Chapitre 2

Calcul propositionnel

C'est le formalisme logique le plus simple. Mais il est fondamental pour plusieurs raisons :

— Bien sûr, il sert d'introduction pédagogique.
— Plusieurs résultats en calcul des prédicats, en logique temporelle etc... s'obtiennent par "relèvement" de résultats du calcul propositionel.
— En fait, en pratique, il est très utilisé à cause de sa simplicité et de l'algorithmique relativement efficace qu'on peut mettre en oeuvre.

Il y a aussi plusieurs formalismes pour le calcul propositionnel. On commencera par le plus standard "à la Hilbert", puis on s'interessera au calcul des séquents, à la déduction naturelle (dans les deux cas, dans le cas classique et dans le cas intuitioniste), ainsi qu'à d'autres représentations comme les anneaux Booléens.

2.1 Syntaxe

La définition d'une logique passe par trois étapes : la définition des énoncés (syntaxe), la définition des modèles (sémantique) et enfin, la théorie de la preuve.

On suppose ici donné un ensemble de *variables propositionnelles* $\mathcal{P}$.

Definition 2.1.1 *L'ensemble $\mathcal{F}_0(\mathcal{P})$ des formules du calcul propositionel est le plus petit ensemble tel que :*

— *les constantes $\top, \bot$ sont dans $\mathcal{F}_0(\mathcal{P})$*
— *$\mathcal{P} \subseteq \mathcal{F}_0(\mathcal{P})$*
— *Si $\phi \in \mathcal{F}_0(\mathcal{P})$ alors $\neg\phi \in \mathcal{F}_0(\mathcal{P})$*
— *Si $\phi, \psi \in \mathcal{F}_0(\mathcal{P})$, alors $\phi \vee \psi, \phi \wedge \psi, \phi \to \psi \in \mathcal{F}_0(\mathcal{P})$*

Dans cette définition, $\neg, \vee, \wedge, \to$ sont les *connecteurs logiques.*

On définit aussi les *formules de taille n* par récurrence sur $n \in \mathbb{N}$:

— Si $\phi \in \mathcal{P} \cup \{\bot, \top\}$, alors ϕ est une formule de taille 1
— Si ϕ est une formule de taille n et ψ est une formule de taille m, alors $\neg\phi$ est une formule de taille $n+1$ et $\phi \wedge \psi$, $\phi \vee \psi$, $\phi \to \psi$ sont des formules de taille $n+m+1$.

Soit $\mathcal{F}_0(\mathcal{P})_n$ l'ensemble des formules de taille n ainsi défini.

Proposition 2.1.1 $\mathcal{F}_0(\mathcal{P}) = \bigcup_{n\in\mathbb{N}} \mathcal{F}_0(\mathcal{P})_n$.

Exercice 2 (3)
Prouver la proposition précédente.

Cette proposition permet des définitions par récurrence sur la taille de la formule.

Exemple 2.1.1 Soit

$\mathcal{P} = \{\texttt{La\_boîte\_1\_contient\_une\_bombe}, \ldots, \texttt{La\_boîte\_n\_contient\_une\_bombe}\}$

un ensemble de n variables propositionnelles. Voici des exemples de formules de $\mathcal{F}_0(\mathcal{P})$:

$$\texttt{La\_boîte\_1\_contient\_une\_bombe} \wedge \texttt{La\_boîte\_2\_contient\_une\_bombe}$$
$$\texttt{La\_boîte\_1\_contient\_une\_bombe} \wedge \neg\texttt{La\_boîte\_1\_contient\_une\_bombe}$$

Exemple 2.1.2 Soit $\mathcal{P} = \{A_n \mid n \in \mathbb{N}\}$. Sont des formules de $\mathcal{F}_0(\mathcal{P})$:

$$A_2 \wedge A_2 \wedge (A_2 \vee \neg A_2)$$
$$A_2 \rightarrow (A_1 \rightarrow A_2)$$

N'est pas une formule :

$$A_1 \vee A_2 \vee \ldots \vee A_n \vee \ldots \quad \text{(disjonction infinie)}$$

Remarques :

1. Le parenthésage doit permettre de désambigüer. Habituellement la négation a priorité sur les autres connecteurs.
2. Le cas des disjonctions infinies sera (entre autres) étudié ultérieurement ; il s'agit d'une logique plus expressive que $\mathcal{F}_0(\mathcal{P})$.

2.2 Sémantique

Une *interprétation* est une application I de $\mathcal{P}$ dans $\{0, 1\}$.

Definition 2.2.1 *Une interprétation* I satisfait *une formule* $\phi \in \mathcal{F}_0(\mathcal{P})$*, ce que l'on note* $I \models \phi$ *(*$\models \subseteq 2^{\mathcal{P}} \times \mathcal{F}_0(\mathcal{P})$*), si*

— $\phi = \top$ *ou bien*
— $\phi \in \mathcal{P}$ *et* $I(\phi) = 1$ *ou bien*
— $\phi = \phi_1 \wedge \phi_2$ *et (*$I \models \phi_1$ et $I \models \phi_2$*) ou bien*
— $\phi = \phi_1 \vee \phi_2$ *et (*$I \models \phi_1$ ou $I \models \phi_2$*) ou bien*
— $\phi = \phi_1 \rightarrow \phi_2$ *et (* si $I \models \phi_1$ alors $I \models \phi_2$*) ou bien*
— $\phi = \neg\psi$ *et* $I \not\models \psi$

Definition 2.2.2 *Une interprétation I satisfait un ensemble de formules S (noté $I \models S$) si I satisfait chacune des formules de S.*

Un modèle *d'un ensemble S de formules est une interprétation I telle que $I \models S$.*

Une formule ϕ (resp. un ensemble de formules S') est une conséquence logique *de ψ (resp. d'un ensemble de formules S) si tout modèle de ψ (resp. tout modèle de S) est un modèle de ϕ (resp. est un modèle de l'une des formules de S'). On note alors $\psi \models \phi$ (resp. $S \models S'$).*

Une formule est satisfaisable *si elle a au moins un modèle.*

Une formule ϕ est valide *si toute interprétation est un modèle de ϕ.*

On dit que deux formules sont logiquement équivalentes *lorsqu'elles ont les mêmes modèles.*

Exercice 3 (1)
Donner l'ensemble de tous les modèles de la formule $\phi \stackrel{\text{def}}{=} ((P \to Q) \vee (\neg P \to \neg Q)) \wedge (Q \wedge R \to \neg P)$ lorsque $\mathcal{P} = \{P, Q, R\}$.

Exercice 4 (1)
Montrer que :

1. ϕ est insatisfaisable si et seulement si $\neg\phi$ est valide
2. $\phi \models \psi$ si et seulement si $\phi \to \psi$ est valide.

Exercice 5 (4)
Montrer que, si $\mathcal{P}$ est fini, alors dans tout ensemble de formules fini de cardinal assez grand (on précisera cette borne), il existe deux formules logiquement équivalentes (i.e. qui ont même ensembles de modèles).

Exercice 6 (5)

1. Montrer que, lorsque $\mathcal{P}$ est fini, pour tout ensemble d'interprétations S, il existe un ensemble de formules E tel que S est exactement l'ensemble des modèles de E.
2. Montrer que ce résultat est faux lorsque $\mathcal{P}$ est infini.

Exercice 7 (6)
Donner un exemple d'un ensemble de formules dont l'ensemble des modèles est infini et dénombrable.

Exercice 8 (5)
(théorème d'interpolation) Soient ϕ, ψ telles que $\phi \models \psi$. Montrer que il existe une formule θ telle que $\phi \models \theta$, $\theta \models \psi$ et les variables propositionnelles apparaissant dans θ, apparaissent aussi dans ϕ et dans ψ.

Exercice 9 (6)
(théorème de compacité) $\{0, 1\}$ est muni de la topologie pour laquelle tout sous-ensemble est un ouvert. $\{0, 1\}$ muni de cette topologie est ainsi un compact. L'ensemble $\{0, 1\}^A$ des interprétations des formules propositionnelles construites sur A est alors muni de la topologie produit : les ouverts sont les unions (arbitraires) de produits $\Pi_{a \in A} \mathcal{O}_a$ où l'ensemble des $a \in A$ tels que $\mathcal{O}_a \neq \{0, 1\}$ est fini.

Tout produit de compacts étant compact (ce qui est admis), l'espace $\mathcal{I}$ de toutes les interprétations est ainsi un compact.

1. Montrer que, pour toute formule ϕ, l'ensemble des interprétations qui satisfont ϕ est un fermé de $\mathcal{I}$.
2. En déduire que tout ensemble de formules insatisfaisable contient un sous-ensemble fini insatisfaisable.

Les connecteurs logiques ne sont pas tous indépendants. Par exemple, pour toutes formules ϕ et ψ, $\phi \to \psi$ est logiquement équivalent à $\neg\phi \vee \psi$.

Exercice 10 (1)
Le démontrer.

Ainsi, $\to$ est *définissable* à l'aide de $\vee, \wedge, \neg$.

Exercice 11 (2)
Montrer que $\vee, \wedge, \neg$ sont définissables à l'aide du seul connecteur $\to$ et de la constante $\bot$. On dit alors que l'ensemble $\{\to, \bot\}$ est *fonctionnellement complet*.

On peut aussi définir de nouveaux connecteurs logiques, par exemple

$$\phi \leftrightarrow \psi \stackrel{\text{def}}{=} (\phi \to \psi) \wedge (\psi \to \phi)$$

ou

$$\phi \oplus \psi \stackrel{\text{def}}{=} (\phi \wedge \neg\psi) \vee (\neg\phi \wedge \psi)$$

Exercice 12 (3)
Plus généralement, les connecteurs logiques peuvent être vus comme des fonctions Booléennes. Si F est un ensemble de fonctions Booléennes, on note $A(F)$ l'ensemble de toutes les fonctions Booléennes obtenues à l'aide des fonctions de F et de la composition et des projections (fonctions $\pi_n^i(x_1, \ldots, x_n) \stackrel{\text{def}}{=} x_i$).

Pour tout entier $n \geq 1$ on note d_n (resp. c_n) la fonction Booléenne à n arguments qui renvoie 0 (resp. 1) si et seulement si tous ses arguments valent 0 (resp. 1).

1. Montrer que, pour tous $n, m, k \geq 2$, $A(c_n, f_\neg) = A(d_m, f_\neg)$ contient toutes les fonctions Booléennes à k arguments.
2. Montrer que $f_\neg$ n'est pas dans $A(f_\vee, f_\wedge, f_\to, f_\leftrightarrow)$

Exercice 13 (4)
Donner un connecteur logique binaire qui est, seul, fonctionnellement complet.

Exercice 14 (5)
Montrer que $\{\leftrightarrow, \neg\}$ n'est pas fonctionnellement complet.

Exercice 15 (6)
Un ensemble de formules E est *indépendant* si, pour toute formule $\phi \in E$, $E \setminus \{\phi\} \not\models \phi$.

1. Montrer que, pour tout ensemble fini de formules E, il existe un sous-ensemble fini $E' \subseteq E$ indépendant tel que, pour tout $\phi \in E$, $E' \models \phi$.

2. Montrer que, pour tout ensemble dénombrable E de formules, il existe un ensemble E' de formules tel que E' est indépendant et, pour toute formule $\phi \in E'$, $E \models \phi$, pour toute formule $\psi \in E$, $E' \models \psi$.
3. Montrer qu'il n'est pas toujours possible d'avoir (en plus) $E' \subseteq E$.

Exercice 16 (8)
On considère n coffres, chacun contenant un trésor ou une bombe. Le problème est de déterminer le contenu exact de chacun des coffres. Pour cela, on peut poser par écrit une liste de N questions (formules du calcul propositionnel, les variables propositionelles étant le contenu des coffres). On obtient, une fois la liste complète des questions établies, la réponse (i.e. l'interprétation) aux N questions. Mais il est possible que (au plus) k des N réponses soient incorrectes.

Etant donnés n, k, on s'intéresse au problème de trouver le N minimal, et les questions correspondantes, de manière à déterminer à coup sûr le contenu des coffres.

Donner le N minimal (et les questions correspondantes) dans les cas suivants.

1. $k = 0$ et n quelconque
2. $n = k = 1$
3. $n \leq 5$, $k = 1$
4. $k = 1$ et n quelconque

Prendre soin dans chaque cas de justifier la réponse.

Parmi les théorèmes célèbres (en calcul des prédicats), le théorème de compacité, énoncé ici dans le cas propositionnel, permet de ramener l'insatisfaisabilité à l'insatisfaisabilité finie.

Théorème 2.2.1 (compacité) *Un ensemble de formules du calcul propositionnel sur $\mathcal{P} = \{A_n \mid n \in \mathbb{N}\}$ est insatisfaisable si et seulement si il contient un sous-ensemble fini de formules insatisfaisable.*

Preuve:
Soit $\geq$ la relation d'ordre sur $\mathcal{P}$ définie par $A_n \geq A_m$ si et seulement si $n \geq m$. Une *interprétation partielle* est une fonction de $\mathcal{P}$ dans $\{0, 1\}$ dont le domaine de définition est un ensemble $\{Q \in \mathcal{P} \mid Q < P\}$ pour un certain $P \in \mathcal{P}$. (on notera en indice de l'interprétation partielle le majorant P de son domaine de définition). L'ensemble des interprétations partielles est alors ordonné par prolongement : $I_{P_1} \leq I_{P_2}$ si $P_1 \leq P_2$ et I_{P_2} restreinte aux variables propositionelles inférieures à P_1 coïncide avec I_{P_1}.

On peut représenter graphiquement cet ordre sous forme d'un arbre des interprétations partielles (cf. figure 2.1).

Soit maintenant un ensemble S insatisfaisable. On peut supposer sans perdre de généralité que S ne contient pas deux formules logiquement équivalentes. Si l'ensemble des variables propositionnelles intervenant dans les formules de S est fini, alors S est fini (cf. exercice 5). On peut donc supposer sans perdre de

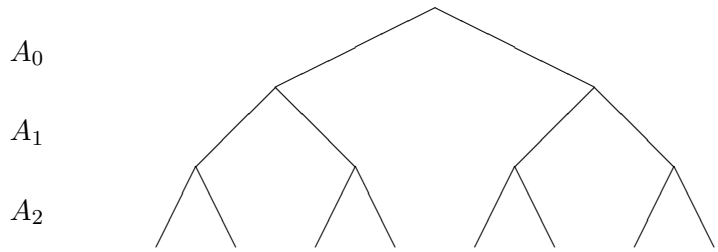

FIGURE 2.1 – arbre des interprétations partielles

généralité que l'ensemble $\mathcal{P}$ est infini et que toute variable de $\mathcal{P}$ apparaît dans au moins une formule de S.

Une interprétation partielle I *falsifie* une formule $\phi \in S$ si les variables de ϕ sont dans le domaine de définition de I et $I \not\models \phi$.

Considérons l'arbre des interprétations partielles qui ne falsifient aucune formule de S. Formellement : soit

$$\mathcal{E} = \{I_P \mid I_P \models S \cap \mathcal{F}(\{Q \in \mathcal{P}, Q \leq P\})\}$$

Si I ne falsifie aucune formule de S et $J \leq I$, alors J ne falsifie aucune formule de S : $I \in \mathcal{E}$ et $J \leq I$ entraine $J \in \mathcal{E}$.

Par l'absurde, supposons que $\mathcal{E}$ est infini. On construit alors par récurrence une suite $I_{A_n} \in \mathcal{E}$, strictement croissante, et telle que $\{J \mid J \geq I_{A_n}\} \cap \mathcal{E}$ est infini. (Autrement dit, on construit un chemin infini dans l'arbre) :

— I_{A_0} est l'interprétation de domaine vide (elle est dans $\mathcal{E}$ puisque $\mathcal{E}$ est clos par le bas).

— I_{A_n} étant construite, soient $I^j_{A_n}$ les deux prolongements de I_{A_n} à A_n : $Dom(I^j_{A_n}) = \{Q \mid Q \leq A_n\}$ et $I^j_{A_n}(A_n) = j$, pour $j = 0, 1$. $\mathcal{E}_n = \{J \in \mathcal{E}, J \geq I_{A_n}\}$ est infini par hypothèse de récurrence et, de plus,

$$\mathcal{E}_n = \{I_{A_n}\} \cup \{J \in \mathcal{E} \mid J \geq I^0_{A_n}\} \cup \{J \in \mathcal{E} \mid J \geq I^1_{A_n}\}$$

L'un de ces deux derniers ensembles au moins est donc infini. On pose alors $I_{A_{n+1}} = I^j_{A_n}$ pour j tel que $\{J \in \mathcal{E} \mid J \geq I^j_{A_n}\}$ est infini. On a bien $I_{A_{n+1}} > I_{A_n}$.

Soit alors l'interprétation I définie par : pour tout $i \in \mathbb{N}$, $I(A_i) = I_{A_{i+1}}(A_i)$. Notons que, par croissance de la suite I_{A_i}, si $j < i$, $I(A_j) = I_{A_{i+1}}(A_j)$. Pour toute formule $\phi \in S$, si i est l'indice maximal d'une variable propositionnelle de ϕ, $I_{A_{i+1}} \models \phi$, et donc $I \models \phi$. Il en résulte que $I \models S$, ce qui contredit l'insatisfaisabiliteé de S.

Il en résulte que l'arbre $\mathcal{E}$ est fini. L'ensemble des domaines des interprétations partielles de $\mathcal{E}$ est donc borné : soit N tel que $\bigcup_{I \in \mathcal{E}} Dom(I) \subseteq \{Q \mid Q < A_N\}$. $S_0 = S \cap \mathcal{F}(\{Q \mid Q \leq A_N\})$ est alors insatisfaisable et c'est un ensemble fini (d'après l'exercice 5 et puisque nous avons supposé que S ne contient pas deux

formules logiquement équivalentes). □

Exercice 17 (3)
Montrer qu'un graphe est coloriable avec k couleurs si et seulement si chacun de ses sous-graphes finis est coloriable avec k couleurs.

Exercice 18 (5)
Soit E un ensemble de formules du calcul propositionnel sur $\mathcal{P}$. On dira que E est *maximal cohérent* si E est satisfaisable et que, pour toute formule ϕ du calcul propositionnel, ou bien $\phi \in E$ ou bien $E \cup \{\phi\}$ est insatisfaisable.

1. Supposant que $\mathcal{P}$ est fini, montrer que tout ensembe de formules E satisfaisable est contenu dans un ensemble maximal cohérent.
2. Montrer que cet ensemble maximal cohérent n'est pas unique : donner (toujours dans le cas où $\mathcal{P}$ est fini) un ensemble E et deux ensembles maximaux cohérents distincts contenant E.
3. Que devient le résultat de la première question lorsque $\mathcal{P}$ est infini dénombrable ?

Exercice 19 (7)
Étant données une famille d'interprétations $(I_\alpha)_{\alpha \in E}$, leur interesection est l'interprétation I telle que $I(P) = 1$ ssi ($I_\alpha(P) = 1$ pour tout $\alpha \in E$).

Soit Σ un ensemble de formules de $\mathcal{F}_0(\mathcal{P})$. On dit que Σ est *préservé par intersections finies* si, l'intersection de deux modèles de Σ est un modèle de Σ. Σ est *préservé par intersections* si toute intersection de modèles de Σ est un modèle de Σ. Σ est *axiomatisé* par Γ si, pour tout $\phi \in \mathcal{F}_0(\mathcal{P})$, $\Gamma \models \phi$ si et seulement si $\Sigma \models \phi$.

1. Montrer que Σ est préservé par intersections finies si et seulement si Σ est préservé par intersections.
2. Une *clause* est une formule

   $$A_1 \vee \ldots \vee A_n$$

   dans laquelle les A_i sont des variables propositionnelles (appelés *littéraux positifs*) ou des négations de variables propositionnelles (appelées *littéraux négatifs*). Une *clause de Horn* est une clause contenant au plus un littéral positif.

   Montrer que Σ est axiomatisable par un ensemble de clauses de Horn si et seulement si Σ est stable par intersections. (On pourra supposer, sans perte de généralité, que Σ est un ensemble de clauses).

Exercice 20 (6)
On suppose ici que $\mathcal{P}$ est dénombrable.

1. Soient $\mathcal{E}_1$, $\mathcal{E}_2$ deux ensembles de formules de $\mathcal{F}_0(\mathcal{P})$ et $\mathcal{M}_1$, $\mathcal{M}_2$ leurs ensembles respectifs de modèles. Donner un ensemble de formules $\mathcal{E}$ dont $\mathcal{M}_1 \cup \mathcal{M}_2$ est l'ensemble des modèles.
2. Plus généralement, montrer que, si $\mathcal{M}$ est un sous-ensemble fermé de $2^{\mathcal{P}}$ (cf. exercice 9 pour la définition de la topologie), alors il existe un ensemble de formules $\mathcal{E}$ dont $\mathcal{M}$ est l'ensemble des modèles.

$$
\begin{array}{rcl}
\phi \to \psi & \Rightarrow & (\neg\phi) \vee \psi \\
\neg\neg\phi & \Rightarrow & \phi \\
\neg(\phi \wedge \psi) & \Rightarrow & (\neg\phi) \vee (\neg\psi) \\
\neg(\phi \vee \psi) & \Rightarrow & (\neg\phi) \wedge (\neg\psi) \\
(\phi \wedge \psi) \vee \theta & \Rightarrow & (\phi \vee \theta) \wedge (\psi \vee \theta) \\
\theta \vee (\phi \wedge \psi) & \Rightarrow & (\theta \vee \phi) \wedge (\theta \vee \psi) \\
\top \vee \phi & \Rightarrow & \top \\
\phi \vee \top & \Rightarrow & \top \\
\phi \wedge \top & \Rightarrow & \phi \\
\top \wedge \phi & \Rightarrow & \phi \\
\bot \vee \phi & \Rightarrow & \phi \\
\phi \vee \bot & \Rightarrow & \phi \\
\phi \wedge \bot & \Rightarrow & \bot \\
\bot \wedge \phi & \Rightarrow & \bot \\
\neg\top & \Rightarrow & \bot \\
\neg\bot & \Rightarrow & \top
\end{array}
$$

FIGURE 2.2 – Règles de mise en forme clausale

2.3 Forme clausale

On considère les règles de simplification de la figure 2.2.

Dans les règles de la figure 2.2, ϕ, ψ, θ sont des *variables logiques* : elles peuvent être remplacées par n'importe quelle formule de $\mathcal{F}_0(\mathcal{P})$.

De plus, les règles peuvent être appliquées dans n'importe quel contexte. Plus formellement, un *contexte* est une formule de $\mathcal{F}_0(\mathcal{P} \cup \{\Box\})$ où $\Box \notin \mathcal{P}$, qui ne comporte qu'une seule occurrence de $\Box$. Si C est un contexte et $\phi \in \mathcal{F}_0(\mathcal{P})$, $C[\phi]$ est la formule de $\mathcal{F}_0(\mathcal{P})$ obtenue en repmplaçant $\Box$ dans C par ϕ. La relation $\Rightarrow$ est alors la (plus petite) relation binaire sur $\mathcal{F}_0(\mathcal{P})$ qui contient toutes les instances des règles de la figure 2.2 et telle que, pour tout contexte C, si $\phi \Rightarrow \psi$, alors $C[\phi] \Rightarrow C[\psi]$.

Proposition 2.3.1 *Les règles de la figure 2.2 transforment des formules en des formules logiquement équivalentes.*

Proposition 2.3.2 *Les règles de la figure 2.2 se terminent (quel que soit l'ordre dans lequel elles sont appliquées) : il n'existe aucune suite infinie $\phi_n, n \in \mathbb{N}$ de formules de $\mathcal{F}_0(\mathcal{P})$ telle que, pour tout i, $\phi_i \Rightarrow \phi_{i+1}$.*

Ce résultat reste vrai si les règles sont appliquées modulo l'associativité-commutativité de $\wedge, \vee$: si une (instance de) règle s'applique à ϕ et ψ est identique à ϕ modulo l'associativité-commutativité de $\wedge, \vee$, elle s'applique à ψ, avec le même résultat.

Preuve:
On interprète comme suit les formules dans les entiers :

- $f(\bot) = f(\top) \stackrel{\text{def}}{=} 2$
- $f(P) \stackrel{\text{def}}{=} 2$ si P est une variable propositionnelle.
- $f(\phi \wedge \psi) \stackrel{\text{def}}{=} g_1(f(\phi), f(\psi))$ où $g_1(x, y) \stackrel{\text{def}}{=} x + y + 1$
- $f(\phi \vee \psi) \stackrel{\text{def}}{=} g_2(f(\phi), f(\psi))$ où $g_2(x, y) \stackrel{\text{def}}{=} x \times y$
- $f(\neg\phi) \stackrel{\text{def}}{=} g_3(f(\phi))$ où $g_3(x) \stackrel{\text{def}}{=} 2^x$
- $f(\phi \to \psi) \stackrel{\text{def}}{=} g_4(f(\phi), f(\psi))$ où $g_4(x, y) \stackrel{\text{def}}{=} 2^{1+x+y}$

L'interprétation des formules est ensuite compatible avec l'associativité-commutativité de $\wedge, \vee$: $f(\phi \wedge \psi) = f(\psi \wedge \phi)$, $f(\psi \vee \phi) = f(\phi \vee \psi)$ et $f(\phi \wedge (\psi \wedge \theta)) = f((\phi \wedge \psi) \wedge \theta)$, $f(\phi \vee (\psi \vee \theta)) = f((\phi \vee \psi) \vee \theta)$. f est donc bien définie, indépendemment du représentant choisi, dans la classe d'équivalence modulo associativité et commutativité.

On montre d'abord par récurrence sur ϕ que $f(\phi) \geq 2$.

Ensuite, toutes les fonctions g_i sont strictement croissantes dans leurs deux arguments pour $x, y \geq 2$. Il en résulte que, si $f(\phi) > f(\psi)$, alors $f(C[\phi]) > f(C[\psi])$ pour tout contexte C.

Il suffit ainsi de démontrer que, pour toutes les formules ϕ, ψ, chacune des règles fait décroître f. Pour plus de clarté, on notera $x = f(\phi)$, $y = f(\psi)$, $z = f(\theta)$ dans ce qui suit.

- $f(\phi \to \psi) = 2^{1+x+y}$ et $f(\neg\phi \vee \psi) = 2^x \times y$. Mais, pour $y \geq 0$, $2^y > y$ donc $2^{1+x+y} > 2^x \times y$.
- $f(\neg\neg\phi) = 2^{2^x} > x$
- $f(\neg(\phi \wedge \psi)) = 2^{x+y+1} > f(\neg\phi \vee \neg\psi) = 2^x \times 2^y$
- $f(\neg(\phi \vee \psi)) = 2^{x \times y}$ et $f(\neg\phi \wedge \neg\psi) = 2^x + 2^y + 1$. Or, pour $x, y \geq 2$, $x \times y \geq x + y$, donc $2^{x \times y} \geq 2^x \times 2^y \geq 2^x + 2^y \times (2^x - 1)$. Mais $2^x - 1 > 2$ pour $x \geq 2$, donc $2^{x \times y} > 2^x + 2 \times 2^y > 2^x + 2^y + 1$.
- $f((\phi \wedge \psi) \vee \theta) = f(\theta \vee (\phi \wedge \psi)) = (x + y + 1) \times z$ et $f((\phi \vee \theta) \wedge (\psi \vee \theta)) = x \times z + y \times z + 1$ qui est strictement inférieur à $x \times z + y \times z + z$ pour $z \geq 2$.
- Les autre cas sont immédiats.

□

Une *forme irréductible* d'une formule ϕ est une formule ψ telle que $\phi \Rightarrow \cdots \Rightarrow \psi$ et aucune règle ne s'applique à ψ.

Proposition 2.3.3 *Les règles de la figure 2.2 sont confluentes : toute formule ϕ possède une forme irréductible unique, modulo l'associativité et la commutativité de $\wedge, \vee$.*

Exercice 21 (4)
Montrer que le résultat ci-dessus est faux si on enlève "modulo l'associativité de $\wedge, \vee$".

L'ordre d'application des règles n'influe donc pas sur le résultat. En revanche, certaines réductions pourront être beaucoup (exponentiellement) plus longues que d'autres.

Definition 2.3.1 *Une formule est en* forme normale conjonctive *si elle est irréductible pour les règles de la figure 2.2.*

Definition 2.3.2 *Un* littéral *est une variable propositionnelle ou la négation d'une variable propositionnelle.*

Une clause *est une disjonction de littéraux ou bien* $\bot$*.*

Proposition 2.3.4 *Toute formule en forme normale conjonctive est une conjonctions de clauses ou bien* $\top$*.*

Definition 2.3.3 *Une* forme clausale *d'une formule* $\phi \in \mathcal{F}_0(\mathcal{P})$ *est une formule en forme normale conjonctive, logiquement équivalente à* ϕ*.*

Exercice 22 (3)
Donner un exemple de formule ayant deux formes clausales distinctes.

L'exercice suivant montre que les formes clausales peuvent inévitablement conduire à une croissance exponentielle de la formule.

Exercice 23 (6)
Si $\phi \in \mathcal{F}_0(\mathcal{P})$, on note $\tau(\phi)$ la taille minimale d'une forme clausale de ϕ.

1. Donner un exemple d'une famille de formules ϕ_n telles que $\lim_{n\to+\infty} |\phi_n| = +\infty$ et $\lim_{n\to+\infty} \frac{\tau(\phi_n)}{\sqrt{2^{|\phi_n|}}} > 0$.
2. Montrer que, pour toute formule ϕ, $\tau(\phi) < |\phi| \times 2^{\frac{|\phi|+5}{2}}$

$$\text{Résolution binaire} \quad \frac{\neg A \vee C \quad A \vee C'}{C \vee C'}$$

$$\text{Factorisation binaire} \quad \frac{L \vee L \vee C}{L \vee C}$$

FIGURE 2.3 – Règle de résolution

2.4 Résolution

Dans cette partie, on ne considère que des formes clausales.

Décider de la satisfaisabilité d'une formule en forme clausale n'est pas (algorithmiquement) facile. C'est un problème NP-complet (voir calculabilité).

Les règles d'inférence de la figure 2.3 ont en prémisse une ou deux clauses et en conclusion une clause. Dans ces règles, C est ou bien une disjonction de littéraux, ou bien la clause vide $\perp$ (on suppose que $C \vee \perp = C$) et L est un littéral.

On note $E \vdash_R C$ lorsque la clause C peut être obtenue à partir de E. par une application d'un nombre quelconque de règles de la figure 2.3. De manière équivalente, $E \vdash C$ s'il existe un arbre dont les noeuds sont étiquetés par des clauses, la racine est étiquetée par C, les étiquettes des feuilles sont dans E et, chaque noeud qui n'est pas une feuille

- ou bien a un seul fils et, dans ce cas, son étiquette est obtenue par factorisation à partir de l'étiquette de son fils
- ou bien a deux fils et, dans ce cas, son étiquette est obtenue par résolution binaire à partir des étiquettes de ses deux fils.

La *taille* d'une preuve est le nombre de noeuds de l'arbre correspondant.

Exemple 2.4.1 Si $E = \{P \vee \neg Q \vee R, P \vee \neg R\}$ alors $E \vdash_R P \vee \neg Q$ et voici un arbre de preuve :

$$\dfrac{\dfrac{P \vee \neg Q \vee R \quad P \vee \neg R}{P \vee P \vee \neg Q}\, R}{P \vee \neg Q}\, F$$

Exercice 24 (2)
Montrer comment les règles de la figure 2.3 permettent de dériver la clause vide $\perp$ de l'ensemble de clauses

$$E = \{P \vee \neg Q, \neg P \vee \neg Q, P \vee Q, \neg P \vee Q\}$$

Exercice 25 (2)
Montrer qu'une même clause peut avoir plusieurs arbres de preuve distincts (à permutation près des fils).

Proposition 2.4.1 *Les règles de la figure 2.3 sont correctes. ($\vdash_R \subseteq \models$).*

Preuve:
Il suffit de montrer que, pour chacune des deux règles, lorsqu'une interprétation satisfait les prémisses, elle satisfait aussi la conclusion, puis de faire une récurrence sur la longueur de la preuve (taille de l'arbre de preuve). Les détails sont laissés en exercice. □

Pour démontrer le théorème qui suit, on utilisera les *arbres sémantiques* que nous définissons maintenant formellement (après les avoir utilisés dans la preuve du théorème 2.2.1).

On suppose, ainsi que dans toute la suite, que l'ensemble des variables propositionnelles est dénombrable : $\mathcal{P} = \{P_i, i \in \mathbb{N}\}$. Une *interprétation partielle* est une application de $\{P_1, \ldots, P_n\}$ dans $\{0, 1\}$. $\{P_1, \ldots, P_n\}$ est alors le domaine de l'interprétation partielle. Les interprétations partielles sont ordonnées par prolongement : $I \leq J$ si $Dom(I) \subseteq Dom(J)$ et $\forall x \in Dom(I), I(x) = J(x)$. Si $Dom(I) \neq \mathcal{P}$, il existe exactement deux interprétations partielles I_0 et I_1 telles que $I_0, I_1 > I$ et $\forall J, J > I \Rightarrow J \geq I_0$ ou $J \geq I_1$. I_0 et I_1 sont les *successeurs* de I. Si $Dom(I) = \{P_1, \ldots, P_n\}$, I_0 est l'interprétation qui prolonge I par $I_0(P_{n+1}) = 0$. C'est le *fils droit* de I. I_1 prolonge I par $I_1(P_{n+1}) = 1$. C'est le *fils gauche* de I.

Une interprétation partielle I *falsifie* une clause C si toutes les variables propositionnelles de C sont dans le domaine de I et $I \not\models C$.

Si E est un ensemble de clauses, l'*arbre sémantique* $A(E)$ est défini comme suit. On confond les chemins finis de l'arbre, les noeuds de l'arbre et les interprétations partielles qui correspondent. On précise ci-dessous la correspondance.

- La racine correspond au chemin vide, c'est à dire à l'interprétation de domaine vide.
- Si N est un noeud de l'arbre correspondant à l'interprétation I de domaine $\{P_1, \ldots, P_n\}$,
  - Ou bien il existe une clause $C \in E$ telle que I falsifie C et N est un *noeud d'échec*. C'est alors une feuille de l'arbre et on l'étiquette par une clause de E falsifiée par I
  - Ou bien on n'est pas dans le premier cas et I est une interprétation totale sur $Var(t)$. Dans ce cas N est une feuille de l'arbre. C'est un *noeud de succès*.
  - Dans les autres cas, N a deux fils qui correspondent aux deux successeurs de I.

Exemple 2.4.2 Soit $E = \{P_1, \neg P_2 \vee \neg P_1, P_3 \vee \neg P_1\}$. L'arbre sémantique de E est représenté dans la figure 2.4. L'arbre comporte un noeud de succès (et un seul) qui correspond à la seule interprétation qui satisfait E.

Lemme 2.4.1 *Si E est un ensemble de clauses, alors E est satisfaisable si et seulement si ou bien $A(E)$ contient un noeud de succès, ou bien $A(E)$ contient un chemin infini.*

Preuve:

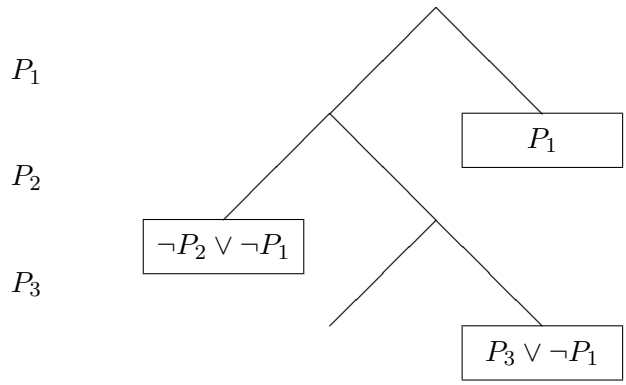

FIGURE 2.4 – Arbre sémantique de l'ensemble E de l'exemple 2.4.2

Si E est satisfaisable, alors l'interprétation I qui satisfait E définit ou bien un chemin conduisant à un noeud de succès (cas où $\mathcal{P}$ est fini) ou bien un chemin infini de $A(E)$ (cas où $\mathcal{P}$ est infini).

Réciproquement, si $A(E)$ contien un noeud de succès, alors l'interprétation I qui lui correspond est totale et ne falsifie aucune clause de E et donc $I \models E$. Si $A(E)$ contient un chemin infini, il existe une suite infinie d'interprétations partielles I_n (les noeuds de ce chemin) telles que $Dom(I_n) = \{P_1, \ldots, P_n\}$, $I_n < I_{n+1}$ et, pour tout n, I_n ne falsifie aucune clause de E. On définit alors I par $I(P_i) = I_i(P_i)$ pour tout i. Pour toute clause $C \in E$, si n_C est l'indice maximal d'une variable propositionnelle de C, $I_{n_C} \models C$ par construction, et, puisque I_{n_C} prolonge I_k pour $k \leq n_C$, I et I_C coïncident sur le domaine de I_{n_C}. Il en résulte que $I \models C$. □

Exercice 26 (2)
Construire l'arbre sémantique associé à $E = \{\neg P_2, P_1 \vee P_2 \vee P_3, P_1 \vee \neg P_3, \neg P_1 \vee P_2 \vee \neg P_3, \neg P_1 \vee P_3\}$ E est-il satisfaisable ? Pourquoi ?

Théorème 2.4.1 (Complétude réfutationnelle) *Un ensemble de clauses E est insatisfaisable si et seulement si $E \vdash_R \bot$.*

Preuve:
Si $E \vdash_R \bot$, alors E est insatisfaisable par le résultat de correction.

Supposons maintenant que E est insatisfaisable et montrons que $E \vdash_R \bot$.

Soit E^* l'ensemble des clauses C telles que $E \vdash_R C$. Comme $E \subseteq E^*$ est insatisfaisable, il en est de même pour E^*. Donc, d'après le lemme 2.4.1, $A(E^*)$ ne contient ni noeud de succès, ni chemin infini. Raisonnons alors par l'absurde et supposons que $A(E^*)$ n'est pas réduit à la racine. Soit alors N un noeud maximal ayant deux fils. Ces deux fils sont des feuilles, par maximalité, donc des noeuds d'échec. Soit I l'interprétation correspondant à N et I_0, I_1 ses deux successeurs, obtenus en interprétant la variable $P \notin Dom(I)$. Il existe des clauses de E^* qui sont falsifiées respectivement par I_0 et I_1. Soient $C_0, C_1 \in E^*$

de taille minimale qui sont falsifiées respectivement par I_0 et I_1. Comme I ne falsifie ni C_0 ni C_1, $C_0 = P \vee C'_0$ et $C_1 = \neg P \vee C'_1$. De plus si $C'_0 = P \vee C''_0$, alors, par factorisation, $C_0 \vdash_R P \vee C''_0$ et I_0 falsifie $P \vee C''_0$, ce qui contredit la minimalité de C_0. De plus C'_0 ne peut s'écrire $\neg P \vee C''_0$, car I_0 falsifie C_0. Il en résulte que $Var(C'_0) \subseteq Dom(I)$. De même, $Var(C'_1) \subseteq Dom(I)$. Par résolution, $C_0, C_1 \vdash_R C'_0 \vee C'_1$, donc $C'_0 \vee C'_1 \in E^*$. De plus I_0 falsifie C'_0, donc I falsifie C'_0 et, de même, I_1 falsifie C'_1, donc I falsifie C'_1. Il en résulte que I falsifie $C'_0 \vee C'_1$ et donc que N est un noeud d'échec. Absurde.

On en conclut que l'arbre sémantique de E^* est réduit à la racine : la racine est un noeud d'échec, ce qui ne peut se produire que si $\bot \in E^*$, c'est à dire $E \vdash_R \bot$. □

Le résultat suivant montre que l'on peut obtenir le théorème de compacité comme corollaire au théorème de complétude.

Corollaire 2.4.1 *Si E est un ensemble de clauses insatisfaisables, alors E contient un sous-ensemble fini de clauses insatisfaisable.*

Preuve:
Si E est insatisfaisable, alors $E \vdash_R \bot$. Or la preuve correspondante est un arbre fini. Si E_0 est le sous-ensemble des clauses qui étiquettent des feuilles de l'arbre, $E_0 \subseteq E$, E_0 est fini et E_0 est insatisfaisable. □

La *longueur* d'une preuve est le nombre de sous-arbres distincts dans cette preuve.

Une preuve Π est *sans boucle* si, pour toute clause C, tout sous-arbre de Π dont la racine est étiquetée par C ne contient pas lui-même de sous-arbre propre dont la racine est étiquetée par C.

Exercice 27 (6)
Soit $\mathcal{P}$ un ensemble fini de variables propositionnelles, de cardinal n. On appelle 2-clause toute clause contenant au plus deux littéraux.

1. Montrer que, si E est ensemble de 2-clauses insatisfaisable, toute preuve sans boucle de $\bot$ est de longueur polynômiale en n
2. Montrer par contre que la taille peut être exponentielle : donner un exemple d'ensemble de 2-clauses E tel que E est insatisfaisable et une preuve sans boucle de $\bot$ à partir de E dont la taille est exponentielle en n.
3. Donner un algorithme polynômial en n pour décider de la satisfaisabilité d'un ensemble de 2-clauses

Exercice 28 (6)
Soit $\mathcal{P}$ un ensemble de variables propositionnelles fini. Donner un ensemble de clauses E qui est insatisfaisable et tel qu'il existe une preuve de $\bot$ de taille exponentielle en $|E|$ et ne contenant aucune redondance (i.e. deux noeuds distincts de l'arbre de preuve qui ne sont pas des feuilles sont étiquetés par des formules distinctes).

$$\text{TE}\ \ \frac{}{P \vee \neg P} \qquad \text{A}\ \ \frac{C}{C \vee L}$$

FIGURE 2.5 – Tiers exclu et affaiblissement

En fait, on peut généraliser ce résultat (mais il n'est pas demandé de le montrer) : il existe des ensembles de clauses insatisfaisables dont *aucune* preuve de contradiction n'est de taille polynômiale.

On considère maintenant, en plus des règles d'inférence de la figure 2.3, les deux règles d'inférence de la figure 2.5. Dans ces règles, C est une clause quelconque, L est un littéral quelconque et P est une variable propositionnelle quelconque. On note $\vdash$ la relation de déduction associée.

Théorème 2.4.2 (Complétude) *Si E est un ensemble de clauses et C est une clause. Alors $E \models C$, si et seulement si $E \vdash C$. (Autrement dit $\models = \vdash$).*

Preuve:
La correction des règles d'inférence de la figure 2.5 est une vérification de routine. Il en résulte, par récurrence sur la longueur de la preuve que $E \vdash C$ entraine $E \models C$.

Réciproquement, montrons, par récurrence sur la longueur de la preuve par résolution que, pour tout ensemble de clauses E, tous littéraux $L_1, \ldots, L_k$ et toute clause C,

$$E, L_1, \ldots, L_k \vdash C$$

entraine

$$E \vdash C \vee \overline{L_1} \vee \ldots \vee \overline{L_k}$$

— Si la preuve ne contient aucune application de règle d'inférence : ou bien il existe un i tel que $C = L_i$ ou bien $C \in E$. dans le premier cas, par la règle du tiers exclu $\vdash L_i \vee \overline{L_i}$, puis, par affaiblissements, $\vdash L_i \vee \overline{L_1} \vee \ldots \vee \overline{L_k}$. Dans le deuxième cas, $E \vdash C$ et, par affaiblissements, $E \vdash C \vee \overline{L_1} \vee \ldots \vee \overline{L_k}$.
— Sinon, au moins une règle d'inférence est appliquée. Considérons la dernière règle appliquée dans la preuve.
  — Si c'est le tiers exclu, $E, L_1, \ldots, L_k \vdash P \vee \neg P$, et on obtient une preuve de $E \vdash \overline{L_1} \vee \ldots \vee \overline{L_k} \vee P \vee \neg P$:

$$\dfrac{\dfrac{}{P \vee \neg P}\, TE}{\overline{L_1} \vee \ldots \vee \overline{L_k} \vee P \vee \neg P}\, Aff$$

  — Si c'est un affaiblissement : $E, L_1, \ldots, L_k \vdash C_1$ et $C = C_1 \vee L$. Par hypothèse de récurrence, $E \vdash C_1 \vee \overline{L_1} \ldots \vee \overline{L_k}$. Par affaiblissement, $E \vdash C_1 \vee \overline{L_1} \ldots \vee \overline{L_k} \vee L$.

— Si c'est une factorisation : $C = L \vee C_1$ et $E, L_1, \ldots, L_k \vdash L \vee L \vee C_1$. Par hypothèse de récurrence,

$$E \vdash L \vee L \vee C_1 \vee \overline{L_1} \vee \ldots \vee \overline{L_k}$$

et, par factorisation,

$$L \vee L \vee C_1 \vee \overline{L_1} \vee \ldots \vee \overline{L_k} \vdash C \vee \overline{L_1} \vee \ldots \vee \overline{L_k}.$$

— Si c'est une résolution : $C = C_1 \vee C_2$ et $E, L_1, \ldots, L_k \vdash C_1 \vee P$, $E, L_1, \ldots, L_k \vdash C_2 \vee \neg P$. Par hypothèse de récurrence (appliquée deux fois) :

$$E \vdash C_1 \vee P \vee \overline{L_1} \vee \ldots \vee \overline{L_k}$$

et

$$E \vdash C_2 \vee \neg P \vee \overline{L_1} \vee \ldots \vee \overline{L_k}$$

Par résolution, on obtient alors

$$E \vdash C_1 \vee C_2 \vee \overline{L_1} \vee \ldots \vee \overline{L_k} \vee \overline{L_1} \vee \ldots \vee \overline{L_k}$$

puis, par factorisations, $E \vdash C \vee \overline{L_1} \vee \ldots \vee \overline{L_k}$.

On applique maintenant ce résultat avec $C = \bot$: pour une clause $C_0 = \overline{L_1} \vee \ldots \vee \overline{L_k}$ arbitraire, $E, L_1, \ldots, L_k \vdash \bot$ entraine $E \vdash C_0$.

Si maintenant $E \not\models C_0$, alors $E, L_1, \ldots, L_k$ est insatisfaisable et, par le théorème 2.4.1, $E, L_1, \ldots, L_k \vdash_R \bot$ et donc $E, L_1, \ldots, L_k \vdash \bot$.

D'après ce que nous venons de voir, cela entraine $E \vdash C_0$. □

Exercice 29 (3)

On considère ici un raffinement de la résolution. On définit un ordre sur les littéraux de la manière suivante : $L > L'$ si la variable propositionnelle de L a un indice strictement plus grand que la variable propositionnelle de L'. (autrement dit, on étend l'ordre sur les variables propositionnelles aux littéraux). On restreint alors l'application de la résolution binaire

$$\frac{P \vee C \qquad \neg P \vee C'}{C \vee C'}$$

au cas où P est un littéral maximal de $P \vee C$ et $\neg P$ est un littéral maximal de $\neg P \vee C'$. De même, la règle de factorisation

$$\frac{L \vee L \vee C}{L \vee C}$$

est restreinte au cas où L est maximal dans $L \vee C$.

Montrer qu'avec ces restrictions, l'ensemble de règles d'inférence est encore réfutationnellement complet.

Exercice 30 (3)
On considère le système d'inférence constitué de l'unique règle :

$$\frac{P \vee P \ldots \vee P \vee C \qquad \neg P \vee \ldots \vee \neg P \vee C'}{C \vee C'}$$

Montrer que cette règle est (à elle seule) réfutationellement complète.

Exercice 31 (3)
On dira qu'une clause C *subsume* une clause C' si $C \models C'$.

On considère la stratégie de résolution+factorisation suivante : on n'applique une règle d'inférence que lorsqu'aucune des prémisses n'est subsumée par une clause différente ancêtre dans l'arbre de preuve.

Montrer que cette stratégie est réfutationnellement complète.

Definition 2.4.1 *On appelle* clause de Horn *une clause qui contient au plus un littéral positif.*

Exercice 32 (6)
On considère ici un autre raffinement de la résolution : la règle de résolution est restreinte au cas où l'une des prémisse au moins est dans E (l'ensemble de clauses initial). Cette stratégie est dite *input*.

1. Montrer que cette stratégie n'est pas réfutationnellement complète en général.
2. Montrer qu'elle est réfutationnellement complète lorsque E est un ensemble de clauses de Horn

Exercice 33 (5)
Donner un algorithme polynômial qui permet, étant donné un ensemble fini de clauses de Horn, de dire s'il est satisfaisable ou non.

Exercice 34 (6)
Une clause est *négative* si elle ne contient que des littéraux négatifs. On se propose d'étudier la stratégie suivante de résolution, appelée *stratégie négative* : l'application de la règle de résolution est restreinte au cas où l'une des prémisse est négative. On notera $\vdash_\neg$ la relation de déduction associée.

1. Soit E un ensemble de clauses tel que toute clause de E contient au moins un littéral positif. Montrer que E est satisfaisable.
2. Soit $E = \{\neg P \vee Q, P \vee Q, P \vee \neg Q, \neg P \vee \neg Q\}$. Montrer que $E \vdash_\neg \bot$ (exhiber une preuve).
3. Si I, J sont des interprétations partielles, on note $I >_{lex} J$ lorsqu'il existe un entier $k \geq 1$ tel que
   (a) pour tout $j < k$, P_j est dans le domaine de I et dans le domaine de J et $I(P_j) = J(P_j)$
   (b) P_k est dans le domaine de I et dans le domaine de J et $I(P_k) = 1$ et $J(P_k) = 0$.

On note aussi $I \leq J$ l'ordre de prolongement des interprétations partielles.

Montrer que $\geq_{lex}$ est un ordre sur les interprétations partielles et que, pour toutes interprétations partielles, $I \leq J$ ou $J \leq I$ ou $I \leq_{lex} J$ ou $J \leq_{lex} I$

4. Soit A l'arbre sémantique d'un ensemble E de clauses. On suppose que A est fini, non vide et que toutes ses feuilles sont des noeuds d'échec. Montrer qu'il existe une unique interprétation partielle maximale pour $\geq_{lex}$ qui soit un noeud d'échec et ne falsifie aucune clause négative de E.
5. Montrer la complétude réfutationnelle de $\vdash_{\neg}$ par la méthode des arbres sémantiques

2.5 Stratégies de sélection

Une *fonction de sélection* est une application qui associe à toute clause $L_1 \vee \cdots \vee L_n$ (où $n \geq 1$) l'un des littéraux L_i. Étant donnée une fonction de sélection f, on considère la restriction suivante de la résolution :

$$(R_f) \qquad \frac{P \vee C \quad \neg P \vee C'}{C \vee C'} \qquad \text{Si } f(P \vee C) = P \ ET \ f(\neg P \vee C') = \neg P$$

La règle de factorisation binaire et la règle R_f définissent une relation de déduction $\vdash_f$ pour le calcul propositionnel en forme clausale.

Exercice 35 (5)

1. Montrer que $F + R_f$ n'est pas réfutationnellement complète : donner un exemple de fonction de sélection f et d'un ensemble de clauses $\mathcal{E}$ insatisfaisable tel que $\mathcal{E} \nvdash_f \bot$.
2. Qu'en est il si on suppose que la fonction de sélection sélectionne toujours un littéral négatif quand c'est possible ?

Une clause *de Horn* est une clause contenant au plus un littéral positif.

Théorème 2.5.1 *Pour toute fonction de sélection f, R_f est réfutationellement compète pour les clauses de Horn.*

Preuve:
Si $\mathcal{E}$ est un ensemble de clauses de Horn, on note $\mathcal{E}^* = \{C \mid \mathcal{E} \vdash_f C\}$ et $I_0 = \mathcal{E}^* \cap \mathcal{P}$.

On considère d'abord le cas où $f(C) \in \mathcal{P}$ seulement si $C \in \mathcal{P}$, puis le cas général.

1. On remarque tout d'abord que, si la règle de résolution est appliquée à deux clauses de Horn (et a fortiori la résolution avec une stratégie de sélection), la clause résultante est à nouveau une clause de Horn, puisqu'un littéral positif des deux clauses prémisses a disparu. Il en résulte que $\mathcal{E}^*$ est un ensemble de clauses de Horn.

   Considérons l'interprétation I_0. Comme $\mathcal{E}$ est insatisfaisable, $I_0 \not\models \mathcal{E}$. Donc il existe une clause $C \in \mathcal{E}^*$ telle que $I_0 \not\models C$. Considérons une clause C contenant un nombre minimal de littéraux et telle que $I_0 \not\models C$. Supposons par l'absurde que C contient au moins un littéral. Dans ce cas, C contient au moins un littéral négatif (sinon $C \in I_0$). Soit $f(C) = \neg Q$. Comme $I_0 \not\models C$, $Q \in I_0$. Donc, par définition, $Q \in \mathcal{E}^*$. Alors, par r'esolution (comme $f(Q) = Q$ et $f(C) = \neg Q$), on obtient une clause $C' \in \mathcal{E}^*$ telle que $C = \neg Q \vee C'$. Mais I_0 falsifie C' puisqu'elle falsifie tous les littéraux de C. Ce qui contredit la minimalité du nombre de littéraux de C. Donc $C = \bot$ et $\bot \in \mathcal{E}^*$: la stratégie est réfutationnellement complète.
2. On considère la suite I_n définie par

$$I_{n+1} = I_n \cup \{P \in \mathcal{P} \mid \exists P \vee \neg Q_1 \vee \cdots \vee \neg Q_k \in \mathcal{E}^*, f(C) = P,\ Q_1, \ldots, Q_k \in I_n\}$$

et l'interprétation $I = \bigcup_{n\in\mathbb{N}} I_n$. À chaque $P \in I$ on associe le plus petit entier n_P tel que $P \in I_{n_P}$. À chaque clause $C = (P) \vee \neg P_1 \vee \cdots \vee \neg P_m$ falsifiée par I, on associe la suite $N(C) = (n_1(C), \ldots, n_m(C))$ des n_{P_i}, triée par ordre décroissant (m dépend de C ; dans la suite on l'écrira $m(C)$). Si bien que ou bien $m(C) = 0$ et $C \in \mathcal{P} \cup \{\bot\}$, ou bien $n_1(C)$ est le plus petit entier tel que $I_{n_1(C)}$ falsifie C.

Comme $\mathcal{E}$ est insatisfaisable, il existe une clause $C \in \mathcal{E}^*$ telle que $I \not\models C$. On choisit une telle clause minimisant $N(C)$ pour l'ordre lexicographique (la suite vide est plus petite que toutes les autres).

Montrons d'abord que c'est possible, c'est à dire qu'il n'existe pas de suite infinie strictement décroissante $N(C_1) > N(C_2) \ldots$. Pour cela on raisonne par récurrence sur la paire constitutée de $(n_1(C_1), k(C_1))$ où $k(C_1)$ est le nombre d'entiers de la séquence $N(C_1)$ qui sont égaux à $n_1(C_1)$. Si $n_1(C_1) = 0$, $N(C_1) = \underbrace{(0, \ldots, 0)}_{k(C_1)}$ et $N(C_1) > N(C_2)$ si et seulement si $k(C_1) > k(C_2)$, d'où le résultat. Sinon, pour toute suite infinie $N(C_1) = (\underbrace{n(C_1), \ldots, n(C_1)}_{k(C_1)}, L_1) > N(C_2) \ldots >$ ou bien, pour tout i, $n_1(C_i) = n_1(C_1)$ et $k(C_i) = k(C_1)$ et, dans ce cas, $N(C_i) = (\underbrace{n(C_1), \ldots, n(C_1)}_{k(C_1)}, L_i)$ et la suite $L_1, \ldots, L_i, \ldots$ est une suite strictement décroissante infinie, ce qui contredit l'hypothèse de récurrence, ou bien il existe un i tel que $(n_1(C_1), k(C_1)) > (n_1(C_i), k(C_i))$ et il suffit d'appliquer l'hypothese de récurrence à la sous-suite de premier terme C_i.

Soit donc C une clause minimale de $\mathcal{E}^*$ qui est falsifiée par I. $C \in \mathcal{P} \cup \{\bot\}$ ou bien C est falsifiée par $I_{n_1(C)}$. Montrons que ce dernier cas est impossible et donc que $C \in \mathcal{P} \cup \{\bot\}$.

Si $f(C) = P \in \mathcal{P}$, alors, par définition de $I_{n_1(C)+1}$, $P \in I_{n_1(C)+1}$, ce qui contredit le fait que I falsifie C. Donc $f(C)$ est un littéral négatif $\neg Q$ et $n_Q \leq n_1(C)$. Soit $C = (P\vee)\neg Q \vee C'$. Par définition de n_Q, ou bien $Q \in \mathcal{E}^*$ (si $n_Q = 0$) ou bien il existe une clause $C_1 \in \mathcal{E}^*$ telle que $C_1 = Q \vee \neg Q_1 \vee \ldots \vee \neg Q_k$ et $n_1(C_1) < n_Q$.

Dans le premier cas, par une étape de R_f on obtient une clause $(P\vee)C' \in \mathcal{E}^*$ falsifiée par I et telle que $N(C') < N(C)$, ce qui est absurde.

Dans le deuxième cas, en une étape de R_f, on obtient la clause $C'' = (P\vee)C'\vee\neg Q_1\vee\ldots\vee\neg Q_k \in \mathcal{E}^*$. C'' est falsifiée par I puisque C' est falsifiée par I (I falsifie C) et $Q_1, \ldots, Q_k \in I_{n_Q-1} \subseteq I$. De plus, $N(C') < N(C)$ puisque $n_{Q_1}, \ldots, n_{Q_k} < n_Q$. Ceci contredit la minimalité de C.

Il en résulte que $C \in \mathcal{P} \cup \{\bot\}$. Comme $C \in \mathcal{E}^*$, si $C \in \mathcal{P}$, alors $C \in I_0 \subseteq I$. Ce n'est pas possible puisque I falsifie C. Il en résulte que $C = \bot$ et donc $\bot \in \mathcal{E}^*$.

Exercice 36 (3)
Soit $\mathcal{E}$ un ensemble de clauses insatisfaisable quelconque (pas nécessairement des clauses de Horn). Montrer qu'il existe une fonction de sélection telle que la

résolution binaire avec stratégie de sélection + factorisation binaire permet de déduire la clause vide de $\mathcal{E}$.

Exercice 37
Soit $\mathcal{P}$ un ensemble dénombrable de variables propositionnelles. On notera $\sqsubseteq$ la relation sur les clauses définie par $C \sqsubseteq C'$ si $C \models C'$.

Soit $\geq$ un ordre total bien fondé sur les *littéraux*. On considère la restriction suivante de la règle de résolution :

$$\frac{C \vee P \quad \neg P \vee C'}{C \vee C'} \quad \text{Si } P \text{ est maximal dans } C \vee P \text{ ET } \neg P \text{ est maximal dans } \neg P \vee C'$$

Noter qu'il s'agit d'une généralisation de la résolution avec stratégie ordonnée puisqu'on peut avoir $P \geq Q \geq \neg P$ par exemple.

Si $\mathcal{E}$ est un ensemble de clauses, on note $\mathcal{E}^*$ l'ensemble des conséquences de $\mathcal{E}$ par factorisation et résolution suivant la stratégie $\mathcal{S}$ ci-dessus.

1. Montrer que $\sqsubseteq$ est une relation d'ordre bien fondée sur l'ensemble des clauses.
2. Montrer que la stratégie négative est un cas particulier de la stratégie ci-dessus (rappel : la stratégie négative consiste à ne faire de résolution que sur des clauses dont l'une des prémisses ne contient que des littéraux négatifs).
3. La stratégie *unitaire* consiste à restreindre la règle de résolution au cas où l'une des prémisses est réduite à un littéral.

   Si $\mathcal{E}$ est un ensemble de clauses, soit $\mathcal{E}_U$ l'ensemble des clauses que l'on peut déduire de $\mathcal{E}^*$ par la stratégie unitaire et $\mathcal{E}_S$ l'ensemble des clauses minimales de $\mathcal{E}_U$ pour l'ordre $\sqsubseteq$.

   Montrer que, si $\mathcal{E}^*$ ne contient pas $\bot$, alors $\mathcal{E}_S$ ne contient pas $\bot$ et $\mathcal{E}_S^* = \mathcal{E}_S$.
4. Montrer que, si $\mathcal{E}^*$ ne contient ni $\bot$ ni clause unitaire, et L est un littéral minimal de $\mathcal{E}*$, alors $(\mathcal{E}^* \cup \{\overline{L}\})^* = \mathcal{E}^* \cup \{\overline{L}\}$.
5. Montrer que la stratégie $\mathcal{S}$ est réfutationellement complète.

Exercice 38 (5)
$\mathcal{L}$ est un ensemble fini d'entiers, appelés étiquettes. Un *littéral étiqueté* est une paire d'un littéral et d'un élément de $\mathcal{L}$, noté L et e. Une *clause étiquetée* est une disjonction de littéraux étiquetés. Comme d'habitude, la disjonction vide est notée $\bot$. La sémantique d'une clause étiquetée est la même que celle de la clause à laquelle on a retiré les étiquettes. Une *fonction de sélection* s est une application qui associe à toute clause étiquetée un sous-ensemble des littéraux de c. Dans cette partie, on considère les deux règles d'inférence suivantes :

$$R \quad \frac{L \text{ et } e \vee C \quad \overline{L} \text{ et } e' \vee C'}{C \vee C'} \quad \texttt{Si} \begin{cases} L \text{ et } e \in s(L \text{ et } e \vee C) \\ \overline{L} \text{ et } e' \in s(\overline{L} \text{ et } e' \vee C') \end{cases}$$

$$F \quad \frac{L \text{ et } e \vee L \text{ et } e' \vee C}{L \text{ et } e \vee C} \quad \texttt{Si} L \text{ et } e' \in s(L \text{ et } e \vee L \text{ et } e' \vee C)$$

Soit C un ensemble de clauses. On affecte à chaque formule littéral de chaque clause de C une étiquette dans un ensemble fini (on peut affecter des étiquettes différentes à un même littéral apparaissant dans deux clauses différentes). C est ainsi considéré comme un ensemble de clauses étiquetées. Soit $\geq$ un ordre sur les littéraux étiquetés. On considère la fonction de sélection suivante : $s(c)$ est l'ensemble des littéraux L et e tels que L et e est maximal dans c. On note S_e cette stratégie (paramétrée par $\geq$ et l'étiquetage).

On suppose d'abord que $\geq$ est un ordre total bien fondé. À une clause $C = L_1 \text{ et } a_1 \vee \cdots \vee L_n \text{ et } a_n$ on associe le multi-ensemble des littéraux étiquetés $m(C) = \{L_1 \text{ et } a_1, \ldots, L_n \text{ et } a_n\}$. Les clauses sont ainsi ordonnées par l'extension multi-ensemble de $\geq$. Si $\mathcal{S}$ est un ensemble de clauses et L et a est un littéral étiqueté, on note $\mathcal{S}(L)$ l'ensemble des clauses C ne contenant aucun littéral L et b et telles que $C \in \mathcal{S}$ ou bien $C \vee \overline{L}$ et $b \in \mathcal{S}$ pour au moins un b. (Autrement dit, on remplace L par $\top$ dans les clauses de $\mathcal{S}$ et on simplifie). Si $\mathcal{E}$ est un ensemble de clauses, on note de plus $\mathcal{E}^*$ l'ensemble des clauses déductibles de $\mathcal{E}$ par la stratégie S_e. Montrer que, si $\bot \notin \mathcal{E}^*$, C est une clause minimale de $\mathcal{E}^*$ et L est un littéral maximal de C, alors $\bot \notin (\mathcal{E}^*(L))^*$. Montrer la complétude réfutationnelle de la stratégie S_e sur les clauses étiquetées.

$$\frac{}{\Gamma, \phi \vdash \phi}\,(Ax) \qquad \frac{}{\Gamma \vdash \top}$$

$$\frac{\Gamma \vdash \phi}{\Gamma, \psi \vdash \phi}\,(Aff) \qquad \frac{\Gamma, \neg\phi \vdash \bot}{\Gamma \vdash \phi}\,(Abs)$$

$$\frac{\Gamma \vdash \phi \qquad \Gamma \vdash \psi}{\Gamma \vdash \phi \wedge \psi}\,(\wedge I) \qquad \frac{\Gamma \vdash \phi \wedge \psi}{\Gamma \vdash \phi}\,(\wedge E_1) \qquad \frac{\Gamma \vdash \phi \wedge \psi}{\Gamma \vdash \psi}\,(\wedge E_2)$$

$$\frac{\Gamma \vdash \phi}{\Gamma \vdash \phi \vee \psi}\,(\vee I_1) \qquad \frac{\Gamma \vdash \psi}{\Gamma \vdash \phi \vee \psi}\,(\vee I_2) \qquad \frac{\Gamma \vdash \phi \vee \psi \quad \Gamma, \phi \vdash \theta \quad \Gamma, \psi \vdash \theta}{\Gamma \vdash \theta}\,(\vee E)$$

$$\frac{\Gamma, \phi \vdash \bot}{\Gamma \vdash \neg\phi}\,(\neg I) \qquad \frac{\Gamma \vdash \neg\phi \quad \Gamma \vdash \phi}{\Gamma \vdash \bot}\,(\neg E)$$

$$\frac{\Gamma, \phi \vdash \psi}{\Gamma \vdash \phi \to \psi}\,(\to I) \qquad \frac{\Gamma \vdash \phi \to \psi \quad \Gamma \vdash \phi}{\Gamma \vdash \psi}\,(\to E)$$

FIGURE 2.6 – Règles d'inférence de la déduction naturelle propositionnelle classique $\mathbf{NK}_0$

2.6 Déduction naturelle

2.6.1 Syntaxe

Les énoncés en déduction naturelle, appelés *jugements* sont des expressions $\Gamma \vdash \phi$ où Γ est un ensemble fini de formules de $\mathcal{F}_0(\mathcal{P})$ et ϕ est une formule de $\mathcal{F}_0(\mathcal{P})$. Il faut comprendre de tels jugements comme "De l'ensemble d'hypothèses Γ on peut déduire ϕ". Inclure les hypothèses dans le jugement permet par exemple d' énoncer de manière naturelle (et formelle) que, si l'on veut prouver $\phi \to \psi$, sous les hypothèses Γ, il suffit de montrer ψ sous les hypothèses Γ, ϕ.

2.6.2 Sémantique (classique)

Si I est une interprétation des variables propositionnelles, $I \models \Gamma \vdash \phi$ si, ou bien il existe une formule $\psi \in \Gamma$ telle que $I \not\models \psi$, ou bien $I \models \phi$.

2.6.3 Déduction naturelle classique

Les règles d'inférence de la déduction naturelle classique propositionnelle, appelée $\mathbf{NK}_0$ sont données dans la figure 2.6.

Proposition 2.6.1 *Tout jugement prouvable dans $\mathbf{NK}_0$ est valide.*

Exemple 2.6.1 On peut prouver par exemple la double négation dans $\mathbf{NK}_0$

$$\dfrac{\dfrac{\dfrac{}{\neg\neg\phi, \neg\phi \vdash \neg\neg\phi}\,(Ax) \qquad \dfrac{}{\neg\neg\phi, \neg\phi \vdash \neg\neg\phi}\,(Ax)}{\neg\neg\phi, \neg\phi \vdash \bot}\,(\neg E)}{\neg\neg\phi \vdash \phi}\,(Abs)$$

Exercice 39 (5)
Montrer comment dériver le tiers exclu $\vdash P \vee \neg P$ dans $\mathbf{NK}_0$.

Lemme 2.6.1 *Si $\Gamma, \phi \vdash \psi$ et $\Gamma \vdash \phi$ sont prouvables dans $\boldsymbol{NK}_0$, alors $\Gamma \vdash \psi$ est prouvable.*

Preuve:

$$\dfrac{\dfrac{\Gamma, \phi \vdash \psi}{\Gamma \vdash \phi \to \psi}\,(\to I) \qquad \Gamma \vdash \phi}{\Gamma \vdash \psi}\,(\to E)$$

□

Lemme 2.6.2 *$\neg(\phi \vee \psi) \vdash \neg\phi$ et $\neg(\phi \vee \psi) \vdash \neg\psi$ sont prouvables dans $\boldsymbol{NK}_0$.*

Preuve:

$$\dfrac{\dfrac{\dfrac{}{\neg(\phi_1 \vee \phi_2), \phi_2 \vdash \neg(\phi_1 \vee \phi_2)}\,(Ax) \qquad \dfrac{\dfrac{}{\neg(\phi_1 \vee \phi_2), \phi_2 \vdash \phi_2}\,(Ax)}{\neg(\phi_1 \vee \phi_2), \phi_2 \vdash \phi_1 \vee \phi_2}\,(\vee I_2)}{\neg(\phi_1 \vee \phi_2), \phi_2 \vdash \bot}\,(\neg I)}{\neg(\phi_1 \vee \phi_2) \vdash \neg\phi_2}$$

□

Lemme 2.6.3 *Si $\Gamma, \phi, \psi \vdash \theta$ est prouvable, alors $\Gamma, \phi \wedge \psi \vdash \theta$ est prouvable.*

Preuve:

$$\frac{\Gamma, \phi, \psi \vdash \theta}{\Gamma, \phi, \psi, \phi \wedge \psi \vdash \theta} Aff$$

et

$$\frac{\dfrac{}{\Gamma, \phi, \phi \wedge \psi \vdash \phi \wedge \psi} Ax}{\Gamma, \phi, \phi \wedge \psi \vdash \psi} \wedge E$$

Donc, d'après le lemme 2.6.1, $\Gamma, \phi, \phi \wedge \psi \vdash \theta$ est prouvable.

$$\frac{\dfrac{}{\Gamma, \phi \wedge \psi \vdash \phi \wedge \psi}}{\Gamma, \phi \wedge \psi \vdash \phi} \wedge E$$

Donc, d'après le lemme 2.6.1 à nouveau, $\Gamma, \phi \wedge \psi \vdash \theta$ est prouvable.

□

Théorème 2.6.1 (Complétude) *Si Γ est un ensemble fini de formules et ϕ est une formule telles que $\Gamma \models \phi$, alors $\Gamma \vdash \phi$ est prouvable dans $\boldsymbol{NK}_0$.*

Preuve:
Noter d'abord que $\Gamma \models \phi$ est équivalent à la validité de $\Gamma \vdash \phi$.

On considère la mesure suivante sur les formules : $w(\bot) = 0 = w(P) = w(\neg P)$ si P est une variable propositionnelle, $w(\neg\phi) = 1 + w(\phi)$ si ϕ n'est pas une variable propositionnelle et $w(\phi \vee \psi) = 2 + w(\phi) + w(\psi) = w(\phi \to \psi) = w(\phi \wedge \psi)$. $w(\Gamma \vdash \phi) = w(\phi) + \sum_{\psi \in \Gamma} w(\psi)$. On montre le résultat par récurrence sur $w(\Gamma \vdash \phi)$.

Cas de base $w(\Gamma \vdash \phi) = 0$ lorsque $\phi = \top$, $\phi = \bot$ ou Γ, ϕ ne contiennent que des littéraux.

On distingue 3 cas :

Cas 1 : $\phi = \top$ il suffit d'appliquer la règle correspondante du calcul.

Cas 2 : Γ **est insatisfaisable** (ce qui est le cas lorsque $\phi = \bot$).

— Si $\bot \in \Gamma$, alors $\Gamma \vdash \phi$ est prouvable pour toute formule ϕ :

$$\frac{\dfrac{}{\Gamma, \neg\phi \vdash \bot} Ax}{\Gamma \vdash \phi} Abs$$

— Sinon, Soit I_Γ l'interprétation qui contient exactelement les variables propositonnelles de Γ. I_Γ doit falsifier une formule de Γ. Comme Γ

ne contient que des littéraux, il existe une variable propositionnelle $P \in I_\Gamma$ telle que $\neg P \in \Gamma$. Dans ce cas, $\Gamma = \Gamma_1, P, \neg P$ et

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma \vdash P}\,Ax \quad \dfrac{}{\Gamma \vdash \neg P}\,Ax}{\Gamma \vdash \bot}\,\neg E}{\Gamma, \neg\phi \vdash \bot}\,Aff}{\Gamma \vdash \phi}\,Abs$$

Cas 3 : Γ est satisfaisable et $\phi \notin \{\top, \bot\}$: Si $\phi \in \mathcal{P}$, soit I_Γ l'interprétation définie par $I_\Gamma = \mathcal{P} \cap \Gamma$. I_Γ satisfait toutes les formules de Γ, puisque Γ ne contient pas une variable propositionnelle et sa négation (Γ serait insatisfaisable). $\Gamma \models \phi$ entraine alors que $I_\Gamma \models \phi$. Il en résulte $\phi \in I_\Gamma$ et donc $\phi \in \Gamma$.

Si $\phi = \neg P$ avec $P \in \mathcal{P}$, soit I l'interprétation définie par $I = \{Q \mid \neg Q \notin \Gamma\}$. Comme Γ ne contient pas une variable propositionnelle et sa négation, I satisfait toutes les formules de Γ. Par conséquent $I \models \phi$. Donc $P \notin I$ et donc $\neg P \in \Gamma$ par construction. Il en résulte que, à nouveau, $\phi \in \Gamma$.

Dans tous les cas $\Gamma \vdash \phi$ est prouvable par la règle Axiome.

Récurrence Si maintenant $w(\Gamma \vdash \phi) \geq 1$, on distingue plusieurs cas :

1. $\phi = \phi_1 \wedge \phi_2$. Dans ce cas, $\Gamma \models \phi$ entraine $\Gamma \models \phi_1$ et $\Gamma \models \phi_2$ et $w(\Gamma \vdash \phi_1), w(\Gamma \vdash \phi_2) < w(\Gamma \vdash \phi)$. Donc, par hypothèse de récurrence, $\Gamma \vdash \phi_1$ et $\Gamma \vdash \phi_2$ sont dérivables dans $\mathbf{NK}_0$ (soient π_1, π_2 leurs preuves). On conclut alors en construisant la preuve

$$\pi = \dfrac{\overset{\pi_1}{\Gamma \vdash \phi_1} \qquad \overset{\pi_2}{\Gamma \vdash \phi_2}}{\Gamma \vdash \phi_1 \wedge \pi_2}\,(\wedge I)$$

2. $\phi = \neg\phi_1$ et $\phi_1 \notin \mathcal{P}$. Dans ce cas, $\Gamma \models \phi$ entraine $\Gamma, \phi_1 \models \bot$ et $w(\Gamma \vdash \phi) = 1 + w(\gamma, \phi_1 \vdash \bot)$. Par hypothèse de récurrence, il existe une preuve π_1 de $\Gamma, \phi_1 \vdash \bot$ dans $\mathbf{NK}_0$. On construit alors comme suit une preuve de $\Gamma \vdash \phi$:

$$\dfrac{\overset{\pi_1}{\Gamma, \phi_1 \vdash \bot}}{\Gamma \vdash \neg\phi_1}\,(\neg I)$$

3. $\phi = \phi_1 \vee \phi_2$. Dans ce cas, $\Gamma \models \phi$ entraine $\Gamma, \neg\phi_1 \models \phi_2$ et $w(\Gamma, \neg\phi_1 \vdash \phi_2) = w(\Gamma \vdash \phi_1 \vee \phi_2) - 1$. Par hypothèse de récurrence, il existe donc une preuve π_0 de $\Gamma, \neg\phi_1 \vdash \phi_2$. On construit alors comme suit une preuve de $\Gamma \vdash \phi$: par le lemme 2.6.2, il existe une preuve π_2 de $\Gamma, \neg(\phi_1 \vee \phi_2) \vdash \neg\phi_2$ et une preuve π_1 de $\Gamma, \neg(\phi_1 \vee \phi_2) \vdash \neg\phi_1$.

$$\dfrac{\dfrac{\pi_2}{\Gamma, \neg(\phi_1 \vee \phi_2) \vdash \neg\phi_2} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\pi_0}{\Gamma, \neg\phi_1 \vdash \phi_2}(Aff)}{\Gamma, \neg(\phi_1 \vee \phi_2), \neg\phi_1 \vdash \phi_2}(\to I)}{\Gamma, \neg(\phi_1 \vee \phi_2) \vdash (\neg\phi_1) \to \phi_2} \qquad \dfrac{\pi_1}{\Gamma, \neg(\phi_1 \vee \phi_2) \vdash \neg\phi_1}(\to E)}{\Gamma, \neg(\phi_1 \vee \phi_2) \vdash \phi_2}(\neg E)}{\dfrac{\Gamma, \neg(\phi_1 \vee \phi_2) \vdash \bot}{\Gamma \vdash \phi_1 \vee \phi_2}(abs)}$$

4. $\phi = \phi_1 \to \phi_2$. Dans ce cas, $\Gamma \models \phi$ entraine $\Gamma, \phi_1 \models \phi_2$ et $w(\Gamma \vdash \phi_1 \to \phi_2) = 2 + w(\Gamma, \phi_1 \vdash \phi_2)$. Par hypothèse de récurrence, il existe donc une preuve π_1 de $\Gamma, \phi_1 \vdash \phi_2$. On construit alors la preuve π comme suit :

$$\dfrac{\dfrac{\pi_1}{\Gamma, \phi_1 \vdash \phi_2}}{\Gamma \vdash \phi_1 \to \phi_2}(\to I)$$

5. $\Gamma = \Gamma_1, \psi_1 \wedge \psi_2$. Dans ce cas $\Gamma \models \phi$ entraine que $\Gamma_1, \psi_1, \psi_2 \models \phi$. Or $w(\Gamma \vdash \phi) = 2 + w(\Gamma_1, \psi_1, \psi_2 \vdash \phi)$. Il existe donc, par hypothèse de récurrence, une preuve π_1 de $\Gamma_1, \psi_1, \psi_2 \vdash \phi$. D'après le lemme 2.6.3, il existe donc une preuve de $\Gamma_1, \psi_1 \wedge \psi_2 \vdash \phi$.
6. $\Gamma = \Gamma_1, \psi_1 \vee \psi_2$. Dans ce cas $\Gamma \models \phi$ entraine que $\Gamma_1, \psi_1 \models \phi$ et $\Gamma_1, \psi_2 \models \phi$. $w(\Gamma_1, \psi_1 \vee \psi_2 \vdash \phi) = 2 + w(\Gamma_1, \psi_1 \vdash \phi) = 2 + w(\Gamma_1, \psi_2 \vdash \phi)$. Par hypothèse de récurrence, il existe donc des preuves π_1, π_2 de $\Gamma_1, \psi_1 \vdash \phi$ et $\Gamma_1, \psi_2 \vdash \phi$ respectivement. On construit alors la preuve :

$$\dfrac{\dfrac{}{\Gamma_1, \psi_1 \vee \psi_2 \vdash \psi_1 \vee \psi_2}(Ax) \qquad \dfrac{\dfrac{\pi_1}{\Gamma_1, \psi_1 \vdash \phi}}{\Gamma_1, \psi_1 \vee \psi_2, \psi_1 \vdash \phi}(Aff) \qquad \dfrac{\dfrac{\pi_2}{\Gamma_1, \psi_2 \vdash \phi}}{\Gamma_1, \psi_1 \vee \psi_2, \psi_2 \vdash \phi}(Aff)}{\Gamma_1, \psi_1 \vee \psi_2 \vdash \phi}(\vee E)$$

7. $\Gamma = \Gamma_1, \neg\psi_1$ et ϕ est un littéral et $\psi_1 \notin \mathcal{P}$. Soit $\overline{\phi}$ le littéral complémentaire de ϕ ($\neg\phi$ si $\phi \in \mathcal{P}$ et P si $\phi = \neg P$ avec $P \in \mathcal{P}$).
   $\Gamma \models \phi$ entraine $\Gamma_1, \overline{\phi} \models \psi_1$. De plus $w(\Gamma_1, \overline{\phi} \vdash \psi_1) = w(\Gamma \vdash \phi) - 1$ puisque $w(\phi) = w(\overline{\phi}) = 0$. Par hypothèse de récurrence, il existe donc une preuve π_0 de $\Gamma_1, \overline{\phi} \vdash \psi_1$.

$$\dfrac{\dfrac{\dfrac{\pi_0}{\Gamma_1, \overline{\phi} \vdash \psi_1}}{\Gamma_1, \overline{\phi}, \neg\psi_1 \vdash \psi_1}\,Aff \qquad \dfrac{}{\Gamma_1, \overline{\phi}, \neg\psi_1 \vdash \neg\psi_1}\,Ax}{\dfrac{\Gamma_1, \overline{\phi}, \neg\psi_1 \vdash \bot}{\Gamma_1, \neg\psi_1 \vdash \phi}\,R}\,\neg E$$

   où R est Abs si $\phi \in \mathcal{P}$ et $\neg I$ sinon.

8. $\Gamma = \Gamma_1, \psi_1 \to \psi_2$. Dans ce cas, $\Gamma \models \phi$ entraine que $\Gamma_1, \neg\psi_1 \models \phi$ et $\Gamma_1, \psi_2 \models \phi$. Or $w(\Gamma_1, \psi_1 \to \psi_2 \vdash \phi) = 1 + w(\Gamma_1, \neg\psi_1 \vdash \phi) = 2 + w(\Gamma_1, \psi_2 \vdash \neg\phi)$. Donc, par hypothèse de récurrence, il existe des preuves π_1, π_2 de $\Gamma_1, \neg\psi_1 \vdash \phi$ et $\Gamma_1, \psi_2 \vdash \phi$ respectivement. On construit alors une preuve π_3 de $\Gamma_1, \psi_1 \to \psi_2, \neg\phi \vdash \psi_2$:

$$\dfrac{\dfrac{}{\Gamma_1, \psi_1 \to \psi_2, \neg\phi \vdash \psi_1 \to \psi_2}\,(Ax) \qquad \dfrac{\dfrac{\dfrac{\dfrac{\pi_1}{\Gamma_1, \neg\psi_1 \vdash \phi}}{\Gamma_1, \psi_1 \to \psi_2, \neg\phi, \neg\psi_1 \vdash \phi}\,(Aff) \qquad \dfrac{}{\Gamma_1, \psi_1 \to \psi_2, \neg\phi, \neg\psi_1 \vdash \neg\phi}\,(Ax)}{\Gamma_1, \psi_1 \to \psi_2, \neg\phi, \neg\psi_2 \vdash \bot}\,(\neg E)}{\Gamma_1, \psi_1 \to \psi_2, \neg\phi \vdash \psi_1}\,(abs)}{\Gamma_1, \psi_2 \to \psi_2, \neg\phi \vdash \psi_2}\,\to E$$

puis une preuve π_4 de $\Gamma_1, \psi_1 \to \psi_2, \neg\phi \vdash \neg\psi_2$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\pi_2}{\Gamma_1, \psi_2 \vdash \phi}}{\Gamma_1, \psi_2, \psi_1 \to \psi_2, \neg\phi \vdash \phi}\,(Aff) \qquad \dfrac{}{\Gamma_1, \psi_2, \psi_1 \to \psi_2, \neg\phi \vdash \neg\phi}\,(Ax)}{\Gamma_1, \psi_1 \to \psi_2, \neg\phi, \psi_2 \vdash \bot}\,(\neg E)}{\Gamma_1, \psi_1 \to \psi_2, \neg\phi \vdash \neg\psi_2}\,(\neg I)$$

Et enfin, en combinant π_3, π_4 :

$$\dfrac{\dfrac{\dfrac{\pi_4}{\Gamma_1, \psi_1 \to \psi_2, \neg\phi \vdash \neg\psi_2} \qquad \dfrac{\pi_3}{\Gamma_1, \psi_1 \to \psi_2, \neg\phi \vdash \psi_2}}{\Gamma_1, \psi_1 \to \psi_2, \neg\phi \vdash \bot}\,\neg E}{\Gamma_1, \psi_1 \to \psi_2 \vdash \phi}\,(abs)$$

□

Exercice 40 (5)

1. Montrer que, si l'on retire la règle d'affaiblissement à **NK**, le système de déduction reste complet.
2. Montrer que, si l'on retire les règles d'introduction de $\vee$ à **NK**, le système de déduction n'est plus complet.

$$\frac{\Gamma, \phi, \psi \vdash \Delta}{\Gamma, \phi \wedge \psi \vdash \Delta} \wedge \text{ left} \qquad \frac{\Gamma \vdash \Delta, \phi \quad \Gamma \vdash \Delta, \psi}{\Gamma \vdash \Delta, \phi \wedge \psi} \wedge \text{ right}$$

$$\frac{\Gamma, \phi \vdash \Delta \quad \Gamma, \psi \vdash \Delta}{\Gamma, \phi \vee \psi \vdash \Delta} \vee \text{ left} \qquad \frac{\Gamma \vdash \Delta, \phi, \psi}{\Gamma \vdash \Delta, \phi \vee \psi} \vee \text{ right}$$

$$\frac{\Gamma \vdash \Delta, \phi \quad \Gamma, \psi \vdash \Delta}{\Gamma, \phi \to \psi \vdash \Delta} \to \text{ left} \qquad \frac{\Gamma, \phi \vdash \Delta, \psi}{\Gamma \vdash \Delta, \phi \to \psi} \to \text{ right}$$

$$\frac{\Gamma \vdash \Delta, \phi}{\Gamma, \neg\phi \vdash \Delta} \neg \text{ left} \qquad \frac{\Gamma, \phi \vdash \Delta}{\Gamma \vdash \Delta, \neg\phi} \neg \text{ right}$$

$$\frac{}{\Gamma, \phi \vdash \Delta, \phi} \text{ Axiom}$$

FIGURE 2.7 – Le calcul $\mathbf{LK}_0^-$: règles d'introduction

2.7 Calcul des séquents classiques (sans coupure)

On s'intéresse au problème de la satisfaisabilité : étant donné ϕ, ϕ a-t-elle un modèle ? Ou au problème de la conséquence logique : est-ce que ψ est une conséquence logique de ϕ ?

Remarquer qu'on a un algorithme : il suffit d'énumérer les 2^n interprétations. Mais il y a plusieurs inconvénients : c'est très lourd (pas efficace) et on ne peut pas généraliser au calcul des prédicats, par exemple.

Definition 2.7.1 *Un* séquent *(propositionnel) est une paire de multi-ensembles finis de formules de $\mathcal{F}_0(\mathcal{P})$, notée $\Gamma \vdash \Delta$.*

Cette définition suppose les propriétés d'associativité et de commutativité : $\Gamma, \Gamma' = \Gamma', \Gamma$ par exemple. On identifie également $\Gamma, \top$ avec Γ d'une part et $\Delta, \bot$ avec Δ d'autre part, si Γ est la partie gauche d'un séquent et Δ sa partie droite (en particulier lorsque Γ ou Δ est vide).

Si I est une interprétation, $I \models \Gamma \vdash \Delta$ si et seulement si pour toute formule ϕ de Γ, $I \not\models \phi$ ou bien il existe une formule ϕ de Δ telle que $I \models \phi$.

Les règles de déduction du calcul des séquents propositionnel classique sans coupure (noté $\mathbf{LK}_0^-$dans la suite) sont données dans les figures 2.7 et 2.8.

Lemme 2.7.1 (correction de $\mathbf{LK}_0^-$) *Si Σ est obtenu par application d'une règle d'inférence de la figure 2.7 aux séquents $\Sigma_1, \ldots, \Sigma_n$, alors I est un modèle de Σ si et seulement si I est un modèle de tous les séquents Σ_i.*

$$\frac{\Gamma \vdash \Delta}{\Gamma, \phi \vdash \Delta}\ \text{weakening left} \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, \phi}\ \text{weakening right}$$

$$\frac{\Gamma, \phi, \phi \vdash \Delta}{\Gamma, \phi \vdash \Delta}\ \text{contraction left} \qquad \frac{\Gamma \vdash \Delta, \phi, \phi}{\Gamma \vdash \Delta, \phi}\ \text{contraction right}$$

FIGURE 2.8 – Le calcul $\mathbf{LK}_0^-$: règles structurelles

Preuve:
Par exemple pour $\rightarrow$ left. (Les autres cas sont laissés en exercice) Si $I \models \Gamma, \phi \rightarrow \psi \vdash \Delta$, alors, par définition, ou bien $I \not\models \Gamma, \phi \rightarrow \psi$, ou bien il existe une formule $\theta \in \Delta$ telle que $I \models \theta$.

Premier cas : $I \not\models \Gamma, \phi \rightarrow \psi$. Deux cas se présentent à nouveau :
- ou bien il existe une formule $\eta \in \Gamma$ telle que $I \not\models \eta$ et, dans ce cas, $I \models \Gamma \vdash \phi, \Delta$, $I \models \psi, \Gamma \vdash \Delta$,
- ou bien $I \not\models \phi \rightarrow \psi$. Par définition, ceci entraine que $I \models \phi$ et $I \not\models \psi$. Il en résulte que $I \not\models \psi, \Gamma$ et donc $I \models \psi, \Gamma \vdash \Delta$ d'une part et il existe une formule $\theta \in \phi, \Delta$ (en fait $\theta = \phi$) telle que $I \models \theta$ d'autre part. Ceci entraine $I \models \Gamma \vdash \phi, \Delta$.

Dans tous les cas, I satisfait les deux prémisses.

Deuxième cas : il existe une formule $\theta \in \Delta$ telle que $I \models \theta$. Alors, par définition des modèles des séquents, $I \models \Gamma \vdash \phi, \Delta$ et $I \models \Gamma, \psi \vdash \Delta$.

Réciproquement, si I satisfait les deux prémisses, alors
- ou bien $I \not\models \Gamma$ et $I \models \Gamma, \phi \rightarrow \psi \vdash \Delta$
- ou bien il existe $\theta \in \Delta$ telle que $I \models \theta$ et on conclut directement
- ou bien $I \not\models \psi$ et $I \models \phi$ et, dans ce cas, $I \not\models \phi \rightarrow \psi$, ce qui entraine à nouveau la conclusion voulue.

□

Exercice 41 (2)
Compléter la preuve du lemme 2.7.1.

Exercice 42 (2)
Peut on remplacer la règle d'introduction de la flèche à droite par la règle suivante :

$$\frac{\Gamma, \phi \vdash \Delta \quad \Gamma \vdash \psi, \Delta}{\Gamma \vdash \Delta, \phi \rightarrow \psi}\ \rightarrow \text{right}$$

Justifier la réponse.

Exercice 43 (2)
Peut on remplacer la règle d'introduction de la flèche à gauche par la règle suivante :

$$\frac{\Gamma, \phi \vdash \Delta, \psi}{\Gamma, \psi \to \phi \vdash \Delta} \to \text{left}$$

Un *arbre de preuve* obtenu à l'aide des règles de $\mathbf{LK}_0^-$est un arbre dont les noeuds sont étiquetés par des séquents, chaque étiquette d'un noeud étant obtenue par application d'une des règles aux étiquettes de ses fils.

Exemple 2.7.1

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A \vdash A}\text{ axiom}}{A, B \vdash A}\text{ weak-l} \quad \dfrac{\dfrac{}{B \vdash B}\text{ axiom}}{A, B \vdash B}\text{ weak-l}}{A, B \vdash A \wedge B} \wedge \text{ right}}{A \vdash B \to (A \wedge B)} \to \text{ right}}{\vdash A \to (B \to (A \wedge B))} \to \text{ right}$$

Exercice 44 (1)
Donner une preuve du tiers exclu $\vdash \phi \vee \neg\phi$.

Un séquent Σ est *prouvable* (sous-entendu à l'aide de $\mathbf{LK}_0^-$) s'il existe un arbre de preuve dont la racine est étiquetée par Σ. On dit aussi que Σ est un *théorème*.

Exercice 45 (5)
(Théorème de la déduction) Montrer, sans utiliser le théorème de complétude qui suit, que $\Gamma, \phi \vdash \Delta, \psi$ est prouvable en $\mathbf{LK}_0^-$ssi $\Gamma \vdash \Delta, \phi \to \psi$ est prouvable en $\mathbf{LK}_0^-$.

Lemme 2.7.2 *Si Γ, Δ ne contiennent que des variables, le séquent $\Gamma \vdash \Delta$ est valide si et seulement si $\Gamma \cap \Delta \neq \emptyset$.*

Preuve:
Si le séquent est valide, pour toute interprétation I, $I \models \Gamma \vdash \Delta$. Prenons l'interprétation I qui associe 1 à toutes la variables de Γ et 0 à toutes les autres variables propositionnelles. $I \models \Gamma$ et donc il existe $\theta \in \Delta$, $I \models \theta$, ce qui signifie que l'une des variables de Δ est interprétée à 1 et donc que $\Delta \cap \Gamma \neq \emptyset$.

Réciproquement, si $A \in \Delta \cap \Gamma$, pour toute interprétation I, ou bien $I(A) = 1$ et il existe une formule $\theta \in \Delta$ telle que $I \models \theta$, ou bien $I(A) = 0$ et $I \not\models \Gamma$. □

Théorème 2.7.1 (Complétude) *Un séquent $\Gamma \vdash \Delta$ est valide si et seulement s'il est prouvable à l'aide des règles de la figure 2.7.*

Preuve:
Si $\Gamma \vdash \Delta$ est prouvable, on montre par récurrence sur la longueur de la preuve que $\Gamma \vdash \Delta$ est valide : le cas de base est donné par le lemme 2.7.2 et la récurrence par le lemme 2.7.1.

Réciproquement, si $\Gamma \vdash \Delta$ est valide, on montre le résultat par récurrence sur le nombre de connecteurs logiques de Γ et Δ. Si ce nombre est nul,

- ou bien $\top \in \Delta : \Delta = \top, \Delta'$ et, dans ce cas, $\dfrac{}{\Gamma, \top \vdash \top, \Delta'}\, Ax$ et, par hypothèse, $\Gamma, \top = \Gamma$
- ou bien $\bot \in \Gamma : \Gamma = \bot, \Gamma'$ et, dans ce cas, $\dfrac{}{\bot, \Gamma' \vdash \bot, \Delta}\, Ax$ et, par hypothèse, $\Delta = \bot, \Delta$.
- bien Γ, Δ ne contiennent que des variables propositionnelles et on applique le lemme 2.7.2.

Supposons maintenant que $\Gamma = \phi \to \psi, \Gamma'$ (resp. $\phi \vee \psi, \Gamma'$, resp. $\phi \wedge \psi, \Gamma'$, resp. $\neg\phi, \Gamma'$). Par le lemme 2.7.1, $\Gamma' \vdash \phi, \Delta$ et $\Gamma', \psi \vdash \Delta$ sont valides. Par hypothèse de récurrence, ces deux séquents sont prouvables, et donc $\Gamma \vdash \Delta$ est prouvable par la règle $\to$ left. Les règles d'introduction gauche de $\wedge, \vee, \neg$ permettent de conclure de manière analogue pour les autres connecteurs logiques à gauche. Les règles droites permettent de conclure de manière analogue pour les connecteurs logiques à droite. □

Le calcul des séquents $\mathbf{LK}_0$est obtenu en ajoutant aux règles de $\mathbf{LK}_0^-$la règle de *coupure* :

$$\frac{\Gamma, \phi \vdash \Delta \quad \Gamma' \vdash \phi, \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'}\, (Cut)$$

Bien entendu, $\mathbf{LK}_0$est complet et la règle (cut) n'est pas nécéssaire pour ce résultat. On peut montrer que les coupures sont inutiles, par transformation des preuves (sans utiliser de résultat de complétude), mais cette preuve d'élimination des coupures est hors du champ de ce cours.

Exercice 46 (3)
Donner des règles d'introduction à gauche et à droite de $\leftrightarrow$, dans le style de $\mathbf{LK}_0^-$.

Exercice 47 (5)

1. Montrer que, si l'on retire la règle d'affaiblissement à **NK**, le système de déduction reste complet.
2. Montrer que, si l'on retire les règles d'introduction de $\vee$ à **NK**, le système de déduction n'est plus complet.

Exercice 48 (6)
Montrer qu'il existe une preuve de taille polynômiale (en n)du séquent

$$\vdash \neg A_1 \wedge A_2,\ \neg A_2 \wedge A_3,\ \ldots\ , \neg A_{n-1} \wedge A_n,\ \neg A_n \wedge A_1,\ A_1 \wedge \ldots \wedge A_n,\ \neg A_1 \wedge \ldots \neg A_n$$

Exercice 49 (3)
Expliquer pourquoi l'algorithme de décision de la validité résultant du théorème ci-dessus est exponentielle dans la taille du séquent.

Exercice 50 (7)
A chaque séquent valide Σ on associe la taille de sa preuve de taille minimale (la taille d'une preuve est le nombre de noeuds de l'arbre), $\tau(\Sigma)$. On note aussi $|\Sigma|$ la taille du séquent Σ (nombre de connecteurs logiques dans Σ).

Montrer qu'il existe une suite de séquents valides Σ_n telle qu'il n'existe aucun polynôme P vérifiant $P(|\Sigma_n|) \geq \tau(\Sigma_n)$.

Exercice 51 (4)
(Théorème d'interpolation) On appelle *partition* d'un séquent $\Gamma \vdash \Delta$ un quadruplet $(\Gamma_1, \Gamma_2, \Delta_1, \Delta_2)$ tel que Γ_1, Γ_2 est une partition de Γ et Δ_1, Δ_2 est une partition de Δ.

Montrer que si on peut dériver $\Gamma \vdash \Delta$, alors il existe une partition de $\Gamma \vdash \Delta$ et une formule ϕ tels que $\Gamma_1 \vdash \Delta_1, \phi$ et $\Gamma_2, \phi \vdash \Delta_2$ sont prouvables et les variables de ϕ sont dans $Var(\Gamma_1 \cup \Delta_1) \cap Var(\Gamma_1 \cup \Delta_2)$.

Exercice 52 (5)
(Calcul des séquents et déduction naturelle) Dans cet exercice, on s'interdit d'utiliser les théorèmes de complétude : on veut montrer une méthode effective de traduction d'un système de preuve dans l'autre. Soit $\mathbf{LK}_0$le calcul des séquents avec la règle de coupure.

1. Montrer que, si le jugement $\Gamma \vdash \phi$ est prouvable en $\mathbf{NK}_0$, alors le séquent $\Gamma \vdash \phi$ est prouvable dans $\mathbf{LK}_0$.
2. Montrer que $\Gamma \vdash \phi_1, \ldots, \phi_n$ (où $\phi_1, \ldots, \phi_n$ sont des formules) est prouvable en $\mathbf{LK}_0$ssi $\Gamma, \neg\phi_1, \ldots, \neg\phi_n \vdash \bot$ est prouvable en $\mathbf{LK}_0$.
3. Montrer que si $\Gamma \vdash \phi_1, \ldots, \phi_n$ est prouvable dans $\mathbf{LK}_0$, alors $\Gamma, \neg\phi_1, \ldots, \neg\phi_n \vdash \bot$ est prouvable dans $\mathbf{NK}_0$.
4. Montrer que, si $\Gamma \vdash \phi_1, \ldots, \phi_n$ est prouvable dans $\mathbf{LK}_0$, alors $\Gamma \vdash \phi_1 \vee \ldots \vee \phi_n$ est prouvable dans $\mathbf{NK}_0$.

$$\begin{array}{rcl} \phi \wedge \top & \Rightarrow & \phi \\ \phi \wedge \bot & \Rightarrow & \bot \\ \top \vee \phi & \Rightarrow & \top \\ \neg \bot & \Rightarrow & \top \\ \phi \rightarrow \bot & \Rightarrow & \neg\phi \end{array} \qquad \begin{array}{rcl} \top \wedge \phi & \Rightarrow & \phi \\ \phi \vee \bot & \Rightarrow & \phi \\ \phi \vee \top & \Rightarrow & \top \\ \bot \rightarrow \phi & \Rightarrow & \top \\ \phi \rightarrow \top & \Rightarrow & \top \end{array} \qquad \begin{array}{rcl} \bot \wedge \phi & \Rightarrow & \bot \\ \bot \vee \phi & \Rightarrow & \phi \\ \neg \top & \Rightarrow & \bot \\ \top \rightarrow \phi & \Rightarrow & \phi \end{array}$$

FIGURE 2.19 –

2.10 Diagrammes de décision binaire

Il s'agit d'une structure de données compacte utilisée pour représenter l'arbre sémantique associé à une formule, et donc en particulier toutes les interprétations qui la satisfont.

Si ϕ est une formules du calcul propositionnel, $\phi\{P \mapsto \top\}$ et $\phi\{P \mapsto \bot\}$ sont les formules obtenues en remplaçant P par $\top$ dans ϕ (resp. P par $\bot$ dans ϕ) puis en simplifiant par les règles de la figure 2.19.

Un *Graphe de décision* est un quadruplet (V, l, d, E) où V est un ensemble fini de sommets, l est une application de V dans $\mathcal{P} \cup \{\top, \bot\}$, d est une application de V dans $\mathcal{F}_0(\mathcal{P})$ et $E \subseteq V \times \{0,1\} \times V$ tel que

1. G est enraciné et connexe : $\exists r \in V, \forall v \in V, v \neq r \rightarrow \exists v_1 = r, \ldots, v_n = v \in V, \exists i_1, \ldots, i_{n-1}, (v_1, i_1, v_2), \ldots, (v_{n-1}, i_{n-1}, v_n) \in E$
2. G est acyclique (pas de cycle $(v_1, i_1, v_2), \ldots (v_n, i_n, v_1) \in E$)
3. Chaque noeud est ou bien une feuille ou bien a deux successeurs, l'un par 0 et l'autre par 1 :

$$\forall i, \forall v, v', v''.((v, i, v') \in E \wedge (v, i, v'') \in E) \rightarrow v' = v''$$

$$\forall v \in V, \{i \mid \exists v' \in V.(v, i, v') \in E\} \in \{\emptyset, \{0,1\}\}$$

Deux graphes de décision G_1, G_2 sont *isomorphes* (ce qui est noté $G_1 \sim G_2$) s'il existe une bijection f de V_1 dans V_2 telle que :

1. pour tous $v_1, v_1' \in V_1, i \in \{0,1\}$, $(v_1, i, v_1') \in E_1$ ssi $(f(v_1), i, f(v_1')) \in E_2$
2. pour tout $v_1 \in V_1$, $l(v_1) = l(f(v_1))$.

Definition 2.10.1 *Un* diagramme de décision binaire *(BDD) associé à la formule ϕ sur l'ensemble $\{P_1, \ldots, P_n\}$ de variables propositionnelles est un graphe de décision tel que $d(r) = \phi$ et tel que :*

- *Si $v \in V$ est tel que $l(v) \in \{\bot, \top\}$, alors v n'a pas de successeur et $d(v)$ est valide (si $l(v) = \top$) ou insatisfaisable (si $l(v) = \bot$).*
- *Si $l(v) \in \mathcal{P}$, alors v a exactement deux successeurs et les sous-graphes enracinés dans ces deux successeurs ne sont pas isomorphes.*
- *Si un noeud N est tel que $l(N) = P_i$ et $(N, 0, N_1), (N, 1, N_2) \in E$, alors $\phi_1 = d(N_1) \uplus d(N)\{P_i \mapsto \bot\}$ et $\phi_2 = d(N_2) \uplus d(N)\{P_i \mapsto \top\}$ et $Var(\phi_1 \vee \phi_2) \subseteq \{P_j \mid j > i\}$.*

Exemple 2.10.1 Soit ϕ la formule $(P_1 \wedge P_2) \vee \neg((P_1 \wedge P_2) \vee \neg P_3)$. Un BDD associé est donné dans la figure 2.20 (par convention les fils gauche correspondent toujours à l'interprétation 1 de la variable du noeud correspondant).

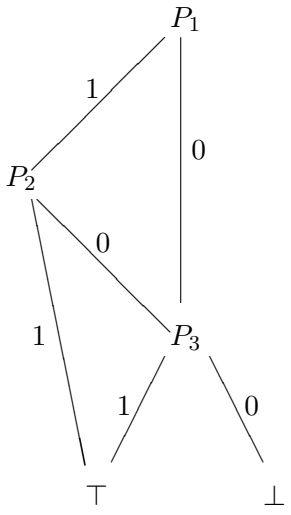

FIGURE 2.20 – Un BDD associé à ϕ

L'intérêt des BDDs est d'une part une représentation compacte et, d'autre part, une représentation unique :

Theorem 2.10.1 (Canonicité) *Soient G, G' deux diagrammes de décision binaires (l'ordre sur les variables propositionnelles est fixé) associés respectivement aux formules ϕ et ϕ'. $G \sim G'$ si et seulement si $\phi \models\!\!\models \phi'$.*

Preuve:
Si $G \sim G'$, alors $\phi \models\!\!\models \phi'$ se montre par récurrence sur la taille de G : si G est réduit à une feuille, alors, ou bien c'est $\top$ et, par définition, ϕ et ϕ' sont valides. Ou bien c'est $\bot$ et, par définition ϕ, ϕ' sont insatisfaisables. Si maintenant G n'est pas réduit à une feuille, par hypothèse de récurrence, $\phi\{P \mapsto \top\} \models\!\!\models \phi'\{P \mapsto \top\}$ et $\phi\{P \mapsto \bot\} \models\!\!\models \phi'\{P \mapsto \bot\}$ d'où $\phi \models\!\!\models \phi'$.

Pour l'implication inverse, remarquons d'abord que, si ϕ est valide (resp. insatisfaisable), alors G est réduit à une feuille. En effet, si ϕ est valide, tout chemin conduisant à une feuille conduit à $\top$ (par récurrence sur le nombre de variables propositionnelles) et, comme aucun noeud n'a deux fils identiques, G ne peut contenir de sous-graphe dont les deux successeurs sont $\top$. Il en résulte que G est réduit à une feuille. (Le raisonnement est identique dans le cas où ϕ est insatisfaisable).

Si $\phi \models\!\!\models \phi'$. On montre $G \sim G'$ par récurrence sur le nombre de variables propositionnelles. S'il n'y en a pas, c'est immédiat. Sinon, si les deux graphes sont réduits à des feuilles, ils sont isomorphes. Si l'un d'eux au moins n'est pas réduit à une feuille, disons G, alors la racine est étiquetée par P_i et les deux fils de la racine correspondent aux formules $\phi\{P_i \mapsto \top\}$ et $\phi\{P_i \mapsto \bot\}$. Comme nous l'avons vu, dans ce cas, ϕ est satisfaisable et non valide. Il en est donc de même pour ϕ'. La racine de G' a donc deux fils correspondant aux formules $\phi'\{P_j \mapsto \top\}$ et $\phi'\{P_j \mapsto \bot\}$. On peut supposer sans perdre de généralité que

$j \geq i$. Si $j > i$, alors $P_i \notin Var(\phi')$ et donc $\phi\{P_i \mapsto \top\} \leftrightarrows \phi\{P_i \mapsto \bot\}$ et, par hypothèse de récurrence, les deux fils de la racine de G sont alors isomorphes, ce qui est impossible. Donc $j = i$.

Comme $\phi \leftrightarrows \phi'$ on a aussi $\phi\{P_i \mapsto \top\} \leftrightarrows \phi'\{P_i \mapsto \top\}$ et $\phi\{P_i \mapsto \bot\} \leftrightarrows \phi'\{P_i \mapsto \bot\}$. Donc, par hypothèse de récurrence, les deux successeurs de la racine de G sont isomorphes aux deux successeurs de la racine de G' : $G \sim G'$. □

Exercice 73 (2)
Donner le BDD associé à la formule

Exercice 74
L'objet de l'exercice est la construction de BDDs associés à des formules.

Tout d'abord, si on dispose de BDDs G_1, G_2 pour les formules $\phi\{P \mapsto \top\}$ et $\phi\{P \mapsto \bot\}$ il suffit de définir $G(\phi)$ par :

— Si $G_1 = G_2$ alors G_1
— Sinon $G(\phi)$ est le graphe de racine étiquetée par P et ayant deux fils respectivement G_1 et G_2.

On note alors $G = G_1 +_P G_2$.

Donner des algorithmes de construction de BDDs associés à $\phi_1 \wedge \phi_2, \phi_1 \vee \phi_2, \phi_1 \rightarrow \phi_2, \neg\phi_1$, supposant connus des BDDs associés à ϕ_1 et ϕ_2 respectivement.

$$\begin{array}{rcl} \phi \oplus \psi & \equiv & \psi \oplus \phi \\ \phi \oplus (\psi \oplus \theta) & \equiv & (\phi \oplus \psi) \oplus \theta \\ \phi \oplus 0 & \equiv & \phi \\ \phi * (\psi \oplus \theta) & \equiv & (\phi * \psi) \oplus (\phi * \theta) \\ \phi \oplus \phi & \equiv & 0 \end{array} \qquad \begin{array}{rcl} \phi * \psi & \equiv & \psi * \phi \\ \phi * (\psi * \theta) & \equiv & (\phi * \psi) * \theta \\ \psi * 1 & \equiv & \psi \\ & & \\ \phi * \phi & \equiv & \phi \end{array}$$

FIGURE 2.21 – Equivalences structurelles

2.11 Anneaux Booléens

On considère dans cette partie une autre syntaxe du calcul propositionnel : on utilise les connecteurs $*$ (binaire), $\oplus$ (binaire), 1,0 (constantes). Les variables propositionnelles sont plutôt notées $X, Y, Z, ...$ L'ensemble des formules obtenues sur les variables propositionnelles $X_1, \ldots, X_n$ est alors noté $B(X_1, \ldots, X_n)$.

On interprète $*$ comme la conjonction, $\oplus$ comme le "ou exclusif" : $I \models \phi \oplus \psi$ si et seulement si $I \models \phi$ et $I \not\models \phi$ ou bien $I \not\models \phi$ et $I \models \phi$. 1 et 0 sont interprétés comme on s'y attend.

Les connecteurs habituels du calcul propositionnel s'expriment à l'aide de ceux-ci. Par exemple :

$$\phi \vee \psi \stackrel{\text{def}}{=} (\phi \oplus \psi) \oplus (\phi * \psi)$$

ou

$$\neg\phi \stackrel{\text{def}}{=} \phi \oplus 1$$

Les règles d'équivalence structurelle des formules sont données dans la figure 2.21. Ces règles engendrent une congruence notée $\equiv$. ($\equiv$ est la plus petite relation d'équivalence sur les formules contenant les équivalences de la figure 2.21 et telle que, si $\phi \equiv \psi$, alors $\phi \oplus \theta \equiv \psi \oplus \theta$ et $\phi * \theta \equiv \psi * \theta$ pour toute formule θ).

Lemme 2.11.1 *Si $\phi \equiv \psi$, alors $\phi \models\!\!\models \psi$.*

Preuve:
Il suffit de le vérifier pour chacune des règles : comme $\equiv$ est la plus petite congruence les satisfaisant, $\equiv \subseteq \models\!\!\models$. □

L'avantage de cette notation pour le calcul propositionnel est d'avoir (au contraire de la forme clausale) une forme canonique : on oriente les équivalences de la figure 2.21 autres que l'associativité et la commutativité de la gauche vers la droite, obtenant ainsi un ensemble de règles de simplification $\Rightarrow$. On note encore $\Rightarrow^*$ la fermeture réflexive et transitive de $\Rightarrow$. (i.e. l'itération de la simplification).

Théorème 2.11.1 *Pour toute formule ϕ de $B(X_1, \ldots, X_n)$, il existe une unique (modulo l'associativité et la commutativité) formule $\phi \Downarrow$ telle que $\phi \Rightarrow^* \phi \Downarrow$ et $\phi \Downarrow$ est irréductible par ces règles.*

Les formules irréductibles sont ou bien 0*, ou bien des sommes de monômes distincts*

$$m_1 \oplus \ldots \oplus m_p$$

où chaque m_i *est ou bien 1 ou bien un produit* $X_{i_1} * \ldots * X_{i_k}$ *où* $X_{i_1}, \ldots, X_{i_k}$ *sont des variables propositionnelles distinctes.*

Preuve:
Les règles de simplification des formules qui se terminent : il suffit d'utiliser une interprétation simple dans les entiers, par exemple $g(\phi \oplus \psi) \stackrel{\text{def}}{=} g(\phi) + g(\psi) + 1$, $g(X_i) = 2 = g(1) = g(0)$, $g(\phi * \psi) = g(\phi) * g(\psi)$; g décroit stictement par application de n'importe quelle règle.

Les formes irréductibles sont bien des sommes de monômes : il suffit de vérifier qu'une règle s'applique à toutes les autres formules.

Montrons maintenant que la forme irréductible est unique : si une formule a deux formes irréductibles ϕ et ψ, alors $\phi \equiv \psi$ et donc, par le lemme 2.11.1, $\phi \models\!\!\models \psi$. On montre que $\phi = \psi$ par récurrence sur n (nombre de variables propositionnelles) :

- Si $n = 0$, alors $\phi = \psi = 1$ ou bien $\phi = \psi = 0$
- Si $n > 0$, on écrit les deux formules sous la forme $\phi = X_n * \phi_1 \oplus \phi_2$ et $\psi = X_n * \psi_1 \oplus \psi_2$ où $\phi_1, \phi_2, \psi_1, \psi_2$ ne contiennent pas X_n. $\phi \models\!\!\models \psi$ entraîne que $\phi\{X_n \mapsto 0\} \models\!\!\models \psi\{X_n \mapsto 0\}$ et $\phi\{X_n \mapsto 1\} \models\!\!\models \psi\{X_n \mapsto 1\}$, d'où $\phi_1 \models\!\!\models \psi_1$ et $\phi_2 \models\!\!\models \psi_2$ d'où, par hypothèse de récurrence, $\phi_1 = \psi_1$ et $\phi_2 = \psi_2$, et donc $\phi = \psi$.

□

Corollaire 2.11.1 *Si* $\phi, \psi \in B(X_1, \ldots, X_n)$*, alors* $\phi \equiv \psi$ *si et seulement si* $\phi \models\!\!\models \psi$*.*

Corollaire 2.11.2 $B(X_1, \ldots, X_n)/\equiv$ *est un anneau commutatif isomorphe à* $\mathbb{Z}_2[X_1, \ldots, X_n]/\mathcal{I}$ *où* $\mathcal{I}$ *est l'idéal engendré par les polynômes* $(X_i^2 - X_i)$*.*

Chapitre 3

Calcul des prédicats

Nous abordons dans ce chapitre la *logique du premier ordre classique* aussi appelée *calcul des prédicats*.

Il y a plusieurs notations (calcul des séquents, déduction naturelle, systèmes à la Hilbert etc...) Nous suivons ici le même plan que pour le calcul propositionnel : syntaxe, sémantique, mise en forme clausale et complétude réfutationnelle de la résolution, avant de revenir si le temps le permet à d'autres systèmes de preuve. Au passage, via le théorème de Herbrand et les résultats vus en calcul propositionnel, nous obtiendrons un théorème de compacité (dans le cas d'un alphabet dénombrable) pour le calcul des prédicats.

3.1 Syntaxe

3.1.1 Les termes

$\mathcal{F}$ est un ensemble (fini) de symboles de fonction. Chaque symbole $f \in \mathcal{F}$ est muni d'une *arité* $a(f) \in \mathbb{N}$ qui fixe le nombre d'arguments.

$\mathcal{X}$ est un ensemble de symboles de variables (du premier ordre), disjoint de $\mathcal{F}$.

Un *arbre t étiqueté par* $\mathcal{F}$ est consitué d'un *ensemble de positions* $Pos(t) \subseteq \mathbb{N}_+^*$ (mots sur les entiers non nuls) et d'une application de ce domaine dans $\mathcal{F}$ tels que :

- $Pos(t)$ est stable par préfixe : si $w \cdot i \in Pos(t)$, alors $w \in Pos(t)$. En particulier le mot vide $\epsilon \in Pos(t)$.
- Si $w \in Pos(t)$, $t(w) = f$, $a(f) = n$, alors $w \cdot i \in Pos(t)$ si et seulement si $i \in \{1, ..., n\}$.

On appelle *terme* (sur l'alphabet $\mathcal{F}$ et les variables $\mathcal{X}$) un arbre étiqueté par $\mathcal{F} \cup \mathcal{X}$, les symboles de $\mathcal{X}$ ayant une arité 0, et dont l'ensemble des positions est fini. L'ensemble des termes sur $\mathcal{F}$ et $\mathcal{X}$ est noté $T(\mathcal{F}, \mathcal{X})$.

Exemple 3.1.1 Si l'on suppose que $\mathcal{F}$ est composé des symboles $+, 0, s, eq$ d'arités respectives $2, 0, 1, 2$, et $x \in \mathcal{X}$, quelques exemples d'éléments de $T(\mathcal{F}, \mathcal{X})$ sont donnés dans la figure 3.1. Les ensembles de positions de ces trois termes sont respectivement $\{\epsilon, 1, 1 \cdot 1, 2\}$, $\{\epsilon, 1, 2\}$, $\{\epsilon, 1, 1 \cdot 1, 1 \cdot 2, 1 \cdot 2 \cdot 1, 1 \cdot 2 \cdot 2, 2\}$.

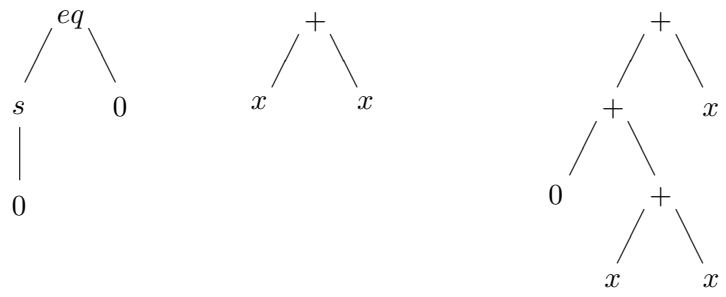

FIGURE 3.1 – Exemples d'arbres finis

L'ensemble des variables d'un terme t, noté $\mathrm{Var}(t)$ est l'intersection de $\mathcal{X}$ et des étiquettes de t.

Exemple 3.1.2 Dans les exemples de la figure 3.1, le premier terme a pour ensemble de variables $\emptyset$ et les deux autres $\{x\}$.

Les termes tels que $\mathrm{Var}(t)$ est vide sont appelés *termes clos*. L'ensemble des termes clos est noté $T(\mathcal{F})$.

On utilise habituellement une notation parenthésée pour les termes : si f est un symbole d'arité n, alors $f(t_1, \ldots, t_n)$ désigne le terme dont la racine est étiquetée par f et possède n fils, respectivement $t_1, \ldots, t_n$.

Exemple 3.1.3 Les termes de la figure 3.1 s'écrivent, en écriture parenthésée, $+(s(0), 0), +(x, x), \&(eq(x, +(x, 0)), true)$.

On utilise parfois l'écriture en notation infixée pour certains symboles usuels. Par exemple, $+(0, s(0))$ s'écrira aussi $0 + s(0)$.

Si $p \in D(t)$, le *sous-terme* de t à la position p, noté $t|_p$ est défini par récurrence sur la longueur de p : $t|_\epsilon = t$ et $f(t_1, \ldots, t_n)|_{i \cdot w} = t_i|_w$.

Exercice 75 (2)
Dans quel(s) cas est-ce que $T(\mathcal{F})$ est vide ? fini ?

Exercice 76
Montrer que $T(\mathcal{F}, \mathcal{X})$ est le plus petit ensemble S contenant $\mathcal{X}$ et tel que, pour tout $n \in \mathbb{N}$, pour tout $f \in \mathcal{F}$ tel que $a(f) = n$, pour tous $t_1, \ldots, t_n \in S$, $f(t_1, \ldots, t_n) \in S$.

3.1.2 Formules du premier ordre

$\mathcal{P}$ est de même un ensemble (fini) de symboles de prédicat, disjoint de $\mathcal{F}$ et de $\mathcal{X}$. Chaque symbole étant à nouveau muni d'une arité.

Les termes $P(t_1, \ldots, t_n)$ où $t_1, \ldots, t_n \in T(\mathcal{F}, \mathcal{X})$ et $P \in \mathcal{P}$ est d'arité n sont appelés *formules atomiques*.

Definition 3.1.1 *$CP_1(\mathcal{P}, \mathcal{F}, \mathcal{X})$, ensemble des formules du premier ordre sur les symboles de prédicats $\mathcal{P}$, les symboles de fonction $\mathcal{F}$ et les variables $\mathcal{X}$ est le plus petit ensemble tel que :*

- *$\bot, \top \in CP_1(\mathcal{P}, \mathcal{F}, \mathcal{X})$*
- *les formules atomiques sont dans $CP_1(\mathcal{P}, \mathcal{F}, \mathcal{X})$*
- *Si $\phi, \psi \in CP_1(\mathcal{P}, \mathcal{F}, \mathcal{X})$ et $x \in \mathcal{X}$ alors les formules suivantes sont dans $CP_1(\mathcal{P}, \mathcal{F}, \mathcal{X})$:*

$$\phi \wedge \psi,\ \phi \vee \psi,\ \neg\phi,\ \phi \to \psi,\ \forall x.\phi,\ \exists x.\phi$$

Remarquons qu'on retrouve le calcul propositionnel lorsque tous les symboles de $\mathcal{P}$ sont d'arité 0.

Exemple 3.1.4 $\mathcal{F} = \{0(0), s(1)\}$, $\mathcal{P} = \{\geq (2)\}$. L'expression suivante est une formule du premier ordre :

$$\begin{array}{ll} & \forall x. \geq (x, 0) \\ \wedge & \forall x. \geq (s(x), x) \\ \wedge & \forall x, y. \geq (x, y) \to \geq (s(x), s(y)) \end{array}$$

Ici, comme dans la suite, nous abrégeons $\forall x.\forall y.\phi$ en $\forall x, y.\phi$.

Exemple 3.1.5 $\mathcal{F} = \{nil(0), cons(2)\}$, $\mathcal{P} = \{A(2)\}$. La formule suivante est censée définir la concaténation des listes :

$$\begin{array}{lll} \forall x, y, z, z_1.(& & A(nil, x, x) \\ & \wedge & A(y, z, z_1) \to A(cons(x, y), z, cons(x, z_1))) \end{array}$$

Exemple 3.1.6 La formule suivante n'est pas une formule du premier ordre :

$$\forall P.(P(0) \wedge \forall x.P(x) \to P(s(x))) \to \forall x.P(x)$$

On utilisera aussi certains symboles (de fonction ou de prédicat) en notation infixée. Par exemple, on se permettra d'écrire $a + b$ au lieu de $+(a, b)$ ou bien $a = b$ au lieu de $= (a, b)$.

Exemple 3.1.7 $\mathcal{F}$ est un ensemble fini de symboles de fonction avec leur arité. $\mathcal{P} = \mathcal{P}_0 \cup \{= (2)\}$ où $\mathcal{P}_0$ est un ensemble quelconque fini de symboles de prédicat avec leur arité. L'ensemble (fini) de formules suivants est appelé *axiomes de de l'égalité* :

$$\forall x, y, z.x = y \wedge y = z \to x = z$$
$$\forall x, y.x = y \to y = x$$
$$\forall x.x = x$$
$$\forall x_1, \ldots, x_n, y_1, \ldots, y_n. \bigwedge_{i=1}^{n} x_i = y_i \to f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n)$$
Pour tout $f \in \mathcal{F}$ d'arité n
$$\forall x_1, \ldots, x_n. \bigwedge_{i=1}^{n} x_i = y_i \wedge P(x_1, \ldots, x_n) \to P(y_1, \ldots, y_n)$$
Pour tout $P \in \mathcal{P}_0$ d'arité n

Exemple 3.1.8 L'ensemble de formules suivant définit la théorie des ordres denses. On suppose les axiomes de l'égalité (donnée dans l'exemple précédent) et les deux symboles de prédicat binaires $=, \geq$ utilisés en notation infixée. On écrit en outre $a \neq b$ pour $\neg(a = b)$.

$$\forall x, y, z.x \geq y \wedge y \geq z \rightarrow x \geq z$$
$$\forall x, y.x \geq y \wedge y \geq x \rightarrow x = y$$
$$\forall x.x \geq x$$
$$\forall x.y.(x \geq y \vee y \geq x)$$
$$\forall x, y.(x \neq y \wedge x \geq y) \rightarrow (\exists z.x \geq z \wedge x \neq z \wedge z \geq y \wedge z \neq y)$$

Exemple 3.1.9 $\mathcal{F} = \{*(2)\}$. $\mathcal{P} = \{= (2)\}$. On suppose les axiomes de l'égalité. Les axiomes des groupes sont alors obtenus en ajoutant les formules :

$$\forall x, y, z.x * (y * z) = (x * y) * z$$
$$\exists e.\forall x.x * e = x \wedge e * x = x$$
$$\forall x.\exists y.\forall z.(x * y) * z = z \wedge x * y = y * x \wedge z * (x * y) = z$$

Les quantificateurs *lient* les variables. On définit ainsi les variables liées ($\mathsf{VB}(\phi)$) et les variables libres ($\mathsf{VL}(\phi)$) d'une formule ϕ (resp. d'un terme t), par récurrence sur le terme t, puis la formule :

$$\begin{array}{rcll}
\mathsf{VL}(x) & = & \{x\} & \text{Si } x \in \mathcal{X} \\
\mathsf{VB}(x) & = & \emptyset & \\
\mathsf{VL}(f(t_1, \ldots, t_n)) & = & \mathsf{VL}(t_1) \cup \ldots \cup \mathsf{VL}(t_n) & \text{Pour tout } f \in \mathcal{F} \text{ d'arité } n \\
\mathsf{VB}(f(t_1, \ldots, t_n)) & = & \emptyset & \text{Pour tout } f \in \mathcal{F} \text{ d'arité } n \\
\mathsf{VL}(P(t_1, \ldots, t_n)) & = & \mathsf{VL}(t_1) \cup \ldots \cup \mathsf{VL}(t_n) & \text{Pour tout } P \in \mathcal{P} \text{ d'arité } n \\
\mathsf{VB}(P(t_1, \ldots, t_n)) & = & \emptyset & \text{Pour tout } P \in \mathcal{P} \text{ d'arité } n \\
\mathsf{VL}(\bot) = \mathsf{VL}(\top) & = & \emptyset & \\
\mathsf{VB}(\bot) = \mathsf{VL}(\bot) & = & \emptyset & \\
\mathsf{VL}(\phi \wedge \psi) = \mathsf{VL}(\phi \vee \psi) & = & \mathsf{VL}(\phi) \cup \mathsf{VL}(\psi) & \\
\mathsf{VL}(\phi \rightarrow \psi) & = & \mathsf{VL}(\phi) \cup \mathsf{VL}(\psi) & \\
\mathsf{VB}(\phi \wedge \psi) = \mathsf{VB}(\phi \vee \psi) & = & \mathsf{VB}(\phi) \cup \mathsf{VB}(\psi) & \\
\mathsf{VB}(\phi \rightarrow \psi) & = & \mathsf{VB}(\phi) \cup \mathsf{VB}(\psi) & \\
\mathsf{VL}(\neg\phi) & = & \mathsf{VL}(\phi) & \\
\mathsf{VB}(\neg\phi) & = & \mathsf{VB}(\phi) & \\
\mathsf{VL}(\exists x.\phi) = \mathsf{VL}(\forall x.\phi) & = & \mathsf{VL}(\phi) \setminus \{x\} & \\
\mathsf{VB}(\exists x.\phi) = \mathsf{VB}(\forall x.\phi) & = & \mathsf{VB}(\phi) \cup \{x\} &
\end{array}$$

Exemple 3.1.10 Si ϕ est la formule

$$P(x) \wedge \exists x.Q(f(x)) \wedge \exists x, z.Q(g(x, y, z))$$

Alors $\mathsf{VL}(\phi) = \{x, y\}$ et $\mathsf{VB}(\phi) = \{x, z\}$.

L'exemple ci-dessus montre que l'ensemble des variables liées et l'ensemble des variables libres d'une formule ne sont pas nécessairement des ensembles disjoints. De plus, une variable peut avoir deux *occurrences de liaison*. Par exemple, ci dessus, x a deux occurrences de liaison ; chacune d'elles correspond à une quantification sur x.

3.2 Sémantique

3.2.1 $\mathcal{F}$-algèbres

Etant donné un ensemble de symboles de fonction avec leur arité une *$\mathcal{F}$-algèbre* $\mathcal{A}$ est constituée d'un domaine (ensemble) $D_{\mathcal{A}}$ non vide et, pour chaque symbole de fonction $f \in \mathcal{F}$ d'arité n, d'une fonction $f_{\mathcal{A}}$ de $D_{\mathcal{A}}^n$ dans $D_{\mathcal{A}}$.

$T(\mathcal{F})$ et $T(\mathcal{F}, \mathcal{X})$ sont des $\mathcal{F}$-algèbres, avec $f_{T(\mathcal{F})} = f = f_{T(\mathcal{F},\mathcal{X})}$.

Exemple 3.2.1 Soit $\mathcal{F} = \{0(0), s(1), +(2)\}$. Alors $(\mathbb{N}, succ_{\mathbb{N}}, +_{\mathbb{N}})$ est une $\mathcal{F}$-algèbre et $(\mathbb{Q}_+, 1, \div 2, \div)$ est aussi une $\mathcal{F}$-algèbre. ($\mathbb{Q}_+$ est l' ensemble des rationnels strictement positifs).

Si $\mathcal{A}$ et $\mathcal{B}$ sont deux $\mathcal{F}$-algèbres, un *homomorphisme* h de $\mathcal{A}$ dans $\mathcal{B}$ est une application de $D_{\mathcal{A}}$ dans $D_{\mathcal{B}}$ telle que, pour tout symbole $f \in \mathcal{F}$, pour tous éléments $a_1, \ldots, a_n \in D_{\mathcal{A}}$,

$$h(f_{\mathcal{A}}(a_1, \ldots, a_n)) = f_{\mathcal{B}}(h(a_1), \ldots, h(a_n))$$

Exemple 3.2.2 Soit $\mathcal{F} = \{0(0), s(1), +(2)\}$. On considère la $\mathcal{F}$-algèbre $\mathbb{N}$ et la $\mathcal{F}$-algèbre $\mathbb{Z}_2$. L'application qui a tout entier associe son reste modulo 2 est un homomorphisme de $\mathcal{F}$-algèbres.

Exercice 77 (2)
Montrer que le logarithme népérien est un homomorphisme de F-algèbre de $]0, +\infty[$ dans $\mathbb{R}$, où $F = \{0(0);\ h(1);\ f(2)\}$. On précisera les structures de F-algèbres de $]0, +\infty[$ et de $\mathbb{R}$.

Exercice 78 (3)
Reprenant l'exemple 3.2.1, existe-t-il un homomorphisme entre ces deux algèbres ?

Exercice 79 (4)
Soit $F = \{0(0);\ f(2)\}$. Donner une opération $f_{\mathbb{Z}}$ sur $\mathbb{Z}$ telle que l'application qui à tout entier associe son opposé soit un morphisme de $(\mathbb{Z}, 0, *)$ dans $(\mathbb{Z}, 0, f_{\mathbb{Z}})$ (considérés comme F-algèbres).

Exercice 80 (5)
On suppose que $\mathcal{F} = \{s(1)\}$

1. Donner un exemple de deux $\mathcal{F}$-algèbres finies ayant même domaine telles qu'il n'existe aucun morphisme de l'une dans l'autre.
2. Donner un exemple de deux $\mathcal{F}$-algèbres finies distinctes, de même domaine et isomorphes.
3. Lorsque D a 1,2,3 éléments, combien y a-t-il de $\mathcal{F}$-algèbres de domaine D, à isomorphisme près ?

Théorème 3.2.1 (propriété universelle de $T(\mathcal{F}, \mathcal{X})$)
Soit $\mathcal{A}$ une F-algèbre. Soit i l'injection (canonique) de X dans $T(\mathcal{F}, \mathcal{X})$. Pour toute application f de X dans $\mathcal{A}$, il existe un unique homomorphisme $\widehat{f}$ de $T(\mathcal{F}, \mathcal{X})$ dans $\mathcal{A}$ tel que

$$\forall x \in X,\ \ \widehat{f} \circ i(x) = f(x)$$

La construction de $\widehat{f}$ est effectuée par récurrence structurelle sur les termes (ou, si l'on préfère, par récurrence sur la profondeur des termes).

Si $\mathcal{A}$ est une F-algèbre, on appelle $\mathcal{A}$-*affectation* toute application σ de X dans $\mathcal{A}$. D'après le théorème 3.2.1, on confond σ et le morphisme $\widehat{\sigma}$ de $T(\mathcal{F}, \mathcal{X})$ dans $\mathcal{A}$ correspondant. On note $t\sigma$ l'application d'une affectation σ à t.

Les endomorphismes de $T(\mathcal{F}, \mathcal{X})$ sont appelés *substitutions*. On note Σ l'ensemble des substitutions. Les homomorphismes de $T(\mathcal{F}, \mathcal{X})$ dans $T(F)$ sont appelés *substitutions closes*. L'ensemble des substitutions closes est noté Σ_g.

Si σ est une substitution, on appelle *domaine* de σ l'ensemble $\{x \in X \mid x\sigma \neq x\}$ noté $Dom(\sigma)$.

Lorsque σ est de domaine fini, on note aussi $VIm(\sigma)$ le sous-ensemble de X :

$$VIm(\sigma) = \bigcup_{x \in Dom(\sigma)} Var(x\sigma)$$

Une substitution σ est dite *idempotente* si $\sigma \circ \sigma = \sigma$.

On note $\{x_1 \to t_1; \ldots, ; x_n \to t_n\}$ la substitution de domaine $Dom(\sigma) = \{x_1, \ldots, x_n\}$ et telle que $\forall i, x_i\sigma = t_i$. Bien sûr, on suppose ici que $x_1, \ldots, x_n$ sont des variables distinctes et que, pour tout i, x_i est de même sorte que t_i.

Cette notation est aussi employée pour les $\mathcal{A}$-affectations dont les seules valeurs significatives sont celles qui sont prises sur $\{x_1, \ldots, x_n\}$.

Un *renommage* est une substitution σ qui associe à toute variable une variable et qui est une bijection de $Dom(\sigma)$ sur $VIm(\sigma)$. On supposera toujours implicitement que le domaine d'un renommage contient les variables des termes auxquels il est appliqué.

Exercice 81
Existe-t-il des renommages idempotents autres que l'identité ?

Si t est un terme tel que $\mathsf{VL}(t) \subseteq \{x_1, \ldots, x_n\}$ et si σ est l'affectation $\{x_1 \mapsto a_1, \ldots, x_n \mapsto a_n\}$ dans la $\mathcal{F}$-algèbre $\mathcal{A}$, on notera

$$[\![t]\!]_{\sigma,\mathcal{A}} \stackrel{\text{def}}{=} \hat{\sigma}(t)$$

Exemple 3.2.3

$$[\![x + x]\!]_{x \mapsto 1, \mathbb{N}} = 2$$

3.2.2 $\mathcal{F}, \mathcal{P}$-structures

Definition 3.2.1 *Une* $\mathcal{F}, \mathcal{P}$-structure $\mathcal{S}$ *est une* $\mathcal{F}$*-algèbre* $\mathcal{A} = (D_\mathcal{A}, \{f_\mathcal{A} \mid f \in \mathcal{F}\})$ *et, pour chaque symbole de prédicat* P*, d'arité* n*, une relation* $P_\mathcal{A} \subseteq D_\mathcal{A}^n$.

On confondra parfois (abusivement), une structure et la $\mathcal{F}$-algèbre sous-jacente.

3.2.3 Modèles des formules

Soit ϕ une formule, $\mathsf{VL}(\phi) = \{x_1, \ldots, x_n\}$, $\mathcal{S}$ une $\mathcal{F}, \mathcal{P}$-structure (d'algèbre sous-jacente $\mathcal{A}$) et σ une $\mathcal{A}$-affectation dont le domaine contient $\{x_1, \ldots, x_n\}$. On définit la relation de satisfaction $\sigma, \mathcal{S} \models \phi$ par récurrence sur ϕ :

- $\sigma, \mathcal{S} \models P(t_1, \ldots, t_n)$ si et seulement si $([\![t_1]\!]_{\sigma,\mathcal{A}}, \ldots, [\![t_n]\!]_{\sigma,\mathcal{A}}) \in P_{\mathcal{S}}$
- $\sigma, \mathcal{S} \models \phi * \psi$ où $*$ est l'un des connecteurs logiques binaires est défini, comme en calcul propositionnel, à partir des modèles de ϕ et des modèles de ψ. Par exemple, $\sigma, \mathcal{S} \models \phi \vee \psi$ si et seulement si ($\sigma, \mathcal{S} \models \phi$ ou $\sigma, \mathcal{S} \models \psi$)
- $\sigma, \mathcal{S} \models \neg\phi$ si et seulement si $\sigma, \mathcal{S} \not\models \phi$
- $\sigma, \mathcal{S} \models \exists x.\phi$ si et seulement si il existe $a \in D_{\mathcal{A}}$ tel que $\sigma \uplus \{x \mapsto a\}, \mathcal{S} \models \phi$.
- $\sigma, \mathcal{S} \models \forall x.\phi$ si et seulement si pour tout $a \in D_{\mathcal{A}}$ tel que $\sigma \uplus \{x \mapsto a\}, \mathcal{S} \models \phi$.

Ici $\sigma \uplus \{x \mapsto a\}$ désigne l'affectation σ' dont le domaine est $Dom(\sigma') = Dom(\sigma) \cup \{x\}$, qui coïncide avec σ, sur $Dom(\sigma) \setminus \{x\}$ et telle que $\sigma'(x) = a$.

Si ϕ ne contient pas de variable libre, une structure $\mathcal{S}$ est un *modèle* de ϕ si $\mathcal{S} \models \phi$.

Voyons quelques exemples sous forme d'exercice :

Exercice 82 (4)
On reprend l'exemple 3.1.4 : l'algèbre des entiers naturels (avec l'ordre habituel sur les entiers) satisfait la formule

$$\begin{array}{ll} & \forall x. \geq (x, 0) \\ \wedge & \forall x. \geq (x, x) \\ \wedge & \forall x, y. \geq (x, y) \rightarrow \geq (s(x), s(y)) \end{array}$$

Donner une autre interprétation de $\geq$ (mais toujours sur les entiers naturels avec l'interprétation usuelle de s (sucesseur) et 0).

Quels sont tous les modèles de cette formule, si l'on fixe seulement l'algèbre des entiers naturels comme $\mathcal{F}$-algèbre sous-jacente à la structure ?

Exercice 83
Même que dans l'exercice précédent, mais en remplaçant la formule de l'exemple 3.1.4 par la formule de l'exemple 3.1.5 et l'algèbre par l'algèbre des listes dans laquelle *nil* est interprété par la liste vide et *cons* par l'ajout d'un élément à une liste.

On étend les notions de conséquence logique, d'équivalence logique définies dans le paragraphe 2.2 sur les formules et ensembles de formules du calcul propositionnel au calcul des prédicats.

Exercice 84 (2)
Montrer que les formules $\exists x.\forall y.P(x, y)$ et $\forall y.\exists x.P(x, y)$ ne sont pas logiquement équivalentes. L'une d'elles est une conséquence logique de l'autre. Laquelle ?

Exercice 85 (2)
Mêmes questions que dans l'exercice précédent, mais avec les formules $\forall x.(P(x) \vee Q(x))$ et $(\forall x.P(x)) \vee (\forall x.Q(x))$.

Si σ est la substitution $\{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\}$, on note $\phi\sigma$ la formule ϕ dans laquelle toutes les occurrences libres de $x_1, \ldots, x_n$ ont été remplacées respectivement par $t_1, \ldots, t_n$. Plus formellement, par récurrence sur la structure de la formule, cette substitution a été définie au paragraphe 3.2.1 pour les formules atomiques, $(\phi * \psi)\{x \mapsto t\} \stackrel{\text{def}}{=} (\phi\{x \mapsto t\}) * (\psi\{x \mapsto t\})$ pour tous les connecteurs logiques $*$ et enfin :

— $(\exists y.\phi)\sigma \stackrel{\text{def}}{=} \exists y.(\phi\sigma)$ si $y \notin Dom(\sigma)$ et $y \notin VIm(\sigma)$
— $(\forall y.\phi)\sigma \stackrel{\text{def}}{=} \forall y.(\phi\sigma)$ si $y \notin Dom(\sigma)$ et $y \notin VIm(\sigma)$
— $(\exists x.\phi)\sigma \stackrel{\text{def}}{=} \exists x.\phi$ si $x \in Dom(\sigma)$
— $(\exists x.\phi)\sigma \stackrel{\text{def}}{=} \exists y.(\phi\{x \mapsto y\})\sigma$ si $y \notin \mathsf{VL}(\phi)$, $x \in Vim(\sigma)$ et $x \notin Dom(\sigma)$.

Proposition 3.2.1 *Si $y \notin \mathsf{VL}(\phi)$, alors $\exists x.\phi \models\!\dashv \exists y.\phi\{x \mapsto y\}$.*

Grâce à cette proposition, on pourra supposer désormais, sans perdre de généralité, que les variables n'ont qu'une occurrence liée dans chaque formule et que les variables liées sont disjointes des variables libres.

Deux stuctures sont *élémentairement équivalentes* si elles satisfont les mêmes formules du premier ordre.

Exercice 86 (7)

1. Donner deux structures élémentairement équivalentes et non isomorphes.
2. Même question, en supposant de plus que $\mathcal{P}$ contient un prédicat interprété comme l'égalité.
3. Montrer que si $\mathcal{F}$ est vide, $\mathcal{P} = \{=\}$, alors deux structures de domaine dénombrable qui sont élémentairement équivalentes et satisfont les axiomes de l'égalité sont isomorphes.
4. On suppose que $\mathcal{F} \subseteq \{0(0), s(1)\}$ et $\mathcal{P} \subseteq \{=\}$. Donner deux structures élémentairement équivalentes, non isomorphes, dénombrables et dans lesquelles $=$ est interprété comme l'égalité.

Exercice 87 (6)

Supposant que $\mathcal{P}$ ne contient que des symboles de prédicat unaires, et $\mathcal{F}$ ne contient que des symboles de fonction unaires, montrer que si une formule ϕ est satisfaisable, alors elle a un modèle fini. (On pourra se limiter au cas où $\mathcal{F}$ est vide).

Exercice 88 (5)

Donner un exemple de $\mathcal{F}, \mathcal{P}$ et d' une formule ϕ qui est satisfaisable mais n'a pas de modèle dont le domaine est fini.

Exercice 89 (5)

Soit $\mathcal{F} = \{0(0), s(1), +(2), \times(2)\}$ et $\mathcal{P} = \{=\}$. On considère l'ensemble A_{el}de formules formé des axiomes de l'égalité et des 7 formules de l'arithmétique

élémentaire :

$$\begin{array}{ll}
\forall x. & 0 + x = x \\
\forall x, y. & s(x) + y = s(x + y) \\
\forall x. & 0 \times x = 0 \\
\forall x, y. & s(x) \times y = (x \times y) + y \\
\forall x. \exists y. & x = 0 \vee x = s(y) \\
\forall x. & s(x) \neq 0 \\
\forall x, y. & s(x) = s(y) \rightarrow x = y
\end{array}$$

Donner un modèle $\mathcal{S}$ de A_{el} tel que $\mathcal{S} \not\models \forall x. x + 0 = x$.

Exercice 90 (5)
Soit $\mathcal{P} = \{\geq\}$, $\mathcal{F} = \emptyset$. On considère les $\mathcal{F}, \mathcal{P}$-structures $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, $\geq$ étant interprété comme l'ordre habituel sur ces ensembles. Par abus de notation, les structures $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ seront ci-dessous confondues avec les ensembles (resp. algèbres) sous-jacents.

1. Montrer que $\mathbb{Z}$ et $\mathbb{Q}$ ne sont pas élémentairement équivalents.
2. On veut montrer que $\mathbb{Q}$ et $\mathbb{R}$ sont élémentairement équivalents. Soit $\mathcal{S} \in \{\mathbb{R}, \mathbb{Q}\}$. Si σ est une application d'un ensemble fini de variables D dans $\mathcal{S}$, on note $\geq_\sigma$ la relation d'ordre sur D définie par $x \geq_\sigma y$ ssi $x\sigma \geq_{\mathcal{S}} y\sigma$.
   (a) Montrer que, $\mathcal{S}, \sigma \models \phi$ si et seulement si, pour toute affectation θ des variables libres de ϕ telle que $\geq_\theta$ est identique à $\geq_\sigma$, $\mathcal{S}, \theta \models \phi$.
   (b) En déduire le résultat souhaité.

Chapitre 11

Théorèmes de Complétude

Nous avons déjà vu la complétude réfutationnelle de la résolution dans la partie 3.7. Ce chapitre reprend essentiellement les mêmes idées pour montrer la complétude d'autres systèmes de preuve. La différence essentielle est ne plus s'appuyer sur la mise en forme clausale. On ne peut donc plus utiliser le théorème de Herbrand ; la construction d'un modèle à partir d'un ensemble de formules cohérent requiert l'introduction de nouveaux symboles de fonction (de constantes, en fait).

11.1 Déduction naturelle

Les règles de déduction naturelle s'obtiennent à partir de celles du calcul propositionnel, en ajoutant les règles d'introduction/élimination des quantificateurs. Elles sont données dans la figure 11.1.

Lemme 11.1.1 $\vdash_{\boldsymbol{NK}} \forall x.\phi(x) \leftrightarrow \neg\exists x.\neg\phi(x)$

Preuve:
On prouve $\forall x.\phi(x) \vdash_{\mathbf{NK}} \neg\exists x\neg\phi(x)$ et $\neg\exists x\neg\phi(x) \vdash_{\mathbf{NK}} \forall x.\phi(x)$, puis on utilise la complétude de la déduction naturelle propositionnelle.

$$\dfrac{\dfrac{\dfrac{}{\forall x.\phi(x), \exists x.\neg\phi(x) \vdash \exists x.\neg\phi(x)} \quad \dfrac{\dfrac{\forall x.\phi(x), \neg\phi(x) \vdash \neg\phi(x) \quad \dfrac{\forall x\phi(x), \neg\phi(x) \vdash \forall x\phi(x)}{\forall x\phi(x), \neg\phi(x) \vdash \phi(x)}\,\forall_e}{\forall x.\phi(x), \neg\phi(x) \vdash \bot}\,\neg_e}{\forall x.\phi(x), \exists x.\neg\phi(x) \vdash \bot}\,\exists_e}{\forall x.\phi(x) \vdash \neg\exists x\neg\phi(x)}\,\neg_i$$

Exemple 11.1.1 On considère la formule du buveur : $\vdash \exists x.\forall y.(P(x) \to P(y))$. La figure 11.2 donne une preuve de cet énoncé dans **NK**.

Lemme 11.1.2 *Si c est un symbole de constante qui n'apparait ni dans Γ ni dans ϕ et $x \notin Var(\Gamma)$, $\Gamma \vdash \phi[x := c]$ est prouvable dans **NK** si et seulement si $\Gamma \vdash \forall x.\phi$ est prouvable dans **NK**.*

$$\frac{}{\Gamma, \phi \vdash \phi}\,(Ax) \qquad \frac{}{\Gamma \vdash \top}$$

$$\frac{\Gamma \vdash \phi}{\Gamma, \psi \vdash \phi}\,(Aff) \qquad \frac{\Gamma, \neg\phi \vdash \bot}{\Gamma \vdash \phi}\,(Abs)$$

$$\frac{\Gamma \vdash \phi \qquad \Gamma \vdash \psi}{\Gamma \vdash \phi \wedge \psi}\,(\wedge I) \qquad \frac{\Gamma \vdash \phi \wedge \psi}{\Gamma \vdash \phi}\,(\wedge E_1) \qquad \frac{\Gamma \vdash \phi \wedge \psi}{\Gamma \vdash \psi}\,(\wedge E_2)$$

$$\frac{\Gamma \vdash \phi}{\Gamma \vdash \phi \vee \psi}\,(\vee I_1) \qquad \frac{\Gamma \vdash \psi}{\Gamma \vdash \phi \vee \psi}\,(\vee I_2) \qquad \frac{\Gamma \vdash \phi \vee \psi \quad \Gamma, \phi \vdash \theta \quad \Gamma, \psi \vdash \theta}{\Gamma \vdash \theta}\,(\vee E)$$

$$\frac{\Gamma, \phi \vdash \bot}{\Gamma \vdash \neg\phi}\,(\neg I) \qquad \frac{\Gamma \vdash \neg\phi \quad \Gamma \vdash \phi}{\Gamma \vdash \bot}\,(\neg E)$$

$$\frac{\Gamma, \phi \vdash \psi}{\Gamma \vdash \phi \to \psi}\,(\to I) \qquad \frac{\Gamma \vdash \phi \to \psi \quad \Gamma \vdash \phi}{\Gamma \vdash \psi}\,(\to E)$$

$$\frac{\Gamma \vdash \phi \quad x \notin \mathrm{Var}(\Gamma)}{\Gamma \vdash \forall x.\phi}\,\forall_i \qquad \frac{\Gamma \vdash \forall x.\phi}{\Gamma \vdash \phi[x := t]}\,\forall_e$$

$$\frac{\Gamma \vdash \phi[x := t]}{\Gamma \vdash \exists x.\phi}\,\exists_i \qquad \frac{\Gamma \vdash \exists x.\phi \quad \Gamma, \phi \vdash \psi \quad x \notin \mathrm{Var}(\Gamma) \cup \mathrm{Var}(\psi)}{\Gamma \vdash \psi}\,\exists_e$$

FIGURE 11.1 – Règles d'inférence de la déduction naturelle classique **NK**

$$\dfrac{\dfrac{\dfrac{}{\neg\exists z\neg P(z) \vdash \forall z.P(x)}}{\vdash \forall z.P(z) \vee \exists z\neg P(z)} \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{\forall z.P(z), P(x) \vdash \forall z.P(z)}\,Ax}{\forall z.P(z), P(x) \vdash P(y)}\,\forall_e}{\forall z.P(z) \vdash P(x) \to P(y)}\,\to_i}{\forall z.P(z) \vdash \forall y(P(x) \to P(y))}\,\forall_i}{\forall z.P(z) \vdash \exists x\forall y(P(x) \to P(y))}\,\exists_i \qquad \dfrac{\dfrac{}{\exists z.\neg P(z) \vdash \exists z.\neg P(z)}\,Ax}{\exists z.\neg P(z) \vdash \exists x\forall y(P($$

$$\vdash \exists x\forall y.(P(x) \to P(y))$$

FIGURE 11.2 – Preuve de la formule du buveur dans **NK**

Preuve:
On montre, par récurrence sur la preuve, que, si $\Gamma \vdash \phi\{x \mapsto c\}$ est prouvable, alors $\Gamma \vdash \phi$ est prouvable. On conclut enfin à l'aide de $\forall_i$.

Exercice 238
Parmi les jugements suivants, dire lesquels sont valides ; donner une preuve dans **NK** de ceux qui le sont et donner un contre-modèle de ceux qui ne le sont pas.

1. $\vdash \exists x.\forall y.(P(y) \to P(x))$
2. $\vdash \exists x.(P(x) \to P(s(x)))$
3. $\vdash \forall x \exists y.(P(x) \to P(s(y)))$

L'objectif de cette partie est de montrer le théorème suivant :

Théorème 11.1.1 (Complétude) *Si S est un ensemble de fomules et ϕ une formule telle que $S \models \phi$, alors il existe un sous-ensemble fini Γ de S tel que $\Gamma \vdash \phi$ est dérivable dans NK.*

Si $\mathcal{S}$ est un ensemble de formules, on note $\mathcal{S} \vdash_{\mathbf{NK}} \phi$ s'il existe un sous-ensemble fini Γ de $\mathcal{S}$ tel que $\Gamma \vdash \phi$ est prouvable dans **NK**. Un ensemble $\mathcal{S}$ de formules est *cohérent* si $\mathcal{S} \nvdash_{\mathbf{NK}} \bot$.

Le théorème de complétude est une conséquence de :

Théorème 11.1.2 (Compétude réfutationnelle) *Si $\mathcal{S}$ est cohérent, alors $\mathcal{S}$ est satisfaisable.*

On suppose que les alphabets de symboles de prédicat et de fonction sont dénombrables. On définit $\mathcal{S}_n$ et $\mathcal{F}_n$ par récurrence sur n :

— $\mathcal{S}_0 = \mathcal{S}$ et $\mathcal{F}_0 = \mathcal{F}$
— Soit $\mathcal{E}_n$ l'ensemble des formules du premier ordre sur l'alphabet $\mathcal{F}_n$ et ayant pour seule variable libre x. $\mathcal{F}_{n+1} = \{c_\phi \ : \ \phi \in \mathcal{E}_n\}$ et $\mathcal{S}_{n+1} = \{\exists x.\phi(x) \to \phi(c_\phi) \ : \ \phi \in \mathcal{E}_n\}$.

Soit $\mathcal{S}^* = \bigcup_{n\in\mathbb{N}} \mathcal{S}_n$ et $\mathcal{F}^* = \bigcup_{n\in\mathbb{N}} \mathcal{F}_n$.

Lemme 11.1.3 *Soit $\mathcal{M}$ un modèle de domaine $T(\mathcal{F})$ et ϕ une formule construite sur $\mathcal{F}$, de variables libres $x_1, \ldots, x_n$. $\mathcal{M}, \{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\} \models \phi$ si et seulement si $\mathcal{M} \models \phi\{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\}$.*

Preuve:
On note $\sigma = \{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\}$. On raisonne par récurrence sur la formule ϕ : s'il s'agit d'une formule atomique, $\mathcal{M}, \sigma \models P(u_1, \ldots, u_m)$ si et seulement si $([\![u_1]\!]_\sigma, \ldots, [\![u_n]\!]_\sigma) \in P^{\mathcal{M}}$. Par récurrence sur la structure des termes $u_1, \ldots, u_m$, $[\![u_i]\!]_\sigma = u_i\sigma$. Donc $\mathcal{M}, \sigma \models P(u_1, \ldots, u_m)$ ssi $(u_1\sigma, \ldots, u_m\sigma) \in P^{\mathcal{M}}$ ssi $\mathcal{M} \models P(u_1\sigma, \ldots, u_m\sigma)$.

Nous ne traitons que la négation et le quantificateur existentiel dans la récurrence (les autres cas sont laissés au lecteur) :

Si $\phi = \neg\psi$. $\mathcal{M}, \sigma \models \phi$ ssi $\mathcal{M}, \sigma \not\models \psi$ ssi (par hypothèse de récurrence), $\mathcal{M} \not\models \psi\sigma$ ssi $\mathcal{M} \models \neg(\psi\sigma)$. Mais $(\neg\psi)\sigma = \neg(\psi\sigma)$ par définition.

Si $\phi = \exists x.\psi$. On note σ' la substitution σ restreinte (si nécéssaire) aux variables différentes de x. $\mathcal{M}, \sigma \models \phi$ ssi il existe $t \in T(\mathcal{F})$, $\mathcal{M}, \sigma' \uplus \{x \mapsto t\} \models \psi$ ssi (par hypothèse de récurrence) il existe $t \in T(\mathcal{F})$, $\mathcal{M} \models \psi(\sigma' \uplus \{x \mapsto t\})$ ssi (par hypothèse de récurrence), il existe $t \in T(\mathcal{F})$, $\mathcal{M}, \{x \mapsto t\} \models \psi\sigma'$ ssi $\mathcal{M} \models \exists x.(\psi\sigma')$. Comme x n'est pas dans le domaine de σ', $\exists x.(\psi\sigma') = (\exists x.\psi)\sigma' = (\exists x.\psi)\sigma$.

Lemme 11.1.4 *$\mathcal{S}$ est cohérent si et seulement si $\mathcal{S}^*$ est cohérent.*

Preuve:
Comme $\mathcal{S} \subseteq \mathcal{S}^*$, il suffit de montrer que, si $\mathcal{S}^* \vdash_{\mathbf{NK}} \bot$, alors $\mathcal{S} \vdash_{\mathbf{NK}} \bot$.

On montre en fait que, si c_ϕ n'apparait pas dans un ensemble de formules Γ, alors $\Gamma, (\exists x.\phi \to \phi\{x \mapsto c_\phi\}) \vdash_{\mathbf{NK}} \bot$ entraine $\Gamma \vdash_{\mathbf{NK}} \bot$. Comme les seules occurrences de c_ϕ sont dans la formule $(\exists x.\phi \to \phi\{x \mapsto c_\phi\})$, on peut ensuite conclure par récurrence sur le nombre de constantes c_ψ qui apparaissent dans $\Gamma \subseteq \mathcal{S}^*$ tel que $\Gamma \vdash \bot$ est prouvable.

Remarquons d'abord que, par complétude propositionnelle, $\Gamma, (\exists x.\phi \to \phi\{x \mapsto c_\phi\}) \vdash_{\mathbf{NK}} \bot$ entraine que $\Gamma \vdash_{\mathbf{NK}} \exists x.\phi$ et $\Gamma \vdash_{\mathbf{NK}} \neg\phi\{x \mapsto c_\phi\}$. D'après le lemme **??**, et comme c_ϕ n'apparait pas dans Γ, $\Gamma \vdash_{\mathbf{NK}} \forall x.\neg\phi$. Mais par ailleurs,

$$\dfrac{\Gamma \vdash \exists x.\phi \qquad \dfrac{\dfrac{\dfrac{\Gamma \vdash \forall x.\neg\phi}{\Gamma, \phi\{x \mapsto y\} \vdash \forall x.\neg\phi}\, Aff}{\Gamma, \phi\{x \mapsto y\} \vdash \neg\phi\{x \mapsto y\}}\, \forall_e \qquad \dfrac{}{\Gamma, \phi\{x \mapsto y\} \vdash \phi\{x \mapsto y\}}\, Ax}{\Gamma, \phi\{x \mapsto y\} \vdash \bot}\, \neg_e}{\Gamma \vdash \bot}\, \exists_e$$

Donc $\Gamma \vdash_{\mathbf{NK}} \bot$.

Étant donnée une énumération des formules closes $\{\phi_n\}_{n\in\mathbb{N}}$, on construit par récurrence sur n une extension $\mathcal{T}_n$ de $\mathcal{S}^*$: $\mathcal{T}_0 = \mathcal{S}^*$ et $\mathcal{T}_{n+1} = \mathcal{T}_n \cup \{\phi_n\}$ si $\mathcal{T}_n \vdash_{NK} \phi_n$ et $\mathcal{T}_{n+1} = \mathcal{T}_n \cup \{\neg\phi_n\}$ sinon. Soit $\mathcal{T}^* = \bigcup_{n\in\mathbb{N}} \mathcal{T}_n$.

Lemme 11.1.5 *Si $\mathcal{S}^*$ est cohérente, alors $\mathcal{T}^*$ est cohérente.*

Preuve:
Par récurrence sur n, on montre que, si $\mathcal{S}^*$ est cohérente, alors $\mathcal{T}_n$ est cohérente. Dans le cas de base, c'est immédiat. Si $\mathcal{T}_n \vdash_{NK} \phi_n$, alors, $\mathcal{T}_{n+1} \vdash \phi$ ssi $\mathcal{T}_n \vdash_{NK} \phi$ et donc la cohérence de $\mathcal{T}_{n+1}$ est une conséquence de celle de $\mathcal{T}_n$. Si maintenant $\mathcal{T}_n \nvdash_{NK} \phi_n$ et $\mathcal{T}_n, \neg\phi_n \vdash_{NK} \bot$, par le raisonnement par l'absurde, $\mathcal{T}_n \vdash_{NK} \phi_n$. Il en résulte que, si $\mathcal{T}_n\neg \vdash_{NK} \phi_n$, alors $\mathcal{T}_{n+1}$ est cohérente.

Si maintenant $\mathcal{T}^* \vdash_{NK} \bot$, alors il existe un sous-ensemble fini Γ de $\mathcal{T}^*$ tel que $\Gamma \vdash_{NK} \bot$. Γ est contenu dans l'un des $\mathcal{T}_n$ et donc il existe un n tel que $\mathcal{T}_n$ est incohérente, ce qui est absurde. Donc $\mathcal{T}^*$ est cohérente.

On construit $\mathcal{M}$, modèle de $\mathcal{S}$ comme suit : $D_\mathcal{M} = T(\mathcal{F}^*)$ et la structure de $\mathcal{F}$-algèbre est la structure de l'algèbre libre. Pour tout symbole de prédicat P, $(t_1, \ldots, t_n) \in P_\mathcal{M}$ ssi $P(t_1, \ldots, t_n) \in \mathcal{T}^*$.

Lemme 11.1.6 *Si $\mathcal{S}$ est cohérent, alors $\mathcal{M} \models \mathcal{T}^*$.*

Preuve:
Si $\mathcal{S}$ est cohérente, alors $\mathcal{T}^*$ est cohérente, par les lemmes 11.1.4 et 11.1.5. On montre alors, par récurrence sur la taille de la fomule ϕ sans variable libre que $\phi \in \mathcal{T}^*$ ssi $\mathcal{M} \models \phi$:

- Si ϕ est une formule atomique $P(t_1, \ldots, t_n) \in \mathcal{T}^*$, alors, par construction, $\mathcal{M} \models \phi$ (et réciproquement).
- Si $\phi = \neg\psi$. Par cohérence, $\mathcal{T}^* \not\vdash_{NK} \psi$ et donc, par définition de $\mathcal{T}^*$, $\psi \notin \mathcal{T}^*$ et, par hypothèse de récurrence, $\mathcal{M} \not\models \psi$ donc $\mathcal{M} \models \neg\psi$.
- Si $\phi = \phi_1 \wedge \phi_2$, $\phi_1 \wedge \phi_2 \in \mathcal{T}^*$ entraine $\mathcal{T}^* \vdash_{NK} \phi_1$ et $\mathcal{T}^* \vdash_{NK} \phi_2$ (en utilisant $\wedge E$) donc, par hypothèse de récurrence, $\mathcal{M} \models \phi_1$ et $\mathcal{M} \models \phi_2$, donc $\mathcal{M} \models \phi_1 \wedge \phi_2$. Réciproquement, si $\mathcal{M} \models \phi_1 \wedge \phi_2$, alors $\mathcal{M} \models \phi_1$ et $\mathcal{M} \models \phi_2$ et donc, par hypothèse de récurrence, $\phi_1, \phi_2 \in \mathcal{T}^*$. Donc $\mathcal{T}^* \vdash_{NK} \phi_1 \wedge \phi_2$ (en utilisant $\wedge I$). Par construction, on a donc $\phi_1 \wedge \phi_2 \in \mathcal{T}^*$.
- Si $\phi = \phi_1 \vee \phi_2 \in \mathcal{T}^*$, alors ou bien pour $i = 1$ ou $i = 1$, $\phi_i \in \mathcal{T}^*$ et dans ce cas, par hypothèse de récurrence $\mathcal{M} \models \phi_i$ et donc $\mathcal{M} \models \phi_1 \vee \phi_2$, ou bien $\phi_1, \phi_2 \notin \mathcal{T}^*$. Il en résulte que $\neg\phi_1, \neg\phi_2 \in \mathcal{T}^*$, par construction. Et donc $\mathcal{T}^*, \phi_i \vdash_{NK} \bot$. Par $\vee E$ on a ainsi $\mathcal{T}^* \vdash_{NK} \bot$ et $\mathcal{T}^*$ serait incohérent. Réciproquement, si $\mathcal{M} \models \phi_1 \vee \phi_2$ alors, pour $i = 1$ ou $i = 2$, $\mathcal{M} \models \phi_i$ et donc, par hypothèse de récurrence, $\phi_i \in \mathcal{T}^*$. Par $\vee I$, $\mathcal{T}^* \vdash_{NK} \phi_1 \vee \phi_2$ et donc $\phi_1 \vee \phi_2 \in \mathcal{T}^*$
- Si $\phi = \phi_1 \to \phi_2 \in \mathcal{T}^*$, ou bien $\phi_1 \in \mathcal{T}^*$ et, par $\to E$, $\mathcal{T}* \vdash_{NK} \phi_2$ et donc, par hypothèse de récurrence, $\mathcal{M} \models \phi_2$ et donc $\mathcal{M} \models \phi_1 \to \phi_2$. Ou bien $\phi_1 \notin \mathcal{T}^*$ et dans ce cas, par hypothèse de récurrence, $\mathcal{M} \not\models \phi_1$ et donc $\mathcal{M} \models \phi_1 \to \phi_2$.
  Réciproquement, si $\mathcal{M} \models \phi_1 \to \phi_2$, alors ou bien $\mathcal{M} \models \phi_2$ et dans ce cas, par hypothèse de récurrence, $\phi_2 \in \mathcal{T}^*$ et donc $\mathcal{T}^*, \phi_1 \vdash_{NK} \phi_2$ et donc, par $\to I$, $\mathcal{T}^* \vdash_{NK} \phi_1 \to \phi_2$. Ou bien $\mathcal{M} \not\models \phi_1$ et, par hypothèse de récurrence, $\neg\phi_1 \in \mathcal{T}^*$. Dans ce cas, $\mathcal{T}^*, \phi_1 \vdash_{NK} \phi_2$ et, à nouveau, $\mathcal{T}^* \vdash \phi_1 \to \phi_2$. Dans tous les cas $\phi_1 \to \phi_2 \in \mathcal{T}^*$.
- Si $\phi = \exists x.\psi \in \mathcal{T}^*$. Par construction, $\phi \to \psi(c_\psi) \in \mathcal{T}^*$. Donc, par $\to E$, $\psi(c_\psi) \in \mathcal{T}^*$ et, par hypothèse de récurrence, $\mathcal{M} \models \psi(c_\psi)$ et donc $\mathcal{M} \models \phi$. Réciproquement, si $\mathcal{M} \models \phi$, il existe un terme $t \in T(\mathcal{F}^*)$ tel que $\mathcal{M}, x \mapsto t \models \psi$ et donc, par le lemme 11.1.3, $\mathcal{M} \models \psi\{x \mapsto t\}$ et donc, par hypothèse de récurrence, $\psi\{x \mapsto t\} \in \mathcal{T}^*$. Par $\exists_i$, $\mathcal{T}^* \vdash_{NK} \phi$ et donc, par construction, $\phi \in \mathcal{T}^*$.
- Si $\phi = \forall x.\psi \in \mathcal{T}^*$. Alors, pour tout terme $t \in T(\mathcal{F}^*)$, $\mathcal{T}^* \vdash_{NK} \psi\{x \mapsto t\}$ (par $\forall_e$). Donc, par hypothèse de récurrence, $\mathcal{M} \models \psi\{x \mapsto t\}$ pour tout $t \in T(\mathcal{F}^*)$ et donc $\mathcal{M} \models \forall x.\psi(x)$.
  Réciproquement, si $\mathcal{M} \models \forall x.\psi(x)$, alors pour tout terme $t \in T(\mathcal{F}^*)$, $\mathcal{M}, \{x \mapsto t\} \models \psi$. Donc, par le lemme 11.1.3, pour tout terme t, $\mathcal{M} \models \psi\{x \mapsto t\}$ donc, par hypothèse de récurrence, $\psi\{x \mapsto t\} \in \mathcal{T}^*$ pour tout t. En particulier, $\psi\{x \mapsto c_{\neg\psi}\} \in \mathcal{T}^*$. Comme $(\exists x.\neg\psi(x)) \to \neg\psi\{x \mapsto c_{\neg\psi}\} \in \mathcal{T}^*$, on en déduit $\neg\exists x\neg\psi(x) \in \mathcal{T}^*$. D'après le lemme 11.1.1, $\neg\exists x.\neg\psi(x) \vdash_{NK} \forall x.\psi(x)$. Donc $\phi \in \mathcal{T}^*$.

Ce lemme achève la preuve du théorème 11.1.2

Exercice 239
Donner un exemple de formule ϕ à une variable libre x telle que, pour tout terme t sans variable, $\vdash_{\mathbf{NK}} \phi\{x \mapsto t\}$, mais $\nvdash_{\mathbf{NK}} \forall x.\phi$.

Exercice 240
Quelles sont les règles de **NK** utilisées dans la preuve de complétude ? Quelles règles de **NK** peut on retirer tout en assurant la complétude ?