Épreuve orale d'Informatique Fondamentale

Patrick Baillot, Nicolas Ollinger, Alexis Saurin

ULC MPI 2013

Résumé

Ce document consiste en une sélection, à titre d'exemples, de 3 sujets proposés à l'épreuve d'informatique fondamentale ULC MPI en 2012. Cette épreuve consiste en un oral de 45 minutes sans préparation. Le lecteur pourra se référer au rapport de jury pour plus d'informations sur le déroulement de l'épreuve.

1. Automates, bisimulation et minimisation

L'objectif de cet exercice est d'étudier une notion d'équivalence entre automates finis non-déterministes (AFN) plus fine que celle définie simplement en identifiant les automates acceptant le même langage. On va montrer en particulier que cette nouvelle notion d'équivalence est pertinente pour étudier les AFN minimaux.

Un automate fini non-déterministe $\mathcal{A}$ est ici défini par la donnée de :

$$(Q, \Sigma, \delta, S, F)$$

où :

— Q est un ensemble fini d'états,
— Σ est un alphabet fini,
— $\delta : Q \times \Sigma \to \mathcal{P}(Q)$ est la fonction de transition,
— S est l'ensemble (non-vide) d'états initiaux,
— F est l'ensemble des états acceptants.

Si E est un ensemble d'états et $w \in \Sigma^\star$, on note $\delta(E, w)$ l'ensemble des états accessibles dans l'automate à partir d'un état dans E, en lisant le mot w. En particulier pour $w = \epsilon$ on a $\delta(E, \epsilon) = E$.

On consière deux AFN $\mathcal{A}_1$ et $\mathcal{A}_2$, avec les notations suivantes ($i = 1, 2$) :

$$\mathcal{A}_i = (Q_i, \Sigma, \delta_i, S_i, F_i).$$

Soit $\approx$ une relation entre Q_1 et Q_2, c'est-à-dire $\approx \subseteq Q_1 \times Q_2$.

On étend $\approx$ en une relation entre sous-ensembles de Q_1 et Q_2, aussi notée $\approx$:

$E_1 \approx E_2$ ssi $(\forall p \in E_1,\ \exists q \in E_2,\ p \approx q)$ et $(\forall q \in E_2,\ \exists p \in E_1,\ p \approx q)$.

Observer qu'on a : $\{p\} \approx \{q\}$ ssi $p \approx q$.

Pour $E_2 \subseteq Q_2$, $E_1 \subseteq Q_1$, on définit :

$$\begin{aligned} C_\approx(E_2) &= \{p \in Q_1 \ / \ \exists q \in E_2,\ p \approx q\}, \\ C_\approx(E_1) &= \{q \in Q_2 \ / \ \exists p \in E_1,\ p \approx q\}. \end{aligned}$$

On dit que $\approx$ est une *bisimulation* entre $\mathcal{A}_1$ et $\mathcal{A}_2$ si on a :

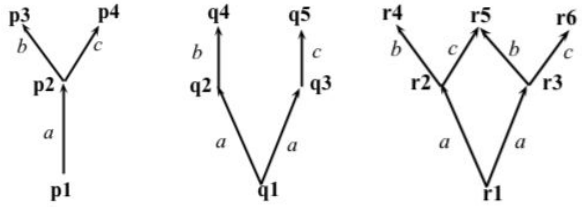
1. $S_1 \approx S_2$,
2. si $p \approx q$, alors pour tout $a \in \Sigma$, $\delta_1(p, a) \approx \delta_2(q, a)$,
3. si $p \approx q$, alors $p \in F_1$ ssi $q \in F_2$.

On dit que $\mathcal{A}_1$ est *bisimilaire* à $\mathcal{A}_2$ s'il existe une bisimulation entre $\mathcal{A}_1$ et $\mathcal{A}_2$.

Question 1. Montrer que la relation de bisimililarité est :

— symétrique : si $\mathcal{A}_1$ est *bisimilaire* à $\mathcal{A}_2$, alors $\mathcal{A}_2$ est *bisimilaire* à $\mathcal{A}_1$,
— transitive : si $\mathcal{A}_1$ est *bisimilaire* à $\mathcal{A}_2$ et si $\mathcal{A}_2$ est *bisimilaire* à $\mathcal{A}_3$, alors $\mathcal{A}_1$ est *bisimilaire* à $\mathcal{A}_3$.

Question 2. On considère les trois AFN $\mathcal{A}_1$, $\mathcal{A}_2$ et $\mathcal{A}_3$ suivants :



$\mathcal{A}_1$	$\mathcal{A}_2$	$\mathcal{A}_3$
$S_1 = \{p_1\}$	$S_2 = \{p_2\}$	$S_3 = \{p_3\}$
$F_1 = \{p_3, p_4\}$	$F_2 = \{q_4, q_5\}$	$F_3 = \{r_4, r_5, r_6\}$

Montrer que $\mathcal{A}_1$ et $\mathcal{A}_3$ sont bisimilaires, et que $\mathcal{A}_1$ et $\mathcal{A}_2$ ne le sont pas.

Question 3. Montrer que si $I \neq \emptyset$ et si pour tout $i \in I$, $\approx_i$ est une bisimulation entre $\mathcal{A}_1$ et $\mathcal{A}_2$, alors la relation $\approx$ définie comme $\cup_{i \in I} \approx_i$ est une bisimulation.

Question 4. Soit $\approx$ une bisimulation entre $\mathcal{A}_1$ et $\mathcal{A}_2$, E_1 et E_2 deux ensembles d'états de $\mathcal{A}_1$ et $\mathcal{A}_2$ respectivement, tels que $E_1 \approx E_2$. Soit w un mot. Montrer que $\delta_1(E_1, w) \approx \delta_2(E_2, w)$.

Question 5. Montrer que deux automates bisimilaires acceptent le même langage.

Soit $\approx$ une bisimulation entre $\mathcal{A}_1$ et $\mathcal{A}_2$. Le *support de* $\approx$ *dans* $\mathcal{A}_1$ est l'ensemble $C_\approx(Q_2)$, défini par :

$$C_\approx(Q_2) = \{p \in Q_1 \ / \ \exists q \in Q_2, \ p \approx q\}.$$

Question 6. Montrer qu'un état de A appartient au support dans $\mathcal{A}_1$ de toutes les bisimulations entre $\mathcal{A}_1$ et un autre automate ssi il est accessible.

Question 7. Soit $\mathcal{A}_1^{acc}$ l'automate obtenu en restreignant $\mathcal{A}_1$ aux états accessibles. Montrer que $\mathcal{A}_1$ et $\mathcal{A}_1^{acc}$ sont bisimilaires.

Une *auto-bisimulation* est une bisimulation entre un automate et lui-même.

Dans la suite on considère un AFN $\mathcal{A} = (Q, \Sigma, \delta, S, F)$.

Question 8. On considère l'ensemble des relations de $Q \times Q$ muni de l'ordre d'inclusion $\subseteq$. Montrer qu'il existe une autobisimulation $\equiv_\mathcal{A}$ maximale pour $\subseteq$. Montrer que la relation $\equiv_\mathcal{A}$ est une relation d'équivalence (c'est-à-dire réflexive, symétrique, transitive) sur Q.

(On rappelle qu'une relation R sur Q est symétrique si : $\forall q \in Q,\ qRq$).

Supposons maintenant que tous les états de $\mathcal{A}$ sont accessibles et notons $\equiv_{\mathcal{A}}$ par $\equiv$.

On définit alors :

— si $p \in Q$, $[p] =_{def} \{q \in Q \ / \ p \equiv q\}$

— $\gtrsim =_{def} \{(p, [p]) \ / \ p \in Q\}$,

— pour tout $E \subseteq Q$, $E' =_{def} \{[p] \ / \ p \in E\}$.

Question 9. Montrer les propriétés suivantes, pour tous $D, E \subseteq Q$:

1. $D \subseteq C_{\equiv}(E) \Leftrightarrow D' \subseteq E'$,
2. $D \equiv E \Leftrightarrow D' = E'$,
3. $D \gtrsim D'$.

On définit maintenant l'AFN $\mathcal{A}'$ appelé *automate quotient de* $\mathcal{A}$:

$$\mathcal{A}' = (Q', \Sigma, \delta', S', F'),$$

où Q', S', F' sont construits comme indiqué précédemment, et δ' est défini par :

$$\delta'([p], a) =_{def} \delta(p, a)'.$$

Question 10. Montrer que δ' est bien définie.

Question 11. Montrer que la relation $\gtrsim$ est une bisimulation entre $\mathcal{A}$ et $\mathcal{A}'$.

Question 12. Montrer que l'unique auto-bisimulation sur $\mathcal{A}'$ est la relation identité $=$.

Question 13. Démontrer le résultat suivant :

Proposition 1 *Soit $\mathcal{A}$ un AFN sans état inaccessible et $\equiv$ l'autobisimulation maximale sur $\mathcal{A}$.*

L'automate quotient $\mathcal{A}'$ est minimal, pour le nombre d'états, parmi les automates bisimilaires à $\mathcal{A}$. De plus si $\mathcal{A}''$ est un automate bisimilaire à $\mathcal{A}$ minimal, alors $\mathcal{A}''$ est isomorphe à $\mathcal{A}'$.

2. Mots et périodes

Dans cet exercice, Σ est un alphabet fini contenant au moins deux lettres. On note ε le mot vide et $|u|$ la *longueur* d'un mot $u \in \Sigma^*$. On note u^n le mot u répété n fois (donc $|u^n| = n|u|$). Soit $u = a_1 \dots a_n \in \Sigma^n$ un mot de longueur n. Les *préfixes* de u sont les mots de la forme $a_1 \dots a_i$ et les *suffixes* de u sont les mots de la forme $a_i \dots a_n$ où $1 \leqslant i \leqslant n$. Un préfixe (resp. suffixe) v d'un mot u est un *préfixe propre* (resp. *suffixe propre*) si $v \neq u$.

Question 1. Montrer que deux mots u et v commutent, *i.e.* $uv = vu$, si et seulement s'il existe un mot z et deux entiers m et n tels que $u = z^m$ et $v = z^n$.

Un mot $u = a_1 \dots a_n$ est périodique de période $m > 0$ si pour toute paire d'entiers $1 \leqslant i \leqslant n$ et $1 \leqslant j \leqslant n$, si $j - i = m$ alors $a_i = a_j$. On note $p(u)$ la plus petite période de u.

Question 2. Calculer la période du mot $w = abbabaab$.

Question 3. Montrer que si u et v commutent alors $p(u) \leqslant \mathrm{pgcd}(|u|, |v|)$.

La *rotation* $\pi(u)$ d'un mot $u = a_1 \dots a_n$ est le mot obtenu en déplaçant la première lettre de u de la première à la dernière position, *i.e.* $\pi(u) = a_2 \dots a_n a_1$. On note π^k l'application de k rotations successives.

Question 4. Calculer les rotations $\pi^n(w)$ du mot $w = abbabaab$.

On fixe un ordre total $\leqslant$ sur Σ. L'*ordre lexicographique* induit par $\leqslant$ sur Σ^* est défini par $u \leqslant v$ si les mots u et v satisfont l'un des deux cas suivants :

— u est un préfixe de v ;

— $u = wau'$ et $v = wbv'$ avec $a < b$.

Question 5. Montrer que si le mot u n'est pas un préfixe du mot v alors si $u \leqslant v$, pour toute paire de mots w, z, on a $uw \leqslant vz$.

Un mot est *Lyndon* s'il est strictement inférieur à chacun de ses suffixes propres.

Question 6. Monter qu'un mot est Lyndon si et seulement si pour tout entier $1 \leqslant n < |u|$ on a $u < \pi^n(u)$.

Question 7. Montrer que si u est Lyndon et si $u = vw$ alors $u \leqslant wv$.

Un *bord* v d'un mot u est un mot non vide tel que u se factorise en vwv pour un certain mot w.

Question 8. Montrer que si u est Lyndon alors u est sans bord.

Un mot w non vide est un *chevauchement* pour une paire de mots (u, v) si $\Sigma^* w$ intersecte $\Sigma^* u$ et $w\Sigma^*$ intersecte $v\Sigma^*$. La *période locale* $l(u, v)$ d'une paire de mots (u, v) est la longueur d'un plus petit chevauchement pour (u, v).

Question 9. Calculer chacune des périodes locales des factorisations (u, v) où $uv = abbabaab$.

Question 10. Montrer que $l(u, v) \leqslant p(uv)$ pour toute paire de mots u, v.

Question 11. Montrer que si $l(u, v) \geqslant \max\{|u|, |v|\}$ alors $l(u, v) = p(uv)$, pour toute paire de mots u, v.

Question 12. Montrer que pour tout mot u tel que $p(u) = |u|$ on a $l(u, u) = |u|$.

Question 13. Montrer que pour tout mot w tel que $|w| \geqslant 3p(w)$, la borne de la question 10 est atteinte : $p(w) = l(u, v)$ pour une factorisation $w = uv$ de w.

3. Théorème de complétude pour la logique propositionnelle

On considère dans ce problème la question de la correspondance entre la validité d'une formule et sa prouvabilité dans un système de déduction, c'est-à-dire un système formel dont les objets représentent des démonstrations.

Question 1. Rappeler la définition des formules propositionnelles construites à partir d'un ensemble de variables propositionnelles $\mathcal{P}(\ni p, q, \dots)$ avec l'implication, la négation, la conjonction et la disjonction, qu'on notera $\Rightarrow$, $\neg$, $\wedge$ et $\vee$ et la définition des assignations de valeurs de vérité.

Question 2. Rappeler comment définir l'implication en fonction des autres connecteurs et énoncer les lois de de Morgan.

On considère l'ensemble $\mathcal{F}$ défini comme le plus petit ensemble de formules propositionnelles contenant les littéraux ainsi que les disjonctions et les conjonctions de formules de $\mathcal{F}$.

On peut associer à toute formule logique une formule de $\mathcal{F}$ qui lui est logiquement équivalente.

Question 3. Pour $A \in \mathcal{F}$, définir une formule $\overline{A}$ de $\mathcal{F}$ associée à $\neg A$.

LK. Dans la suite de l'exercice, on ne considérera plus que des formules de $\mathcal{F}$.

Un ***séquent*** est la donnée d'une liste de formules, noté $\vdash A_1, \dots, A_n$. Un séquent $\vdash A_1, \dots, A_n$ a pour interprétation intuitive : "la disjonction des formules $A_1, \dots, A_n$ est vraie". On étend la notion d'assignation de valeur de vérité aux séquents de la manière suivante :

$$\delta(\vdash A_1, \dots, A_n) = max(0, \delta(A_1), \dots, \delta(A_n))$$

On dira qu'un séquent $\vdash \mathcal{S}$ est ***valide*** lorsque $\delta(\vdash \mathcal{S}) = 1$ pour toute assignation δ et qu'il est ***satisfaisable*** lorsqu'il existe une assignation δ telle que $\delta(\vdash \mathcal{S}) = 1$.

Question 4. Les séquents $\vdash p \vee \neg p$, $\vdash p \vee p$ et $\vdash p \wedge \neg p$ sont-ils valides ?

Les ***règles d'inférence*** de LK sont données dans la figure 1. Les règles d'inférence ont en commun que chaque règle possède

- une unique ***conclusion*** qui est le séquent en-dessous de la barre d'inférence et
- 0,1 ou 2 ***prémisses***, qui sont les séquents au-dessus de la barre d'inférence.

Les règles de la figure 1 définissent des schémas de règles d'inférence où les variables A, B (resp. Γ, Δ) désignent n'importe quelle formule (resp. liste de formules) de $\mathcal{F}$ et p n'importe quelle variable propositionnelle.

On travaillera dans la suite avec des ***instances*** de ces règles. Par exemple

$$\frac{\vdash p \vee q, \neg p \vee \neg r \quad \vdash r, \neg p \vee \neg r}{\vdash (p \vee q) \wedge r, \neg p \vee \neg r}\ \wedge^- \qquad \text{est une instance de} \qquad \frac{\vdash A, \Gamma \quad \vdash B, \Gamma}{\vdash A \wedge B, \Gamma}\ \wedge^-$$

FIGURE 1 – Règles d'inférence de LK.

$$\frac{}{\vdash p, \neg p}\ Ax \qquad \frac{\vdash \Gamma, B, A, \Delta}{\vdash \Gamma, A, B, \Delta}\ E \qquad \frac{\vdash \Gamma}{\vdash A, \Gamma}\ A \qquad \frac{\vdash A, A, \Gamma}{\vdash A, \Gamma}\ C$$

$$\frac{\vdash A, \Gamma \quad \vdash B, \Gamma}{\vdash A \wedge B, \Gamma}\ \wedge^- \qquad \frac{\vdash A, B, \Gamma}{\vdash A \vee B, \Gamma}\ \vee^-$$

$$\frac{\vdash A, \Gamma \quad \vdash B, \Delta}{\vdash A \wedge B, \Gamma, \Delta}\ \wedge^+ \qquad \frac{\vdash A, \Gamma}{\vdash A \vee B, \Gamma}\ \vee_1^+ \qquad \frac{\vdash B, \Gamma}{\vdash A \vee B, \Gamma}\ \vee_2^+$$

Question 5. Montrer que pour toute règle d'inférence de prémisses $(\vdash \mathcal{S}_i)_{i \in I}$ et de conclusion $\vdash \mathcal{S}$ et pour toute assignation δ, si $\forall i \in I, \delta(\vdash \mathcal{S}_i) = 1$ alors $\delta(\vdash \mathcal{S}) = 1$.

Preuves dans LK. L'ensemble des preuves des séquents de LK est défini comme le plus petit ensemble tel qu'***une preuve d'un séquent*** $\vdash \mathcal{S}$ est la donnée

- d'une instance d'une règle d'inférence (issue de la figure ci-dessus), de prémisses $(\vdash \mathcal{S}_i)_{i \in I}$ et de conclusion $\vdash \mathcal{S}$, et
- de preuves π_i des séquents $\vdash \mathcal{S}_i$ pour tout $i \in I$

Un séquent est dit ***prouvable*** lorsqu'il existe une preuve de ce séquent.

On représentera les preuves de manière arborescente comme suit :

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash p, \neg p}\ Ax}{\vdash A, p, \neg p}\ A}{\vdash A \vee p, \neg p}\ \vee^- \quad \dfrac{\dfrac{\dfrac{}{\vdash q, \neg q}\ Ax}{\vdash \neg q, q}\ E}{\vdash \neg q \vee B, q}\ \vee_1^+}{\vdash (A \vee p) \wedge q, \neg p, \neg q \vee B}\ \wedge^+ \quad \dfrac{\vdash q, \neg q \vee B}{}\ E$$

Question 6. Donner une preuve pour le séquent :

$$\vdash p \wedge q, \neg p \vee \neg q.$$

Question 7. Montrer que tout séquent prouvable est valide.

LK$_{\wedge^\epsilon\vee^{\epsilon'}}$. Pour $\epsilon, \epsilon' \in \{+, -\}$, on notera $LK_{\wedge^\epsilon\vee^{\epsilon'}}$ le sous-système de LK qui ne contient que les règles de disjonction et de conjonction correspondant au signe qui lui est assigné.

Question 8. Montrer que le choix de ϵ et ϵ' ne change pas les séquents prouvables dans $LK_{\wedge^\epsilon\vee^{\epsilon'}}$ et qu'il s'agit exactement des séquents prouvables de LK.

Complétude de LK. Le reste du problème consiste à démontrer le théorème suivant qui est une réciproque de la propriété de la question 7 :

Théorème 1 (Complétude de LK) *Tout séquent $\vdash \mathcal{S}$ valide est prouvable dans LK.*

Question 9. Montrer que pour toute instance des inférences $\wedge^-$ et $\vee^-$, une assignation δ qui satisfait la conclusion d'une de ces règles satisfait chacune de ses prémisses.

En déduire en particulier que si la conclusion d'une de ces inférences est valide, alors toutes ses prémisses le sont.

Comparer cette propriété à une propriété déjà établie.

Question 10. Montrer qu'on peut remplacer la règle axiome par la règle $Ax^\star$:

$$\frac{}{\vdash p, \neg p, \Gamma}\ Ax^\star$$

et que le système $LK^\star$ ainsi obtenu prouve les mêmes séquents que LK.

Preuve de la complétude de LK. On va en fait montrer que le fragment de $LK^\star$ contenant simplement les règles $Ax^\star$, E, $\vee^-$ et $\wedge^-$ est suffisant pour avoir la complétude complet, c'est-à-dire que tout séquent $\vdash \mathcal{S}$ valide est prouvable en utilisant simplement les règles $Ax^\star$, E, $\vee^-$ et $\wedge^-$.

On omettra dans la suite de prendre en compte la règle d'échange en supposant qu'on peut appliquer les inférences à n'importe quelle formule d'un séquent.

On ajoute une nouvelle règle d'inférence, ✠, dont tout séquent de littéraux $\vdash l_1, \ldots, l_n$ tel que $\forall 1 \leq i, j \leq n, l_i \neq \neg l_j$ est conclusion :

$$\frac{}{\vdash l_1, \ldots, l_n}\ ✠ \qquad \text{Si pour tous } 1 \leq i, j \leq n, l_i \neq \neg l_j$$

On appellera ***parapreuve*** une preuve dans $LK^-_✠ = LK^- \cup \{✠\}$

Question 11. Montrer que tout séquent admet une parapreuve.

Question 12. Montrer que si un séquent admet une parapreuve contenant ✠, alors il n'est pas valide.

Question 13. En déduire la complétude de LK.