Exercices de logique

Rappel : système G pour le calcul propositionnel

$$\frac{A, B, \Gamma \longrightarrow \Delta}{A \wedge B, \Gamma \longrightarrow \Delta}\wedge_G \qquad \frac{\Gamma \longrightarrow A, \Delta \quad \Gamma \longrightarrow B, \Delta}{\Gamma \longrightarrow A \wedge B, \Delta}\wedge_D$$

$$\frac{A, \Gamma \longrightarrow \Delta \quad B, \Gamma \longrightarrow \Delta}{A \vee B, \Gamma \longrightarrow \Delta}\vee_G \qquad \frac{\Gamma \longrightarrow A, B, \Delta}{\Gamma \longrightarrow A \vee B, \Delta}\vee_D$$

$$\frac{\Gamma \longrightarrow A, \Delta \quad B, \Gamma \longrightarrow \Delta}{A \to B, \Gamma \longrightarrow \Delta}\to_G \qquad \frac{A, \Gamma \longrightarrow B, \Delta}{\Gamma \longrightarrow A \to B, \Delta}\to_D$$

$$\frac{\Gamma \longrightarrow A, \Delta}{\neg A, \Gamma \longrightarrow \Delta}\neg_G \qquad \frac{A, \Gamma \longrightarrow \Delta}{\Gamma \longrightarrow \neg A, \Delta}\neg_D$$

Calcul des propositions

1. Donner une interprétation qui valide la formule

$$(a \wedge b) \to (a \leftrightarrow (c \vee b))$$

2. On s'intéresse à des formules propositionnelles sur l'ensemble de variables $\{p, q, r\}$.

   (a) Donner une formule F non tautologique qui soit conséquence logique de $p \wedge q$:

$$\begin{array}{rcl} & \not\models & F \\ p \wedge q & \models & F \end{array}$$

   (b) Donner une formule G non satisfiable qui soit conséquence logique de $p \vee q$.

3. Soit le jugement suivant :

«

> Si un algorithme est simple, il est correct. Donc un algorithme est correct *ou* compliqué.»

   Montrer avec un argument sémantique (par exemple une table de vérité) que ce propos est ou n'est pas une tautologie suivant qu'on interprète le «ou» classiquement ou exclusivement.

4. On appelle *base de connecteur*, un ensemble de connecteurs qui permettent de définir tous les autres ($\{\neg, \vee\}$ en est une).

   (a) Montrer que $\{\wedge, \vee\}$ n'est pas une base de connecteurs.
   Indication : montrer que pour toute fonction f de $\{v, f\}$ dans $\{v, f\}$ définie avec $\wedge$ et $\vee$, on a $f(v) = v$ (par exemple par récurrence sur le nombre de connecteurs utilisés).

   (b) Le connecteur $\neg\wedge$ est défini par la table de vérité suivante :

p	q	$p \neg\wedge q$
f	f	v
f	v	v
v	f	v
v	v	f

   Montrer que $\{\neg\wedge\}$ est une base de connecteurs.

5. Étendre le système G pour le connecteur d'équivalence et pour le connecteur $\neg\wedge$.

6. Soit $\mathcal{F}^2$ l'ensemble des formules propositionnelles sur n atomes $\{p_1, ..., p_n\}$ s'écrivant comme une conjonction de clauses à 2 littéraux :

$$\bigwedge_{i=1}^{k} (l_i^1 \vee l_i^2)$$

avec $l_i^1 = p_j$ ou $l_i^1 = \neg p_j$ (idem pour l_i^2).

   (a) Estimer le nombre de clauses distinctes à 2 littéraux que l'on peut écrire avec n atomes.

   (b) Donner un algorithme pour prouver une formule de $\mathcal{F}^2$ dont le nombre d'étapes élémentaires (la *complexité temporelle*) est $p(n)$ où p est un polynôme et n le cardinal de l'ensemble des variables. Indication : utiliser le principe de résolution.

7. Soit le système de preuve PM[1] (analogue à la « méthode axiomatique ») constitué des axiomes

$$\begin{aligned} (p \vee p) &\rightarrow p \\ q &\rightarrow (p \vee q) \\ (p \vee q) &\rightarrow (q \vee p) \\ (q \rightarrow r) &\rightarrow ((p \vee q) \rightarrow (p \vee r)) \end{aligned}$$

et de la règles d'inférence (*modus ponens*)

$$\frac{\vdash A \quad \vdash A \rightarrow B}{\vdash B}$$

Une démonstration est une suite de formules qui sont soit des instances des axiomes, soit conclusion de la règle d'inférence.

Montrer que le système PM est correct, i.e. que toutes les formules démontrables avec PM sont des tautologies.

8. Montrer en utilisant le principe de résolution et le calcul des séquents que c est déductible des formules suivantes :

$$a \rightarrow (b \rightarrow c)$$
$$a \rightarrow (d \rightarrow b)$$
$$a$$
$$d$$

9. Montrer à l'aide du système G qu'on peut déduire s des quatre formules suivantes :
   h
   $b \rightarrow a$
   $(h \wedge i \wedge a) \rightarrow d$
   $((i \wedge b) \rightarrow d) \rightarrow s$

10. Montrer avec le système G que

$$((A \rightarrow C) \wedge (B \rightarrow C)) \rightarrow ((A \vee B) \rightarrow C)$$

est une tautologie.

11. Montrer à l'aide du système G qu'on peut déduire $g \wedge p$ des quatre formules suivantes (deux démonstrations possibles) :
   $np \vee p$
   g
   $d \rightarrow g$
   $np \rightarrow (p \wedge d)$

[1]Il s'agit du système proposé dans les *Principia Mathematica* de A. N. Whitehead et B. Russell, publié en 1910

12. À partir des hypothèses qui suivent, montrer que Superman n'existe pas[2]

    Si Superman était capable et voulait éradiquer le mal, il le ferait. Si Superman n'était pas capable d'éradiquer le mal, il serait faible ; s'il ne voulait pas éradiquer le mal, il serait malveillant. Superman n'éradique pas le mal ; s'il existe, il n'est ni faible ni malveillant.

13. Avec la méthode de démonstration de votre choix (excepté le langage naturel !), montrer qu'un club privé écossais dont les règles sont les suivantes ne contient pas de membres :
    (a) Tout membre non écossais porte des chaussettes rouges.
    (b) Tout membre porte un kilt ou ne porte pas des chaussettes rouges.
    (c) Les membres mariés ne sortent pas le dimanche.
    (d) Un membre sort le dimanche si et seulement si il est écossais.
    (e) Tout membre qui porte un kilt est marié et écossais.
    (f) Tout membre écossais porte un kilt.

14. On veut montrer que n'importe quelle formule du calcul des propositions possède une forme clausale avec des clauses à exactement trois éléments, c-à-d que pour toute formule F, il existe une formule F', équivalente à F, qui est une forme normale conjonctive dont les disjonctions possèdent 3 littéraux.

    On utilise pour cela la transformation suivante : soit $C = \{c_1, ..., c_m\}$ un ensemble de clauses quelconques sur les variables propositionnelles $U = \{u_1, ..., u_n\}$. A chaque clause $c_j = \{l_1, \ldots, l_k\}$ de C on associe un ensemble de clauses C'_j et un ensemble de nouvelles variables U'_j. La construction est différente suivant le nombre de littéraux de la clause initiale c_j :

    – si $k = 1$

    $$\begin{aligned} U'_j &= \{u_j^1, u_j^2\} \\ C'_j &= \{\{l_1, u_j^1, u_j^2\}, \{l_1, \neg u_j^1, u_j^2\}, \{l_1, u_j^1, \neg u_j^2\}, \{l_1, \neg u_j^1, \neg u_j^2\}\} \end{aligned}$$

    – si $k = 2$

    $$\begin{aligned} U'_j &= \{u_j^1\} \\ C'_j &= \{\{l_1, l_2, u_j^1\}, \{l_1, l_2, \neg u_j^1\}\} \end{aligned}$$

    – si $k = 3$, $U'_j = \emptyset$ et $C'_j = \{c_j\}$

    – si $k > 3$

    $$\begin{aligned} U'_j &= \{u_j^1, ..., u_j^{k-3}\} \\ C'_j &= \{\{l_1, l_2, u_j^1\}, \{\neg u_j^1, l_3, u_j^2\}, ..., \{\neg u_j^{k-3}, l_{k-1}, l_k\}\} \end{aligned}$$

    On considère alors l'ensemble C', l'union des ensembles de clauses associées à chacune des clauses de C :

    $$C' = \bigcup_{j=1}^{m} C'_j$$

    Ces clauses sont écrites avec les variables de U ainsi que celles des ensembles U'_1, ..., U'_m.

    (a) Montrer que l'ensemble de clauses obtenues C' est satisfiable si et seulement si l'ensemble initial C est satisfiable.
    (b) Transformer l'ensemble suivant :

    $$\{\{p, q\}, \{\neg p, \neg q, r, s\}, \{\neg r\}\}$$

[2] Gries & Schneider, *a logical approach to discrete math*

Calcul des prédicats

Les exercices 3 et 5 sont tirés de *Mathematical theory of computation* de Z. Manna.

1. Montrer par résolution qu'on peut déduire

$$\exists X(\exists Y(sur(X,Y) \wedge \neg vert(Y) \wedge vert(X)))$$

des formules suivantes :

$$\begin{aligned} \forall X(bleu(X) \rightarrow \neg vert(X)) \\ bleu(c) \\ vert(a) \\ sur(b,c) \\ sur(a,b) \\ \forall X(\neg vert(X) \vee vert(X)) \end{aligned}$$

2. On veut montrer que l'ensemble des nombres premiers est infini. Soient les prédicats :
   - $p(x)$ pour "x est premier"
   - $g(x,y)$ pour "x est plus grand que y"
   - $d(x,y)$ pour "x est un diviseur de y"

   On considère les deux formules suivantes :

$$\begin{aligned} \forall x \exists y(g(y,x) \wedge \forall z(d(z,y) \supset g(z,x))) \\ \forall x(\neg p(x) \supset \exists y(p(y) \wedge d(y,x))) \end{aligned}$$

qui expriment respectivement
   - pour tout x, il existe y plus grand que x tel que tout diviseur (z) de y est plus grand que x (par exemple $y = x! + 1$) ;
   - tout nombre (x) non premier a un diviseur premier (y).

   Montrer par résolution que pour tout x, il existe y plus grand que x qui est premier, c'est-à-dire :

$$\forall x \exists y(g(y,x) \wedge p(y))$$

3. Prouver par résolution que tout prédicat p qui a les propriétés suivantes :

$$\begin{aligned} \forall x \forall y(p(x,y) \supset p(y,x)) & \quad \text{Symétrie} \\ \forall x \forall y \forall z((p(x,y) \wedge p(y,z)) \supset p(x,z)) & \quad \text{Transitivité} \\ \forall x \exists y\ p(x,y) & \end{aligned}$$

est réflexif, c'est-à-dire :

$$\forall x\ p(x,x)$$

4. Formaliser les faits suivants et montrer par résolution que si la bonne a dit vrai, le majordome a menti :

«

> La bonne dit qu'elle a vu le majordome dans la salle à manger. La salle à manger et la cuisine sont deux pièces voisines. Le coup de feu a été tiré dans la cuisine et a pu être entendu dans toutes les pièces voisines. Le majordome, qui entend correctement, dit qu'il n'a pas entendu le coup de feu. »

5. Formuler les faits et la réponse suivants en calcul des prédicats. Montrer par résolution que la réponse peut être déduite des faits.

Tony, Mike, and John belong to the Alpine Club. Every member of the Alpine Club is either a skier or a mountain climber (or both). No mountain climber likes rain, and all skiers like snow. Mike dislikes whatever Tony likes and likes whatever Tony dislikes. Tony likes rain and snow.

Is there a member of the Alpine Club who is a mountain climber but not a skier ?[3]

6. Montrer avec ce système qu'on peut déduire $s(j)$ des formules suivantes :

$$
\begin{aligned}
h(j)\\
\forall x(b(x) \to a(x))\\
\forall x \forall y((h(y) \land i(x,y) \land a(x)) \to d(x))\\
\forall y((\forall x(i(x,y) \land b(x)) \to d(x)) \to s(y))
\end{aligned}
$$

Indication pour l'utilisation du calcul des séquents : Lors de l'utilisation de la règle $\forall_G$, pour un $\forall y$, on choisira $t = j$ et pour un $\forall x$, on choisira $t = c$, c étant la constante introduite par l'emploi de la règle $\forall_D$ (à appliquer le plus tôt possible).

7. On considère la signature $\Sigma = \{v_0, d_0\}$ et l'ensemble de prédicats $P = \{p_3, r_1\}$.
   (a) Montrer par résolution qu'on peut déduire

   $$\exists x \exists y \exists z(p(x,y,z) \land \neg r(x) \land \neg r(y) \land r(z))$$

   des formules suivantes :

   $$
   \begin{aligned}
   \exists x(p(v,v,x) \land p(x,v,d))\\
   \neg r(v)\\
   r(d)
   \end{aligned}
   $$

   (b) Refaire la démonstration précédente en utilisant le calcul des séquents. Pour cela, on commencera par montrer (en calcul des séquents) le lemme suivant :

   $$\forall x(p(x) \lor \neg p(x))$$

   et on ajoutera alors ce lemme aux hypothèses.

8. On considère une signature $\Sigma = \{c_2, n_0\}$, des symboles de prédicat l_1, mb_2, ap_3 et l'ensemble $\mathcal{P}$ de formules suivant :

$$l(n) \tag{1}$$
$$\forall x \forall y\ l(y) \to l(c(x,y)) \tag{2}$$
$$\forall x \forall y\ mb(x, c(x,y)) \tag{3}$$
$$\forall x \forall y \forall z\ mb(x,y) \to mb(x, c(z,y)) \tag{4}$$
$$\forall y\ ap(n,y,y) \tag{5}$$
$$\forall e \forall x \forall y \forall z\ ap(x,y,z) \to ap(c(e,x), y, c(e,z)) \tag{6}$$

   (a) Montrer par résolution que $\mathcal{P} \vdash \forall x \forall y\ mb(x, c(y, c(x,n)))$.
   (b) Montrer en utilisant le calcul des séquents que $\mathcal{P} \vdash \forall a \forall x\ ap(c(a,n), x, c(a,x))$.
   (c) On considère le domaine $\mathcal{L}$, le plus petit ensemble vérifiant :
   – le tuple vide $<>\in \mathcal{L}$;
   – pour tout $x \in \mathbb{N}$ et $y \in \mathcal{L}$, la paire $< x, y >\in \mathcal{L}$.
      i. Décrire les éléments de $\mathcal{L}$.

[3]La traduction sera aussi bien faite par vos soins !

ii. Donner une interprétation des symboles c, n, l, mb, ap dans $\mathcal{L} \cup \mathbb{N}$ telle que toutes les formules de $\mathcal{P}$ soient valides dans $\mathcal{L} \cup \mathbb{N}$ (i.e. $\mathcal{L} \cup \mathbb{N}$ est un modèle pour $\mathcal{P}$). Indication : on pourra prendre $\hat{c} : \mathbb{N} \times \mathcal{L} \longrightarrow \mathcal{L}$ où $\hat{c}$ est l'interprétation du symbole c.

9. Soit la signature $\Sigma = \{s_1, a_0\}$ et l'ensemble de symbole de prédicat $P = \{p_3\}$. On veut montrer que $\exists x_1 \exists x_2 p(x_1, x_2, s(a))$ est conséquence de :

$$\forall y\ p(a, y, y) \tag{7}$$

$$\forall x \forall y \forall z\ p(x, y, z) \rightarrow p(s(x), y, s(z)) \tag{8}$$

   (a) Donner deux preuves en utilisant la résolution. Ces deux preuves permettent d'exhiber des valeurs solution pour x_1 et x_2 (les valeurs avec lesquelles sont unifiées ces variables lors de la preuve).

   (b) Donner deux preuves en utilisant le calcul des séquents. Ces deux preuves permettent d'exhiber des valeurs solution pour x_1 et x_2 (par unification des termes t introduits lors de l'utilisation de la règle $\exists_D$).

   (c) En prenant comme domaine d'interprétation l'ensemble des entiers, interpréter les résultats des deux questions précédentes.

10. On axiomatise le domaine des entiers naturels à l'aide de deux symboles fonctionnels : z d'arité 0 pour l'entier 0 et s d'arité 1 pour la fonction $x \mapsto x + 1$ (i.e $\lambda x.(x + 1)$). Il s'agit de l'axiomatisation de Peano.

   (a) Montrer que tout entier peut être représenté avec ces deux symboles. Montrer que la représentation est unique.

   (b) On veut axiomatiser l'addition. Pour cela, on choisit de représenter la fonction $x, y, z \mapsto (x + y = z)$ (i.e. $\lambda xyz.(x + y = z)$) où la fonction $=$ est la fonction de test d'égalité dans les entiers, par un symbole de prédicat p d'arité 3. Donner la formule sous forme clausale qui définit p. Indication : donner deux clauses correspondant aux deux cas pour y, nul ou non nul.