

Examen 1ère session du 09/01/2019

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. Le 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. Expliquer pourquoi la formule $\forall x (p(f(x), y) \Rightarrow q(y, f(x, y)))$ n'est pas syntaxiquement correcte.
2. Le schéma de raisonnement par récurrence sur les entiers peut s'écrire :

$$\forall P ((P(0) \wedge \forall n (P(n) \Rightarrow P(\text{plus}(n, 1)))) \Rightarrow \forall n P(n))$$

où plus est la fonction d'addition sur les entiers. Expliquer pourquoi la formule ci-dessus n'est pas une formule de $\mathcal{IF}(X, \mathcal{F}, \mathcal{P})$.

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

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 :

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

1. Calculer $[\odot^5(k_3)]^{\mathbf{M}}$.
2. Montrer (par récurrence sur n) que $[\odot^n(k_m)]^{\mathbf{M}} = (m, m + n)$.
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+1)=6 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 B est valide, a-t-on nécessairement $A \models A \Rightarrow B$? Si oui, en donner une démonstration, si non donner un contre-exemple.
3. Soit F la formule $B \Rightarrow (A \Rightarrow (A \Rightarrow B))$.
 - (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 une formule valide (indiquer à chaque étape le nom de l'équivalence utilisée).
- (c) En utilisant les règles de la déduction naturelle, montrer que F est une formule prouvable.

Exercice 4 (7 points)

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

$$(\forall x (p(x) \Rightarrow \neg q(x))) \Rightarrow \neg \exists x (p(x) \wedge q(x))$$

Exercice 5 (1+4+(1+6)=12 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. Formellement ce prédicat désigne une relation d'équivalence qui est une congruence pour f , c-à-d vérifie les quatre formules suivantes :

$$\begin{array}{ll} (F_1) & \forall x \text{eq}(x, x) \quad (\text{réflexivité}) \\ (F_2) & \forall x \forall y (\text{eq}(x, y) \Rightarrow \text{eq}(y, x)) \quad (\text{symétrie}) \\ (F_3) & \forall x \forall y \forall z ((\text{eq}(x, y) \wedge \text{eq}(y, z)) \Rightarrow \text{eq}(x, z)) \quad (\text{transitivité}) \\ (F_4) & \forall x \forall y (\text{eq}(x, y) \Rightarrow \text{eq}(f(x), f(y))) \quad (\text{congruence}) \end{array}$$

On considère la formule $F = \forall x_1 \forall x_2 (\text{eq}(f(x_1), f(x_2)) \Rightarrow \text{eq}(x_1, x_2))$ exprimant que la fonction f est injective.

- 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.
- 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).
- On considère la formule $F_5 = \forall x \text{eq}(x, f(f(x)))$ exprimant que la fonction f est involutive.
 - Définir une structure \mathbf{M}_3 telle que $\text{eq}^{\mathbf{M}_3} = \{(m, m) \mid m \in |\mathbf{M}_3|\}$ et $[F_5]_v^{\mathbf{M}_3} = 1$ (quelle que soit la valuation v). Justifier votre réponse.
 - En utilisant les règles de la déduction naturelle, montrer que toute fonction involutive est injective, c-à-d que la formule F est prouvable à partir des hypothèses F_1, F_2, F_3, F_4 et F_5 . Concrètement, il s'agit de compléter la preuve suivante :

$\langle 1 \rangle$ supposons $h_1 : F_1, h_2 : F_2, h_3 : F_3, h_4 : F_4, h_5 : F_5$ montrons F <div style="border: 1px solid black; padding: 5px; margin: 5px auto; width: 80%;"> ... à compléter ... </div>
$\langle 1 \rangle$ CQFD (?)

Afin d'alléger la preuve, on pourra utiliser les trois règles dérivées suivantes qui permettent d'éliminer un, deux ou trois quantificateurs universels (simultanément) en tête d'une formule à partir d'une hypothèse pour prouver une formule.

$\langle i \rangle$ supposons $h_1 : A_1, \dots, h_n : A_n, h : \forall x A$ montrons $A[x := t_1]$	$\langle i \rangle$ supposons $h_1 : A_1, \dots, h_n : A_n, h : \forall x \forall y A$ montrons $A[x := t_1][y := t_2]$
$\langle i \rangle$ CQFD (D_{\forall}^1 avec h)	$\langle i \rangle$ CQFD (D_{\forall}^2 avec h)

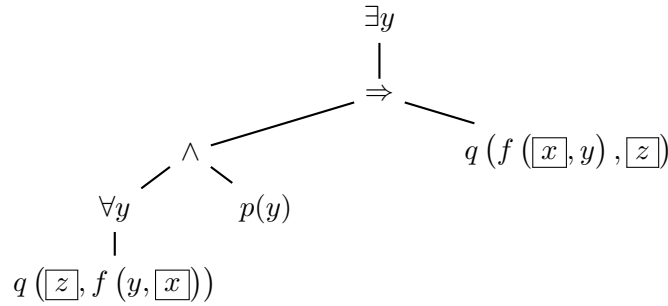
$\langle i \rangle$ supposons $h_1 : A_1, \dots, h_n : A_n, h : \forall x \forall y \forall z A$ montrons $A[x := t_1][y := t_2][z := t_3]$
$\langle i \rangle$ CQFD (D_{\forall}^3 avec h)

Indication. Il s'agit de formaliser le raisonnement suivant : si $f(x_1) = f(x_2)$, alors en appliquant f des deux côtés de l'égalité on obtient $f(f(x_1)) = f(f(x_2))$ et puisque f est involutive on a $f(f(x_1)) = x_1$ et $f(f(x_2)) = x_2$ et donc $x_1 = x_2$.

Corrigé de l'examen 1ère session du 09/01/2019

► CORRIGÉ DE L'EXERCICE 1.

1. Dans la formule atomique $p(f(x), y)$ qui figure à gauche de l'implication, f est un symbole de fonction d'arité 1, mais ce symbole est utilisé comme un symbole de fonction d'arité 2 dans la formule atomique $q(y, f(x, y))$ qui figure à droite de l'implication.
2. Dans la formule, le symbole de prédicat P 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 y apparaît dans le terme $g(x, y, z)$, pour calculer $F[x := g(x, y, z)]$ il faut renommer les occurrences liées de y dans la formule F . On peut utiliser deux symboles de variable différents pour le renommage puisque y est dans la portée de deux quantificateurs différents :

$$\exists w_1 (((\forall w_2 q(z, f(w_2, x))) \wedge p(w_1)) \Rightarrow q(f(x, w_1), z))$$

On peut à présent appliquer la substitution pour obtenir la formule :

$$\exists w_1 (((\forall w_2 q(z, f(w_2, g(x, y, z)))) \wedge p(w_1)) \Rightarrow q(f(g(x, y, z), w_1), z))$$

Puisque $y \notin \text{Free}(F)$, on a $F[y := g(x, y, z)] = F$.

► CORRIGÉ DE L'EXERCICE 2.

1.
$$\begin{aligned} [\odot^5(k_3)]^{\mathbf{M}} &= \odot^{\mathbf{M}}(\odot^{\mathbf{M}}(\odot^{\mathbf{M}}(\odot^{\mathbf{M}}(\odot^{\mathbf{M}}(k_3^{\mathbf{M}})))) = \odot^{\mathbf{M}}(\odot^{\mathbf{M}}(\odot^{\mathbf{M}}(\odot^{\mathbf{M}}(\odot^{\mathbf{M}}((3, 3))))) \\ &= \odot^{\mathbf{M}}(\odot^{\mathbf{M}}(\odot^{\mathbf{M}}(\odot^{\mathbf{M}}((3, 4))))) = \odot^{\mathbf{M}}(\odot^{\mathbf{M}}(\odot^{\mathbf{M}}((3, 5)))) = \odot^{\mathbf{M}}(\odot^{\mathbf{M}}((3, 6))) = \odot^{\mathbf{M}}((3, 7)) \\ &= (3, 8) \end{aligned}$$
2. Par récurrence sur n . Pour $n = 0$, on a bien $[\odot^0(k_m)]^{\mathbf{M}} = [k_m]^{\mathbf{M}} = (m, m) = (m, m + 0)$. Supposons, par hypothèse de récurrence, que $[\odot^n(k_m)]^{\mathbf{M}} = (m, m + n)$. On a bien :
$$[\odot^{n+1}(k_m)]^{\mathbf{M}} = \odot^{\mathbf{M}}([\odot^n(k_m)]^{\mathbf{M}}) = \odot^{\mathbf{M}}((m, m + n)) = (m, m + n + 1)$$
3. Puisque $[\odot^n(k_m)]^{\mathbf{M}} = (m, m + n)$, lorsque $(m, m + n) = (n_1, n_2)$ on a $m = n_1$ et $n_2 = m + n = n_1 + n$ et donc $n = n_2 - n_1$. On a donc $[\odot^{n_2 - n_1}(k_{n_1})]^{\mathbf{M}} = (n_1, n_2)$. Aussi, lorsque $n_1 \leq n_2$ (et donc $n_2 - n_1 \in \mathbb{N}$) le terme $t = \odot^{n_2 - n_1}(k_{n_1})$ est tel que $[t]^{\mathbf{M}} = (n_1, n_2)$.
4. Par induction sur t . Si $t = k_i \in \mathcal{F}_0$, alors $[k_i]^{\mathbf{M}} = (i, i)$ et on peut conclure puisque $i \leq i$. Si $t = \odot(t')$, alors $[\odot(t')]^{\mathbf{M}} = \odot^{\mathbf{M}}([t']^{\mathbf{M}}) = \odot^{\mathbf{M}}((n'_1, n'_2)) = (n'_1, n'_2 + 1)$ où $(n'_1, n'_2) = [t']^{\mathbf{M}}$ et puisque, par hypothèse d'induction $n'_1 \leq n'_2$ on a bien $n'_1 \leq n'_2 + 1$.

► 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. Oui. En effet, supposons que B est valide (c-à-d que $\mathbf{I}_{\mathbf{M}}(B) = 1$ pour toute structure \mathbf{M}) et montrons que $A \models A \Rightarrow B$. Soit \mathbf{M} une structure telle que $[A]^{\mathbf{M}} = 1$, on montre que $[A \Rightarrow B]^{\mathbf{M}} = 1$:

$$[A \Rightarrow B]^{\mathbf{M}} = \overline{[A]^{\mathbf{M}}} + [B]^{\mathbf{M}} = \overline{\mathbf{I}_{\mathbf{M}}(A)} + \mathbf{I}_{\mathbf{M}}(B) = \overline{\mathbf{I}_{\mathbf{M}}(A)} + 1 \stackrel{(E3.7)}{=} 1$$

$$\begin{aligned} 3.a. \quad [F]^{\mathbf{M}} &= \overline{[B]^{\mathbf{M}}} + [(A \Rightarrow (A \Rightarrow B))^{\mathbf{M}}] = \overline{[B]^{\mathbf{M}}} + (\overline{[A]^{\mathbf{M}}} + [A \Rightarrow B]^{\mathbf{M}}) \\ &= \overline{[B]^{\mathbf{M}}} + (\overline{[A]^{\mathbf{M}}} + (\overline{[A]^{\mathbf{M}}} + [B]^{\mathbf{M}})) = \overline{\mathbf{I}_{\mathbf{M}}(B)} + (\overline{\mathbf{I}_{\mathbf{M}}(A)} + (\overline{\mathbf{I}_{\mathbf{M}}(A)} + \mathbf{I}_{\mathbf{M}}(B))) \end{aligned}$$

3.b. Posons $x = \mathbf{I}_{\mathbf{M}}(A)$ et $y = \mathbf{I}_{\mathbf{M}}(B)$.

$$\begin{aligned} [F]^{\mathbf{M}} &= \overline{y} + (\overline{x} + (\overline{x} + y)) \stackrel{(E3.4)}{=} \overline{y} + ((\overline{x} + \overline{x}) + y) \stackrel{(E3.5)}{=} \overline{y} + (\overline{x} + y) \\ &\stackrel{(E3.1)}{=} (\overline{x} + y) + \overline{y} \stackrel{(E3.4)}{=} \overline{x} + (y + \overline{y}) \stackrel{(E1.4)}{=} \overline{x} + 1 \stackrel{(E3.7)}{=} 1 \end{aligned}$$

3.c

(1) montrons $B \Rightarrow (A \Rightarrow (A \Rightarrow B))$
(2) supposons $h_1 : B$, montrons $A \Rightarrow (A \Rightarrow B)$
(3) supposons $h_2 : A$, montrons $A \Rightarrow B$
(4) supposons $h_3 : A$, montrons B c'est l'hypothèse h_1
(4) CQFD (Ax)
(3) CQFD (I_{\Rightarrow})
(2) CQFD (I_{\Rightarrow})
(1) CQFD (I_{\Rightarrow})

► CORRIGÉ DE L'EXERCICE 4.

(1) montrons $(\forall x (p(x) \Rightarrow \neg q(x))) \Rightarrow \neg \exists x (p(x) \wedge q(x))$
(2) supposons $h_1 : \forall x (p(x) \Rightarrow \neg q(x))$, montrons $\neg \exists x (p(x) \wedge q(x))$
(3) supposons $h_2 : \exists x (p(x) \wedge q(x))$, montrons false
(4) montrons $\exists x (p(x) \wedge q(x))$ c'est l'hypothèse h_2
(4) CQFD (Ax)
(5) soit une nouvelle variable y , supposons $h_3 : p(y) \wedge q(y)$, montrons false
(6) montrons $\neg q(y)$
(7) montrons $p(y) \Rightarrow \neg q(y)$
(8) montrons $\forall x (p(x) \Rightarrow \neg q(x))$ c'est l'hypothèse h_1
(8) CQFD (Ax)
(7) CQFD (E_{\forall})
(8) montrons $p(y)$
(9) montrons $p(y) \wedge q(y)$ c'est l'hypothèse h_3
(9) CQFD (Ax)
(8) CQFD (E_{\wedge}^g)
(6) CQFD (E_{\Rightarrow})
(7) montrons $q(y)$
(8) montrons $p(y) \wedge q(y)$ c'est l'hypothèse h_3
(8) CQFD (Ax)
(7) CQFD (E_{\wedge}^d)
(5) CQFD (E_{-})
(3) CQFD (E_{\exists})
(2) CQFD (I_{-})
(1) CQFD (I_{\Rightarrow})

► CORRIGÉ DE L'EXERCICE 5.

1. Il suffit de considérer la fonction $x \mapsto x^2$ définie sur \mathbb{Z} qui n'est pas injective (puisque par exemple $(-1)^2 = 1^2$ mais $-1 \neq 1$). 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 $m_1 \in \mathbf{M}_2$:

$$[\forall x_2 (\text{eq}(f(x_1), f(x_2)) \Rightarrow \text{eq}(x_1, x_2))]_{v[x_1 \leftarrow m_1]}^{\mathbf{M}_2} = 1$$

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

$$[\forall x_2 (\text{eq}(f(x_1), f(x_2)) \Rightarrow \text{eq}(x_1, x_2))]_{v[x_1 \leftarrow a]}^{\mathbf{M}_2} = 1$$

De même $[\forall x_2 (\text{eq}(f(x_1), f(x_2)) \Rightarrow \text{eq}(x_1, x_2))]_{v[x_1 \leftarrow a]}^{\mathbf{M}_2} = 1$ si et seulement si pour chaque $m_2 \in \mathbf{M}_2$:

$$[\text{eq}(f(x_1), f(x_2)) \Rightarrow \text{eq}(x_1, x_2)]_{v[x_1 \leftarrow a][x_2 \leftarrow m_2]}^{\mathbf{M}_2} = 1$$

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

$$[\text{eq}(f(x_1), f(x_2)) \Rightarrow \text{eq}(x_1, x_2)]_{v[x_1 \leftarrow a][x_2 \leftarrow a]}^{\mathbf{M}_2} = 1$$

Puisque $([x_1]_{v[x_1 \leftarrow a][x_2 \leftarrow a]}^{\mathbf{M}_2}, [x_2]_{v[x_1 \leftarrow a][x_2 \leftarrow a]}^{\mathbf{M}_2}) = (a, a) \in \text{eq}^{\mathbf{M}_2}$, on peut alors conclure que $[F]_v^{\mathbf{M}_2} = 1$ puisque :

$$\begin{aligned} & \frac{[\text{eq}(f(x_1), f(x_2)) \Rightarrow \text{eq}(x_1, x_2)]_{v[x_1 \leftarrow a][x_2 \leftarrow a]}^{\mathbf{M}_2}}{[\text{eq}(f(x_1), f(x_2))]_{v[x_1 \leftarrow a][x_2 \leftarrow a]}^{\mathbf{M}_2} + [\text{eq}(x_1, x_2)]_{v[x_1 \leftarrow a][x_2 \leftarrow a]}^{\mathbf{M}_2}} \\ &= \frac{[\text{eq}(f(x_1), f(x_2))]_{v[x_1 \leftarrow a][x_2 \leftarrow a]}^{\mathbf{M}_2}}{[\text{eq}(f(x_1), f(x_2))]_{v[x_1 \leftarrow a][x_2 \leftarrow a]}^{\mathbf{M}_2} + 1} \stackrel{(E3.7)}{=} 1 \end{aligned}$$

3.a. Il suffit de considérer la fonction $x \mapsto \bar{x}$ définie sur l'ensemble \mathbb{B} des booléens qui est involutive (puisque $\bar{\bar{x}} = x$). Formellement, on considère donc la structure \mathbf{M}_3 de domaine $|\mathbf{M}_3| = \mathbb{B}$ telle que $f^{\mathbf{M}_3}(b) = \bar{b}$.

3.b.

⟨1⟩	supposons $h_1 : F_1, h_2 : F_2, h_3 : F_3, h_4 : F_4, h_5 : F_5$, montrons F
⟨2⟩	soit une nouvelle variable w_1 , montrons $\forall x_2 (eq(f(w_1), f(x_2)) \Rightarrow eq(w_1, x_2))$
⟨3⟩	soit une nouvelle variable w_2 , montrons $eq(f(w_1), f(w_2)) \Rightarrow eq(w_1, w_2)$
⟨4⟩	supposons $h_6 : eq(f(w_1), f(w_2))$, montrons $eq(w_1, w_2)$
⟨5⟩	montrons $(eq(w_1, f(f(w_1))) \wedge eq(f(f(w_1)), w_2)) \Rightarrow eq(w_1, w_2)$
⟨5⟩	CQFD (D_{\forall}^3 avec h_3)
⟨6⟩	montrons $eq(w_1, f(f(w_1))) \wedge eq(f(f(w_1)), w_2)$
⟨7⟩	montrons $eq(w_1, f(f(w_1)))$
⟨7⟩	CQFD (D_{\forall}^1 avec h_5)
⟨8⟩	montrons $eq(f(f(w_1)), w_2)$
⟨9⟩	montrons $(eq(f(f(w_1)), f(f(w_2))) \wedge eq(f(f(w_2)), w_2)) \Rightarrow eq(f(f(w_1)), w_2)$
⟨9⟩	CQFD (D_{\forall}^3 avec h_3)
⟨10⟩	montrons $eq(f(f(w_1)), f(f(w_2))) \wedge eq(f(f(w_2)), w_2)$
⟨11⟩	montrons $eq(f(f(w_1)), f(f(w_2)))$
⟨12⟩	montrons $eq(f(w_1), f(w_2)) \Rightarrow eq(f(f(w_1)), f(f(w_2)))$
⟨12⟩	CQFD (D_{\forall}^2 avec h_4)
⟨13⟩	montrons $eq(f(w_1), f(w_2))$
	c'est l'hypothèse h_6
⟨13⟩	CQFD (Ax)
⟨11⟩	CQFD (E_{\Rightarrow})
⟨12⟩	montrons $eq(f(f(w_2)), w_2)$
⟨13⟩	montrons $eq(w_2, f(f(w_2))) \Rightarrow eq(f(f(w_2)), w_2)$
⟨13⟩	CQFD (D_{\forall}^2 avec h_2)
⟨14⟩	montrons $eq(w_2, f(f(w_2)))$
⟨14⟩	CQFD (D_{\forall}^1 avec h_5)
⟨12⟩	CQFD (E_{\Rightarrow})
⟨10⟩	CQFD (I_{\wedge})
⟨8⟩	CQFD (E_{\Rightarrow})
⟨6⟩	CQFD (I_{\wedge})
⟨4⟩	CQFD (E_{\Rightarrow})
⟨3⟩	CQFD (I_{\Rightarrow})
⟨2⟩	CQFD (I_{\forall})
⟨1⟩	CQFD (I_{\forall})