w' \geq w, \mathscr{K}, w' \overset{KPK}{\not\models} p$

D'où en particulier :

$$\forall p \in \mathscr{P} \backslash \mathscr{Q},\ \ p \in I \Longleftrightarrow \mathscr{K}, w \overset{KPK}{\models} p \Longleftrightarrow p \in \alpha_{\mathscr{K}}(w)$$

Donc comme $I, \alpha_{\mathscr{K}}(w) \subseteq \mathscr{P}$, il vient que :

$$I \backslash \mathscr{Q} = \alpha_{\mathscr{K}}(w) \backslash \mathscr{Q}$$

> Montrons que : *si*
>
> - $I \overset{CL}{\models} \varphi$
> - $(fv(\varphi) \cup bv(\varphi)) \cap \mathscr{Q} = \emptyset$
>
> *alors* $w \overset{KPK}{\models} \varphi^* = \varphi$, par induction sur la taille $|\varphi|$ de φ :

Cas de base : $|\varphi| = 1$

- $\varphi = \top$: c'est immédiat.
- $\varphi = \bot$: ce cas est exclus puisque $I \overset{CL}{\models} \varphi$
- $\varphi \in \mathscr{P}$:
  comme
  - $(\underbrace{fv(\varphi)}_{=\{\varphi\}} \cup \underbrace{bv(\varphi)}_{=\emptyset}) \cap \mathscr{Q} = \emptyset$, d'où $\varphi \notin \mathscr{Q}$
  - et $\varphi \in I$ (car $I \overset{CL}{\models} \varphi$)

  il vient que $\varphi \in I \backslash \mathscr{Q} = \alpha_{\mathscr{K}}(w) \backslash \mathscr{Q} \subseteq \alpha_{\mathscr{K}}(w)$, soit $w \overset{KPK}{\models} \varphi$

Hérédité : $|\varphi| > 1$

- $\varphi = \varphi_1 \wedge \varphi_2$ ou $\varphi = \varphi_1 \vee \varphi_2$: le résultat découle directement de $I \overset{CL}{\models} \varphi$ et de l'application de l'hypothèse d'induction à φ_1 et φ_2
- $\varphi = \varphi_1 \longrightarrow \varphi_2$:
  Soit $w' \geq w$ tel que $w' \overset{KPK}{\models} \varphi_1$. Montrons que $w' \overset{KPK}{\models} \varphi_2$.
  - *Cas 1* : $I \overset{CL}{\models} \varphi_1$:
    Comme $I \overset{CL}{\models} \varphi$, alors $I \overset{CL}{\models} \varphi_2$, et d'après l'hypothèse d'induction : $w \overset{KPK}{\models} \varphi_2$. Donc par monotonicité : $w' \overset{KPK}{\models} \varphi_2$
  - *Cas 2* : $I \overset{CL}{\not\models} \varphi_1$, *i.e* $I \overset{CL}{\models} \neg\varphi_1$:
    Comme $|\neg\varphi_1| < |\varphi|$, on peut appliquer l'hypothèse d'induction à $\neg\varphi_1$: il vient que $w \overset{KPK}{\models} \neg\varphi_1$. Donc par définition sémantique : $w' \overset{KPK}{\not\models} \varphi_1$, ce qui contredit notre hypothèse : ce cas est exclus.
- $\varphi = \neg\psi$:
  Soit $w' \geq w$. Montrons que $w' \overset{KPK}{\not\models} \psi$. Sachant qu'on sait que $I \overset{CL}{\not\models} \psi$, le résultat sera acquis si on montre la contraposée :

  $$w' \overset{KPK}{\models} \psi \Longrightarrow I \overset{CL}{\models} \psi$$

  Supposons que $w' \overset{KPK}{\models} \psi$. Alors $\alpha(w') \overset{CL}{\models} \psi$ (on le vérifie aisément puisque les règles de la sémantique intuitioniste sont plus fortes que les règles sémantiques de la logique classique).
  Or, comme $(fv(\psi) \cup bv(\psi)) \cap \mathscr{Q} = \emptyset$, il est clair que :

  $$\alpha(w') \backslash \mathscr{Q} \overset{CL}{\models} \psi$$

Par ailleurs : $\alpha(w')\backslash\mathscr{Q} \supset \alpha(w)\backslash\mathscr{Q} = I\backslash\mathscr{Q}$.
Supposons, par l'absurde, que $\Big(\alpha(w')\backslash\mathscr{Q}\Big)\backslash\Big(I\backslash\mathscr{Q}\Big) \neq \emptyset$: alors il existerait $p \notin I$ tel que $\mathscr{K}, w' \overset{KPK}{\models} p$. Mais comme $w' \geq w$, cela contredirait : $p \notin I \Longrightarrow \forall w' \geq w, \mathscr{K}, w' \overset{KPK}{\not\models} p$.
Donc $\alpha(w')\backslash\mathscr{Q} = I\backslash\mathscr{Q}$, et :

$$I\backslash\mathscr{Q} \overset{CL}{\models} \psi$$

et comme $(fv(\psi) \cup bv(\psi)) \cap \mathscr{Q} = \emptyset$:

$$I \overset{CL}{\models} \psi$$

Le résultat est acquis.

Hérédité : si $\varphi \overset{\text{def}}{=} Qp.\,\psi$ a $n > 0$ quantificateurs :

(avec les notations de l'énoncé)

Soient $I \subseteq \mathscr{P}$, $\mathscr{K} \overset{\text{def}}{=} (W, \leq_{\mathscr{K}}, \alpha_{\mathscr{K}})$ un modèle de Kripke, $\varphi \overset{\text{def}}{=} Qp.\,\psi$ une formule QBF à $n > 0$ quantificateurs bien quantifiée telle que $(fv(\varphi) \cup bv(\varphi)) \cap \mathscr{Q} = \emptyset$.

Supposons que $I \overset{QBF}{\models} \varphi = Qp.\,\psi$, et que $\mathscr{K}$ force I sur $\mathscr{P}\backslash(\underbrace{bv(\varphi)}_{=\{p\}\cup bv(\psi)} \cup \mathscr{Q})$.

Soit $w \in W$.

Pour toute variable $q \notin \{p\} \cup bv(\psi) \cup \mathscr{Q}$,

- $q \in I \Longrightarrow \mathscr{K}, w \overset{KPK}{\models} q$
- $q \notin I \Longrightarrow \forall w' \geq w, \mathscr{K}, w' \overset{KPK}{\not\models} q$

D'où en particulier, de même que précédemment :

$I\backslash\Big(\{p\} \cup bv(\psi) \cup \mathscr{Q}\Big) = \alpha_{\mathscr{K}}(w)\backslash\Big(\{p\} \cup bv(\psi) \cup \mathscr{Q}\Big)$

On remarque par ailleurs que :

- $p \notin bv(\psi)$ car φ est bien quantifiée
- $p \notin \mathscr{Q}$ car $(fv(\varphi) \cup bv(\varphi)) \cap \mathscr{Q} = \emptyset$

Montrons que $w \overset{KPK}{\models} \varphi^*$.

Cas 1 : Si $Q = \forall$

Soit $w' \geq w$.

Supposons que $w' \overset{KPK}{\models} p \vee \neg p$, *i.e* $w' \overset{KPK}{\models} p$ ou $w' \overset{KPK}{\models} \neg p$, et montrons que $w' \overset{KPK}{\models} \psi^*$.

Considérons la structure de Kripke :

$$\mathscr{K}_{w'} \overset{\text{def}}{=} (\{w'' \in W \mid w'' \geq w'\}, \leq_{\mathscr{K}}, \alpha)$$

Le point clé est que, par monotonicité :

- si $w' \overset{KPK}{\models} p$: tous les mondes de $\mathscr{K}_{w'}$ forcent p
- si $w' \overset{KPK}{\models} \neg p$: tous les mondes de $\mathscr{K}_{w'}$ forcent $\neg p$

On sait par ailleurs que $I \cup \{p\} \overset{CL}{\models} \psi$ et $I\backslash\{p\} \overset{CL}{\models} \psi$

Donc :

- *si* $w' \overset{KPK}{\models} p$: $\mathscr{K}_{w'}$ force $I \cup \{p\} \subseteq \mathscr{P}$ sur $\mathscr{P}\backslash\Big(bv(\psi) \cup \mathscr{Q}\Big)$ puisque
  - $\mathscr{K}$ force I sur $\mathscr{P}\backslash\Big(\{p\} \cup bv(\psi) \cup \mathscr{Q}\Big)$
  - $p \in I \cup \{p\}$, et pour tout $w'' \geq w'$, $w'' \overset{KPK}{\models} p$ par monotonicité

  et on applique l'hypothèse d'induction à ψ : par suite, pour tout $w'' \geq w'$, $w'' \overset{KPK}{\models} \psi^*$.
  Le résultat est donc acquis.
- *si* $w' \overset{KPK}{\models} \neg p$: $\mathscr{K}_{w'}$ force $I\backslash\{p\} \subseteq \mathscr{P}$ sur $\mathscr{P}\backslash\Big(bv(\psi) \cup \mathscr{Q}\Big)$ puisque
  - $\mathscr{K}$ force I sur $\mathscr{P}\backslash\Big(\{p\} \cup bv(\psi) \cup \mathscr{Q}\Big)$
  - $p \notin I\backslash\{p\}$, et pour tout $w'' \geq w'$, $w'' \overset{KPK}{\models} \neg p$ par monotonicité

  et on conclut de même en appliquant l'hypothèse d'induction à ψ.

Cas 2 : Si $Q = \exists$

Soit $w' \geq w$.

Supposons que $w' \overset{KPK}{\models} \psi^* \longrightarrow q_n$, et montrons que

- $w' \overset{KPK}{\models} \Big((p \longrightarrow q_n) \vee (\neg p \longrightarrow q_n)\Big)$
- *i.e* $w' \overset{KPK}{\models} p \longrightarrow q_n$ ou $w' \overset{KPK}{\models} \neg p \longrightarrow q_n$
- *i.e* $\Big($ pour tout $w'' \geq w'$: *si* $w'' \overset{KPK}{\models} p$, *alors* $w'' \overset{KPK}{\models} q_n\Big)$ OU $\Big($ pour tout $w'' \geq w'$: *si* $w'' \overset{KPK}{\models} \neg p$, *alors* $w'' \overset{KPK}{\models} q_n\Big)$

On sait par ailleurs que $I \cup \{p\} \overset{CL}{\models} \psi$ ou $I \backslash \{p\} \overset{CL}{\models} \psi$

- *si* $I \cup \{p\} \overset{CL}{\models} \psi$:
  On pose

  $$\mathscr{K}_{w'} \overset{\text{def}}{=} (\underbrace{\{w'' \in W \mid w'' \geq w' \text{ et } w'' \overset{KPK}{\models} p\}}_{\overset{\text{def}}{=} W'}, \leq_{\mathscr{K}}, \alpha)$$

  Il vient que $\mathscr{K}_{w'}$ force $I \cup \{p\} \subseteq \mathscr{P}$ sur $\mathscr{P} \backslash \Big(bv(\psi) \cup \mathscr{Q}\Big)$ puisque
  - $\mathscr{K}$ force I sur $\mathscr{P} \backslash \Big(\{p\} \cup bv(\psi) \cup \mathscr{Q}\Big)$
  - $p \in I \cup \{p\}$, et pour tout $w'' \in W'$, $w'' \overset{KPK}{\models} p$

  On applique l'hypothèse d'induction à ψ : par suite, pour tout $w'' \geq w'$ tel que $w'' \overset{KPK}{\models} p$, $w'' \overset{KPK}{\models} \psi^*$.
  Il s'ensuit que $w'' \overset{KPK}{\models} q_n$, puisque $w' \overset{KPK}{\models} \psi^* \longrightarrow q_n$.
  On a donc montré que : pour tout $w'' \geq w'$: *si* $w'' \overset{KPK}{\models} p$, *alors* $w'' \overset{KPK}{\models} q_n$, et le résultat est acquis.
- *si* $I \backslash \{p\} \overset{CL}{\models} \psi$:
  On procède de la même manière, avec $\mathscr{K}_{w'} \overset{\text{def}}{=} (\underbrace{\{w'' \in W \mid w'' \geq w' \text{ et } w'' \overset{KPK}{\models} \neg p\}}_{\overset{\text{def}}{=} W'}, \leq_{\mathscr{K}}, \alpha)$, pour montrer que pour tout $w'' \geq w'$:

  si $w'' \overset{KPK}{\models} \neg p$, *alors* $w'' \overset{KPK}{\models} q_n$.

3.

Par induction sur le nombre de quantificateurs n de φ, montrons que :

> Pour tous φ bien quantifiée telle que $(fv(\varphi) \cup bv(\varphi)) \cap \mathscr{Q} = \emptyset$, $I \subseteq \mathscr{P}$:
>
> *si* $I \overset{QBF}{\not\models} \varphi$, *alors* il existe un modèle de Kripke $\mathscr{K} \overset{\text{def}}{=} (W, \leq_{\mathscr{K}}, \alpha_{\mathscr{K}})$ et un monde $w_0 \in W$ tels que :
>
> - $\mathscr{K}$ force I sur $\mathscr{P} \backslash (bv(\varphi) \cup \mathscr{Q})$
> - $\mathscr{K}, w_0 \overset{KPK}{\not\models} \varphi^*$

NB : Encore une fois, comme φ^* n'est pas définie dans le cas contraire, on fera l'hypothèse que $(fv(\varphi) \cup bv(\varphi)) \cap \mathscr{Q} = \emptyset$

Cas de base : si $n = 0, \varphi \in \mathcal{F}_0(\mathscr{P})$:

Soient $I \subseteq \mathscr{P}$, φ une formule QBF de $\mathcal{F}_0(\mathscr{P})$ telle que $(fv(\varphi) \cup bv(\varphi)) \cap \mathscr{Q} = \emptyset$.

Supposons que $I \overset{QBF}{\not\models} \varphi$, *i.e* $I \overset{CL}{\not\models} \varphi$.

Soit w_0 un monde tel que

$$\alpha(w_0) \overset{\text{def}}{=} I$$

On pose $\mathscr{K} \overset{\text{def}}{=} (\{w_0\}, =, \alpha)$.

$\mathscr{K}$ force I sur $\mathscr{P} \backslash (\underbrace{bv(\varphi)}_{=\emptyset} \cup \mathscr{Q}) = \mathscr{P} \backslash \mathscr{Q}$, puisque pour toute $p \in \mathscr{P} \backslash \mathscr{Q}$:

- $p \in I = \alpha(w_0) \Longrightarrow \mathscr{K}, w_0 \overset{KPK}{\models} p$
- $p \notin I = \alpha(w_0) \Longrightarrow \forall w' \geq w_0, \mathscr{K}, w' \overset{KPK}{\not\models} p$ (le seul monde supérieur à w_0 est w_0)

De plus :

$$\mathscr{K}, w_0 \overset{KPK}{\not\models} \varphi^* = \varphi$$

(on le vérifie aisément puisque $\alpha(w_0) = I \overset{CL}{\not\models} \varphi$, les règles de la sémantique intuitioniste sont plus fortes que les règles sémantiques de la logique classique et w_0 est le seul monde de $\mathscr{K}$).

Hérédité : si $\varphi \overset{\text{def}}{=} Qp.\,\psi$ a $n > 0$ quantificateurs :

(avec les notations de l'énoncé)

Soient $I \subseteq \mathscr{P}$, $\varphi \overset{\text{def}}{=} Qp.\,\psi$ une formule QBF à $n > 0$ quantificateurs bien quantifiée telle que $\big(fv(\varphi) \cup bv(\varphi)\big) \cap \mathscr{Q} = \emptyset$.

Supposons que $I \overset{QBF}{\nvDash} \varphi = Qp.\,\psi$.

Notons que :

- $p \notin bv(\psi)$ car φ est bien quantifiée
- $p \notin \mathscr{Q}$ car $\big(fv(\varphi) \cup bv(\varphi)\big) \cap \mathscr{Q} = \emptyset$

Construisons un modèle de Kripke

$$\mathscr{K} \overset{\text{def}}{=} (W, \leq_{\mathscr{K}}, \alpha_{\mathscr{K}})$$

qui force I sur $\mathscr{P} \backslash (\underbrace{bv(\varphi)}_{=\{p\} \cup bv(\psi)} \cup \mathscr{Q})$, et un monde $w_0 \in W$ tel que $w_0 \overset{KPK}{\nvDash} \varphi^*$

Cas 1 : Si $Q = \forall$

Il vient que $I \cup \{p\} \overset{CL}{\nvDash} \psi$ ou $I \backslash \{p\} \overset{CL}{\nvDash} \psi$

Si $I \cup \{p\} \overset{CL}{\nvDash} \psi$:

On applique l'hypothèse d'induction à ψ et $I \cup \{p\} \subseteq \mathscr{P}$: par suite, il existe un modèle de Kripke $\mathscr{K} \overset{\text{def}}{=} (W, \leq_{\mathscr{K}}, \alpha_{\mathscr{K}})$ et un monde $w_0 \in W$ tels que

- $\mathscr{K}$ force $I \cup \{p\} \subseteq \mathscr{P}$ sur $\mathscr{P} \backslash (bv(\psi) \cup \mathscr{Q})$, donc en particulier :
  - $\mathscr{K}$ force I sur $\mathscr{P} \backslash (\{p\} \cup bv(\psi) \cup \mathscr{Q})$ $\quad \circledast$
  - comme $p \in I \cup \{p\}$: $\forall w \in W, \mathscr{K}, w \overset{KPK}{\vDash} p$
- $\mathscr{K}, w_0 \overset{KPK}{\nvDash} \psi^*$

Il vient donc que $\mathscr{K}, w_0 \overset{KPK}{\vDash} p$ et $\mathscr{K}, w_0 \overset{KPK}{\nvDash} \psi^*$, d'où

$$\mathscr{K}, w_0 \overset{KPK}{\nvDash} p \vee \neg p \longrightarrow \psi^* = \varphi^* \quad \circledast\circledast$$

Avec $\circledast$ et $\circledast\circledast$, le résultat est acquis.

Si $I \backslash \{p\} \overset{CL}{\nvDash} \psi$:

On procède de même $I \backslash \{p\}$: en l'occurrence, on aura $\mathscr{K}, w_0 \overset{KPK}{\vDash} \neg p$ et $\mathscr{K}, w_0 \overset{KPK}{\nvDash} \psi^*$ (ce qui implique aussi que $\mathscr{K}, w_0 \overset{KPK}{\nvDash} p \vee \neg p \longrightarrow \psi^*$).

Cas 2 : Si $Q = \exists$

Il vient que $I \cup \{p\} \overset{CL}{\nvDash} \psi$ et $I \backslash \{p\} \overset{CL}{\nvDash} \psi$

On applique deux fois l'hypothèse d'induction : à ψ et $I \backslash \{p\} \subseteq \mathscr{P}$, et à ψ et $I \cup \{p\} \subseteq \mathscr{P}$.

Par suite, il existe des modèle de Kripke

$$\mathscr{K}_{\neg p} \overset{\text{def}}{=} (W_{\neg p}, \leq_{\mathscr{K}_{\neg p}}, \alpha_{\mathscr{K}_{\neg p}}),\ \mathscr{K}_p \overset{\text{def}}{=} (W_p, \leq_{\mathscr{K}_p}, \alpha_{\mathscr{K}_p})$$

et des mondes

$$w_{\neg p} \in W_{\neg p},\ w_p \in W_p$$

tels que

- $\mathscr{K}_{\neg p}$ force $I \backslash \{p\} \subseteq \mathscr{P}$ sur $\mathscr{P} \backslash (bv(\psi) \cup \mathscr{Q})$, donc en particulier :
  - $\mathscr{K}_{\neg p}$ force I sur $\mathscr{P} \backslash (\{p\} \cup bv(\psi) \cup \mathscr{Q})$
  - comme $p \notin I \backslash \{p\}$: $\forall w \in W_{\neg p}, \mathscr{K}_{\neg p}, w \overset{KPK}{\vDash} \neg p$
- $\mathscr{K}_p$ force $I \cup \{p\} \subseteq \mathscr{P}$ sur $\mathscr{P} \backslash (bv(\psi) \cup \mathscr{Q})$, donc en particulier :
  - $\mathscr{K}_p$ force I sur $\mathscr{P} \backslash (\{p\} \cup bv(\psi) \cup \mathscr{Q})$
  - comme $p \in I \cup \{p\}$: $\forall w \in W_p, \mathscr{K}_p, w \overset{KPK}{\vDash} p$
- $\mathscr{K}_p, w_{\neg p} \overset{KPK}{\nvDash} \psi^*$ et $\mathscr{K}_{\neg p} \overset{KPK}{\nvDash} \psi^*$

On pose

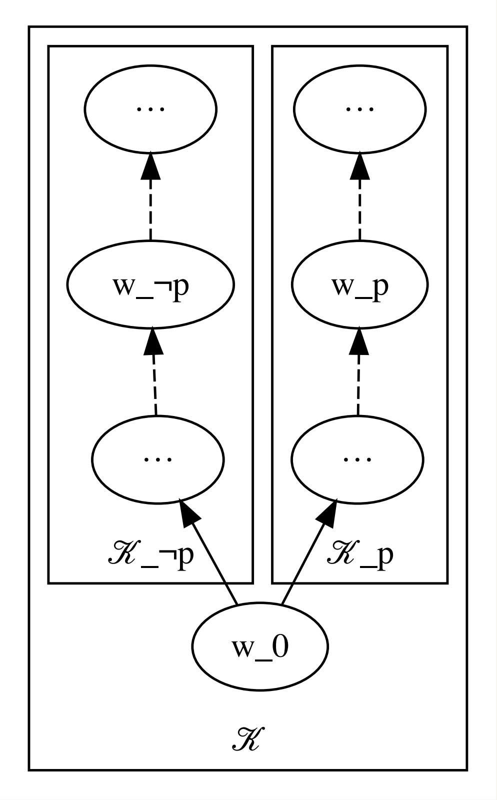
$$\mathscr{K} \overset{\text{def}}{=} (W_p \cup W_{\neg p} \cup \{w_0\}, \leq_{\mathscr{K}}, \alpha_{\mathscr{K}})$$

où :

- on prolonge $\leq_{\mathscr{K}_p}$ et $\leq_{\mathscr{K}_{\neg p}}$ pour construire un monde w_0 tel que
    - $$\forall w \in \mathscr{K}_p, \quad w_0 \leq_{\mathscr{K}_p} w$$
    - $$\forall w \in \mathscr{K}_{\neg p}, \quad w_0 \leq_{\mathscr{K}_{\neg p}} w$$
- $$\leq_{\mathscr{K}} \overset{\text{def}}{\equiv} \leq_{\mathscr{K}_p} \vee \leq_{\mathscr{K}_{\neg p}}$$
- Quitte à le supprimer, on peut supposer que q_n n'appartient à aucun des $\alpha_{\mathscr{K}_p}(w)$ (pour $w \in \mathscr{K}_p$) ni des $\alpha_{\mathscr{K}_{\neg p}}(w)$ (pour $w \in \mathscr{K}_{\neg p}$), puisque q_n n'intervient pas dans ψ^* (ψ a strictement moins de n quantificateurs).
    - on définit alors $\alpha_{\mathscr{K}}$ de la manière suivante :
        - $\alpha_{\mathscr{K}}(w_0) \overset{\text{def}}{\equiv} I \backslash \Big(bv(\varphi) \cup \{q_1, \cdots, q_{n-1}\}\Big)$
        - $\forall w \in W_p$,
          $$\alpha_{\mathscr{K}}(w) \overset{\text{def}}{\equiv} \begin{cases} \alpha_{\mathscr{K}_p}(w) \cup \{q_n\} \text{ si } \mathscr{K}_p, w \overset{KPK}{\models} \psi^* \\ \alpha_{\mathscr{K}_p}(w) \text{ sinon} \end{cases}$$
        - $\forall w \in W_{\neg p}$,
          $$\alpha_{\mathscr{K}}(w) \overset{\text{def}}{\equiv} \begin{cases} \alpha_{\mathscr{K}_{\neg p}}(w) \cup \{q_n\} \text{ si } \mathscr{K}_{\neg p}, w \overset{KPK}{\models} \psi^* \\ \alpha_{\mathscr{K}_{\neg p}}(w) \text{ sinon} \end{cases}$$

NB :

- Notons qu'ajouter q_n ou non aux interprétations des mondes ne change le fait qu'ils forcent ou non ψ^*, puisque q_n n'intervient pas dans ψ^* (ψ a strictement moins de n quantificateurs). Et par monotonicité, cet ajout laisse $\alpha_{\mathscr{K}}$ croissante.
- $\mathscr{K}, w_0 \overset{KPK}{\not\models} \psi^*$ puisque $\mathscr{K}, w_p \text{ (resp. } w_{\neg p}) \overset{KPK}{\not\models} \psi^*$, et $w_p \text{ (resp. } w_{\neg p}) \geq w_0$



Dans $\mathscr{K}$, on a construit w_0 pour que $\mathscr{K}, w_0 \overset{KPK}{\models} \psi^* \longrightarrow q_n$ (puisque pour tous les mondes supérieurs à w_0, q_n est satisfaite dès que ψ^* l'est).

En revanche,

$$\mathscr{K}, w_0 \overset{KPK}{\not\models} (p \longrightarrow q_n) \vee (\neg p \longrightarrow q_n)$$

puisque w_p (resp. $w_{\neg p}$) vérifie

- $\mathscr{K}, w_p \overset{KPK}{\models} p$ (resp. $\mathscr{K}, w_{\neg p} \overset{KPK}{\models} \neg p$)
- $\mathscr{K}, w_p \text{ (resp. } w_{\neg p}) \overset{KPK}{\not\models} \psi^*$, d'où $\mathscr{K}, w_p \text{ (resp. } w_{\neg p}) \overset{KPK}{\not\models} q_n$

et contredit donc $\mathscr{K}, w_0 \overset{KPK}{\not\models} p \longrightarrow q_n$ (resp. $w_0 \overset{KPK}{\not\models} \neg p \longrightarrow q_n$).

Il apparaît donc que

$$\mathscr{K}, w_0 \overset{KPK}{\not\models} (\psi^* \longrightarrow q_n) \longrightarrow \Big((p \longrightarrow q_n) \vee (\neg p \longrightarrow q_n)\Big) = \varphi^*$$

Par ailleurs, $\mathscr{K}$ force I sur $\mathscr{P} \backslash (\{p\} \cup bv(\psi) \cup \mathscr{Q})$, puisque :

- $\mathscr{K}_{\neg p}$ force I sur $\mathscr{P}\backslash(\{p\} \cup bv(\psi) \cup \mathscr{Q})$
- $\mathscr{K}_p$ force I sur $\mathscr{P}\backslash(\{p\} \cup bv(\psi) \cup \mathscr{Q})$
- Pour toute variable $q \notin \{p\} \cup bv(\psi) \cup \mathscr{Q}$,
  - $$\begin{aligned} q \in I \Longrightarrow q \in \alpha_{\mathscr{K}}(w_0) \qquad & \left(I\backslash\Big(\{p\} \cup bv(\psi) \cup \mathscr{Q}\Big) \subseteq I\backslash\Big(\underbrace{bv(\varphi) \cup \{q_1, \cdots, q_{n-1}\}}_{\subseteq \alpha_{\mathscr{K}}(w_0)}\Big)\right) \\ \Longrightarrow \mathscr{K}, w_0 \overset{KPK}{\models} q & \end{aligned}$$
  - $$\begin{aligned} q \notin I \Longrightarrow q \notin \alpha_{\mathscr{K}}(w_0) \qquad & \left(\mathscr{P}\backslash\Big(I \cup \{p\} \cup bv(\psi) \cup \mathscr{Q}\Big) \subseteq \mathscr{P}\backslash\Big(\underbrace{I \cup bv(\varphi) \cup \{q_1, \cdots, q_n\}}_{\supseteq \alpha_{\mathscr{K}}(w_0)}\Big)\right) \\ \Longrightarrow \mathscr{K}, w_0 \overset{KPK}{\not\models} q & \\ \Longrightarrow \forall w' \geq w_0, \mathscr{K}, w' \overset{KPK}{\not\models} q \qquad & \left(\text{car } \mathscr{K}_p \text{ et } \mathscr{K}_{\neg p} \text{ forcent } I \text{ sur } \mathscr{P}\backslash(\{p\} \cup bv(\psi) \cup \mathscr{Q})\right) \end{aligned}$$

Donc le résultat est acquis.

4.

Pour toute formule QBF φ, on note $\widetilde{\varphi}$ la formule bien quantifiée équivalente construite comme dans la **question 1** par renommage éventuel des variables liées, vérifiant en plus $(fv(\widetilde{\varphi}) \cup bv(\widetilde{\varphi})) \cap \mathscr{Q} = \emptyset$, ce qu'il est loisible de supposer si on n'effectue le renommage qu'avec des variables de $\mathscr{P}\backslash\mathscr{Q}$.

NB :

- Il est alors nécessaire de supposer que $|\mathscr{P}\backslash\mathscr{Q}| > |fv(\varphi) \cup bv(\varphi)|$, et ce, pour toute variable φ : il faut donc que $\mathscr{P}\backslash\mathscr{Q}$ soit infini (hypothèse qui n'est pas faite dans l'énoncé, mais qu'il est raisonnable de faire vu le but du DM).
- Notons que si φ est close, $\widetilde{\varphi}$ le reste.

On pose, pour tout formule QBF φ :

$$\varphi^\dagger \overset{\text{def}}{=} (\widetilde{\varphi})^*$$

Montrons que

> $$\overset{QBF}{\models} \varphi \quad \Longleftrightarrow \quad \overset{KPK}{\models} \varphi^\dagger$$

$\Longleftarrow$:

Montrons la contraposée : si il existe $I \subseteq \mathscr{P}$ tel que $I \overset{QBF}{\not\models} \varphi$, soit $I \overset{QBF}{\not\models} \widetilde{\varphi}$ (puisque φ et $\widetilde{\varphi}$ sont équivalentes), alors en appliquant la **question 3** à $\widetilde{\varphi}$, il existe un modèle de Kripke $\mathscr{K} \overset{\text{def}}{=} (W, \leq_{\mathscr{K}}, \alpha_{\mathscr{K}})$ et un monde $w_0 \in W$ tels que

$$\mathscr{K}, w_0 \overset{KPK}{\not\models} (\widetilde{\varphi})^* = \varphi^\dagger$$

Et il en résulte que $\overset{KPK}{\not\models} \varphi^\dagger$.

$\Longrightarrow$:

Supposons que pour tout $I \subseteq \mathscr{P}$, $I \overset{QBF}{\models} \varphi$, soit $I \overset{QBF}{\models} \widetilde{\varphi}$ (puisque φ et $\widetilde{\varphi}$ sont équivalentes).

Soit $\mathscr{K} \overset{\text{def}}{=} (W, \leq_{\mathscr{K}}, \alpha_{\mathscr{K}})$ un modèle de Kripke.

Montrons que $\forall w \in W, \quad \mathscr{K}, w \overset{KPK}{\models} \varphi^* = (\widetilde{\varphi})^*$.

- *S'il existe $I \subseteq \mathscr{P}$ tel que $\mathscr{K}$ force I sur $\mathscr{P}\backslash(bv(\widetilde{\varphi}) \cup \mathscr{Q})$* :
  alors comme $I \overset{QBF}{\models} \widetilde{\varphi}$, on applique le théorème de **question 2** à $\widetilde{\varphi}$, et le résultat s'ensuit.

- *Sinon, si $\mathscr{K}$ ne force pas I sur $\mathscr{P}\backslash(bv(\widetilde{\varphi}) \cup \mathscr{Q})$ pour tout $I \subseteq \mathscr{P}$* :
  alors pour tout $I \subseteq \mathscr{P}$, il existe $w \in W$ et une variable $p \notin bv(\widetilde{\varphi}) \cup \mathscr{Q}$ tels que :
  - $p \in I$ et $\underbrace{\mathscr{K}, w \overset{KPK}{\not\models} p}_{\text{i.e } \; p \notin \alpha_{\mathscr{K}}(w)}$ $\circledast$

  OU
  - $p \notin I$ et $\underbrace{\mathscr{K}, w \overset{KPK}{\not\models} \neg p}_{\text{i.e } \; \exists w' \geq w; \;\; p \in \alpha_{\mathscr{K}}(w')}$ $\circledast\circledast$

  Notons alors que : pour que $\mathscr{K}$ ne force pas I sur $\mathscr{P}\backslash(bv(\widetilde{\varphi}) \cup \mathscr{Q})$ pour tout $I \subseteq \mathscr{P}$, il faut et il suffit qu'il existe une variable $p \notin bv(\widetilde{\varphi}) \cup \mathscr{Q}$ telle que :

  $$\exists w_0, w_1 \in W; \; p \in \alpha_{\mathscr{K}}(w_0) \wedge p \notin \alpha_{\mathscr{K}}(w_1)$$

- La condition est *nécessaire*, car **sinon** : en posant $I_0 \overset{\text{def}}{=} \{p \in \mathscr{P}\backslash(bv(\varphi) \cup \mathscr{Q}) \mid \forall w \in W,\ \mathscr{K}, w \overset{KPK}{\models} p\}$, $\mathscr{K}$ forcerait I sur $\mathscr{P}\backslash(bv(\widetilde{\varphi}) \cup \mathscr{Q})$
    - *en effet* : toute variable $q \in \mathscr{P}\backslash(bv(\varphi) \cup \mathscr{Q})$ n'appartenant pas à I n'appartiendrait pas à l'interprétation d'un certain monde w_1, et donc n'appartiendrait à l'interprétation d'aucun autre, car sinon il existerait $w_0, w_1 \in W$ tels que $q \in \alpha_{\mathscr{K}}(w_0) \land q \notin \alpha_{\mathscr{K}}(w_1)$
- Elle est *suffisante* puisqu'alors : pour tout $I \subseteq \mathscr{P}$, si $p \in I$, p vérifie ⊛ avec $w = w_1$, et si $p \notin I$, p vérifie ⊛⊛ avec $w = w' = w_0$

On pose alors

$$\mathscr{P}_0 \overset{\text{def}}{=} \{p \in \mathscr{P}\backslash(bv(\widetilde{\varphi}) \cup \mathscr{Q}) \mid \exists w_0, w_1 \in W;\ p \in \alpha_{\mathscr{K}}(w_0) \land p \notin \alpha_{\mathscr{K}}(w_1)\} \neq \emptyset$$

Et on note $\mathscr{K}_0$ le modèle de Kripke obtenu à partir de $\mathscr{K}$ en supprimant toutes les variables appartenant à $\mathscr{P}_0$ des interprétations des mondes de $\mathscr{K}$.
On remarque que tout monde de $\mathscr{K}$ force $(\widetilde{\varphi})^*$ si, et seulement si il force $(\widetilde{\varphi})^*$ dans $\mathscr{K}_0$, puisque toutes les variables de $(\widetilde{\varphi})^*$ appartiennent à $bv(\widetilde{\varphi}) \cup \mathscr{Q}$ (et donc n'appartiennent *pas* à $\mathscr{P}_0$) comme $\widetilde{\varphi}$ est close.

Par l'absurde : S'il existait un monde w de $\mathscr{K}$ tel que $\mathscr{K}, w \overset{KPK}{\not\models} (\widetilde{\varphi})^*$, il existerait donc aussi un monde w_0 de $\mathscr{K}_0$ tel que

$$\mathscr{K}_0, w_0 \overset{KPK}{\not\models} (\widetilde{\varphi})^* \qquad ⊛⊛⊛$$

Or, $\mathscr{K}_0$ force $\emptyset$ sur $\mathscr{P}\backslash(bv(\widetilde{\varphi}) \cup \mathscr{Q})$, puisqu'aucune variable de $\mathscr{P}\backslash(bv(\widetilde{\varphi}) \cup \mathscr{Q})$ n'appartient à une interprétation de $\mathscr{K}_0$, donc aucune variable de $\mathscr{P}\backslash(bv(\widetilde{\varphi}) \cup \mathscr{Q})$ n'est satisfaite par un monde de $\mathscr{K}_0$.
⊛ ⊛ ⊛ contredit donc le théorème de la **question 2** appliqué à $\widetilde{\varphi}$, $I = \emptyset$, et $\mathscr{K}_0$.

Donc tous les mondes de $\mathscr{K}$ forcent $(\widetilde{\varphi})^* = \varphi^\dagger$.

Dans tous les cas, le résultat est acquis.

Par ailleurs, on peut construire une fonction qui à toute formule QBF φ associe $(\widetilde{\varphi})^* = \varphi^\dagger$ dans $LOGSPACE$, de la manière suivante :

NB :

- Dans un souci de simplification, on supposera qu'on peut écrire sur le ruban d'entrée : à la fin, ce ruban est recopié sur le ruban de sortie.
- tous les compteurs utilisés seront dans une base $b \geq 2$, pour occuper un espace logarithmique, et chaque variable de $\mathscr{Q}$ comme de $\mathscr{P}\backslash\mathscr{Q}$ sera identifiée par un bit introductif (pour indiquer si elle appartient à $\mathscr{Q}$ ou à $\mathscr{P}\backslash\mathscr{Q}$) concaténé à son numéro dans l'ensemble auquel elle appartient.

Pour toute entrée φ :

- on compte le nombre m de variables distinctes de φ, et on remplace toutes les variables appartenant à $\mathscr{Q}$ par de nouvelles variables de $\mathscr{P}\backslash\mathscr{Q}$
- Pour calculer $\widetilde{\varphi}$, il suffit de remplacer les variables liées comme décrit dans la **question 1** (pour ce faire, on n'a besoin que d'écrire des numéros de $O(1)$ variables sur le ruban de travail, donc on n'occupe encore qu'un espace logarithmique)
- Pour calculer $(\widetilde{\varphi})^* = \varphi^\dagger$, on utilise la procédure décrite dans l'énoncé, en éliminant les quantificateurs de gauche à droite. Si le premier quantificateur sur le ruban d'entrée (en partant de la gauche) est :
    - $\forall$, suivi d'une variable p, on écrit "$(p \lor \neg p) \longrightarrow$" devant la formule qui le suit (quitte à faire un décalage, en espace constant).
    - $\exists$, suivi d'une variable p, on écrit "$($" avant la formule qui le suit, et "$\longrightarrow q_n) \longrightarrow (p \longrightarrow q_n) \lor (\neg p \longrightarrow q_n)$" après, l'indice n étant tenu à jour par un compteur.

L'espace occupé est donc logarithmique en la taille de la formule.

> La fonction $\varphi \mapsto \varphi^\dagger$ précédemment décrite est dans $LOGSPACE$, et donc *a fortiori* dans $PTIME$.

II. De la logique intuitionniste à QBF

5.

$$\frac{}{\Gamma \cup \{\varphi\} \vdash \varphi} \quad (Ax)$$

$$\frac{\Gamma \vdash \varphi_1 \qquad \Gamma \cup \{\varphi_2\} \vdash \psi \qquad \varphi_1 \longrightarrow \varphi_2 \in \Gamma}{\Gamma \vdash \psi} \quad (\longrightarrow L)$$

$$\frac{\Gamma \cup \{\varphi_1\} \vdash \varphi_2}{\Gamma \vdash \varphi_1 \longrightarrow \varphi_2} \quad (\longrightarrow R)$$

Soit φ une formule à m variables dont le seul connecteur logique est $\longrightarrow$.

Si on retire toutes les parenthèses, l'écriture syntaxique de φ est de la forme :

$$p_1 \longrightarrow p_2 \longrightarrow \cdots \longrightarrow p_m$$

où les p_i sont des variables propositionnelles.

φ est donc de taille

$$n \overset{\text{def}}{=} 2m - 1$$

Supposons que $\vdash_{LJ'_O} \varphi$.

On veut borner la profondeur de l'arbre de preuve de plus petite taille (*i.e* ayant le moins de noeuds) de $\vdash_{LJ'_O} \varphi$.

Dans la suite, **on considérera la plus longue branche de cet arbre de plus petite taille** en partant du bas (de la racine $\vdash_{LJ'_O} \varphi$) vers le haut (vers la règle (Ax)) : elle est constituée d'un certain nombre d'applications de règle d'inférences de LJ'_0.

> **Observation 1** : La règle (Ax) n'y est appliquée qu'une et une seule fois, et c'est la dernière règle appliquée.

Preuve : (Ax) ne peut être appliquée qu'une fois au plus, et toute branche finie se termine nécessairement par cette règle.

> **Observation 2** : À chaque étape, l'ensemble des *hypothèses* est un sous-ensemble de l'ensemble des sous-formules de φ, et le *but* est une sous-formule de φ.

Preuve : c'est vrai au départ (l'ensemble des hypothèses est vide, le but vaut φ), et on vérifie aisément que l'invariant est conservé à chaque application d'une des règles d'inférence de LJ'_0.

> **Observation 3** : À chaque application de la règle $(\longrightarrow R)$ ou de la règle $(\longrightarrow L)$, l'ensemble des hypothèses croît (pour l'ordre d'inclusion ensembliste).

Preuve : c'est vrai au départ (l'ensemble des hypothèses de la racine est vide), et on vérifie aisément par induction que la propriété est vérifiée à chaque application d'une des deux règles d'inférence $(\longrightarrow R)$ ou $(\longrightarrow L)$:

$$\frac{\Gamma \vdash \varphi_1 \qquad \Gamma \cup \{\varphi_2\} \vdash \psi \qquad \varphi_1 \longrightarrow \varphi_2 \in \Gamma}{\Gamma \vdash \psi} \quad (\longrightarrow L)$$

$$\frac{\Gamma \cup \{\varphi_1\} \vdash \varphi_2}{\Gamma \vdash \varphi_1 \longrightarrow \varphi_2} \quad (\longrightarrow R)$$

> **Observation 4** : À chaque application de la règle $(\longrightarrow R)$ ou de la règle $(\longrightarrow L)$:
>
> - l'ensemble des hypothèses croît *strictement*
>
> **ou**
>
> - l'ensemble des hypothèses Γ reste constant mais le but ψ (sous-formule de φ) change, et le séquent $\Gamma \vdash \psi$ n'apparaît plus dans la branche ultérieurement.

Preuve :

Dans le cas contraire : le même séquent apparaîtrait deux fois dans la branche : les règles intermédiaires entre ces deux occurrences seraient donc superflues, et on pourrait avoir un arbre de preuve de taille strictement plus petite en les supprimant, ce qui contredirait la minimalité de l'arbre qu'on considère.

Notons de plus qu'il y a au plus n sous-formules de φ, puisque chaque sous-formule correspond à la donnée d'un sous-arbre de l'arbre syntaxique de φ, et chaque sous-arbre est déterminé de manière biunivoque par sa racine (qui est un sommet de l'arbre syntaxique de φ).

Par conséquent, d'après l'observation 2 et l'observation 4 : les règles $(\longrightarrow L)$ et $(\longrightarrow R)$ ne peuvent être appliquées qu'un nombre de fois inférieur à :

$$\underbrace{(n+1)}_{\substack{\text{hypothèses :} \\ \text{cardinal max. d'une suite str. croissante de} \\ \text{sous-ensembles de l'ensemble des sous-formules de } \varphi}} \times \underbrace{n}_{\substack{\text{buts :} \\ \text{nombre de} \\ \text{sous-formules de } \varphi}}$$

La branche considérée est donc de longueur inférieure à

$$p(n) \overset{\text{def}}{=} (n+1)n + \underbrace{1}_{\text{règle } (Ax) \text{ à la fin}}$$

On a montré que

> Pour toute formule φ de taille n :
>
> si $\vdash_{LJ_0'} \varphi$, alors $\vdash_{LJ_0'}^{p(n)} \varphi$, avec $p(n) \overset{\text{def}}{=} n^2 + n + 1$

La réciproque est évidente.

6.

J'énonce quelques idées, mais je n'ai pas le temps de les creuser :

- *Dans* $entails_p^\varphi$: une grande conjonction initiale assurera que chacun des X_i (resp. Y_i) "représente" la sous formule ψ_i au moyen d'une équivalence (les X_i représentant les hypothèses, les Y_i les buts) :

$$(X_i \longrightarrow \psi_i) \wedge (\psi_i \longrightarrow X_i) \wedge (Y_i \longrightarrow \psi_i) \wedge (\psi_i \longrightarrow Y_i)$$

- Dans cette conjonction initiale, on veillera aussi à ce que les implications entre sous-formules de φ soient conservées par cet encodage : pour tout i, si ψ_i s'écrit sous la forme $\psi_{i_1} \longrightarrow \psi_{i_2}$, alors la conjonction contiendra :

$$X_{i_1} \longrightarrow X_{i_2}$$

- L'idée est d'encoder p choix possibles de règles d'inférence de (LJ_0') dans $entails_p^\varphi$ (pour que la preuve résultante soit de longueur inférieure à p) en usant de quantificateurs :
  - une première difficulté peut être de "choisir" existentiellement une des variables X_i (par exemple : la sous-formule (*but*) à laquelle s'appliquera la règle (Ax) ou $(\longrightarrow R)$).
    La difficulté venant du fait que les quantificateurs ne portent que sur des valeurs de vérité binaires (qu'on peut voir comme correspondant à l'activation d'un bit ou non).
    Une astuce pourrait être de se servir de $\lfloor \log n \rfloor + 1$ variables muettes $p_1, \cdots, p_{\lfloor \log n \rfloor + 1}$ qui serviraient à "deviner" existentiellement l'écriture binaire d'un indice $i \in [\![1, n]\!]$ correspondant à X_i, en ajoutant les contraintes :

$$p_i \longrightarrow \neg X_j \text{ pour tout } j \text{ dont le } i\text{-ème bit dans l'écriture binaire vaut } 0$$

    Ainsi, si $n = 7$ et p_1, p_3 ont pour valuation "vrai", p_2 a pour valuation "faux" dans l'interprétation courante : la seule variable X_i qui pourra être évaluée à "vrai" en cas de satisfaction de $entails_p^\varphi$ sera $X_{101_2} = X_5$.

$$\exists p_1, \exists p_2, \ldots, \exists p_{\lfloor \log n \rfloor + 1}, [\cdots]$$

    forcera donc le choix d'une variable X_i