Outils Logiques - 2018-2019, Examen Session 1

Consignes *Durée: 3h. L'utilisation de tout document ou dispositif électronique est* **interdite**. *Toute réponse doit être* **justifiée** *(les réponses sans justification ne sont pas évaluées). Le* **barème** *est donné à titre indicatif.*

Exercice 1 (terminaison) [4 pnt] *Soient* $\mathbf{N} = \{0, 1, 2, \ldots\}$ *l'ensemble des nombres naturels et* $\mathbf{N}^*$ *l'ensemble des mots finis sur* $\mathbf{N}$. *Si* $n, m \in \mathbf{N}$ *alors on dénote par* $(n)^m$ *le mot sur* $\mathbf{N}^*$ *qui contient* m *fois le nombre* n. *Par exemple,* $(9)^3 = 9 \cdot 9 \cdot 9$. *On définit une relation binaire* $\rightarrow$ *sur* $\mathbf{N}^*$ *par:*

$$\rightarrow = \{(\alpha \cdot (n+1) \cdot \beta,\ \alpha \cdot (n)^{(n+1)} \cdot \beta) \mid \alpha, \beta \in \mathbf{N}^*, n \in \mathbf{N}\} \ .$$

En d'autres termes, on peut prendre un nombre positif $(n+1)$ *dans le mot et le remplacer par* $n+1$ *occurrences du nombre* n. *Par exemple, on a* $(3 \cdot 2 \cdot 4,\ 3 \cdot 1 \cdot 1 \cdot 4) \in \rightarrow$. *On écrira aussi* $\alpha \rightarrow \beta$ *pour dire* $(\alpha, \beta) \in \rightarrow$.

1. *La relation* $\rightarrow$ *est-elle transitive?*
2. *Soit* $\mathbf{N}^2$ *le produit cartésien* $\mathbf{N} \times \mathbf{N}$ *et pour* $k > 2$ *soit* $\mathbf{N}^k = \mathbf{N}^{k-1} \times \mathbf{N}$. *Rappelez la définition de l'ordre lexicographique sur* $\mathbf{N}^k$ *pour* $k = 2$ *et expliquez comment généraliser la définition pour* $k > 2$.
3. *Supposons que* $\alpha_0 \in \mathbf{N}^*$ *est un mot constitué de nombres inférieurs à* 5. *Est-ce possible de trouver une suite infinie* $\alpha_0 \rightarrow \alpha_1 \rightarrow \alpha_2 \rightarrow \cdots$ *?*
4. *Le système de réécriture* $(\mathbf{N}^*, \rightarrow)$ *termine-t-il?*

Exercice 2 (calcul des séquents) [3 pnt] *Prouvez les séquents suivants dans le calcul des séquents de Gentzen (les formules* A, B, C *sont arbitraires). Pour ce faire vous pouvez soit appliquer les règles d'inférence pour l'implication soit exprimer d'abord l'implication en fonction de la disjonction et de la négation.*

1. $\vdash A \rightarrow (B \rightarrow (A \wedge B))$.
2. $\vdash (A \vee B) \rightarrow ((A \rightarrow C) \rightarrow ((B \rightarrow C) \rightarrow C))$.
3. $(A \rightarrow C) \wedge (B \rightarrow C) \vdash (A \vee B) \rightarrow C$.

Exercice 3 (résolution) [3 pnt] *Considérons la formule* A *définie comme suit:*

$$((x \vee y) \rightarrow w) \wedge (w \rightarrow (\neg x \wedge z)) \wedge \neg(z \wedge y)$$

1. *Donnez une CNF équivalente à* A.

Ensuite, pour chacune des formules suivantes, déterminez si elle est une conséquence logique de A *en utilisant la méthode de résolution:*

2. $\neg w \wedge \neg y$,
3. $w \wedge y$.

Exercice 4 (BDD) [4 pnt] *On considère des formules booléennes sur l'ensemble des variables* $V = \{x_1, x_2, \ldots, x_n\}$*, pour* $n \geq 1$.

1. *Donnez un BDD réduit pour la fonction* $f_2(x_1, x_2) = x_1 \oplus x_2$*, où* $x_1 \oplus x_2 = (\neg x_1 \wedge x_2) \vee (x_1 \wedge \neg x_2)$.

2. *Généralisez au cas de la fonction* $f_n(x_1, \ldots, x_n) = x_1 \oplus x_2 \oplus \cdots \oplus x_n$*, en considérant l'ordre* $x_1 < x_2 < \ldots < x_n$*. Quelle est précisément la taille du BDD réduit obtenu en fonction de* n*? Existe-t-il un ordre entre les variables de* V *pour lequel le BDD réduit qui représente la fonction* f_n *est de taille exponentielle en* n *? Justifiez la réponse.*

3. *Considérons l'ensemble de variables* $V' = V \cup \{y_1, \ldots, y_n\}$*, et soit* h *la fonction*

$$h(x_1, \ldots, x_n, y_1, \ldots, y_n) = (x_1 \oplus y_1) \wedge (x_2 \oplus y_2) \wedge \ldots \wedge (x_n \oplus y_n)$$

Donnez un BDD pour h *de taille polynomiale en* n *en précisant l'ordre considéré sur les variables de* V'*. Trouvez un ordre entre les variables de* V' *pour lequel le BDD réduit pour* h *est de taille exponentielle en* n *et esquissez la structure du BDD réduit.*

Exercice 5 (CNF, méthode DP, graphes) [6,5 pnt] *Dans cet exercice, nous considérons des formules en forme normale conjonctive (CNF), écrites en utilisant la notation ensembliste. Une affectation* v *satisfait une CNF* A *si pour toute clause* $C \in A$ *il existe un littéral* $\ell \in C$ *tel que* $[\![\ell]\!]v = 1$*. Dans ce cas on dit que* A *est satisfaisable. On dit aussi qu'une affectation* v 01-satisfait *une CNF* A *si pour toute clause* $C \in A$ *ils existent deux littéraux* $\ell, \ell' \in C$ *tels que* $[\![\ell]\!]v = 1$ *et* $[\![\ell']\!]v = 0$*. Et dans ce cas on dit que* A *est 01-satisfaisable.*

1. *Soit* $A = \{\{x_1, \neg x_2\}, \{x_2, x_3\}\}$*. Donnez une affectation* v_1 *qui satisfait* A *mais qui ne 01-satisfait pas* A*, et une affectation* v_2 *qui 01-satisfait* A.

2. *Soit* A *une CNF. Peut-il exister une affectation* v *qui 01-satisfait* A *et qui ne satisfait pas* A*?*

3. *Montrez que* $A = \{\{x_1, x_2\}, \{\neg x_1, \neg x_2\}, \{x_1, \neg x_2\}\}$ *est satisfaisable mais qu'elle n'est pas 01-satisfaisable.*

Si C *est une clause soit* $\overline{C} = \{\neg\ell \mid \ell \in C\}$ *qui est aussi une clause. Si* A *est une CNF, soit* $\overline{A} = \{\overline{C} \mid C \in A\}$ *qui est aussi une CNF.*

4. *Soit* A *une CNF, et soit* A' *la CNF définie par* $A' = A \cup \overline{A}$*. Montrez que* A' *est satisfaisable si et seulement si* A *est 01-satisfaisable. Donnez une borne supérieure à la taille de* A' *en fonction de la taille de* A.

5. *Appliquez l'algorithme DP (Davis-Putnam) à la formule* $A' = A \cup \overline{A}$*, où* A *est la formule du point [1.] ci-dessus.*

On rappelle qu'un graphe non-dirigé est biparti si l'ensemble N *des noeuds peut être partitionné en deux ensembles* N_0 *et* N_1 *tels que* $N = N_0 \cup N_1$*,* $N_0 \cap N_1 = \emptyset$ *et toutes les arêtes du graphe connectent un noeud dans* N_0 *avec un noeud dans* N_1*. Soit* A *une 2-CNF, c.à.d. une CNF dont toutes les clauses possèdent exactement deux littéraux. On associe à* A *un graphe non-dirigé* G_A *dont les* noeuds *sont les littéraux qui apparaissent dans* A *et les* arêtes *sont construites d'après les deux règles suivantes: (i) si* $\{\ell, \ell'\}$ *est une clause dans la 2-CNF* A *alors* $\{\ell, \ell'\}$ *est une arête et (ii) si un littéral* ℓ *et sa négation* $\neg\ell$ *paraissent dans la 2-CNF* A *alors* $\{\ell, \neg\ell\}$ *est une arête.*

6. *Dessinez* G_A *pour la CNF* A *donnée au point [3.] ci-dessus.*

7. *Montrez qu'une formule 2-CNF* A *est 01-satisfaisable si et seulement si* G_A *est biparti.*

Solution à l'exercice 1

1. [0,5 pnt] Non. Par exemple $2 \to 11 \to 01$ mais $2 \not\to 01$.
2. [1 pnt] L'ordre lexicographique (de gauche à droite) sur $\mathbf{N}^2$ est:

$$(x, y) >_{lex} (x', y') \text{ si } x > x' \text{ ou } (x = x' \text{ et } y > y') \ .$$

   Si $>_k$ est l'ordre lexicographique sur $\mathbf{N}^k$ alors l'ordre lexicographique $>_{k+1}$ sur $\mathbf{N}^{k+1}$ est:

$$(x, y) >_{(k+1)} (x', y') \text{ si } x >_k x' \text{ ou } (x = x' \text{ et } y > y') \ .$$

   qu'on peut expliciter comme:

$$(\cdots(x_1, x_2), \cdots x_k) >_k (\cdots(y_1, y_2), \cdots y_k)$$

   si

$$\begin{array}{l} x_1 > y_1 \text{ ou} \\ x_1 = y_1 \text{ et } x_2 > y_2 \text{ ou} \\ \cdots \\ x_1 = y_1 \text{ et } x_2 = y_2 \cdots x_{k-1} = y_{k-1} \text{ et } x_k > y_k \end{array}$$

   On sait que l'ordre standard sur $\mathbf{N}$ est bien fondé et que l'ordre lexicographique sur un produit d'ordres bien fondés est encore bien fondé. Donc on peut montrer par récurrence sur k que l'ordre $>_k$ est bien fondé aussi.
3. [1,5 pnt] Soient $n \in \mathbf{N}$ et $\alpha \in \mathbf{N}^*$. On définit $occ_n(\alpha)$ comme le nombre d'occurrences de n dans α. Par exemple, $occ_3(2 \cdot 3 \cdot 2) = 1$. On définit aussi:

$$\mu(\alpha) = (((occ_4(\alpha), occ_3(\alpha)), occ_2(\alpha)), occ_1(\alpha))$$

   Si $\alpha \to \beta$ alors on remplace un nombre n dans α tel que $1 \leq n \leq 4$ par n fois $(n-1)$. On aura donc:

$$occ_4(\alpha) = occ_4(\beta), \ldots, occ_{(n+1)}(\alpha) = occ_{(n+1)}(\beta), occ_n(\alpha) = 1 + occ_n(\beta) > occ_n(\beta)$$

   Il suit que $\mu(\alpha) >_4 \mu(\beta)$. Il est donc impossible d'avoir une suite infinie $\alpha_0 \to \alpha_1 \to \cdots$ car elle impliquerait l'existence d'une suite $\mu(\alpha_0) >_4 \mu(\alpha_1) >_4 \cdots$.
4. [1 pnt] Il suffit de généraliser l'argument du point précédent. Au lieu de l'ordre $>_4$ on considère l'ordre $>_k$ où k est le plus grand nombre qui paraît dans un mot α. La fonction μ devient:

$$\mu(\alpha) = (\cdots(occ_k(\alpha), occ_{k-1}(\alpha)), \ldots, occ_1(\alpha))$$

Solution à l'exercice 2

1. [1 pnt]

$$\dfrac{\dfrac{\dfrac{A, B \vdash A \quad A, B \vdash B}{A, B \vdash (A \wedge B)}}{A \vdash (B \to (A \wedge B))}}{\vdash A \to (B \to (A \wedge B))}$$

2. [1 pnt] La première partie de la preuve est la suivante:

$$\dfrac{\dfrac{\dfrac{\dfrac{A, (A \to C), (B \to C) \vdash C \qquad B, (A \to C), (B \to C) \vdash C}{(A \vee B), (A \to C), (B \to C) \vdash C}}{(A \vee B), (A \to C) \vdash ((B \to C) \to C))}}{(A \vee B) \vdash ((A \to C) \to ((B \to C) \to C))}}{\vdash (A \vee B) \to ((A \to C) \to ((B \to C) \to C))}$$

Ensuite il reste à prouver deux séquents dont la forme est similaire. On considère celui à gauche:

$$\frac{A, C, (B \to C) \vdash C \qquad A, (B \to C) \vdash A, C}{A, (A \to C), (B \to C) \vdash C}$$

3. [1 pnt] Le séquent est logiquement équivalent au séquent de la question 2 et après 2 inférences on se réduit à une permutation près à un séquent prouvé dans le cas précédent.

$$\cfrac{\cfrac{(A \to C), (B \to C), (A \vee B) \vdash C}{(A \to C), (B \to C) \vdash (A \vee B) \to C}}{(A \to C) \wedge (B \to C) \vdash (A \vee B) \to C}$$

Solution à l'exercice 3

1. [1 pnt] En remplaçant $A \to B$ par $\neg A \vee B$ et en appliquant les lois de de Morgan et de distribution, on dérive que A est équivalente à la conjonction des clauses suivantes:

$$C_1 = \{\neg x, w\}, C_2 = \{\neg y, w\}, C_3 = \{\neg x, \neg w\}, C_4 = \{\neg w, z\}, C_5 = \{\neg y, \neg z\},$$

2. [1 pnt] On rappelle que dans ce cas B est une conséquence logique de A ssi $A \to B$ est valide ssi $A \wedge \neg B$ est réfutable ssi la méthode de résolution dérive la clause vide à partir d'une CNF équivalente à $A \wedge \neg B$. Si $B = \neg y \wedge \neg w$ alors $\neg B$ est équivalente à la clause $C_6 = \{y, w\}$. Ensuite on applique la méthode de résolution. Comme $\neg x$ est monotone on se réduit à:

$$\{C_2, C_4, C_5, C_6\}$$

On peut résoudre z et obtenir:

$$\{C_2, \{\neg y, \neg w\}, C_6\}$$

On peut résoudre w et obtenir:

$$\{\{\neg y\}\}$$

et par monotonicité on derive la CNF vide, donc satisfaisable, donc pas consequence logique.

3. [1 pnt] Dans ce cas $C_6 = \{\neg y, \neg w\}$. Par le même argument on se réduit à:

$$\{C_2, \{\neg y, \neg w\}, C_6\} = \{\{\neg y, w\}, \{\neg y, \neg w\}, \{\neg y, \neg w\}\}$$

et comme $\neg y$ est monotone on obtient la CNF vide. Donc la formule n'est pas réfutable.

Solution à l'exercice 4

1. [0,5 pnt] Le BDD réduit pour le ou exclusif a 5 noeuds (dessin omis).

2. [1,5 pnt] Le BDD réduit a $2n+1$ noeuds (dessin omis). La fonction de parité est une fonction symétrique et on sait que le BDD réduit de telles fonctions est toujours $O(n^2)$.

3. [2 pnt] Si on prend l'ordre $x_1 < y_1 < \cdots < x_n < y_n$ on a un BDD réduit avec $3n+2$ noeuds (dessin omis). Par contre, avec l'ordre $x_1 < \cdots < x_n < y_1 < \cdots < y_n$ le nombre de noeuds croit de façon exponentielle. En ce qui concerne les noeuds avec étiquettes $x_1, \ldots, x_n$, les BDD réduit prend la forme d'un arbre binaire complet (dessin omis).

   Voici une justification plus formelle (qui n'était pas demandée). Soit β un BDD réduit pour un tel ordre. Soit $n(b_1, \ldots, b_n, \beta)$, où $b_i \in \{0, 1\}$, le noeud de β dans lequel on arrive à partir de la racine en ayant examiné la première moitié $(b_1, \ldots, b_n)$ de l'entrée. Si $(b_1, \ldots, b_n) \neq (b'_1, \ldots, b'_n)$ alors on doit avoir $n(b_1, \ldots, b_n, \beta) \neq n(b'_1, \ldots, b'_n, \beta)$. Autrement on ne peut pas distinguer l'entrée $(b_1, \ldots, b_n, NOT(b_1), \ldots, NOT(b_n))$ dont la sortie est 1 de l'entrée $(b'_1, \ldots, b'_n, NOT(b_1), \ldots, NOT(b_n))$ dont la sortie est 0. Il en suit que β contient au moins 2^n noeuds.

Solution à l'exercice 5

1. [0,5 pnt] Par exemple: $v_1(x_1) = 1$, $v_1(x_2) = 0$, $v_1(x_3) = 1$ et $v_2(x_1) = 1$, $v_2(x_2) = 1$, $v_2(x_3) = 0$.

2. [0,5 pnt] Non car si v 01-satisfait une clause C alors v satisfait C. Donc v 01-satisfait A implique v 01-satisfait chaque clause de A implique v satisfait chaque clause de A implique v satisfait A.

3. [0,5 pnt] Par exemple, $v(x_1) = 1$ et $v(x_2) = 0$ satisfait A. Si v 01-satisfait $\{x_1, x_2\}$ on doit avoir $v(x_1) = 1$ ou exclusif $v(x_2) = 1$. Et ceci implique que la troisième clause n'est pas 01-satisfaite.

4. [1,5 pnt] ($\Rightarrow$) On suppose que v satisfait A'. Soit $C \in A$. Comme v satisfait A il existe $\ell \in C([\![\ell]\!]v = 1)$. Comme v satisfait $\overline{A}$ il existe $\neg\ell \in \overline{C}([\![\neg\ell]\!]v = 1)$. C'est-à-dire, il existe $\ell \in C([\![\ell]\!]v = 0)$.

   ($\Leftarrow$) On suppose que v 01-satisfait A. Soit $C \in A$. Comme v 01-satisfait A il existe $\ell \in C([\![\ell]\!]v = 1)$. Soit $\overline{C} \in \overline{A}$ ce qui est équivalent à $C \in A$. Comme v 01-satisfait A il existe $\ell \in C([\![\ell]\!]v = 0)$ et donc il existe $\neg\ell \in \overline{C}([\![\neg\ell]\!]v = 1)$.

   Si la taille de A est n la taille de A' est au plus $3n$ car dans le pire des cas on duplique A et on ajoute des négations devant chaque littéral. Par exemple, si $A = \{\{x_1, \ldots, x_n\}\}$ alors $A' = \{\{x_1, \ldots, x_n\}, \{\neg x_1, \ldots, \neg x_n\}\}$.

5. [0,5 pnt] On a:
   $$A' = \{\{x_1, \neg x_2\}, \{x_2, x_3\}, \{\neg x_1, x_2\}, \{\neg x_2, \neg x_3\}\}.$$
   Si on remplace x_1 par $\mathbf{1}$ on obtient:
   $$\{\{x_2, x_3\}, \{x_2\}, \{\neg x_2, \neg x_3\}\}.$$
   Comme x_2 est unitaire on se réduit à:
   $$\{\{\neg x_3\}\}$$
   et comme $\neg x_3$ est monotone on peut conclure que A' est satisfaisable par l'affectation $[1/x_1, 1/x_2, 0/x_3]$.

6. [0,5 pnt] On a un graphe avec 4 noeuds $\{x_1, x_2, \neg x_1, \neg x_2\}$ et 5 arêtes:
   $$\{\{x_1, x_2\}, \{\neg x_1, \neg x_2\}, \{x_1, \neg x_2\}, \{x_1, \neg x_1\}, \{x_2, \neg x_2\}\}.$$

7. [2,5 pnt] ($\Rightarrow$) Supposons A 01-satisfaisable par l'affectation v. Si $\{\ell, \ell'\}$ est une arête du graphe G_A d'après la règle (i) alors par définition de 01-saisfaisabilité $[\![\ell]\!]v \neq [\![\ell']\!]v$. Sinon, si on a une arête de la forme $\{x, \neg x\}$ d'après la règle (ii) alors forcement $[\![x]\!]v \neq [\![\neg x]\!]v$. Si on définit N_b pour $b \in \{0, 1\}$ comme les noeuds ℓ tels que $[\![\ell]\!]v = b$ on a donc une bipartition des noeuds du graphe G_A.

   ($\Leftarrow$) Soit N_0, N_1 une bipartition des noeuds du graphe G_A. Notons que par la règle (ii) on ne peut pas avoir deux noeuds x et $\neg x$ qui sont du même côté de la partition. On peut donc définir une affectation v telle que pour tout $\ell \in N_b$ on a $[\![\ell]\!]v = b$ pour $b \in \{0, 1\}$. Cette affectation 01-satisfait A car si $\{\ell, \ell'\} \in A$ alors les littéraux ℓ et ℓ' se trouvent l'un dans N_0 et l'autre dans N_1.