I Rappel de logique propositionnelle

Soit V un ensemble de variables propositionnelles. Les formules logiques peuvent aussi être définies par une grammaire :

Définition : Formule logique

L'ensemble des formules logiques $\mathcal{F}$ sur V est le langage engendré par la grammaire :

$$S \to \top \mid \bot \mid x \in V \mid \neg S \mid (S \vee S) \mid (S \wedge S) \mid (S \to S)$$

Exercice 1.
Cette grammaire est-elle ambiguë ? $\mathcal{F}$ est-il régulier ?

Théorème : Induction sur les formules

Soit P une propriété sur $\mathcal{F}$. Si les conditions suivantes sont vérifiées, alors P est vraie pour toute formule de $\mathcal{F}$:

- $P(\top)$, $P(\bot)$, et $\forall x \in V,\ P(x)$
- $P(\varphi) \implies P(\neg\varphi)$
- $P(\varphi_1)$ et $P(\varphi_2) \implies P(\varphi_1 \vee \varphi_2)$
- $P(\varphi_1)$ et $P(\varphi_2) \implies P(\varphi_1 \wedge \varphi_2)$

Définition : Valuation

Une valuation sur V est une fonction de V vers $\{0, 1\}$ (faux, vrai).

Définition : Évaluation

Soit v une valuation sur V. On étend v aux formules logiques inductivement :

- $v(\top) = 1$, $v(\bot) = 0$
- $v(\neg\varphi) = 1 - v(\varphi)$
- $v(\varphi \wedge \psi) = \min(v(\varphi), v(\psi))$
- $v(\varphi \vee \psi) = \max(v(\varphi), v(\psi))$
- $v(\varphi \to \psi) = v(\neg\varphi \vee \psi)$

Si $v(\varphi) = 1$, on dit que v est un modèle pour φ.
On dit que φ est satisfiable s'il existe une valuation v telle que $v(\varphi) = 1$.

Exercice 2.
Définir inductivement l'ensemble $\mathcal{M}(\varphi)$ des modèles de φ.

Définition : Équivalence

Deux formules φ et ψ sont équivalentes (et on note $\varphi \equiv \psi$) si, pour toute valuation v, $v(\varphi) = v(\psi)$.

Remarque : Deux formules sont équivalentes si et seulement si leur table de vérité est identique. On peut donc démontrer l'équivalence de deux formules avec leurs tables de vérité, en revenant à la définition, ou par induction.

Quelques équivalences importantes :

$$\neg(\varphi \vee \psi) \equiv \neg\varphi \wedge \neg\psi$$

$$\neg(\varphi \wedge \psi) \equiv \neg\varphi \vee \neg\psi$$

$$\varphi_1 \vee (\varphi_2 \wedge \varphi_3) \equiv (\varphi_1 \vee \varphi_2) \wedge (\varphi_1 \vee \varphi_3)$$

$$\varphi_1 \wedge (\varphi_2 \vee \varphi_3) \equiv (\varphi_1 \wedge \varphi_2) \vee (\varphi_1 \wedge \varphi_3)$$

Exercice 3.
À quelles formules sont équivalentes $(\bigvee_i \varphi_i) \wedge (\bigvee_j \psi_j)$ et $(\bigwedge_i \varphi_i) \vee (\bigwedge_j \psi_j)$?

Exercice 4.
Montrer que toute formule est équivalente à une forme normale négative, c'est à dire une formule où les $\neg$ ne sont que sur des variables.

Remarque : On peut montrer que $\neg\varphi$ peut être obtenu à partir de φ en inversant $\vee$ et $\wedge$, et chaque littéral avec sa négation.

Théorème : Formes normales disjonctives et conjonctives

1. Toute formule logique est équivalente à une formule sous forme normale disjonctive, c'est à dire de la forme $c_1 \vee ... \vee c_k$ où chaque c_i est une clause disjonctive (un $\vee$ de littéraux).
2. Toute formule logique est équivalente à une formule sous forme normale conjonctive, c'est à dire de la forme $c_1 \wedge ... \wedge c_n$ où chaque c_i est une clause conjonctive (un $\wedge$ de littéraux).

Exercice 5.

1. Montrer que le problème `SAT` restreint aux formes normales disjonctives appartient à P.
2. Existe-t-il un algorithme polynomial pour transformer une formule logique en une formule équivalente sous forme normale disjonctive ?

Exercice 6.
Combien existe-t-il de formules logiques sur un ensemble de n variables, à équivalence près ?

Définition : Modèle

On note $\Gamma \models A$, et on dit que Γ est un modèle pour A (ou que A est une conséquence de Γ), si toute valuation satisfaisant les formules de Γ satisfait aussi A, c'est-à-dire :

$$\text{Pour toute valuation, } (\forall \varphi \in \Gamma,\ v(\varphi) = 1) \implies v(A) = 1$$

Exercice 7.
Montrer que :

1. $\varphi \models \psi$ si et seulement si $\models \varphi \longrightarrow \psi$
2. Loi de Pierce : $\models ((\varphi \longrightarrow \psi) \longrightarrow \varphi) \longrightarrow \varphi$

II Déduction naturelle

La logique propositionnelle de la partie précédente permet de définir la vérité d'une formule alors que la déduction naturelle formalise la notion de preuve. Ces deux notions sont équivalentes mais ce n'est pas évident et seule une implication (correction de la déduction naturelle) est au programme.

Définition : Séquent

Un séquent, noté $\Gamma \vdash A$ et prononcé Γ thèse A, est formé d'un ensemble Γ de formules logiques et d'une formule logique A.

$\Gamma \vdash A$ signifie que sous les hypothèses Γ, on peut déduire A. Γ est l'ensemble des hypothèses à un instant donné d'une démonstration.

Définition : Règle d'inférence

Une règle d'inférence est constituée :

- d'un ensemble de séquents $\Gamma_1 \vdash A_1, ..., \Gamma_n \vdash A_n$ appelés prémisses
- d'un séquent $\Gamma \vdash A$ appelé conclusion.

On le représente :

$$\frac{\Gamma_1 \vdash A_1 \quad \Gamma_2 \vdash A_2 \quad \cdots \quad \Gamma_n \vdash A_n}{\Gamma \vdash A}$$

Une règle sans prémisse est appelée axiome.

Une règle comme ci-dessus est valable pour toutes formules A_1, ..., A_n, A et tous ensembles de formules Γ_1, ..., Γ_n, Γ.

Définition : Preuve

On définit inductivement une preuve (ou arbre de preuve, dérivation) d'un séquent $\Gamma \vdash A$ par :

- si $\Gamma \vdash A$ est un axiome, alors $\dfrac{}{\Gamma \vdash A}$ est une preuve de $\Gamma \vdash A$
- si la règle
$$\frac{\Gamma_1 \vdash A_1 \quad \Gamma_2 \vdash A_2 \quad ... \quad \Gamma_k \vdash A_k}{\Gamma \vdash A}\ R$$
est une règle d'inférence et que $P_1, P_2, ..., P_k$ sont des preuves de $\Gamma \vdash A_1$, $\Gamma \vdash A_2$, ..., $\Gamma_k \vdash A_k$ respectivement, alors
$$\frac{P_1 \quad P_2 \quad ... \quad P_k}{\Gamma \vdash A}$$
est une preuve de $\Gamma \vdash A$.

On dit que $\Gamma \vdash A$ est prouvable s'il existe une preuve de $\Gamma \vdash A$.

Attention : Vous devez utiliser uniquement les règles autorisées pour construire une preuve. Par exemple, vous ne pouvez pas remplacer $\neg\neg A$ par A.

II.1 Axiome

$$\frac{}{} \text{ ax}$$

Si A appartient à l'ensemble des hypothèses alors A est prouvable.

II.2 Vrai $\top$ et faux $\bot$

$$\frac{}{\top_i} \qquad \frac{}{\bot_e}$$

$\top_i$: $\top$ est prouvable.

$\bot_e$: Si $\bot$ est prouvable, alors n'importe quelle formule A est prouvable.

II.3 Implication $\to$

$$\frac{}{} \to_i \qquad \frac{}{} \to_e$$

$\to_i$: Si sous l'hypothèse A, on peut prouver B, alors on peut prouver $A \to B$.

$\to_e$: Si on peut prouver $A \to B$ et A, alors on peut prouver B.

Exercice 8.
Prouver $\vdash A \to A$.

Exercice 9.
Prouver $A \to (B \to C) \vdash (B \to A) \to (B \to C)$.

II.4 Conjonction $\wedge$

$$\frac{}{} \wedge_i \qquad \frac{}{} \wedge_e^g \qquad \frac{}{} \wedge_e^d$$

$\wedge_i$: Si on peut prouver A et B, alors on peut prouver $A \wedge B$.

$\wedge_e^g$: Si on peut prouver $A \wedge B$, alors on peut prouver A.

Exercice 10.

1. Prouver $(A \wedge B) \to C \vdash A \to (B \to C)$.
2. Prouver $A \to (B \to C) \vdash (A \wedge B) \to C$.

II.5 Disjonction $\vee$

$$\frac{}{}\vee_i^g \qquad \frac{}{}\vee_i^d \qquad \frac{}{}\vee_e$$

$\vee_i^g$: Si on peut prouver A, alors on peut prouver $A \vee B$.

$\vee_e$: Si on peut prouver $A \vee B$ et que C est prouvable à partir de A et à partir de B, alors C est prouvable.

Exercice 11.

1. Prouver $A \vee (B \wedge C) \vdash A \vee B$
2. En déduire $\vdash A \vee (B \wedge C) \longrightarrow (A \vee B) \wedge (A \vee C)$.

II.6 Négation ¬

$$\frac{}{} \neg_i \qquad \frac{}{} \neg_e$$

$\neg_i$: Si sous l'hypothèse A, on peut prouver $\bot$, alors on peut prouver $\neg A$.

$\neg_e$: Si on peut prouver $\neg A$ et A, alors on peut prouver $\bot$.

Exercice 12.
Prouver $A \vdash \neg\neg A$.

II.7 Raisonnement par l'absurde, tiers-exclu

Les règles précédentes forment la logique intuitioniste. On peut ajouter le raisonnement par l'absurde (raa) ou le tiers-exclu (te) pour obtenir la logique classique :

$$\frac{}{} \text{ raa} \qquad \frac{}{} \text{ te}$$

Exercice 13.
On ajoute raa à la logique intuitioniste et on veut montrer te.

1. Prouver $\neg(A \vee \neg A) \vdash \neg A$.
2. Prouver $\vdash A \vee \neg A$.

Inversement, on peut démontrer raa à partir de te et les règles de la logique intuitioniste.

III Méthode

Pour prouver un séquent, on peut commencer par appliquer la règle la plus proche de ce qu'on souhaite obtenir.
On peut essayer de réfléchir à la façon dont on prouverait le séquent intuitivement : par exemple, pour prouver $A \to B, A \wedge C \vdash B$, on va utiliser le fait que $A \wedge C$ implique A et, comme $A \to B$, on obtient B. On applique ensuite les règles correspondantes à

l'envers (car on part de la conclusion pour arriver aux prémisses).
Parfois, on peut être bloqué dans une preuve :

$$\dfrac{\dfrac{\dfrac{}{?}}{\neg(A \wedge B) \vdash \neg A}}{\neg(A \wedge B) \vdash \neg A \vee \neg B} \vee_i^g$$

On voit qu'à partir de l'hypothèse $\neg(A \wedge B)$, on ne va pas pouvoir prouver $\neg A$. Il faut donc utiliser une autre règle que $\vee_i^g$.

IV Lien entre prouvabilité et vérité

Théorème : Correction de la déduction naturelle

Si $\Gamma \vdash A$ est prouvable alors $\Gamma \models A$.

Preuve : Soit $P(h)$: « si T est un arbre de preuve de hauteur h pour $\Gamma \vdash A$ alors $\Gamma \models A$ ».
$P(0)$ est vraie : Si T est un arbre de hauteur 0 pour $\Gamma \models A$ alors il est constitué uniquement d'une application de ax, ce qui signifie que $A \in \Gamma$ et implique $\Gamma \models A$.
Soit T un arbre de preuve pour pour $\Gamma \vdash A$ de hauteur $h+1$. Considérons la règle appliquée à la racine de T.

- $(\wedge_i)$ Supposons T de la forme : $\dfrac{\dfrac{T_1}{\Gamma \vdash A} \quad \dfrac{T_2}{\Gamma \vdash B}}{\Gamma \vdash A \wedge B} \wedge_i$
  Par hypothèse de récurrence sur T_1 et T_2, on obtient $\Gamma \models A$ et $\Gamma \models B$.
  Une valuation v satisfaisant toutes les formules de Γ satisfait donc à la fois A et B, et donc $A \wedge B$. On a bien $\Gamma \models A \wedge B$.
- $(\wedge_e)$ Supposons T de la forme : $\dfrac{\dfrac{T_1}{\Gamma \vdash A \wedge B}}{\Gamma \vdash A} (\wedge_e^g)$ Par récurrence sur T_1, $\Gamma \models A \wedge B$ et donc $\Gamma \models A$.
- Les autres cas sont similaires...

Exercice 14.
Montrer que le séquent $\vdash \bot$ n'est pas prouvable (on dit que la déduction naturelle est cohérente).

Théorème : Théorème de complétude (HP)

Si $\Gamma \models A$ alors $\Gamma \vdash A$ est prouvable.

Exercice 15.
On considère les deux problèmes suivants :

DNAT
- Instance : un séquent $\Gamma \vdash \varphi$
- Question : $\Gamma \vdash \varphi$ est-il dérivable ?

TAUTOLOGIE
- Instance : une formule logique φ
- Question : φ est-elle une tautologie ?

On admet le théorème de complétude.

1. Montrer que TAUTOLOGIE se réduit polynomialement à DNAT.
2. Montrer que DNAT se réduit polynomialement à TAUTOLOGIE.
3. Montrer que DNAT est décidable.
4. Montrer que DNAT est co-NP complet.

V Logique du premier ordre

La logique du premier ordre permet de faire des raisonnements dans un langage plus élaboré que celui qui se limite aux variables propositionnelles.

Définition : Langage du premier ordre

Un langage du premier ordre est la donnée de symboles de fonctions, ayant chacune une arité (nombre d'arguments), d'un nombre de symboles de relation, doté chacun d'une arité strictement positive.
Une fonction d'arité 0 est dite constante.

Exemples :

- La théorie des groupes avec la constante e, la fonction $^{-1}$ d'arité 1, la fonction $\star$ d'arité 2 et la relation $=$ d'arité 2.
- La théorie des ensembles avec la constante $\emptyset$, la fonction ^{c} d'arité 1, les fonctions $\cap$ et $\cup$ d'arité 2 et les relations $=$, $\in$, $\subset$ d'arité 2.

Définition : Terme

Soit $\mathcal{X}$ un ensemble de variables. On définit par induction l'ensemble des termes sur $\mathcal{X}$:

- Une variable $x \in \mathcal{X}$ est un terme.
- Une constante est un terme.
- Si f est une fonction d'arité $n > 0$ et $t_1, ..., t_n$ des termes alors $f(t_1, ..., t_n)$ est un terme.

Définition : Formule de la logique du premier ordre

Soit $\mathcal{L}$ un langage du premier ordre. L'ensemble des formules de la logique du premier ordre est alors défini par induction par :

- si R est une relation d'arité n et $t_1, ..., t_n$ des termes alors $R(t_1, t_2, ..., t_n)$ est une formule de la logique du premier ordre.
- si A et B sont des formules de la logique du premier ordre et $x \in \mathcal{X}$, alors :
  - $\neg A$, $A \wedge B$, $A \vee B$ et $A \to B$ sont des formules de la logique du premier ordre.
  - $\exists x\, A$ et $\forall x\, A$ sont des formules de la logique du premier ordre.

Exemples :

- Dans le langage de la théorie des groupes, $\forall x \exists y (x \star y = e)$ est une formule.
- Dans le langage de la théorie des ensembles, $\forall x \forall y ((x \cup y)^c = x^c \cap y^c))$ est une formule.

Attention : il ne faut pas confondre variable (terme décrivant un objet du langage du premier ordre étudié), par exemple un nombre réel, et variable propositionnelle (objet qui possède une valeur de vérité).

Définition : Variable libre, variable liée

Si ϕ est une formule du premier ordre et x une variable, on dit que x est libre dans ϕ si elle n'est pas associée à un $\exists$ ou un $\forall$. Sinon, on dit que x est liée.

Définition : Substitution

Si ϕ est une formule du premier ordre, on note $\phi[x := t]$ la formule obtenue en remplaçant toutes les occurrences libres de x par t dans ϕ, après renommage des variables si nécessaire.

Exemple : Si $A = (\forall x (x = x)) \wedge \exists y (x = y)$. Alors $A[x := y \star y] = (\forall x (x = x)) \wedge \exists z (y \star y = z)$.

V.1 Quantificateur universel $\forall$

Si x n'est pas une variable libre de Γ :

$$\frac{\Gamma \vdash A}{\Gamma \vdash \forall x\, A}\ \forall_i$$

Si A n'a pas de variable liée en commun avec t :

$$\frac{\Gamma \vdash \forall x\, A}{\Gamma \vdash A[x := t]}\ \forall_e$$

$\forall_i$: Si A est vraie sans faire d'hypothèse sur x, alors elle est vraie quelle que soit la valeur de cette variable.

$\forall_e$: Si A est vraie pour toute valeur de x, alors elle est vraie en remplaçant x par t.

V.2 Quantificateur existentiel $\exists$

$$\frac{\Gamma \vdash A[x := t]}{\Gamma \vdash \exists x\, A}\ \exists_i$$

Si x n'est pas une variable libre de B ni de Γ :

$$\frac{\Gamma \vdash \exists\, x A \qquad \Gamma, A \vdash B}{\Gamma \vdash B}\ \exists_e$$

$\exists_i$: Si A est vraie pour une certaine valeur de x, alors elle est vraie pour une certaine variable.

$\exists_e$: Si A est vraie pour une certaine variable, alors B est vraie.

Exercice 16.
Montrer les séquents suivants :

1. $\vdash \forall x\, \exists y\, x \vee y$
2. $\exists x\, (A \vee B) \vdash \exists x\, A \vee \exists x\, B$
3. $\neg(\exists x\, A) \vdash \forall x\, \neg A$

4. $\forall x\,(x \star x^{-1} = e) \vdash \forall x \forall y \exists z\,(x \star y) \star z = e$ dans le langage de la théorie des groupes

	Introduction	**Élimination**
Conjonction	$\dfrac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ \wedge_i$	$\dfrac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\ \wedge_e^g \qquad \dfrac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\ \wedge_e^d$
Disjonction	$\dfrac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ \vee_i^g \qquad \dfrac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ \vee_i^d$	$\dfrac{\Gamma, A \vdash C \quad \Gamma, B \vdash C \quad \Gamma \vdash A \vee B}{\Gamma \vdash C}\ \vee_e$
Implication	$\dfrac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}\ \to_i$	$\dfrac{\Gamma \vdash A \to B \quad \Gamma \vdash A}{\Gamma \vdash B}\ \to_e$
Négation	$\dfrac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}\ \neg_i$	$\dfrac{\Gamma \vdash A \quad \Gamma \vdash \neg A}{\Gamma \vdash \bot}\ \neg_e$
Vrai $\top$	$\dfrac{}{\Gamma \vdash \top}\ \top_i$	
Faux $\bot$		$\dfrac{\Gamma \vdash \bot}{\Gamma \vdash A}\ \bot_e$
Universel	Si x n'est pas une variable libre de Γ : $\dfrac{\Gamma \vdash A}{\Gamma \vdash \forall x\, A}\ \forall_i$	Si A n'a pas de variable liée en commun avec t : $\dfrac{\Gamma \vdash \forall x\, A}{\Gamma \vdash A[x := t]}\ \forall_e$
Existentiel	$\dfrac{\Gamma \vdash A[x := t]}{\Gamma \vdash \exists x\, A}\ \exists_i$	Si x n'est pas une variable libre de B ni de Γ : $\dfrac{\Gamma \vdash \exists x A \quad \Gamma, A \vdash B}{\Gamma \vdash B}\ \exists_e$

Règles de logique classique, où A, B, C sont des formules quelconques

Axiome	**Réduction à l'absurde**
$\dfrac{}{\Gamma, A \vdash A}\ \text{ax}$	$\dfrac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}\ \text{raa}$

Règles supplémentaires