# Examen partiel du 16/03/2023

**Durée 1h30**

Tout appareil électronique interdit.
Les seuls documents autorisés sont le formulaire des équivalences sur les expressions booléennes et celui des règles de la Déduction Naturelle.
Le barème sur 41 est donné à titre indicatif.

**Inscrire votre nom et votre numéro d'étudiant sur votre copie.**

## Exercice 1 ((0,5+0,5+1)+(2+1+1+1)=7 points)

1. Soit la formule $F = ((\forall x\,((\exists x\,p(x)) \wedge q(x,x))) \wedge p(x)) \Rightarrow ((\forall x\,q(x,x)) \wedge p(x))$.
   (a) Dessiner l'arbre de syntaxe abstraite de la formule $F$.
   (b) Donner une formule $F'$ qui est une clôture universelle de $F$.
   (c) Renommer certains symboles de variables de $F$ pour obtenir une formule $F''$ logiquement équivalente à $F$ dans laquelle les quantificateurs portent sur des symboles de variables différents et ne correspondant pas au symbole d'une variable libre.
2. A partir de l'ensemble de symboles de variable $X = \{w, x, y, z\}$ on définit la formule $G \in \mathbb{F}(X, \mathcal{F}, \mathcal{P})$ suivante : $\forall y\,(s_1(s_2(s_3(x), y)) \wedge \forall x\,(s_4(s_3(z), x) \Rightarrow \exists z\,s_1(s_2(z, w))))$
   (a) Pour chacun des symboles $s_1$, $s_2$, $s_3$ et $s_4$ dire s'il s'agit :
   - d'une fonction ou d'un prédicat,
   - unaire ou binaire

   (b) Quelles sont les formules atomiques apparaissant dans $G$ ?
   (c) Quels sont les termes apparaissant en argument des symboles de prédicat de $G$ ?
   (d) Soit $f$ un nouveau symbole de fonction, calculer la formule $G'=G[z := f(x)]$.

## Exercice 2 (6+8=14 points)

Avec les règles de la déduction naturelle prouver les deux formules ci-dessous (on pourra utiliser les règles dérivées du formulaire).

$$((A \Rightarrow B) \vee C) \Rightarrow (A \Rightarrow (B \vee C)) \qquad (A \Rightarrow (B \vee C)) \Rightarrow ((A \Rightarrow B) \vee C)$$

## Exercice 3 (0,5+(0,5+0,5+4)+(1+1+4)=11,5 points)

1. Soient $F_1$ et $F_2$ deux formules de $\mathbb{F}_0(\mathcal{F}, \mathcal{P})$. Donner la définition mathématique de $F_1 \models\!\models F_2$.
2. On considère les deux formules $F_1 = (A \Rightarrow B) \vee C$ et $F_2 = A \Rightarrow (B \vee C)$.
   (a) Etant donnée une structure $\mathbf{M}$, calculer les expressions booléennes $[F_1]^{\mathbf{M}}$ et $[F_2]^{\mathbf{M}}$ en fonction de $\mathbf{I}_{\mathbf{M}}(A)$, $\mathbf{I}_{\mathbf{M}}(B)$ et $\mathbf{I}_{\mathbf{M}}(C)$.
   (b) A-t-on $F_1 \models\!\models F_2$ ? Justifier votre réponse. Si votre réponse est oui, votre justification peut-être le numéro ou le nom des équivalences permettant de conclure.
   (c) Les formules ci-dessous sont-elles valides ? satisfiables ? insatisfiables ? Justifier vos réponses.

   i. $F_1 \Rightarrow \neg F_2$ ii. $\neg F_1 \Rightarrow \neg F_2$
   iii. $\neg F_1 \wedge F_2$ iv. $\neg F_1 \wedge \neg F_2$

3. On définit un nouveau connecteur logique ternaire, noté `ite`, tel que :

$$\texttt{ite}(F_1, F_2, F_3) \Leftrightarrow (F_1 \wedge F_2) \vee (\neg F_1 \wedge F_3)$$

   (a) Etant donnée une structure $\mathbf{M}$, calculer une expression booléenne pour $[\texttt{ite}(F_1, F_2, F_3)]^{\mathbf{M}}$ en fonction de $[F_1]^{\mathbf{M}}$, $[F_2]^{\mathbf{M}}$ et $[F_3]^{\mathbf{M}}$.

   (b) Etant donnée une structure $\mathbf{M}$, calculer $[\texttt{ite}(F_1, F_2, F_3)]^{\mathbf{M}}$ en fonction de $[F_2]^{\mathbf{M}}$ et $[F_3]^{\mathbf{M}}$ lorsque :

   i. $[F_1]^{\mathbf{M}} = 1$
   ii. $[F_1]^{\mathbf{M}} = 0$

   (c) Dans les quatre propriétés ci-dessous, remplacer les ? par une des trois formules $F$, $F_1$ et $F_2$ ou par une des deux constantes logiques true et false :

   i. $(F_1 \wedge F_2) \Leftrightarrow \texttt{ite}(?, ?, ?)$ ii. $(F_1 \vee F_2) \Leftrightarrow \texttt{ite}(?, ?, ?)$
   iii. $\neg F \Leftrightarrow \texttt{ite}(?, ?, ?)$ iv. $(F_1 \Rightarrow F_2) \Leftrightarrow \texttt{ite}(?, ?, ?)$

**Exercice 4 (0,5+2+(3+3)=8,5 points)**
Soit $\mathcal{F} = \mathcal{F}_0 \cup \mathcal{F}_1$ un ensemble de symboles de fonction avec $\mathcal{F}_0 = \{a, b, c\}$ et $\mathcal{F}_1 = \{f\}$. Etant donné un entier naturel $n$ et un symbole de constante $k \in \mathcal{F}_0$, on note $f^n(k)$ le terme :

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

On admettra sans démonstration que $f^{n+m}(k) = f^n(f^m(k))$.

1. Particulariser la définition de l'ensemble de termes $\mathcal{T}_0(\mathcal{F})$.

2. Montrer que $\mathcal{T}_0(\mathcal{F}) = \bigcup_{n \in \mathbb{N}} \{f^n(k) \mid k \in \mathcal{F}_0\}$. Vous pourrez montrer les deux inclusions suivantes :

   - $\mathcal{T}_0(\mathcal{F}) \subseteq \bigcup_{n \in \mathbb{N}} \{f^n(k) \mid k \in \mathcal{F}_0\}$
   - $\bigcup_{n \in \mathbb{N}} \{f^n(k) \mid k \in \mathcal{F}_0\} \subseteq \mathcal{T}_0(\mathcal{F})$

3. Soit $\mathbf{M}$ une structure de domaine $|\mathbf{M}| = \{(n_1, n_2) \in \mathbb{N} \times \mathbb{N} \mid n_1 \neq n_2\}$ telle que pour tout couple $(n_1, n_2) \in |\mathbf{M}|$, $f^{\mathbf{M}}((n_1, n_2)) = (n_2, n_1)$.

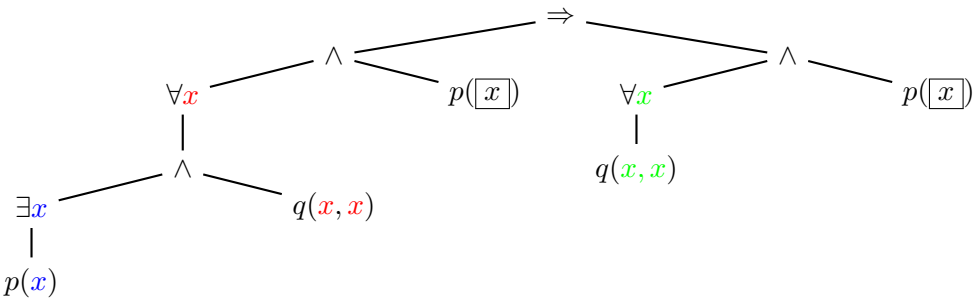
   (a) Montrer par récurrence sur $n$ que pour tout entier $n \in \mathbb{N}$, pour toute interprétation de la constante $k$ ($k^{\mathbf{M}} = (k_1, k_2) \in |\mathbf{M}|$), $[f^{2n}(k)]^{\mathbf{M}} = k^{\mathbf{M}}$ et $[f^{2n+1}(k)]^{\mathbf{M}} = f^{\mathbf{M}}(k^{\mathbf{M}})$.

   (b) On considère le prédicat binaire $p \in \mathcal{P}_2$ à partir duquel pour tout entier $i \in \mathbb{N}$ et toute constante $k \in \mathcal{F}_0$, on définit la formule atomique $F_{i,k} = p(k, f^i(k))$. Compléter la structure $\mathbf{M}$ en définissant l'interprétation $p^{\mathbf{M}}$ de $p$ pour que $[\neg F_{2i,k} \wedge F_{2i+1,k}]^{\mathbf{M}} = 1$ pour tout entier $i$ et toute constante $k$.

# Corrigé de l'examen partiel du 16/03/2023

▶ Corrigé de l'exercice 1.

(1.a) et (1.b) Les occurrences de variables libres sont encadrées sur l'arbre de syntaxe abstraite de la formule $F$ (les autres occurrences sont liées) :



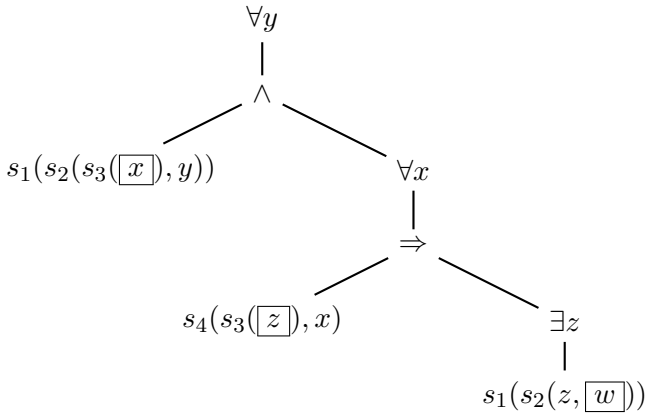

On a donc $\text{Free}(F) = \{x\}$ et $F' = \forall x\, F$.

(1.c) Les variables sous la portée du même quantificateur sont de la même couleur dans l'arbre de la question précédente, elles doivent être renommées de façon identique. Les occurrences libres de $x$ ne doivent pas être modifiées. Voici une solution :

$$F'' = ((\forall x_1\, ((\exists x_2\, p(x_2)) \wedge q(x_1, x_1))) \wedge p(x)) \Rightarrow ((\forall x_3\, q(x_3, x_3)) \wedge p(x))$$

(2.a) $s_1 \in \mathcal{P}_1$, $s_2 \in \mathcal{F}_2$, $s_3 \in \mathcal{F}_1$, $s_4 \in \mathcal{P}_2$

(2.b) Arbre de syntaxe abstraite de la formule $G$ (les variables libres sont encadrées). Cet arbre n'est pas demandé.




Les formules atomiques sont sur les feuilles de l'arbre, il s'agit donc de $s_1(s_2(s_3(x), y))$, $s_4(s_3(z), x)$ et $s_1(s_2(z, w))$.

(2.c) Les termes en paramètres des prédicats de $G$ sont $s_2(s_3(x), y)$, $s_3(z)$, $x$, et $s_2(z, w)$.

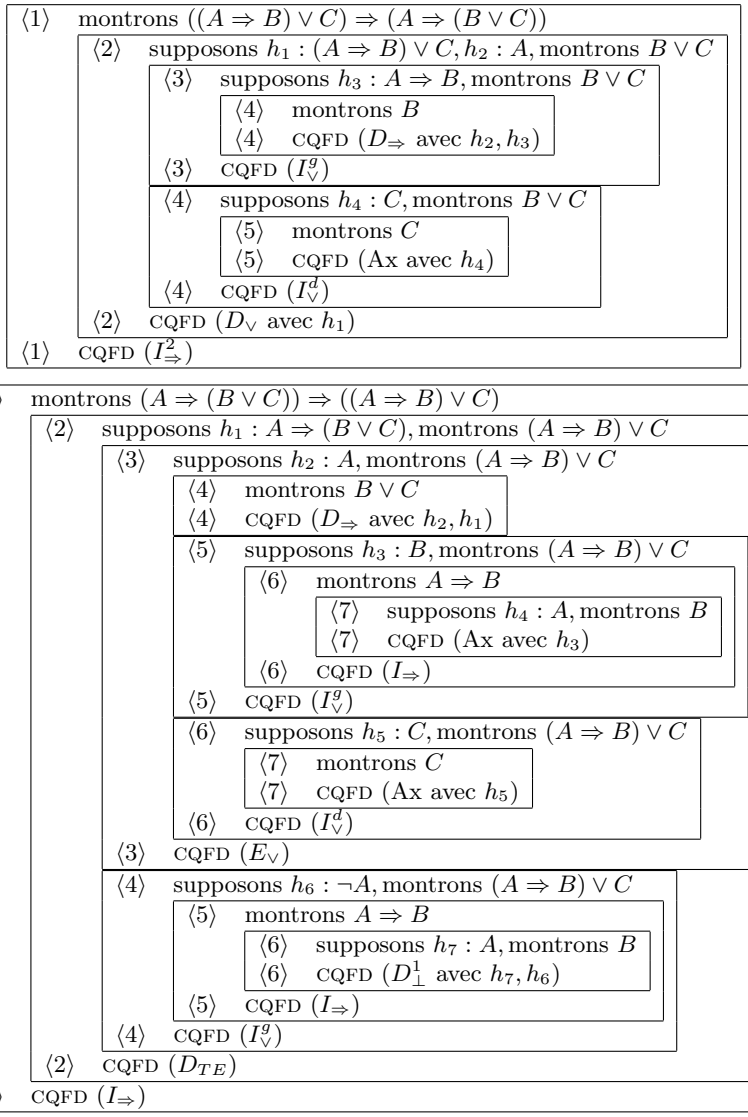
(2.d) On commence par renommer les occurrences liées de $x$ apparaissant dans une sous-formule contenant une occurrence libre de $z$. On obtient :

$$\forall y\, (s_1(s_2(s_3(x), y)) \wedge \forall x_1\, (s_4(s_3(z), x_1) \Rightarrow \exists z\, s_1(s_2(z, w))))$$

On effectue ensuite la substitution des occurrences libres de $z$. On obtient :

$$G' = \forall y\, (s_1(s_2(s_3(x), y)) \wedge \forall x_1\, (s_4(s_3(f(x)), x_1) \Rightarrow \exists z\, s_1(s_2(z, w))))$$

▶ Corrigé de l'exercice 2.







▶ Corrigé de l'exercice 3.

(1) $F_1 \not\equiv F_2$ si et seulement si pour toute structure $\mathbf{M}$, $[F_1]^{\mathbf{M}} = [F_2]^{\mathbf{M}}$.

(2.a)
$$[F_1]^{\mathbf{M}} = [A \Rightarrow B]^{\mathbf{M}} + [C]^{\mathbf{M}} = \left(\overline{[A]^{\mathbf{M}}} + [B]^{\mathbf{M}}\right) + [C]^{\mathbf{M}} = \left(\overline{\mathbf{I}_{\mathbf{M}}(A)} + \mathbf{I}_{\mathbf{M}}(B)\right) + \mathbf{I}_{\mathbf{M}}(C)$$
$$[F_2]^{\mathbf{M}} = \overline{[A]^{\mathbf{M}}} + [B \vee C]^{\mathbf{M}} = \overline{[A]^{\mathbf{M}}} + \left([B]^{\mathbf{M}} + [C]^{\mathbf{M}}\right) = \overline{\mathbf{I}_{\mathbf{M}}(A)} + (\mathbf{I}_{\mathbf{M}}(B) + \mathbf{I}_{\mathbf{M}}(C))$$

(2.b) $F_1 \not\equiv F_2$ car $[F_1]^{\mathbf{M}} \overset{E3.4}{=} [F_2]^{\mathbf{M}}$.

(2.c) $F_1$ et $F_2$ sont des formules satisfiables et non valides :

- lorsque $\mathbf{I}_{\mathbf{M}}(A) = 0$, $[F_1]^{\mathbf{M}} = [F_2]^{\mathbf{M}} = 1$
- lorsque $\mathbf{I}_{\mathbf{M}}(A) = 1$, $\mathbf{I}_{\mathbf{M}}(B) = 0$ et $\mathbf{I}_{\mathbf{M}}(C) = 0$, $[F_1]^{\mathbf{M}} = [F_2]^{\mathbf{M}} = 0$

i. $F_1 \Rightarrow \neg F_2$ est satisfiable mais n'est ni valide, ni insatisfiable (lorsque $[F_1]^{\mathbf{M}} = [F_2]^{\mathbf{M}} = 0$ on a $[F_1 \Rightarrow \neg F_2]^{\mathbf{M}} = 1$ et lorsque $[F_1]^{\mathbf{M}} = [F_2]^{\mathbf{M}} = 1$ on a $[F_1 \Rightarrow \neg F_2]^{\mathbf{M}} = 0$)

ii. $\neg F_1 \Rightarrow \neg F_2$ est valide (donc satisfiable) car $F_1 \not\equiv F_2$ et donc $\neg F_1 \not\equiv \neg F_2$ et donc $\neg F_1 \not\models \neg F_2$

iii. $\neg F_1 \wedge F_2$ est insatisfiable (donc ni valide ni satisfiable) car $F_1 \not\models\!\models F_2$ et donc, pour toute structure $\mathbf{M}$, $[\neg F_1 \wedge F_2]^{\mathbf{M}} = \overline{[F_1]^{\mathbf{M}}} \cdot [F_1]^{\mathbf{M}} = 0$

iv. $\neg F_1 \wedge \neg F_2$ est satisfiable mais n'est ni valide, ni insatisfiable (lorsque $[F_1]^{\mathbf{M}} = [F_2]^{\mathbf{M}} = 0$ on a $[\neg F_1 \wedge \neg F_2]^{\mathbf{M}} = 1$ et lorsque $[F_1]^{\mathbf{M}} = [F_2]^{\mathbf{M}} = 1$ on a $[\neg F_1 \wedge \neg F_2]^{\mathbf{M}} = 0$)

(3) $\mathtt{ite}(F_1, F_2, F_3) \models\!\models (F_1 \wedge F_2) \vee (\neg F_1 \wedge F_3)$

(3.a) $[\mathtt{ite}(F_1, F_2, F_3)]^{\mathbf{M}} = ([F_1]^{\mathbf{M}} \cdot [F_2]^{\mathbf{M}}) + (\overline{[F_1]^{\mathbf{M}}} \cdot [F_3]^{\mathbf{M}})$

(3.b) Soit $\mathbf{M}$ une structure.

- si $[F_1]^{\mathbf{M}} = 1$ alors $[\mathtt{ite}(F_1, F_2, F_3)]^{\mathbf{M}} = (1 \cdot [F_2]^{\mathbf{M}} t) + (0 \cdot [F_3]^{\mathbf{M}}) = [F_2]^{\mathbf{M}} + 0 = [F_2]^{\mathbf{M}}$
- si $[F_1]^{\mathbf{M}} = 0$ alors $[\mathtt{ite}(F_1, F_2, F_3)]^{\mathbf{M}} = (0 \cdot [F_2]^{\mathbf{M}}) + (1 \cdot [F_3]^{\mathbf{M}}) = 0 + [F_3]^{\mathbf{M}} = [F_3]^{\mathbf{M}}$

(3.c) **Les justifications ne sont pas demandées aux étudiants**.

i. On veut $([F_i]^{\mathbf{M}} \cdot [F_j]^{\mathbf{M}}) + (\overline{[F_i]^{\mathbf{M}}} \cdot [F_k]^{\mathbf{M}}) = [F_1]^{\mathbf{M}} \cdot [F_2]^{\mathbf{M}}$ pour toute structure $\mathbf{M}$. Posons $F_i = F_1$, $F_j = F_2$ et $F_k = \mathsf{false}$, on obtient

$$\begin{aligned}([F_i]^{\mathbf{M}} \cdot [F_j]^{\mathbf{M}}) + (\overline{[F_i]^{\mathbf{M}}} \cdot [F_k]^{\mathbf{M}}) &= ([F_1]^{\mathbf{M}} \cdot [F_2]^{\mathbf{M}}) + (\overline{[F_1]^{\mathbf{M}}} \cdot [\mathsf{false}]^{\mathbf{M}}) \\ &= ([F_1]^{\mathbf{M}} \cdot [F_2]^{\mathbf{M}}) + (\overline{[F_1]^{\mathbf{M}}} \cdot 0) \\ &= [F_1]^{\mathbf{M}} \cdot [F_2]^{\mathbf{M}}\end{aligned}$$

On a donc $(F_1 \wedge F_2) \models\!\models \mathtt{ite}(F_1, F_2, \mathsf{false})$

ii. On veut $([F_i]^{\mathbf{M}} \cdot [F_j]^{\mathbf{M}}) + (\overline{[F_i]^{\mathbf{M}}} \cdot [F_k]^{\mathbf{M}}) = [F_1]^{\mathbf{M}} + [F_2]^{\mathbf{M}}$ pour toute structure $\mathbf{M}$. Posons $F_i = F_1$, $F_j = \mathsf{true}$ et $F_k = F_2$, on obtient

$$\begin{aligned}([F_i]^{\mathbf{M}} \cdot [F_j]^{\mathbf{M}}) + (\overline{[F_i]^{\mathbf{M}}} \cdot [F_k]^{\mathbf{M}}) &= ([F_1]^{\mathbf{M}} \cdot [\mathsf{true}]^{\mathbf{M}}) + (\overline{[F_1]^{\mathbf{M}}} \cdot [F_2]^{\mathbf{M}}) \\ &= ([F_1]^{\mathbf{M}} \cdot 1) + (\overline{[F_1]^{\mathbf{M}}} \cdot [F_2]^{\mathbf{M}})) \\ &= [F_1]^{\mathbf{M}} + (\overline{[F_1]^{\mathbf{M}}} \cdot [F_2]^{\mathbf{M}}) \\ &= ([F_1]^{\mathbf{M}} + \overline{[F_1]^{\mathbf{M}}}) \cdot ([F_1]^{\mathbf{M}} + [F_2]^{\mathbf{M}}) \\ &= 1 \cdot ([F_1]^{\mathbf{M}} + [F_2]^{\mathbf{M}}) \\ &= [F_1]^{\mathbf{M}} + [F_2]^{\mathbf{M}}\end{aligned}$$

On a donc $(F_1 \vee F_2) \models\!\models \mathtt{ite}(F_1, \mathsf{true}, F_2)$

iii. On veut $([F_i]^{\mathbf{M}} \cdot [F_j]^{\mathbf{M}}) + (\overline{[F_i]^{\mathbf{M}}} \cdot [F_k]^{\mathbf{M}}) = \overline{[F]^{\mathbf{M}}}$ pour toute structure $\mathbf{M}$. Posons $F_i = F$, $F_j = \mathsf{false}$ et $F_k = \mathsf{true}$, on obtient

$$\begin{aligned}([F_i]^{\mathbf{M}} \cdot [F_j]^{\mathbf{M}}) + (\overline{[F_i]^{\mathbf{M}}} \cdot [F_k]^{\mathbf{M}}) &= ([F]^{\mathbf{M}} \cdot [\mathsf{false}]^{\mathbf{M}}) + (\overline{[F]^{\mathbf{M}}} \cdot [\mathsf{true}]^{\mathbf{M}}) \\ &= ([F]^{\mathbf{M}} \cdot 0) + (\overline{[F]^{\mathbf{M}}} \cdot 1)) \\ &= 0 + \overline{[F]^{\mathbf{M}}} = \overline{[F]^{\mathbf{M}}}\end{aligned}$$

On a donc $\neg F \models\!\models \mathtt{ite}(F, \mathsf{false}, \mathsf{true})$

iv. On veut $([F_i]^{\mathbf{M}} \cdot [F_j]^{\mathbf{M}}) + (\overline{[F_i]^{\mathbf{M}}} \cdot [F_k]^{\mathbf{M}}) = \overline{[F_1]^{\mathbf{M}}} + [F_2]^{\mathbf{M}}$ pour toute structure $\mathbf{M}$. Posons $F_i = F_1$, $F_j = F_2$ et $F_k = \mathsf{true}$, on obtient

$$\begin{aligned}([F_i]^{\mathbf{M}} \cdot [F_j]^{\mathbf{M}}) + (\overline{[F_i]^{\mathbf{M}}} \cdot [F_k]^{\mathbf{M}}) &= ([F_1]^{\mathbf{M}} \cdot [F_2]^{\mathbf{M}}) + (\overline{[F_1]^{\mathbf{M}}} \cdot [\mathsf{true}]^{\mathbf{M}}) \\ &= ([F_1]^{\mathbf{M}} \cdot [F_2]^{\mathbf{M}}) + (\overline{[F_1]^{\mathbf{M}}} \cdot 1) \\ &= ([F_1]^{\mathbf{M}} \cdot [F_2]^{\mathbf{M}}) + \overline{[F_1]^{\mathbf{M}}} \\ &= ([F_1]^{\mathbf{M}} + \overline{[F_1]^{\mathbf{M}}}) \cdot ([F_2]^{\mathbf{M}} + \overline{[F_1]^{\mathbf{M}}}) \\ &= 1 \cdot (\overline{[F_1]^{\mathbf{M}}} + [F_2]^{\mathbf{M}}) \\ &= \overline{[F_1]^{\mathbf{M}}} + [F_2]^{\mathbf{M}}\end{aligned}$$

On a donc $(F_1 \Rightarrow F_2) \models\!\models \texttt{ite}(F_1, F_2, \texttt{true})$

▶ Corrigé de l'exercice 4.
(1) Définition inductive de $\mathcal{T}_0(\mathcal{F})$ :
- si $k \in \{a, b, c\}$ alors $k \in \mathcal{T}_0(\mathcal{F})$;
- si $t \in \mathcal{T}_0(\mathcal{F})$, alors $f(t) \in \mathcal{T}_0(\mathcal{F})$

(2) Pour montrer $\mathcal{T}_0(\mathcal{F}) = \bigcup_{n\in\mathbb{N}}\{f^n(k)\}$, il suffit de montrer la double inclusion.
($\subseteq$) Pour montrer que $\mathcal{T}_0(\mathcal{F}) \subseteq \bigcup_{n\in\mathbb{N}}\{f^n(k)\}$, nous montrons $t \in \bigcup_{n\in\mathbb{N}}\{f^n(k)\}$ par induction sur $t$. Si $t = k \in \mathcal{F}_0$ alors on a $t = f^0(k)$ ce qui permet de conclure, sinon, $t = f(t')$ et, par hypothèse d'induction, $t' \in \bigcup_{n\in\mathbb{N}}\{f^n(k)\}$. Il existe donc un entier $m$ tel $t' = f^m(k)$ et on obtient alors $t = f(t') = f(f^m(k)) = f^{m+1}(k)$ ce qui permet de conclure.
($\supseteq$) Pour montrer $\bigcup_{n\in\mathbb{N}}\{f^n(k)\} \subseteq \mathcal{T}_0(\mathcal{F})$, il suffit de montrer que pour tout entier $m$, $f^m(k) \in \mathcal{T}_0(\mathcal{F})$. On procède par récurrence sur $m$. Si $m = 0$, alors $f^0(k) = k \in \mathcal{T}_0(\mathcal{F})$, puisque $k$ est un symbole de constante. Supposons que $f^m(k) \in \mathcal{T}_0(\mathcal{F})$, et montrons que $f^{m+1}(k) \in \mathcal{T}_0(\mathcal{F})$. On a $f^{m+1}(k) = f(f^m(k))$ et puisque $f^m(k) \in \mathcal{T}_0(\mathcal{F})$ et $f$ est un symbole de fonction d'arité 1, on a bien $f^{m+1}(k) \in \mathcal{T}_0(\mathcal{F})$.

(3.a) par récurrence sur $n$

- (B) $n = 0$, $[f^0(k)]^{\mathbf{M}} = [k]^{\mathbf{M}} = k^{\mathbf{M}}$ et $[f^1(k)]^{\mathbf{M}} = [f(f^0(k))]^{\mathbf{M}} = f^{\mathbf{M}}([f^0(k)]^{\mathbf{M}}) = f^{\mathbf{M}}(k^{\mathbf{M}})$
- (I) Soit $n$ un entier, en supposant, par hypothèse de récurrence, que $[f^{2n}(k)]^{\mathbf{M}} = k^{\mathbf{M}}$ et $[f^{2n+1}(k)]^{\mathbf{M}} = f^{\mathbf{M}}(k^{\mathbf{M}})$ il vient :

$$\begin{aligned}[f^{2*(n+1)}(k)]^{\mathbf{M}} &= [f^{(2n+1)+1}(k)]^{\mathbf{M}} = [f(f^{2n+1}(k))]^{\mathbf{M}} = f^{\mathbf{M}}([f^{2n+1}(k)]^{\mathbf{M}}) \\ &= f^{\mathbf{M}}(f^{\mathbf{M}}(k^{\mathbf{M}})) \\ &= f^{\mathbf{M}}(f^{\mathbf{M}}(k_1, k_2)) = f^{\mathbf{M}}(k_2, k_1) = (k_1, k_2) = k^{\mathbf{M}}\end{aligned}$$

$$[f^{2*(n+1)+1}(k)]^{\mathbf{M}} = [f(f^{2*(n+1)}(k))]^{\mathbf{M}} = f^{\mathbf{M}}([f^{2*(n+1)}(k)]^{\mathbf{M}}) = f^{\mathbf{M}}(k^{\mathbf{M}})$$

(3.b)

$$\begin{aligned}[\neg F_{2i,k} \wedge F_{2i+1,k}]^{\mathbf{M}} &= \underline{[\neg F_{2i,k}]^{\mathbf{M}}} \cdot \underline{[F_{2i+1,k}]^{\mathbf{M}}} = [\neg p(k, f^{2i}(k)]^{\mathbf{M}} \cdot [p(k, f^{2i+1}(k)]^{\mathbf{M}} \\ &= \overline{[p(k, f^{2i}(k)]^{\mathbf{M}}} \cdot [p(k, f^{2i+1}(k)]^{\mathbf{M}}\end{aligned}$$

On veut $\overline{[p(k, f^{2i}(k)]^{\mathbf{M}}} \cdot [p(k, f^{2i+1}(k)]^{\mathbf{M}} = 1$ c-à-d $[p(k, f^{2i}(k)]^{\mathbf{M}} = 0$ et $[p(k, f^{2i+1}(k)]^{\mathbf{M}} = 1$. Posons $k^{\mathbf{M}} = (k_1, k_2) \in |\mathbf{M}|$ $(k_1 \neq k_2)$, il faut donc :

$$\begin{aligned}&\big([k]^{\mathbf{M}}, [f^{2i}(k)]^{\mathbf{M}}\big) = \big(k^{\mathbf{M}}, k^{\mathbf{M}}\big) = ((k_1, k_2), (k_1, k_2)) \notin p^{\mathbf{M}} \\ \text{et} \quad &\big([k]^{\mathbf{M}}, [f^{2i+1}(k)]^{\mathbf{M}}\big) = \big(k^{\mathbf{M}}, f^{\mathbf{M}}(k^{\mathbf{M}})\big) = ((k_1, k_2), (k_2, k_1)) \in p^{\mathbf{M}}\end{aligned}$$

Puisque $k_1 \neq k_2$, on peut choisir $p^{\mathbf{M}} = \{(x, y) \mid x \neq y\}$.