Théorie de la démonstration

- L'utilisation de la table de vérité est laborieuse,
- Alternative : Théorie de la démonstration
  - Vérifier la validité des formules
  - Déduire de nouvelles formules à partir d'autres formules

- Moyen : Utilisation des symboles (seulement) : Etude syntaxique

Démonstration par contraposition

- Pour montrer que **P→Q** est une proposition vraie, il suffit de montrer que **¬ Q→ ¬P** est vraie.
- **¬ Q→ ¬P** est appelée **proposition contraposée** de de la proposition **P→Q**
- Idée : Une proposition et sa contraposée sont équivalentes, ce qui signifie que l'on peut démontrer l'une pour démontrer l'autre.

- **Exemple :** Pour démontrer que « S'il pleut, alors le sol est mouillé », il suffit de démontrer que « Si le sol n'est pas mouillé, alors il ne pleut pas ».

Démonstration par contraposition

- Exercice 1 : Soient k et k' deux entiers naturels non nuls.
- Montrons que ($k \times k' = 1 \Rightarrow k = k' = 1$).
- Solution :
  - Supposons que $k \neq 1$ ou $k' \neq 1$.
  - Alors, on a ($k \geq 2$ et $k' \geq 1$) ou ($k \geq 1$ et $k' \geq 2$).
  - Dans les deux cas, on a $k \times k' \geq 2$ et en particulier, $k \times k' \neq 1$.
  - Donc, ($k \neq 1$ ou $k' \neq 1$) $\Rightarrow$ ($k \times k' \neq 1$).

- Par contraposition, on a montré que ($k \times k' = 1$) $\Rightarrow$ ($k = 1$ et $k' = 1$)

Démonstration par contraposition

- Exercice 2 : Montrez que $\models \alpha \wedge \beta \Rightarrow (\models \alpha$ et $\models \beta)$
- Solution :
  - Supposons que $(\models \alpha$ et $\models \beta)$ est fausse

$\Rightarrow \alpha$ n'est pas une tautologie ou β n'est pas une tautologie

$\Rightarrow$ Il existe au moins une ligne dans la table de verité où α est fausse ou β est fausse

$\Rightarrow \alpha \wedge \beta$ est fausse

$\Rightarrow \alpha \wedge \beta$ n'est pas une tautologie

$\Rightarrow (\models \alpha \wedge \beta \Rightarrow (\models \alpha$ et $\models \beta))$ est valide

Démonstration par l'absurde (Apagogie)

- Le raisonnement par l'absurde est un raisonnement qui permet de démontrer qu'une affirmation est vraie en montrant que son contraire est faux.

- On veut montrer qu'une proposition **P** est vraie :

- On suppose que c'est sa négation $\neg$**P** qui est vraie
  - On montre que cela entraîne une proposition fausse.
  - On en conclut que **P** est vraie

Schéma du raisonnement :

Quand $\neg P \Rightarrow Q$ est une proposition vraie, et Q est une proposition fausse, on peut affirmer que P est une proposition vraie.

Démonstration par l'absurde (Apagogie)

- Exercice : Démontrer que 0 n'a pas d'inverse dans $\mathbb{R}$

Solution 1 :

- Supposons que 0 a un inverse

$\Rightarrow \exists\, A \in \mathbb{R} \quad / \quad 0 \times A = 1 \qquad (1)$

Or $\forall\, X \in \mathbb{R} \quad 0 \times X = 0$

$\Rightarrow 0 \times A = 0 \qquad (2)$

- (1) et (2) $\Rightarrow 0 = 1$ (Faux)
- 0 n'a pas d'inverse dans $\mathbb{R}$

Démonstration par l'absurde (Apagogie)

- Exercice : Démontrer que 0 n'a pas d'inverse dans $\mathbb{R}$

<u>Solution 2 :</u>

- Supposons que 0 a un inverse

$\Rightarrow \exists\, A \in \mathbb{R} \quad / \quad A \times 0 = 1 \qquad (1)$

$\Rightarrow A \times 0 = A \times (0+0) = (A \times 0) + (A \times 0) \qquad (2)$

- (1) et (2) $\Rightarrow 1 = 2$ (Faux)
- 0 n'a pas d'inverse dans $\mathbb{R}$

Système formel déductif

- Un système formel de déduction est composé :
  - des axiomes qui représentent un petit nombre de vérités initiales
  - des règles d'inférence qui sont les mécanismes de raisonnement pour révéler des vérités cachées.
  - des hypothèses
- il permet d'inférer des conclusions a partir de prémisses et définit donc une relation de déduction entre formules

Prémisses ⊢ Conclusion

Système formel déductif

- Axiomes :
  - $\alpha \rightarrow (\beta \rightarrow \alpha)$ (Axiome 1)
  - $(\alpha \rightarrow (\beta \rightarrow \gamma)) \rightarrow (\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \gamma)$ (Axiome 2)
  - $(\neg\alpha \rightarrow \neg\beta) \rightarrow ((\neg\alpha \rightarrow \beta) \rightarrow \alpha)$ (Axiome 3)
- Règles d'inférence :
  - $\alpha, \alpha \rightarrow \beta \vdash \beta$ (Modus Ponens)
  - $\alpha \rightarrow \beta, \neg\beta \vdash \neg\alpha$ (Modus Tollens)
  - $\alpha, \neg\alpha \vdash \square$ (Tiers Exclus)
- Transitivité:
  - $\alpha \rightarrow \beta, \beta \rightarrow \gamma \vdash \alpha \rightarrow \gamma$

Système formel déductif

Déduction naturelle

- Pour prouver qu'une formule C est une conséquence logique (conclusion) d'un ensemble de formules (Hypothèses), On utilise à la fois, les axiomes (A_i), les règles d'inférence, les théorèmes (T_i) et les hypothèses (H_i):

$$\{A_i, T_i, H_i\} \vdash C$$

Système formel déductif

Déduction naturelle

- Exemple 1 :
  - $\alpha \rightarrow (\beta \rightarrow \gamma), \beta \vdash \alpha \rightarrow \gamma$?

1: $\alpha \rightarrow (\beta \rightarrow \gamma) \quad (Hyp)$

2: $\beta \quad (Hyp)$

3: $(\alpha \rightarrow (\beta \rightarrow \gamma)) \rightarrow (\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \gamma)$ (A2)

4: $(\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \gamma) \quad (MP\ (1,3))$

5: $\beta \rightarrow (\alpha \rightarrow \beta)$ (A1)

6: $\alpha \rightarrow \beta (MP\ (2,5))$

7: $\alpha \rightarrow \gamma\ (MP\ (4,6))$

- Axiomes :
  - $\alpha \rightarrow (\beta \rightarrow \alpha)$ (Axiome 1)
  - $(\alpha \rightarrow (\beta \rightarrow \gamma)) \rightarrow (\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \gamma)$ (Axiome 2)
  - $(\neg\alpha \rightarrow \neg\beta) \rightarrow ((\neg\alpha \rightarrow \beta) \rightarrow \alpha)$ (Axiome 3)
- Règles d'inférence :
  - $\alpha, \alpha \rightarrow \beta \vdash \beta$ (Modus Ponens)
  - $\alpha \rightarrow \beta, \neg\beta \vdash \neg\alpha$ (Modus Tollens)
  - $\alpha, \neg\alpha \vdash \square$ (Tiers Exclus)
- Transitivité:
  - $\alpha \rightarrow \beta, \beta \rightarrow \gamma \vdash \alpha \rightarrow \gamma$

Système formel déductif

Déduction naturelle

- Exemple 2 :
  - $\alpha \to \beta, \beta \to \gamma \vdash \alpha \to \gamma$?

1: $\alpha \to \beta \quad (Hyp)$

2: $\beta \to \gamma \quad (Hyp)$

3: $\alpha \to \gamma$ (Tran)

- Axiomes :
  - $\alpha \to (\beta \to \alpha)$ (Axiome 1)
  - $(\alpha \to (\beta \to \gamma)) \to (\alpha \to \beta) \to (\alpha \to \gamma)$ (Axiome 2)
  - $(\neg\alpha \to \neg\beta) \to ((\neg\alpha \to \beta) \to \alpha)$ (Axiome 3)
- Règles d'inférence :
  - $\alpha, \alpha \to \beta \vdash \beta$ (Modus Ponens)
  - $\alpha \to \beta, \neg\beta \vdash \neg\alpha$ (Modus Tollens)
  - $\alpha, \neg\alpha \vdash \square$ (Tiers Exclus)
- Transitivité:
  - $\alpha \to \beta, \beta \to \gamma \vdash \alpha \to \gamma$

Système formel déductif

Déduction naturelle

- Exemple 3:
  - $\alpha \rightarrow \beta, \beta \rightarrow \gamma \vdash \alpha \rightarrow \gamma$? (sans utiliser la règle de transitivité)

?

Preuve par résolution

- Le principe de résolution est formé d'une seule **règle de résolution**:

$$\frac{C1: \sigma \vee P,\ C2: \gamma \vee \neg P}{C3: \sigma \vee \gamma}$$

- σ et γ sont deux clauses (disjonctions de littéraux)
- $C3$ est dite clause résolvante de $C1$ et $C2$
- P et $\neg P$ sont deux littéraux complémentaires

Règle de résolution

- Exemples:
  - $$\frac{C1{:}P \lor R, C2{:}\neg P \lor Q}{C3{:}R \lor Q}$$
  - $$\frac{C1{:}\neg P \lor Q \lor R, C2{:}\neg S \lor \neg Q}{C3{:}\neg P \lor R \lor \neg S}$$

Si C1 et C2 sont deux clauses unitaires, leurs résolvant s'il existe est la clause vide □ .

$$\frac{C1: P, C2: \neg P}{C3: \square}$$

Règle de résolution

- Etant donné deux clauses C1 et C2, un résolvant C de C1 et C2 est une conséquence logique de C1 et C2 :

$$\{C1,C2\} \vdash C3$$

Principe de résolution

- Le principe de résolution consiste à appliquer les trois étapes suivantes :
  - Transformer l'ensemble des formules sous F.N.C
  - Eliminer les conjonctions (en écrivant les clauses sur des lignes séparées)
  - Appliquer la règle de résolution

Preuve par règle de résolution

- Exemple 1:
  - $(\alpha \rightarrow \beta) \wedge (\beta \rightarrow \gamma) \vdash \alpha \rightarrow \gamma$?
  - $(\neg\alpha \vee \beta) \wedge (\neg\beta \vee \gamma) \vdash (\neg\alpha \vee \gamma)$ (F.N.C)
  - $1: \neg\alpha \vee \beta$ (Hyp)
  - $2: \neg\beta \vee \gamma$ (Hyp)
  - $3: \neg\alpha \vee \gamma$ *(RR(1,2))*

Preuve par règle de résolution

- Exemple 2:
  - $\alpha \rightarrow (\beta \rightarrow \gamma), \beta \vdash \alpha \rightarrow \gamma$?
  - $\neg\alpha \vee \neg\beta \vee \gamma, \beta \vdash (\neg\alpha \vee \gamma)$ (F.N.C)
  - $1{:}\neg\alpha \vee \neg\beta \vee \gamma$ (Hyp)
  - $2{:}\ \beta$ (Hyp)
  - $3{:}\ \neg\alpha \vee \gamma$ *(RR(1,2))*

Preuve par règle de résolution

- Exemple 3:
  - $\{P \vee Q \vee R, \neg P \vee R \vee Q, \neg Q \vee R\} \vdash R$?
  - 1: $P \vee Q \vee R$ (Hyp)
  - 2: $\neg P \vee R \vee Q$ (Hyp)
  - 3: $\neg Q \vee R$ (Hyp)
  - 4: $Q \vee R$ (RR(1,2))
  - 5: R (RR(3,4))

Résolution par réfutation

- Pour résoudre un problème de logique par la méthode de résolution, on s'appuie sur le théorème de réfutation :

➢ Pour prouver que **H** est une conséquence logique de **G** :

- On transforme **G** et ¬**H** en ensemble de clauses
- On applique le principe de résolution a **G** ∧ ¬**H** jusqu'a trouver la clause vide □

Résolution par réfutation

- Exemple 1:
  - $\{P \vee Q \vee R, \neg P \vee R \vee Q, \neg Q \vee R\} \vdash R$?
  - $\{P \vee Q \vee R, \neg P \vee R \vee Q, \neg Q \vee R, \neg R\} \vdash \square$
  - 1: $P \vee Q \vee R$ (Hyp)
  - 2: $\neg P \vee R \vee Q$ (Hyp)
  - 3: $\neg Q \vee R$ (Hyp)
  - 4: $\neg R$ (Hyp)
  - 5: $Q \vee R$ (RR(1,2))
  - 6: R (RR(3,5))
  - 7: $\square$ (RR(4,6))

Résolution par réfutation

- Exemple 2: Tournoi
- On suppose qu'on a les règles suivantes :
  - Si Salim rate son tournoi alors Salim sera déprimé.
  - Si Salim ne va pas à la piscine, il sera déprimé
  - Si Salim est à la piscine, il ne s'entraine pas
  - Salim ratera son tournoi s'il ne s'entraine pas

✓ **Transformer les énoncés en formules propositionnelles ?**

✓ **Prouver (par réfutation) que Salim sera déprimé ?**

Résolution par réfutation

- Exemple 2: Tournoi (Solution)
  - 1 : Si Salim rate son tournoi alors Salim sera déprimé.
  - 2 : Si Salim ne va pas à la piscine, il sera déprimé
  - 3 : Si Salim est à la piscine, il ne s'entraine pas
  - 4 : Salim ratera son tournoi s'il ne s'entraine pas

  - T : Salim rate son tournoi
  - D : Salim sera déprimé
  - P : Salim va à la piscine
  - E : Salim s'entraine

1 : $T \rightarrow D$
2 : $\neg P \rightarrow D$
3 : $P \rightarrow \neg E$
4 : $\neg E \rightarrow T$
D ?

Résolution par réfutation

- Exemple 2: Tournoi (Solution)
  - 1 : $\neg T \lor D$
  - 2 : $P \lor D$
  - 3 : $\neg P \lor \neg E$
  - 4 : $E \lor T$
  - 5 : $\neg D$
  - 6 : $D \lor \neg E$ RR(2,3)
  - 7 : $D \lor T$ RR(6,4)
  - 8 : D RR(7,1)
  - 9 : $\square$ RR(8,5)

1 : $T \rightarrow D$
2 : $\neg P \rightarrow D$
3 : $P \rightarrow \neg E$
4 : $\neg E \rightarrow T$
D ?

Preuve simple

- La preuve simple consiste à transformer, décomposer et recomposer les prémisses afin de trouver la conclusion.

- Exemple :
  - 1 : $A \rightarrow (B \vee C)$
  - 2 : $B \rightarrow D$
  - 3 : $\neg(E \wedge C)$
  - 4 : $F \wedge A \wedge \neg D$

$\vdash (F \wedge \neg E)$ **?**

Preuve simple

- Exemple :
  - 1 : $A \rightarrow (B \vee C)$
  - 2 : $B \rightarrow D$
  - 3 : $\neg(E \wedge C)$
  - 4 : $F \wedge A \wedge \neg D$
  - 5 : F
  - 6 : A
  - 7 : $\neg D$
  - 8 : $\neg E \vee \neg C$ Transformation de 3
  - 9 : $B \vee C$ MP (1,6)
  - 10 : $\neg B$ MT (2,7)
  - 11 : C RR(9,10)
  - 12 : $\neg E$ RR(8,11)
  - 13 : $F \wedge \neg E$ Addition (5,12)

$\vdash (F \wedge \neg E)$ **?**

$\left.\begin{array}{l} 5 : F \\ 6 : A \\ 7 : \neg D \end{array}\right\}$ Simplification de 4

Arbre sémantique

- Les arbres sémantiques constituent un moyen pour :
  - Vérifier la validité des formules,
  - Prouver des équivalences,
  - Prouver des théorèmes (Faire des déduction).

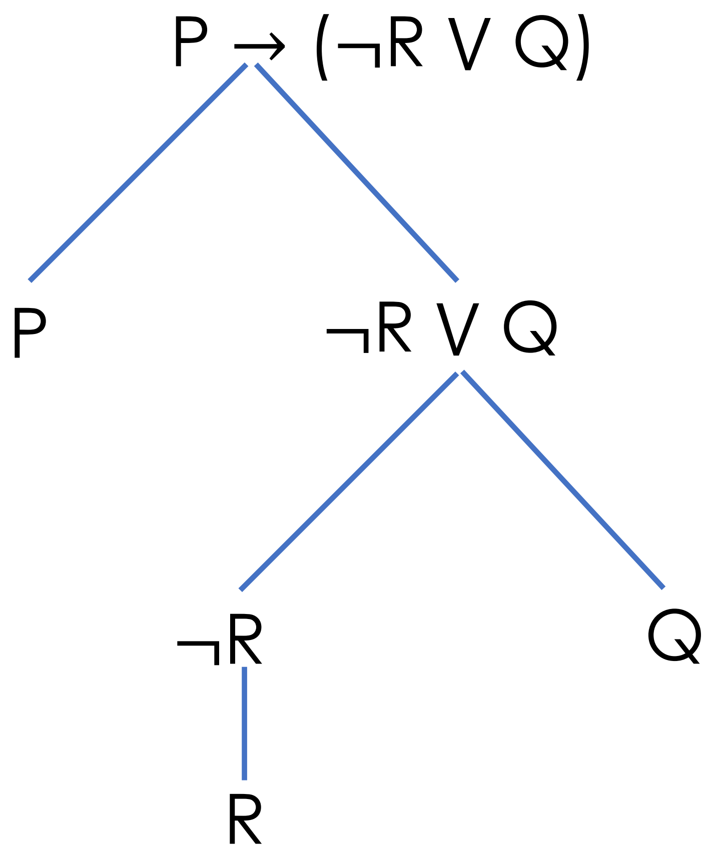
Arbre sémantique VS Arbre syntaxique

- Un arbre syntaxique est un moyen de vérifier la bonne formation des formules (formule bien formée ou pas)

Arbre sémantique VS Arbre syntaxique

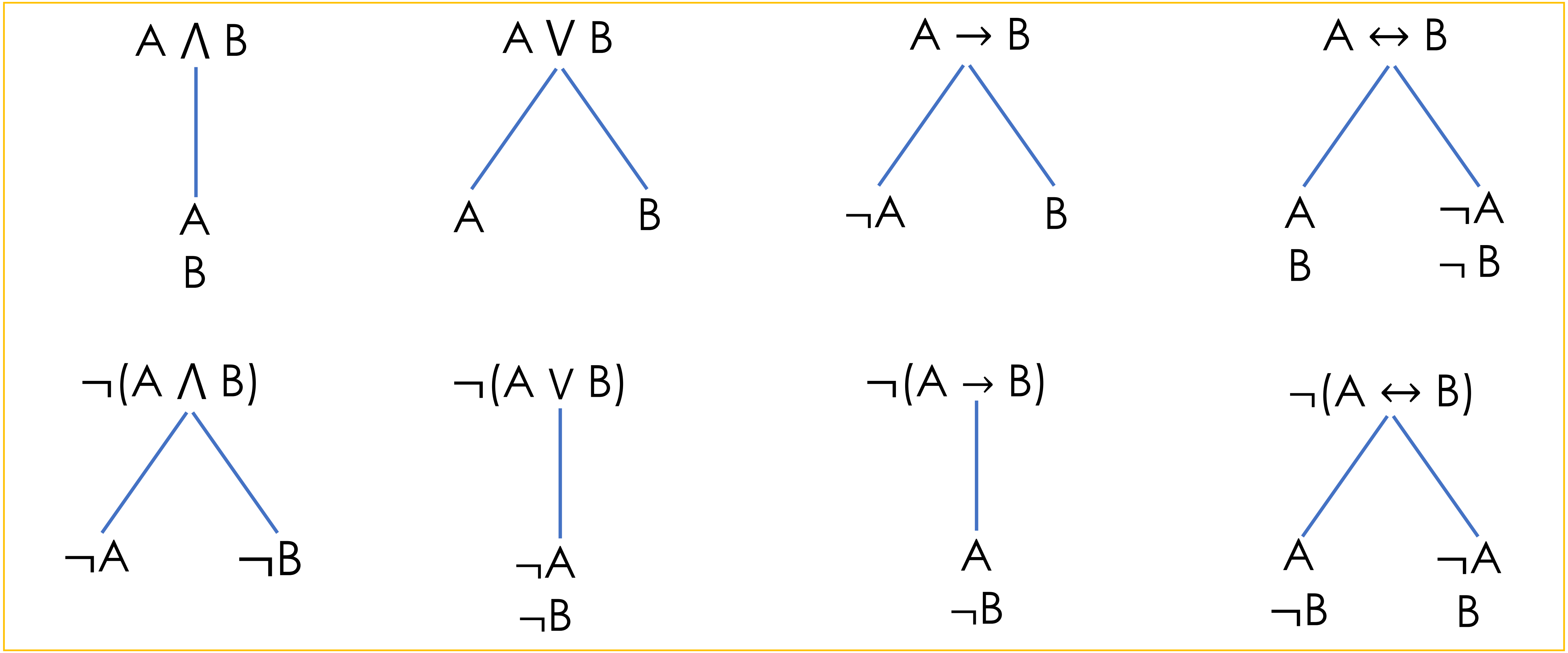
- Arbre syntaxique (Exemple) : Vérifier si la formule suivante est bien formée **?**

  - $P \rightarrow (\neg R \vee Q)$



Arbre sémantique

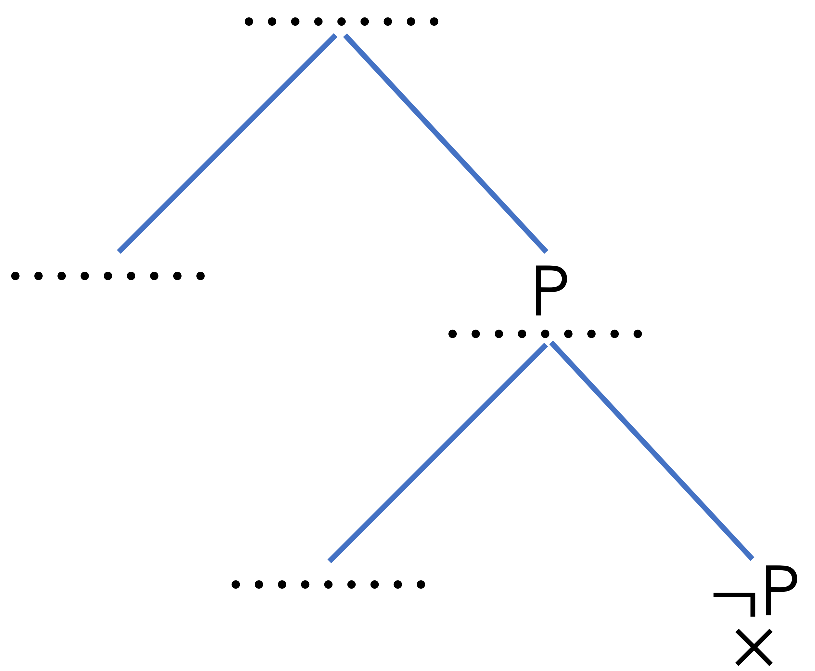
- Règles de branchement:



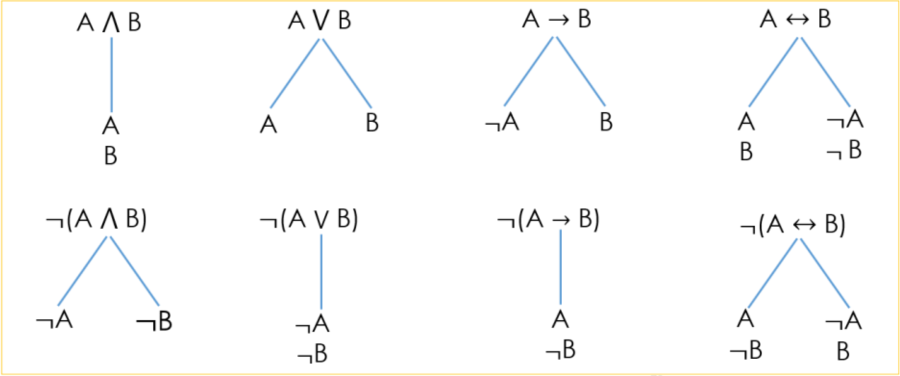
Arbre sémantique

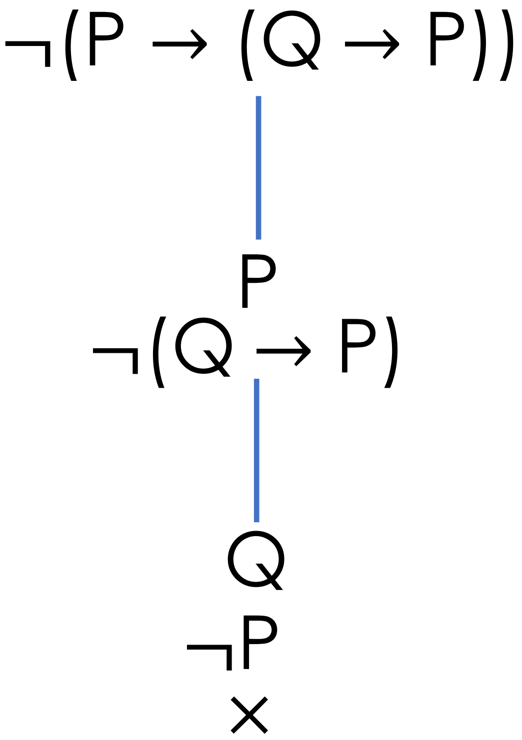
- ## Arbre sémantique clos:

- Un arbre sémantique est dit clos, si et seulement si, toutes ses branches se terminent avec des nœuds d'échec (branches fermées),
- Un nœud d'échec est identifié si la branche contient deux littéraux complémentaires.



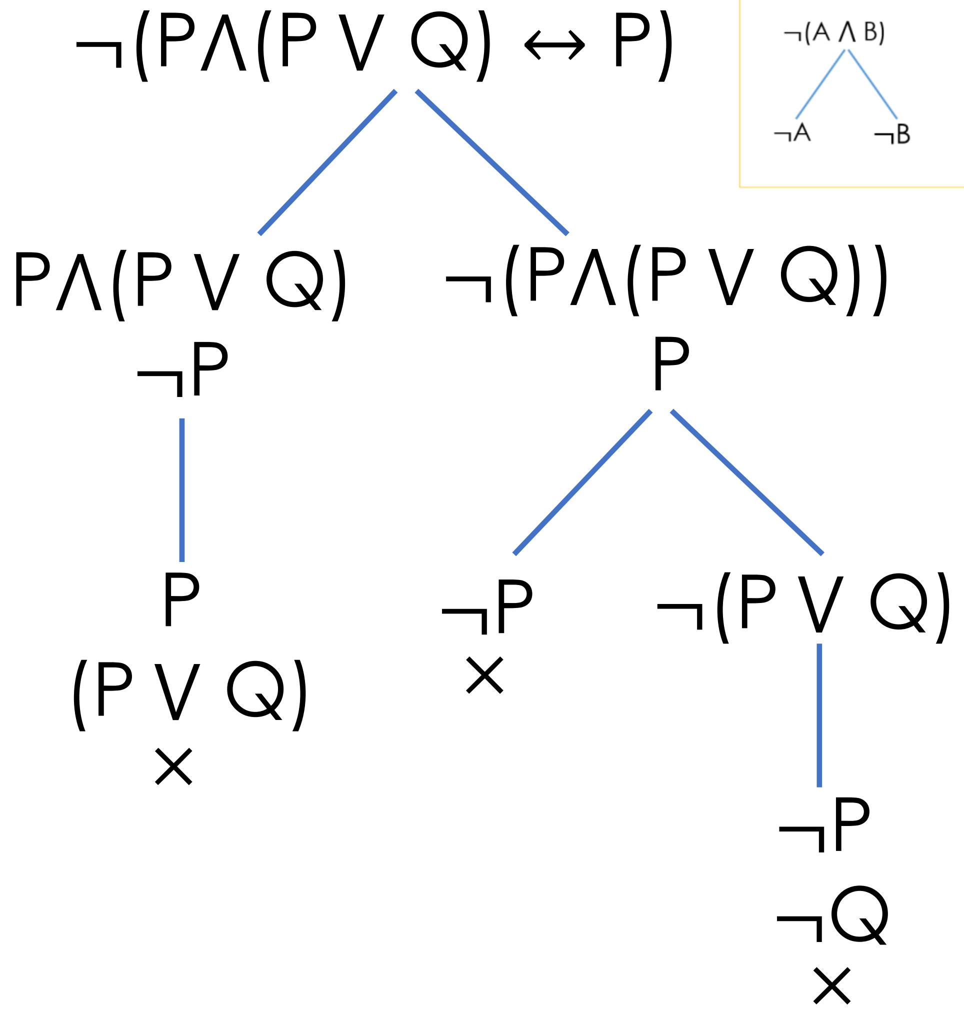
- Exemple 1: Vérifier la validité de la formule suivante :
- $P \rightarrow (Q \rightarrow P)$

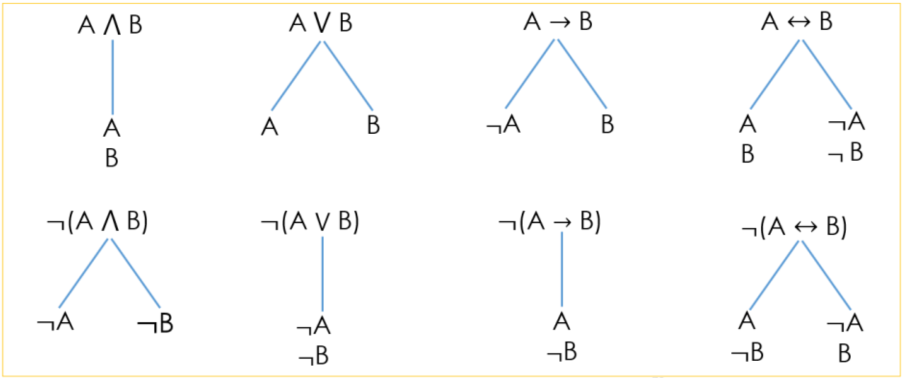




Arbre sémantique

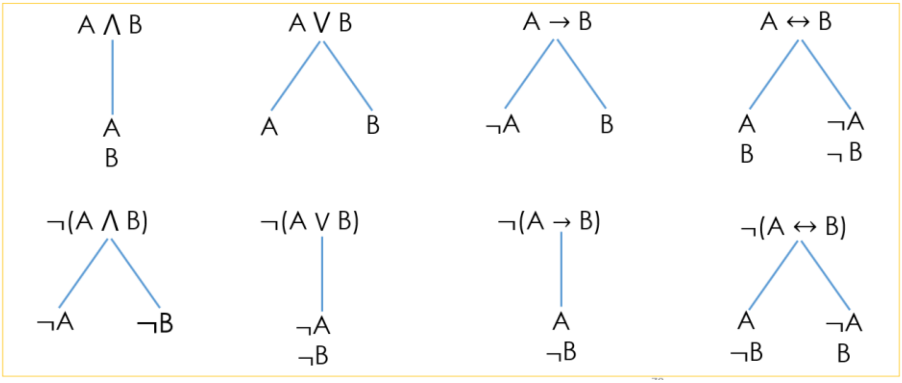
- Exemple 2: Vérifier la validité de la formule suivante :
- PΛ(P V Q) ↔ P

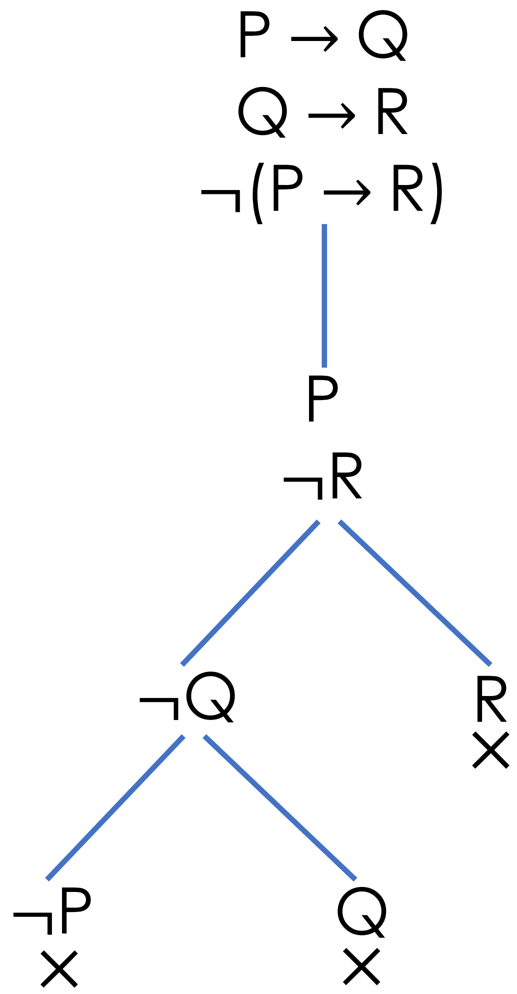




Arbre sémantique

- Exemple 3: Vérifier la déduction suivante :
- $P \rightarrow Q, Q \rightarrow R \vdash P \rightarrow R$





Propriété d'inconsistance

- Un ensemble S de clauses est dit inconsistant, si et seulement si, il existe une déduction de la clause vide à partir de S ($S \vdash \square$):
- Exemple :
- $S = \{\neg P \vee \neg Q \vee R, \neg P \vee Q, P, \neg R\}$
  - C0: $\neg P \vee \neg Q \vee R$
  - C1: $\neg P \vee Q$
  - C2: P
  - C3: $\neg R$
  - C4: $\neg P \vee \neg Q$ RR(C0,C3)
  - C5: $\neg P$ RR (C1,C4)
  - C6: $\square$ RR (C2,C5)

Graphe de déduction

- Une déduction peut être représentée par un graphe G(N,L) dont chaque sommet de N est étiqueté par une clause et dont les arcs de L permettant de relier les clauses à leurs résolvantes.

- $S = \{\neg P \vee \neg Q \vee R,\ \neg P \vee Q,\ P,\ \neg R\}$
  - C0: $\neg P \vee \neg Q \vee R$
  - C1: $\neg P \vee Q$
  - C2: P
  - C3: $\neg R$
  - C4: $\neg P \vee \neg Q$ RR(C0,C3)
  - C5: $\neg P$ RR (C1,C4)
  - C6: $\square$ RR (C2,C5)