Composition d'informatique n°6

Sujet 2 : informatique fondamentale (Durée : 4 heures)

L'utilisation de la calculatrice **n'est pas autorisée** pour cette épreuve.

⋆ ⋆ ⋆

Sémantique de Kripke

L'ensemble du sujet s'intéresse à la sémantique de Kripke, une sémantique basée sur les graphes, différente de la sémantique booléenne usuelle, permettant de caractériser la prouvabilité des formules en logique intuitionniste notamment. La première partie présente la sémantique de Kripke restreinte au cas intuitionniste et montre la correction de la logique intuitionniste pour cette sémantique. La deuxième partie établit la complétude de la logique intuitionniste pour cette sémantique et restreint le cadre d'étude aux modèles finis. Enfin, la troisième partie introduit de nouveaux opérateurs booléens en logique modale et fait le lien avec une définition plus générale des modèles de Kripke.

1 Sémantique de Kripke

On considère un ensemble fini de variables $\mathcal{V} = \{x_0, x_1, \ldots, x_{n-1}\}$, avec $n \in \mathbb{N}$. On définit l'ensemble des formules propositionnelles $\mathcal{F}$ de variables $\mathcal{V}$ par induction par :

- $\bot \in \mathcal{F}$;
- pour $x \in \mathcal{V}$, $x \in \mathcal{F}$;
- si $A, B \in \mathcal{F}$, alors $A \wedge B$, $A \vee B$ et $A \to B$ sont dans $\mathcal{F}$.

On remarque en particulier que la négation ne fait pas partie de la définition par induction des formules.

On rappelle en annexe les règles d'inférence des logiques minimale, intuitionniste et classique. On notera $\Gamma \vdash_m A$, $\Gamma \vdash_i A$ et $\Gamma \vdash_c A$ pour indiquer qu'un séquent $\Gamma \vdash A$ est prouvable en logique minimale, intuitionniste et classique respectivement.

On admet et on pourra utiliser le fait que la logique classique est correcte et complète pour la sémantique booléenne usuelle.

1.1 Premières preuves

Pour $A \in \mathcal{F}$, on définit $\neg A$ par $\neg A = A \to \bot$. Il s'agit de sucre syntaxique, donc ces formules sont bien identiques et pas seulement sémantiquement équivalentes.

Question 1 Montrer que les règles suivantes sont admissibles en logique minimale.

$$\frac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}\ \neg_i \quad \text{et} \quad \frac{\Gamma \vdash \neg A \qquad \Gamma \vdash A}{\Gamma \vdash \bot}\ \neg_e$$

On pourra les utiliser librement par la suite.

Question 2 Montrer que $\vdash_m \neg(A \wedge \neg A)$, c'est-à-dire que $\vdash \neg(A \wedge \neg A)$ est prouvable en logique minimale.

Question 3 Montrer que $\dfrac{\Gamma \vdash \neg\neg A}{\Gamma \vdash A}\ \neg\neg_e$ est admissible en logique classique.

1.2 Modèle de Kripke

On appelle **cadre de Kripke** un couple (W, R) tel que

- W est un ensemble non vide, fini ou infini dénombrable, appelé ensemble des « **mondes** » ;
- R est une relation binaire entre les éléments de W.

On remarque qu'un cadre de Kripke peut être vu comme un graphe orienté éventuellement infini. À ce titre, on peut définir une relation d'accessibilité $\prec$ entre deux éléments de W comme la clôture transitive de R, c'est-à-dire que $u \prec v$ si et seulement s'il existe $u_0 = u, u_1, \ldots, u_k = v$ tels que pour $i < k$, $u_i \prec u_{i+1}$ et $k > 0$. Dans le vocabulaire des graphes, cela signifie qu'il existe un chemin non vide de u à v.

On note également $\preccurlyeq$ la clôture réflexive de $\prec$, c'est-à-dire que $u \preccurlyeq v$ si et seulement si $u = v$ ou $u \prec v$.

Un **modèle de Kripke** est un triplet $\mathcal{K} = (W, R, \Vdash)$ tel que (W, R) est un cadre de Kripke et $\Vdash$ est une relation binaire entre les éléments de W et les variables de $\mathcal{V}$, appelée « **réalise** ».

Lorsque le cadre de Kripke est fini, on le représente comme un graphe orienté. La relation de réalisation est alors représentée en indiquant les variables réalisées à côté de chaque sommet. La figure 1 est une représentation d'un modèle de Kripke. Par exemple, pour ce modèle, $4 \Vdash x_0$ et $3 \Vdash x_1$, mais $2 \nVdash x_0$.

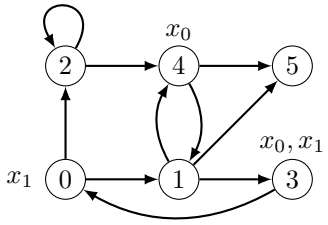

FIGURE 1 – Le modèle de Kripke $\mathcal{K}_1$.

On s'intéresse dans un premier temps, dans cette partie et la suivante, à un cadre réduit des modèles de Kripke $(W, R, \Vdash)$, appelés modèles de Kripke intuitionnistes, où la relation R est supposée **acyclique**, c'est-à-dire qu'il n'existe pas $u \in W$ tel que $u \prec u$, et où la relation $\Vdash$ vérifie, pour $u, v \in W$ et $x \in \mathcal{V}$:

$$\text{si } u \Vdash x \text{ et } u \prec v \text{ alors } v \Vdash x$$

Le modèle $\mathcal{K}_2$ de la figure 2 en est un exemple.

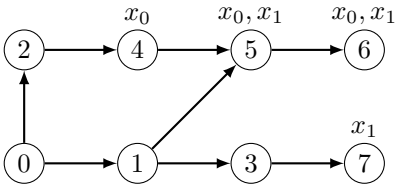

FIGURE 2 – Le modèle de Kripke $\mathcal{K}_2$.

Pour un modèle de Kripke intuitionniste, on étend $\Vdash$ par induction à une relation binaire entre les éléments de W et de $\mathcal{F}$ par :

- pour $u \in W$, $u \nVdash \bot$;
- pour $u \in W$ et $A, B \in \mathcal{F}$:
  - $u \Vdash A \wedge B$ si et seulement si $u \Vdash A$ et $u \Vdash B$;
  - $u \Vdash A \vee B$ si et seulement si $u \Vdash A$ ou $u \Vdash B$;
  - $u \Vdash A \to B$ si et seulement si pour tout $v \in W$, si $u \preccurlyeq v$ et $v \Vdash A$, alors $v \Vdash B$.

Question 4 Pour $u \in W$ et $A \in \mathcal{F}$, montrer que si $u \Vdash \neg A$, alors $u \nVdash A$. La réciproque est-elle vérifiée ? Justifier.

Question 5 Dans le modèle de Kripke $\mathcal{K}_2$ de la figure 2, indiquer les sommets qui réalisent la formule $\neg x_0$. En déduire les sommets qui réalisent $x_1 \vee \neg x_0$.

Soit $\mathcal{K} = (W, R, \Vdash)$ un modèle de Kripke intuitionniste. Pour $A \in \mathcal{F}$ et $\Gamma \subseteq \mathcal{F}$, on note :
- $u \Vdash \Gamma$ (ou $u \Vdash_{\mathcal{K}} \Gamma$ s'il y a ambiguïté) si pour tout $B \in \Gamma$, $u \Vdash B$, pour un certain $u \in W$;
- $\mathcal{K} \Vdash A$ (resp. $\mathcal{K} \Vdash \Gamma$) si pour tout $u \in W$, $u \Vdash A$ (resp. $u \Vdash \Gamma$).

Question 6 Montrer que $\mathcal{K}_3 \Vdash x_0 \to \neg x_1$, où $\mathcal{K}_3$ est le modèle de Kripke intuitionniste défini à la figure 3. Est-ce que $\mathcal{K}_3 \Vdash \neg x_0 \vee \neg x_1$?

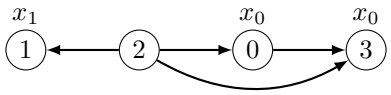

FIGURE 3 – Le modèle de Kripke $\mathcal{K}_3$.

Pour $A \in \mathcal{F}$ et $\Gamma \subseteq \mathcal{F}$, on note :
- $\Gamma \Vdash A$ si pour tout modèle de Kripke $\mathcal{K} = (W, R, \Vdash)$ et $u \in W$, si $u \Vdash \Gamma$, alors $u \Vdash A$;
- $\Vdash A$ si $\emptyset \Vdash A$, c'est-à-dire si pour tout $\mathcal{K}$, $\mathcal{K} \Vdash A$. On dit alors que A est **toujours réalisée**.

Question 7 Montrer que $\neg(A \wedge \neg A)$ est toujours réalisée.

Question 8 Montrer que $\neg\neg A \to A$ n'est pas toujours réalisée.

1.3 Correction

Question 9 Soit $\mathcal{K} = (W, R, \Vdash)$ un modèle de Kripke intuitionniste, $A \in \mathcal{F}$ et $u, v \in W$. Montrer que si $u \Vdash A$ et $u \prec v$, alors $v \Vdash A$.

Soit $\dfrac{\Gamma_1 \vdash A_1 \quad \Gamma_2 \vdash A_2 \quad \dots \quad \Gamma_k \vdash A_k}{\Gamma \vdash A}$ (r) une règle d'inférence. On dit que (r) est **correcte** si le fait que $\Gamma_1 \Vdash A_1$, $\Gamma_2 \Vdash A_2$, …, $\Gamma_k \Vdash A_k$ entraîne que $\Gamma \Vdash A$.

Question 10 Montrer que les règles $\to_i$, $\to_e$, $\vee_e$ et $\bot_e$ sont correctes.

Question 11 On admet que les autres règles de la logique intuitionniste sont correctes. En déduire que la logique intuitionniste est correcte pour la sémantique de Kripke, c'est-à-dire que $\Gamma \vdash_i A$ implique toujours $\Gamma \Vdash A$.

Question 12 Montrer que $A \vee \neg A$ n'est pas prouvable en logique intuitionniste. En déduire que la logique intuitionniste n'est pas complète pour la sémantique booléenne usuelle.

Question 13 La formule $(\neg A \vee B) \to (A \to B)$ n'est pas prouvable en logique minimale. Montrer qu'elle est prouvable en logique intuitionniste. Que dire de la formule réciproque $(A \to B) \to (\neg A \vee B)$?

2 Complétude

Dans cette partie, on souhaite montrer que la logique intuitionniste est complète pour la sémantique de Kripke, c'est-à-dire que si $\Vdash A$, alors $\vdash_i A$.

2.1 Cas général

Soit $\Delta \subseteq \mathcal{F}$ un ensemble de formules. On dit que Δ est **saturé** si et seulement si :

- Δ est **cohérent** pour la logique intuitionniste, c'est-à-dire $\Delta \nvdash_i \bot$;
- pour tout $A, B \in \mathcal{F}$, si $\Delta \vdash_i A \vee B$, alors $A \in \Delta$ ou $B \in \Delta$.

Le lemme de Henkin s'énonce de la manière suivante : soient $\Gamma \subseteq \mathcal{F}$ et $A \in \mathcal{F}$. Si $\Gamma \nvdash_i A$, alors il existe un ensemble saturé Δ tel que $\Gamma \subseteq \Delta$ et $\Delta \nvdash_i A$.

Les deux questions suivantes cherchent à montrer ce lemme. On considère $\Gamma \subseteq \mathcal{F}$ et $A \in \mathcal{F}$ tels que $\Gamma \nvdash_i A$. On considère une énumération $(A_k)_{k\in\mathbb{N}}$ des formules disjonctives, c'est-à-dire de la forme $A_k = B_k \vee C_k$ avec $B_k, C_k \in \mathcal{F}$.

On définit une suite $(\Gamma_m)_{m\in\mathbb{N}}$ de la manière suivante :

- $\Gamma_0 = \Gamma$;
- pour $m \in \mathbb{N}$, on considère le plus petit indice k tel que $\Gamma_m \vdash_i A_k$, avec $B_k \notin \Gamma_m$ et $C_k \notin \Gamma_m$:
  - si un tel indice k n'existe pas, on pose $\Gamma_{m+1} = \Gamma_m$;
  - sinon, si $\Gamma_m, B_k \nvdash_i A$, on pose $\Gamma_{m+1} = \Gamma_m \cup \{B_k\}$, sinon on pose $\Gamma_{m+1} = \Gamma_m \cup \{C_k\}$.

Question 14 On pose $\Delta = \bigcup_{m\in\mathbb{N}} \Gamma_m$. Montrer que $\Delta \nvdash_i A$.

Question 15 En déduire le lemme de Henkin.

Question 16 Soit Δ un ensemble saturé et $A \in \mathcal{F}$. Montrer que $A \in \Delta$ si et seulement si $\Delta \vdash_i A$

Question 17 Soit Δ un ensemble saturé et $B, C \in \mathcal{F}$. Montrer que $B \to C \in \Delta$ si et seulement si pour tout ensemble saturé Δ' tel que $\Delta \cup \{B\} \subseteq \Delta'$, on a $C \in \Delta'$.

Pour montrer la complétude, on procède par l'absurde : on suppose que Γ et A sont tels que $\Gamma \nvdash_i A$ et on souhaite construire un modèle de Kripke intuitionniste $\mathcal{K} = (W, R, \Vdash)$ tel que $\Gamma \not\Vdash A$.

Pour ce faire, on considère Δ_0 un ensemble saturé tel que $\Gamma \subseteq \Delta_0$ et $\Delta_0 \nvdash_i A$, construit avec le lemme de Henkin. On pose alors :

- $W = \{\Delta \subseteq \mathcal{F} \mid \Delta \text{ est saturé et } \Delta_0 \subseteq \Delta\}$;
- $(\Delta, \Delta') \in R$ si et seulement si $\Delta \subsetneq \Delta'$;
- pour tout $x \in \mathcal{V}$, $\Delta \Vdash x$ si et seulement si $x \in \Delta$.

Question 18 Montrer que $\mathcal{K} = (W, R, \Vdash)$ est un modèle de Kripke intuitionniste.

Question 19 Montrer que pour $\Delta \in W$ et $B \in \mathcal{F}$, $\Delta \Vdash B$ si et seulement si $B \in \Delta$ et en déduire que la logique intuitionniste est complète pour la sémantique de Kripke.

2.2 Cas fini

On souhaite montrer un résultat plus fort, en montrant que même si on se restreint aux modèles de Kripke intuitionnistes finis, la logique intuitionniste reste correcte et complète.

Question 20 Justifier que la logique intuitionniste est correcte pour la sémantique formée des modèles de Kripke intuitionnistes finis.

Pour $A \in \mathcal{F}$, on note $SF(A)$ l'ensemble des **sous-formules** de A. On considère $\mathcal{K} = (W, R, \Vdash)$ un modèle de Kripke intuitionniste quelconque, et on définit, pour $u \in W$, $S_A(u) = \{B \in SF(A) \mid u \Vdash B\}$. On pose alors :

- $W_A = \{S_A(u) \mid u \in W\}$;
- $R_A = \{(S_A(u), S_A(v)) \mid S_A(u) \subsetneq S_A(v)\}$;
- pour $u \in W$ et $x \in \mathcal{V}$, $S_A(u) \Vdash_A x$ si et seulement si $x \in S_A(u)$.

Question 21 Montrer que $\mathcal{K}_A = (W_A, R_A, \Vdash_A)$ est un modèle de Kripke intuitionniste fini.

Question 22 Soit $B \in SF(A)$ et $u \in W$. Montrer que $u \Vdash B$ si et seulement si $S_A(u) \Vdash_A B$.

Question 23 En déduire que la logique intuitionniste est complète pour la sémantique formée des modèles de Kripke intuitionnistes finis.

On considère le problème de décision `INTUITIONNISTE` :

* **Instance** : une formule propositionnelle $A \in \mathcal{F}$.
* **Question** : est-ce que $\vdash_i A$?

Question 24 Montrer que `INTUITIONNISTE` est décidable.

On considère le problème de décision `CLASSIQUE` :

* **Instance** : une formule propositionnelle $A \in \mathcal{F}$.
* **Question** : est-ce que $\vdash_c A$?

On admet que le problème `CLASSIQUE` est coNP-complet, ce qui se prouve en utilisant la NP-complétude de `SAT` et la complétude et correction de la logique classique pour la sémantique booléenne usuelle.

On considère la justification suivante :

« Le problème `INTUITIONNISTE` est coNP-difficile. En effet, montrons que `CLASSIQUE` $\leqslant_{\mathsf{m}}^{\mathsf{p}}$ `INTUITIONNISTE`, `CLASSIQUE` étant coNP-complet. Pour une formule $A \in \mathcal{F}$, on considère le cadre de Kripke restreint à un seul monde $\{W = \{u\}, R = \emptyset\}$.

À partir d'une relation $\Vdash$ sur ce cadre de Kripke, on définit une valuation μ sur $\mathcal{V}$ par $\mu(x) = 1$ si et seulement si $u \Vdash x$. On remarque que $\mu(A) = 1$ si et seulement si $\mathcal{K} = (W, R, \Vdash) \Vdash A$. On en déduit que $A \in$ `CLASSIQUE` si et seulement si $A \in$ `INTUITIONNISTE`, ce qui achève la réduction. »

Question 25 Expliquer la ou les failles de raisonnement dans la justification précédente.

On admet que pour toute formule $A \in \mathcal{F}$, $\vdash_c A$ si et seulement si $\vdash_i \neg\neg A$.

Question 26 En déduire que `INTUITIONNISTE` est coNP-difficile.

Ce problème est en fait PSPACE*-complet.*

3 Logique modale

On souhaite étendre la définition de l'ensemble des formules en rajoutant un nouvel opérateur unaire. On définit l'ensemble des formules modales $\mathcal{M}$ de variables $\mathcal{V}$ par induction par :

- $\bot \in \mathcal{M}$;
- pour $x \in \mathcal{V}$, $x \in \mathcal{M}$;
- si $A, B \in \mathcal{M}$, alors $A \wedge B$, $A \vee B$, $A \to B$ et $\Box A$ sont dans $\mathcal{M}$.

On définit également $\Diamond A$ par $\Diamond A = \neg\Box\neg A$.

L'intuition derrière ces deux opérateurs, qui se formalisera avec des modèles de Kripke par la suite, est d'établir des conditions de réalisabilité entre les mondes :

– $\Box A$ signifie que A est **nécessaire** : dans tous les mondes accessibles, A devra être réalisée ;
– $\Diamond A$ signifie que A est **possible** : il existe un monde accessible qui réalise A.

3.1 Système K

Le système K (pour Kripke) est un ensemble de règles d'inférence constitué de la logique classique à laquelle on rajoute les deux règles suivantes :

$$\frac{\Gamma \vdash \Box(A \to B)}{\Gamma \vdash \Box A \to \Box B}\ (K) \quad \text{et} \quad \frac{\vdash A}{\vdash \Box A}\ (N)$$

Attention, dans la règle (N) (nécessitation), les séquents ne contiennent pas de contexte. En particulier, $\dfrac{\Gamma \vdash A}{\Gamma \vdash \Box A}$ n'est pas admissible dans le cas général.

On note $\Gamma \vdash_K A$ pour indiquer que le séquent $\Gamma \vdash A$ est prouvable en système K.

Question 27 Montrer que les séquents $\vdash \Box\neg A \to \neg\Diamond A$ et $\vdash \neg\Diamond A \to \Box\neg A$ sont prouvables en système K.

Question 28 Montrer que $\vdash_K \Box A \to \Box\neg\neg A$.

3.2 Modèles de Kripke modaux

Pour un modèle de Kripke $\mathcal{K} = (W, R, \Vdash)$ quelconque (en particulier pas nécessairement intuitionniste), on étend la relation $\Vdash$ aux formules modales de la manière suivante :

– pour $u \in W$, $u \nVdash \bot$;
– pour $u \in W$ et $A, B \in \mathcal{M}$:
  * $u \Vdash A \wedge B$ si et seulement si $u \Vdash A$ et $u \Vdash B$;
  * $u \Vdash A \vee B$ si et seulement si $u \Vdash A$ ou $u \Vdash B$;
  * $u \Vdash A \to B$ si et seulement si lorsque $u \Vdash A$, alors $u \Vdash B$ (attention, cette définition diffère de celle pour les modèles de Kripke intuitionnistes) ;
  * $u \Vdash \Box A$ si et seulement si pour tout $v \in W$ tel que uRv, alors $v \Vdash A$.

Question 29 Soit $\mathcal{K} = (W, R, \Vdash)$ un modèle de Kripke et $u \in W$. Traduire ce que signifie $u \Vdash \neg A$ et en déduire que $u \Vdash \Diamond A$ si et seulement s'il existe $v \in W$ tel que uRv et $v \Vdash A$.

Question 30 Dans le modèle de Kripke $\mathcal{K}_4$ représenté en figure 4, indiquer quels sommets réalisent les formules $A = \Box x_0$ et $B = \neg\Diamond x_1$.

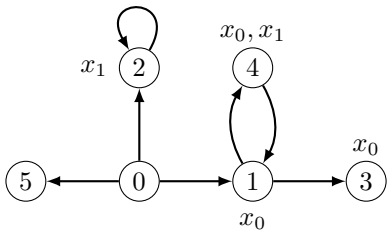

FIGURE 4 – Le modèle de Kripke $\mathcal{K}_4$.

Pour $\Gamma \subseteq \mathcal{M}$ et $A \in \mathcal{M}$, on redéfinit, comme pour les modèles de Kripke intuitionniste, les notations $\mathcal{K} \Vdash A$, $\Gamma \Vdash A$ et $\Vdash A$.

Question 31 En reprenant la définition de correction d'une règle définie en 1.3, montrer que les règles (te), $\rightarrow_i$, (K) et (N) sont correctes.

Question 32 En admettant que les autres règles de la logique classique sont correctes, montrer que le système K est correct pour la sémantique de Kripke.

Question 33 Soit $A \in \mathcal{F}$ (donc sans $\Box$ ni $\Diamond$) prouvable en système K. Montrer que A prouvable en logique classique.

On note SK l'ensemble des règles du système K. On définit les deux règles suivantes :

$$\frac{\Gamma \vdash \Box A}{\Gamma \vdash \Diamond A}\ (D_1) \quad \text{et} \quad \frac{}{\Gamma \vdash \neg\Box\bot}\ (D_2)$$

Question 34 Montrer que $SK \cup \{D_1\}$ et $SK \cup \{D_2\}$ sont équivalents, c'est-à-dire que tout séquent prouvable dans l'un des deux systèmes est prouvable dans l'autre.

La relation binaire R est dite **sérielle** s'il n'existe pas de puits, c'est-à-dire si pour tout $u \in W$, il existe $v \in W$ tel que uRv.

On appelle **structure de formule** une fonction $f : \mathcal{M} \rightarrow \mathcal{M}$. Par abus de notation, on assimile f et $f(A)$. Par exemple, $\neg\neg A \rightarrow \Box A$ est une structure de formule.

On dit qu'une propriété π d'une relation binaire (comme la sérialité ou la réflexivité, par exemple) **caractérise** une structure de formule f si et seulement si :

- pour toute formule A, $f(A)$ est réalisée par les modèles de Kripke $(W, R, \Vdash)$ tels que R vérifie la propriété π ;
- si (W, R) est un cadre de Kripke tel que pour tout $\Vdash$ et pour tout A, $(W, R, \Vdash)$ réalise $f(A)$, alors R vérifie la propriété π.

Question 35 Montrer que la sérialité caractérise $\Box A \rightarrow \Diamond A$.

Question 36 Est-ce que la réflexivité caractérise $\Box A \rightarrow A$?

Question 37 Déterminer une propriété qui caractérise $\Box A \rightarrow \Box\Box A$.

Question 38 Déterminer une structure de formule caractérisée par la symétrie.

$\star\star\star$

Annexe : règles d'inférence

La logique **minimale** est formée des règles suivantes :

- introduction et élimination de $\wedge$:

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ \wedge_i, \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\ \wedge_e \quad \text{et} \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\ \wedge_e$$

- introduction et élimination de $\vee$:

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ \vee_i, \quad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ \vee_i \quad \text{et} \quad \frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C}\ \vee_e$$

- introduction et élimination de $\to$:

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}\ \to_i \quad \text{et} \quad \frac{\Gamma \vdash A \to B \quad \Gamma \vdash A}{\Gamma \vdash B}\ \to_e$$

- axiome et affaiblissement :

$$\frac{}{\Gamma, A \vdash A}\ (\text{ax}) \quad \text{et} \quad \frac{\Gamma \vdash B}{\Delta \vdash B}\ (\text{aff}) \text{ pour } \Gamma \subseteq \Delta$$

La logique **intuitionniste** est formée des règles de la logique minimale et de l'élimination de $\bot$:

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash A}\ \bot_e$$

La logique **classique** est formée des règles de la logique intuitionniste et du tiers-exclu :

$$\frac{}{\Gamma \vdash A \vee \neg A}\ (\text{te})$$