

Examen 2ème session du 11/06/2019

Durée 2h

Téléphones et ordinateurs interdits. Le seul document autorisé est le formulaire des équivalences sur les expressions booléennes et des règles de la Dédution Naturelle. Inscrire votre numéro d'anonymat sur votre copie. La barème sur 38 points est donné à titre indicatif.

Exercice 1 (1+1+(1,5+1,5)=5 points)

Les questions de cet exercice sont toutes indépendantes.

1. Soit \mathcal{F} et \mathcal{P} deux ensembles disjoints (i.e. $\mathcal{F} \cap \mathcal{P} = \emptyset$). Expliquer pourquoi la formule $\forall x (p(f(x), y) \Rightarrow q(f(x), p(y)))$ n'est pas une formule de $\mathbb{F}(X, \mathcal{F}, \mathcal{P})$ syntaxiquement correcte.
2. En s'autorisant l'utilisation du connecteur logique \Leftrightarrow dans les formules, la définition d'une application injective peut s'écrire :

$$\forall f \text{ (injective}(f) \Leftrightarrow (\forall x \forall y (eq(f(x), f(y)) \Rightarrow eq(x, y))))$$

où eq est le prédicat d'égalité. Expliquer pourquoi la formule ci-dessus n'est pas une formule de $\mathbb{F}(X, \mathcal{F}, \mathcal{P})$.

3. Soit F la formule $\forall x (q(x, y) \vee \exists x p(x, y, z))$ (où x, y et z sont des symboles de variable). Calculer $F[x := f(x, y, z)]$ et $F[y := f(x, y, z)]$.

Exercice 2 (1+1,5+1,5+3=7 points)

Soit $\mathcal{F} = \mathcal{F}_0 \cup \mathcal{F}_1$ un ensemble de symboles de fonction où $\mathcal{F}_1 = \{\odot\}$ et \mathcal{F}_0 contient une infinité de symboles de constante numérotés par des entiers ($\mathcal{F}_0 = \{k_0, k_1, k_2, \dots\} = \bigcup_{i \geq 0} \{k_i\}$). Etant donné un entier naturel n et un terme t , on définit le terme $\odot^n(t)$ comme suit :

$$\odot^n(t) = \begin{cases} t & \text{si } n = 0 \\ \odot(\odot^k(t)) & \text{si } n = k + 1 \end{cases}$$

Soit \mathbf{M} une structure dont le domaine est l'ensemble $\mathbb{N} \times \mathbb{N}$ des couples d'entiers naturels définie par :

$$\begin{aligned} k_i^{\mathbf{M}} &= (0, i) & \odot^{\mathbf{M}} : \mathbb{N} \times \mathbb{N} &\rightarrow \mathbb{N} \times \mathbb{N} \\ \text{pour tout } k_i \in \mathcal{F}_0 & & \odot^{\mathbf{M}}((n_1, n_2)) &= (n_1 + 1, n_2 + 1) \end{aligned}$$

1. Calculer $[\odot^3(k_5)]^{\mathbf{M}}$.
2. Montrer (par récurrence sur n) que $[\odot^n(k_m)]^{\mathbf{M}} = (n, m + n)$.
3. Soient quatre entiers naturels n_1, n_2, n et m tels que $[\odot^n(k_m)]^{\mathbf{M}} = (n_1, n_2)$. Exprimer n et m en fonction de n_1 et n_2 . En déduire que si $n_1 \leq n_2$, alors il existe un terme t tel que $[t]^{\mathbf{M}} = (n_1, n_2)$.
4. Montrer par induction sur t , que si $[t]^{\mathbf{M}} = (n_1, n_2)$ alors $n_1 \leq n_2$.

Exercice 3 (1+1+(1+2+3)=8 points)

Soient A et B deux formules atomiques de $\mathcal{L}_0(\mathcal{F}, \mathcal{P})$.

1. Donner la définition mathématique de $A \models B$.
2. Si l'on suppose que $A \models A \Rightarrow B$, la formule B est-elle nécessairement valide ? si oui en donner une démonstration, si non donner un contre-exemple.
3. Soit F la formule $(A \Rightarrow (A \Rightarrow B)) \Rightarrow B$.

- (a) Etant donnée une structure \mathbf{M} , calculer l'expression booléenne $[F]^{\mathbf{M}}$ en fonction de $\mathbf{I}_{\mathbf{M}}(A)$ et $\mathbf{I}_{\mathbf{M}}(B)$ (sans effectuer de simplification).
- (b) En utilisant un raisonnement équationnel, montrer que F est équivalente à $A \vee B$ (indiquer à chaque étape le nom de l'équivalence utilisée).
- (c) En utilisant les règles de la déduction naturelle, montrer que $(A \vee B) \Rightarrow F$ est une formule prouvable.

Exercice 4 (8 points)

En utilisant les règles de la déduction naturelle, prouver la formule :

$$(\exists x \exists y (p(x, y) \vee p(y, x))) \Rightarrow \exists x \exists y p(x, y)$$

Exercice 5 (1+4+(1+4)=10 points)

On considère un langage logique avec variables muni du symbole de fonction unaire $f \in \mathcal{F}_1$ et du symbole de prédicat binaire $\text{eq} \in \mathcal{P}_2$ d'égalité. On considère la formule $F = \forall y \exists x \text{eq}(y, f(x))$ exprimant que la fonction f est surjective.

1. Définir une structure \mathbf{M}_1 dont le domaine d'interprétation $|\mathbf{M}_1|$ contient une infinité de valeurs et telle que $\text{eq}^{\mathbf{M}_1} = \{(m, m) \mid m \in |\mathbf{M}_1|\}$ et $[F]_v^{\mathbf{M}_1} = 0$ (quelle que soit la valuation v). Justifier votre réponse.
2. Soit \mathbf{M}_2 une structure telle que $|\mathbf{M}_2| = \{a\}$. Démontrer que $[F]_v^{\mathbf{M}_2} = 1$ (quelle que soit la valuation v).
3. On considère la formule $F_1 = \forall x \text{eq}(x, f(f(x)))$ exprimant que la fonction f est involutive.
 - (a) Définir une structure \mathbf{M}_3 telle que $\text{eq}^{\mathbf{M}_3} = \{(m, m) \mid m \in |\mathbf{M}_3|\}$ et $[F_1]_v^{\mathbf{M}_3} = 0$ (quelle que soit la valuation v). Justifier votre réponse.
 - (b) En utilisant les règles de la déduction naturelle, montrer que toute fonction involutive est surjective, c-à-d que la formule F est prouvable à partir de l'hypothèse F_1 . Concrètement, il s'agit de compléter la preuve suivante :

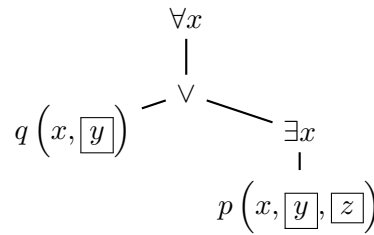
<div style="border: 1px solid black; padding: 5px; margin-bottom: 5px;"> $\langle 1 \rangle$ supposons $h_1 : F_1$ montrons F <div style="border: 1px solid black; padding: 5px; margin: 5px auto; width: 80%;"> ... à compléter ... </div> </div> $\langle 1 \rangle$ CQFD (?)

Indication. Il s'agit de formaliser le raisonnement suivant : étant donné y , $x = f(y)$ vérifie $y = f(x)$ car $f(f(y)) = y$ puisque f est involutive.

Corrigé de l'examen 2ème session du 11/06/2019

► CORRIGÉ DE L'EXERCICE 1.

1. Dans la formule atomique $p(f(x), y)$ qui figure à gauche de l'implication, p est un symbole de prédicat, mais ce symbole est utilisé comme un symbole de fonction dans la formule atomique $q(f(x), p(y))$ qui figure à droite de l'implication.
2. Dans la formule, le symbole de fonction f est quantifié (universellement) ce qui n'est pas possible dans le langage de la logique du premier ordre.
3. L'arbre de syntaxe abstraite de la formule F dans lequel les occurrences libres de symboles de variable sont encadrées est :



Puisque $x \notin \text{Free}(F)$, on a $F[x := f(x, y, z)] = F$. Puisque x apparaît dans le terme $f(x, y, z)$, pour calculer $F[y := f(x, y, z)]$ il faut renommer les occurrences liées de x dans la formule F . On peut utiliser deux symboles de variable différents pour le renommage puisque x est dans la portée de deux quantificateurs différents : $\forall w_1 (q(w_1, y) \vee \exists w_2 p(w_2, y, z))$. On peut à présent appliquer la substitution pour obtenir la formule $\forall w_1 (q(w_1, f(x, y, z)) \vee \exists w_2 p(w_2, f(x, y, z), z))$.

► CORRIGÉ DE L'EXERCICE 2.

1.
$$\begin{aligned}
 [\odot^3(k_5)]^{\mathbf{M}} &= \odot^{\mathbf{M}}(\odot^{\mathbf{M}}(\odot^{\mathbf{M}}(k_5^{\mathbf{M}}))) = \odot^{\mathbf{M}}(\odot^{\mathbf{M}}(\odot^{\mathbf{M}}((0, 5)))) = \odot^{\mathbf{M}}(\odot^{\mathbf{M}}((1, 6))) \\
 &= \odot^{\mathbf{M}}((2, 7)) = (3, 8)
 \end{aligned}$$
2. Par récurrence sur n . Pour $n = 0$, on a bien $[\odot^0(k_m)]^{\mathbf{M}} = [k_m]^{\mathbf{M}} = (0, m) = (0, m + 0)$. Supposons, par hypothèse de récurrence, que $[\odot^n(k_m)]^{\mathbf{M}} = (n, m + n)$. On a bien :
$$[\odot^{n+1}(k_m)]^{\mathbf{M}} = \odot^{\mathbf{M}}([\odot^n(k_m)]^{\mathbf{M}}) = \odot^{\mathbf{M}}((n, m + n)) = (n + 1, m + n + 1)$$
3. Puisque $[\odot^n(k_m)]^{\mathbf{M}} = (n, m + n)$, lorsque $(n, m + n) = (n_1, n_2)$ on a $n = n_1$ et $n_2 = m + n = m + n_1$ et donc $m = n_2 - n_1$. On a donc $[\odot^{n_1}(k_{n_2-n_1})]^{\mathbf{M}} = (n_1, n_2)$. Aussi, lorsque $n_1 \leq n_2$ (et donc $n_2 - n_1 \in \mathbb{N}$) le terme $t = \odot^{n_1}(k_{n_2-n_1})$ est tel que $[t]^{\mathbf{M}} = (n_1, n_2)$.
4. Par induction sur t . Si $t = k_i \in \mathcal{F}_0$, alors $[k_i]^{\mathbf{M}} = (0, i)$ et on peut conclure puisque $0 \leq i$. Si $t = \odot(t')$, alors $[\odot(t')]^{\mathbf{M}} = \odot^{\mathbf{M}}([t']^{\mathbf{M}}) = \odot^{\mathbf{M}}((n'_1, n'_2)) = (n'_1 + 1, n'_2 + 1)$ où $(n'_1, n'_2) = [t']^{\mathbf{M}}$ et puisque, par hypothèse d'induction $n'_1 \leq n'_2$ on a bien $n'_1 + 1 \leq n'_2 + 1$.

► CORRIGÉ DE L'EXERCICE 3.

1. $A \models B$ si et seulement si pour toute structure \mathbf{M} , si $[A]^{\mathbf{M}} = 1$, alors $[B]^{\mathbf{M}} = 1$.
2. Non. En effet, il suffit de considérer la structure \mathbf{M} telle que $\mathbf{I}_{\mathbf{M}}(A) = \mathbf{I}_{\mathbf{M}}(B) = 0$ qui ne contredit pas l'hypothèse $A \models A \Rightarrow B$.

$$\begin{aligned} [F]^{\mathbf{M}} &= \overline{[A \Rightarrow (A \Rightarrow B)]^{\mathbf{M}}} + [B]^{\mathbf{M}} = \overline{[A]^{\mathbf{M}}} + \overline{[A \Rightarrow B]^{\mathbf{M}}} + [B]^{\mathbf{M}} \\ &= \overline{[A]^{\mathbf{M}}} + \left(\overline{[A]^{\mathbf{M}}} + [B]^{\mathbf{M}} \right) + [B]^{\mathbf{M}} = \mathbf{I}_{\mathbf{M}}(\overline{A}) + \left(\mathbf{I}_{\mathbf{M}}(\overline{A}) + \mathbf{I}_{\mathbf{M}}(B) \right) + \mathbf{I}_{\mathbf{M}}(B) \end{aligned}$$
$$\begin{aligned}
[F]^{\mathbf{M}} &= \overline{\bar{x} + (\bar{x} + y)} + y \stackrel{(E3.4)}{=} \overline{(\bar{x} + \bar{x}) + y} + y \stackrel{(E3.5)}{=} \overline{\bar{x} + y} + y \stackrel{(E4.4)}{=} (\overline{\bar{x}.y}) + y \\
&\stackrel{(E1.2)}{=} (x.\bar{y}) + y \stackrel{(E3.1)}{=} y + (x.\bar{y}) \stackrel{(E4.2)}{=} (y + x).(y + \bar{y}) \stackrel{(E1.4)}{=} (y + x).1 \stackrel{(E2.6)}{=} y + x \\
&\stackrel{(E3.1)}{=} x + y = \mathbf{I}_{\mathbf{M}}(A) + \mathbf{I}_{\mathbf{M}}(B) = [A \vee B]^{\mathbf{M}}
\end{aligned}$$

(1) montrons $(A \vee B) \Rightarrow ((A \Rightarrow (A \Rightarrow B)) \Rightarrow B)$

(2) supposons $h_1 : A \vee B$, montrons $(A \Rightarrow (A \Rightarrow B)) \Rightarrow B$

(3) supposons $h_2 : A \Rightarrow (A \Rightarrow B)$, montrons B

(4) montrons $A \vee B$
c'est l'hypothèse h_1

(4) CQFD (Ax)

(5) supposons $h_3 : A$, montrons B

(6) montrons $A \Rightarrow B$

(7) montrons $A \Rightarrow (A \Rightarrow B)$
c'est l'hypothèse h_2

(7) CQFD (Ax)

(8) montrons A
c'est l'hypothèse h_3

(8) CQFD (Ax)

(6) CQFD (E_{\Rightarrow})

(7) montrons A
c'est l'hypothèse h_3

(7) CQFD (Ax)

(5) CQFD (E_{\Rightarrow})

(6) supposons $h_4 : B$, montrons B
c'est l'hypothèse h_4

(6) CQFD (Ax)

(3) CQFD (E_{\vee})

(2) CQFD (I_{\Rightarrow})

(1) CQFD (I_{\Rightarrow})

► CORRIGÉ DE L'EXERCICE 4.

⟨1⟩	montrons $(\exists x \exists y (p(x, y) \vee p(y, x))) \Rightarrow \exists x \exists y p(x, y)$
⟨2⟩	supposons $h_1 : \exists x \exists y (p(x, y) \vee p(y, x))$, montrons $\exists x \exists y p(x, y)$
⟨3⟩	montrons $\exists x \exists y (p(x, y) \vee p(y, x))$ c'est l'hypothèse h_1
⟨3⟩	CQFD (Ax)
⟨4⟩	soit une nouvelle variable z_1 , supposons $h_2 : \exists y (p(z_1, y) \vee p(y, z_1))$ montrons $\exists x \exists y p(x, y)$
⟨5⟩	montrons $\exists y (p(z_1, y) \vee p(y, z_1))$ c'est l'hypothèse h_2
⟨5⟩	CQFD (Ax)
⟨6⟩	soit une nouvelle variable z_2 , supposons $h_3 : p(z_1, z_2) \vee p(z_2, z_1)$ montrons $\exists x \exists y p(x, y)$
⟨7⟩	montrons $p(z_1, z_2) \vee p(z_2, z_1)$ c'est l'hypothèse h_3
⟨7⟩	CQFD (Ax)
⟨8⟩	supposons $h_4 : p(z_1, z_2)$, montrons $\exists x \exists y p(x, y)$
⟨9⟩	montrons $\exists y p(z_1, y)$
⟨10⟩	montrons $p(z_1, z_2)$ c'est l'hypothèse h_4
⟨10⟩	CQFD (Ax)
⟨9⟩	CQFD (I_\exists)
⟨8⟩	CQFD (I_\exists)
⟨9⟩	supposons $h_5 : p(z_2, z_1)$, montrons $\exists x \exists y p(x, y)$
⟨10⟩	montrons $\exists y p(z_2, y)$
⟨11⟩	montrons $p(z_2, z_1)$ c'est l'hypothèse h_5
⟨10⟩	CQFD (Ax)
⟨10⟩	CQFD (I_\exists)
⟨9⟩	CQFD (I_\exists)
⟨6⟩	CQFD (E_\vee)
⟨4⟩	CQFD (E_\exists)
⟨2⟩	CQFD (E_\exists)
⟨1⟩	CQFD (I_{\Rightarrow})

► CORRIGÉ DE L'EXERCICE 5.

1. Il suffit de considérer la fonction $x \mapsto x^2$ définie sur \mathbb{Z} et à valeurs dans \mathbb{Z} qui n'est pas surjective (puisque par exemple $-1 \in \mathbb{Z}$ n'est le carré d'aucun entier relatif). Formellement, on considère donc la structure \mathbf{M}_1 de domaine $|\mathbf{M}_1| = \mathbb{Z}$ telle que $f^{\mathbf{M}_1}(k) = k^2$.

2. Par définition, $[F]_v^{\mathbf{M}_2} = 1$ si et seulement si pour chaque $m_1 \in \mathbf{M}_2$:

$$[\exists x \text{eq}(y, f(x))]_{v[y \leftarrow m_1]}^{\mathbf{M}_2} = 1$$

et donc, puisque $|\mathbf{M}_2|$ contient un unique élément a , $[F]_v^{\mathbf{M}_2} = 1$ si et seulement si :

$$[\exists x \text{eq}(y, f(x))]_{v[y \leftarrow a]}^{\mathbf{M}_2} = 1$$

De plus, $[\exists x \text{eq}(y, f(x))]_{v[y \leftarrow a]}^{\mathbf{M}_2} = 1$ si et seulement si pour au moins un élément $m_2 \in \mathbf{M}_2$:

$$[\text{eq}(y, f(x))]_{v[y \leftarrow a][x \leftarrow m_2]}^{\mathbf{M}_2} = 1$$

c-à-d (puisque $|\mathbf{M}_2|$ contient un unique élément a) si et seulement si :

$$[\text{eq}(y, f(x))]_{v[y \leftarrow a][x \leftarrow a]}^{\mathbf{M}_2} = 1$$

Or, la seule fonction unaire $f^{\mathbf{M}_2} : |\mathbf{M}_2| \rightarrow |\mathbf{M}_2|$ possible est telle que $f^{\mathbf{M}_2}(a) = a$, et puisque :

$$([y]_{v[y \leftarrow a][x \leftarrow a]}^{\mathbf{M}_2}, [f(x)]_{v[y \leftarrow a][x \leftarrow a]}^{\mathbf{M}_2}) = (a, f^{\mathbf{M}_2}(a)) = (a, a) \in \text{eq}^{\mathbf{M}_2}$$

on peut alors conclure que $[F]_v^{\mathbf{M}_2} = 1$.

3.a. Il suffit de considérer la fonction $x \mapsto x^2$ définie sur \mathbb{Z} qui n'est pas involutive (puisque par exemple $(2^2)^2 \neq 2$). Formellement, on considère donc la structure \mathbf{M}_3 de domaine $|\mathbf{M}_3| = \mathbb{Z}$ telle que $f^{\mathbf{M}_3}(k) = k^2$.

3.b.

(1) supposons $h_1 : F_1$, montrons F

(2) soit une nouvelle variable w , montrons $\exists x \text{ eq}(w, f(x))$

(3) montrons $\text{eq}(w, f(f(w)))$

(4) montrons $\forall x \text{ eq}(x, f(f(x)))$
c'est l'hypothèse h_1

(4) CQFD (Ax)

(3) CQFD (E_{\forall})

(2) CQFD (I_{\exists})

(1) CQFD (I_{\forall})