Concision et ambiguïté - ENS Info Fondamentale 2023

Pour toutes les remarques ou corrections, vous pouvez m'envoyer un mail à `galatee.hemery@gmail.com`

1 Déterminisme et ambiguïté

Question 1.1. Il s'agit du langage des mots contenant au moins un b utilisant les lettres a et b.

Question 1.2. Les automates $\mathcal{A}_1$ et $\mathcal{A}_2$ sont non déterministes car $(1, b, 2) \in T$ et $(1, 2, 1) \in T$ pour ces deux automates.
L'automate $\mathcal{A}_3$ est déterministe car pour chaque couple état,lettre on a une unique transition.

Question 1.3. Soit $w \in L(\mathcal{A}_1)$.
Soit w s'écrit a^iba^j avec i, j des entiers naturels et le seul calcul acceptant est $\underbrace{1 \dots 1}_{i+1\text{fois}}\underbrace{2 \dots 2}_{j+1\text{fois}}$.
Soit w s'écrit $w_1bw_2bw_3$ avec w_1, w_2, w_3 dans $\{a, b\}^*$ et on a au moins deux calculs acceptants : celui où l'on passe de l'état 1 à l'état 2 à l'aide du premier b et celui où l'on passe de l'état 1 à l'état 2 à l'aide du second.
Ainsi $\text{Amb}(\mathcal{A}_1) = \{a, b\}^*\{b\}\{a, b\}^*\{b\}\{a, b\}^*$.

Soit $w \in L(\mathcal{A}_2)$.
On peut écrire $w = w_1ba^i$ en repérant le dernier b dans w.
L'unique calcul acceptant est celui qui utiliser $(1, b, 2) \in T$ pour le dernier b. En effet, si la transition est utilisée avant, dans l'état 2, le calcul serait bloqué au b suivant.
Ainsi, $\text{Amb}(\mathcal{A}_2) = \emptyset$.

Dans $\mathcal{A}_3$, l'automate est déterministe et complet donc il existe un unique calcul pour un mot : pour chaque étape de calcul on suit l'unique transition correspondant au couple état courant, lettre suivante. Ainsi $\text{Amb}(\mathcal{A}_3) = \emptyset$.

Question 1.4. Soit $w = a_1...a_n$ un mot de longueur n accepté par $\mathcal{A}$ où a_i désignent les lettres de w et $q_0...q_n$ un calcul acceptant.
On sait donc $\forall i \in \{1, \dots, n\}, (q_{i-1}, a_i, q_i) \in T$.
On sait également que $q_0 \in I$ et $q_n \in F$.
On pose $\tilde{w} = a_n...a_0$. On a $q_n \in \tilde{I}$, $q_0 \in \tilde{F}$ et $\forall i \in \{1, \dots, n\}, (q_i, a_i, q_{i-1}) \in \tilde{T}$ donc $q_n...q_0$ est un calcul acceptant de $\tilde{\mathcal{A}}$ sur $\tilde{w}$.

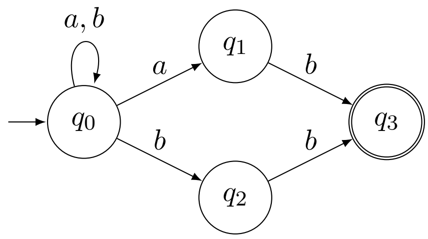
Question 1.5. Soit $\mathcal{A}$ un automate ambigu, alors il existe w un mot de longueur n un entier tel que $q_0...q_n$ et $q'_0...q'_n$ sont des calculs acceptants distincts.
Ainsi, d'après la question précédente $q_n...q_0$ et $q'_n...q'_0$ sont des calculs acceptants distincts sur $\tilde{\mathcal{A}}$ pour $\tilde{w}$ donc $\tilde{\mathcal{A}}$ est ambigu.
On obtient la réciproque en remarquant que $\tilde{\tilde{\mathcal{A}}} = \mathcal{A}$.

Question 1.6. Si $\mathcal{A}$ est déterministe, il existe au plus un calcul de $\mathcal{A}$ pour un mot donné car pour chaque étape de calcul on suit l'unique transition correspondant au couple état courant, lettre suivante.
Ainsi, il ne peut exister deux calculs acceptants d'un même mot et $\mathcal{A}$ n'est pas ambigu.

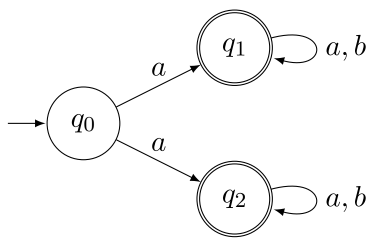
Question 1.7. Soit $\mathcal{A}$ un automate co-déterministe. On a donc $\tilde{\mathcal{A}}$ déterministe.
D'après la question précédente, $\tilde{\mathcal{A}}$ n'est pas ambigu.
D'après la question 1.5, $\mathcal{A}$ n'est pas ambigu.

Question 1.8.

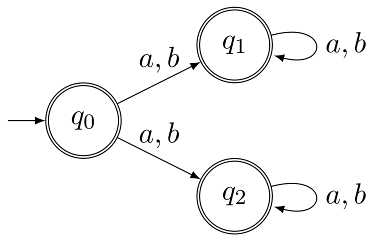
(i) L'automate proposé est non déterministe car $(q_0, a, q_1) \in T$ et $(q_0, a, q_0) \in T$ et il est non co-déterministe car $(q_1, b, q_3) \in T$ et $(q_2, b, q_3) \in T$.
Il n'est pas ambigu. L'ensemble est mots reconnus est $\{a, b\}^*\{ab, bb\}$. Il existe un unique chemin acceptant $q_0 \dots q_0q_1q_3$ pour les mots de la forme w_1ab et un unique chemin acceptant $q_0 \dots q_0q_2q_3$ pour les mots de la forme w_1bb.



(ii) On propose un automate reconnaissant $\{a\}\{a, b\}^*$ infini à trois états : un initial et deux finaux. Tous les mots acceptés ont deux chemins acceptant : $q_0q_1 \dots q_1$ et $q_0q_2 \dots q_2$.



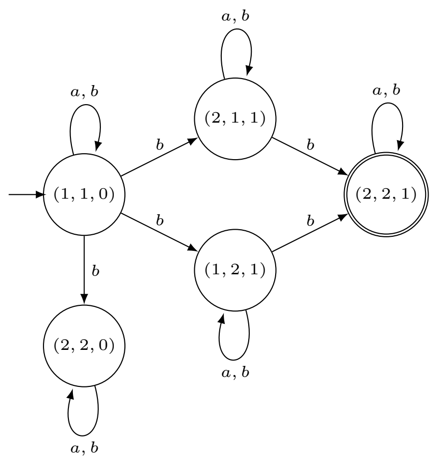
(iii) On propose un automate reconnaissant $\{a, b\}^*$ infini à trois états. Tous les mots acceptés non vides ont deux chemins acceptant : $q_0q_1 \dots q_1$ et $q_0q_2 \dots q_2$. Le mot vide a un unique chemin acceptant.



2 Test d'ambiguïté

2.1 Une construction utile

Question 2.1. $L(\widehat{\mathcal{A}}) = \mathrm{Amb}(\mathcal{A}_1) = \{a, b\}^*\{b\}\{a, b\}^*\{b\}\{a, b\}^*$



Question 2.2.

(i) On pose $w = a_1 ... a_n$.
Comme ρ est un calcul de $\widehat{\mathcal{A}}$, on peut en déduire que $(q_{i-1}, a_i, q_i) \in T$ et $(q'_{i-1}, a_i, q'_i) \in T$ pour tout $1 \leq i \leq n$ par définition de $\widehat{T}$.
Ainsi, μ et μ' sont bien des calculs de $\mathcal{A}$ sur w.

(ii) Pour tout $((s, s', b_s), a, (t, t', b_t)) \in \widehat{T}$, on a $b_s \leq b_t$, ainsi dans le calcul, b_i est une suite croissante.
Si $b_n = 0$ alors $b_i = 0$ pour tout $0 \leq i \leq n$ et les transitions utilisées sont toutes dans T_1.
De plus, $(q_0, q'_0, 0) \in \widehat{I}$ donc $q_0 = q'_0$.
On montre alors par récurrence, on exploitant le fait que le calcul n'utilise que des transitions de T_1 que $q_i = q'_i$ pour tout $0 \leq i \leq n$.
Ainsi $\mu = \mu'$.
Réciproquement, si $\mu = \mu'$ alors $(q_0, q_0, b_0) \in \widehat{I}$ donc $b_0 = 0$.
Par récurrence, on montre que $b_i = 0$ pour $0 \leq i \leq n$ pour tout i car les seules transitions possibles à chaque étape sont dans T_1.
Ainsi $b_n = 0$.

(iii) Si ρ est acceptant, alors $(q_n, q'_n, b_n) \in \widehat{F}$ donc $q_n \in F$ et $q'_n \in F$.
Donc les calculs μ et μ' sont acceptants.

(iv) On considère un mot $w \in L(\mathcal{A})$ et un calcul $q_0 ... q_n$ acceptant.
On prend $\mu = \mu' = q_0 ... q_n$ et $\rho = (q_0, q_0, 0) ... (q_n, q_n, 0)$.
On a $(q_n, q_n, 0) \notin \widehat{F}$ donc ρ n'est pas acceptant.

Question 2.3. Soit $w \in L(\widehat{\mathcal{A}})$. Soit ρ un calcul acceptant de $\widehat{\mathcal{A}}$ sur w.
En utilisant les mêmes notations, d'après la question précédente, on a μ et μ' acceptant et $b_n \neq 0$ car $(q_n, q'_n, b_n) \in \widehat{F}$.
Ainsi, $\mu \neq \mu'$ donc w est un mot accepté par $\mathcal{A}$ avec deux calculs acceptants distincts.
Donc $w \in \mathrm{Amb}(\mathcal{A})$.

Soit $w = a_1 ... a_n \in \mathrm{Amb}(\mathcal{A})$, alors on a $\mu = q_0 ... q_n$ et $\mu' = q'_0 ... q'_n$ deux calculs acceptants distincts.
On a donc $(q_{i-1}, a_i, q_i) \in T$ et $(q'_{i-1}, a_i, q'_i) \in T$.
On considère $\rho = (q_0, q'_0, b_0) ... (q_n, q'_n, b_n)$ avec $b_0 = 0$ si $q_0 = q'_0$ et $b_0 = 1$ sinon et $b_i = 0$ jusqu'au premier rang tel que $q_i \neq q'_i$, ensuite $b_i = 1$.
On a $\rho = (q_0, q_0, 0) ... (q_{i-1}, q_{i-1}, 0)(q_i, q'_i, 1) ... (q_n, q'_n, 1)$ un calcul acceptant.

Ainsi $w \in L(\widehat{\mathcal{A}})$.

Par double inclusion, on obtient l'égalité.

2.2 L'algorithme

Question 2.4. On a $|\widehat{Q}| = 2|Q|^2$ donc $|\widehat{Q}| \in \mathcal{O}(|Q|^2)$.
On a $|\widehat{F}| = |F|(|F|-1)$ donc $|\widehat{F}| \in \mathcal{O}(|F|^2)$.
On a $|\widehat{I}| = |I| + |I|(|I|-1)$ donc $|\widehat{I}| \in \mathcal{O}(|I|^2)$.
On a $|T_1| = |T|$, $|T_2| \leq |T|(|T|-1)$ car chaque transition en exploite exactement deux différente et $|T_3| = |T||T|$ donc $|\widehat{T}| \in \mathcal{O}(|T|^2)$.

Question 2.5. On utilise des listes d'adjacences ou plutôt des listes de transitions sous la forme de couples lettre,état pour chaque état. Ces listes peuvent être stockées par exemple dans un dictionnaire.
Les états finaux et initiaux peuvent être marqués à l'aide d'un dictionnaire. Le nombre d'états, numérotés en 1 à n est également stocké.
Pour chaque couple d'état (q, q'), on parcours l'ensemble des transitions sortantes de q et q' (un seul parcours si $q = q'$) et on ajoute à la liste des transitions depuis $(q, q', 0)$ et $(q, q', 1)$ les éléments correspondants aux descriptions de T_1, T_2, T_3.
Ainsi, on explore chaque couple de transitions et chaque couple d'état, en $O(|Q|^2 + |T|^2)$.
Pour les état initiaux et finaux, on parcourt l'ensemble des couples d'états et on vérifie s'ils sont initiaux ou finaux et on construit un dictionnaire correspondant contenant les informations pour les nouveaux états.
Pour le nouvel automate, on conserve l'ancien nombre d'états ainsi qu'un marqueur indiquant que c'est un tel automate utilisant des triplé (ou une autre structure).
On a une complexité en $\mathcal{O}((|Q| + |T| + |I| + |F|)^2)$.

Question 2.6. On peut réaliser un parcours en profondeur de l'automate depuis chaque état initial. Si on ne rencontre aucun état final, le langage est vide, sinon, il existe un mot reconnu par l'automate et l'automate $\mathcal{A}$ est ambigu d'après la question 2.3.
Un tel parcours se fait en $\mathcal{O}(|\widehat{Q}| + |\widehat{T}| + |\widehat{I}|)$ avec une représentation en liste d'adjacence et en considérant que le test d'appartenance à $\widehat{F}$ est en $O(1)$ (vérification dans un dictionnaire par exemple).
Ainsi, on a une complexité en $\mathcal{O}((|Q| + |T| + |I| + |F|)^2)$.

2.3 Généralisation

Question 2.7.

(i) L'état initial est pris dans $I \subseteq Q$. A chaque étape, on a au plus $|Q|$ choix pour l'état suivant dans le calcul. Ainsi, pour un mot de longueur k, on a au plus $|Q|^{k+1}$ calculs différents au plus. Ainsi $d_{\mathcal{A}}(w) \leq |Q|^{k+1}$

(ii) Pour un automate à un unique état initial et final tel que $(q, a, q) \in T$ pour tout $a \in \Sigma$ convient.
En effet, on a exactement un calcul pour tout mot et $|Q| = 1$.
Plus généralement, on peut prendre un automate à p état tous initiaux et finaux tel que $(q, a, q') \in T$ pour tout q, q', a. L'idée est que l'on peut atteindre tous les autres états depuis tout état en lisant une lettre du mot w.

Question 2.8. On généralise la construction de $\widehat{\mathcal{A}}$ en $\widehat{\mathcal{A}}^k$ pour $k \geq 2$:

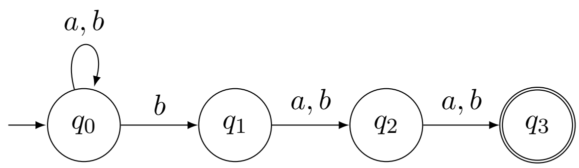
— $\widehat{Q}^k = Q^k \times \{0,1\}^{\binom{k}{2}}$
— $\widehat{I}^k = \{(i_1, ..., i_k, b_{1,2}, ..., b_{k-1}, k) | \forall j \in \{1, ..., k\}, i_j \in I, \forall l \in \{1, ..., k\}, j < l, b_{j,l} = \mathbf{1}_{i_j \neq i_l}\}$
— $\widehat{F}^k = \{(f_1, ..., f_k, 1, ..., 1) | \forall j \in \{1, ..., k\}, f_j \in F\}$
— $\widehat{T}^k = \{((s_1, ..., s_k, b_{1,2}, ..., b_{k-1,k}), a, (t_1, ..., t_k, b'_{1,2}, ..., b'_{k-1,k})) | \forall j \in \{1, ..., k\}, (s_j, a, t_j) \in T, \forall l \in \{1, ..., k\}, j < l, b'_{j,l} = \max(b_{j,l}, \mathbf{1}_{t_j \neq t_l}\}$

Cet automate reconnaît $\mathrm{Amb}_{\geq k}(\mathcal{A})$. En effet, de la même façon que dans la partie précédente, on peut extraire k calculs acceptants de $\mathcal{A}$ d'un calcul acceptant de $\widehat{\mathcal{A}}^k$ tous distincts deux à deux puisque $b_{j,l}$ avec $j < l$ est croissant et devient dans le calcul égal à 1 lorsque les calculs correspondants aux états d'indices j et l deviennent différents.
Ainsi $\mathrm{Amb}_{\geq k}(\mathcal{A})$ est régulier en vertu du théorème de Kleene.
Pour $k = 1$, on a directement le langage reconnu par $\mathcal{A}$ qui est bien régulier.

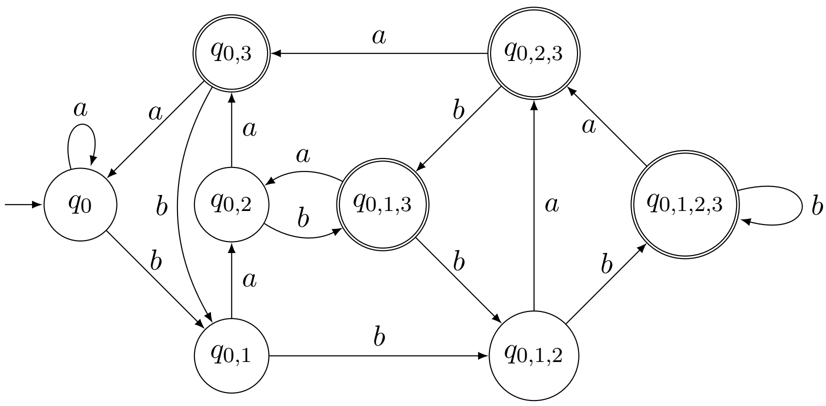
Question 2.9. $\mathrm{Amb}_k(\mathcal{A}) = \mathrm{Amb}_{\geq k}(\mathcal{A}) \cap (\Sigma^* \setminus \mathrm{Amb}_{\geq k+1}(\mathcal{A}))$ est bien régulier comme intersection d'un langage régulier et du complémentaire d'un langage régulier.

3 Concision des automates non ambigus

Question 3.1. $L_3 = \Sigma^*\{baa, bab, bba, bbb\}$ est reconnu par l'automate suivant non ambigu.



On peut le déterminiser :

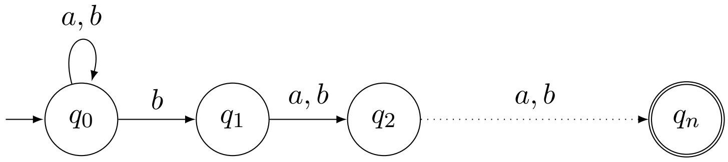


On peut remarquer qu'il y a 8 états avec les correspondances suivantes sur les fins de mots :

— ε, a, aa, aaa pour q_0
— b, ab, aab pour $q_{0,1}$;
— bb, abb pour $q_{0,1,2}$;
— ba, aba pour $q_{0,2}$;
— bbb pour $q_{0,1,2,3}$;
— bba pour $q_{0,2,3}$;

— bab pour $q_{0,1,3}$;
— baa pour $q_{0,3}$.

Question 3.2. On s'inspire de 3.1 et on construit l'automate suivant non ambigu qui reconnaît L_n. En effet, l'unique chemin acceptant pour un mot $w \in L_n$ est $q_0...q_0q_1q_2...q_n$:



Question 3.3. On s'inspire de l'observation faite dans la question 3.1 après la déterminisation. On construit l'automate suivant $\mathcal{B}$:

— $Q = \{w \in \Sigma^n\}$ avec $|Q| = 2^n$
— $I = \{a^n\}$
— $F = \{vw_2 | w_2 \in \Sigma^{n-1}\}$
— $T = \{(w_1, \sigma, w_2) | \exists \alpha \in \Sigma, w_1\sigma = \alpha w_2\}$

Cet automate est déterministe et permet de conserver dans l'état les n dernières lettres du mot. Au lieu de considérer le mot vide, on considère initialement a^n, car les a n'interviennent pas pour la reconnaissance du mot par l'automate, seule la position des b compte.

Question 3.4. *Cette question semble très simple à ce niveau du sujet.*
A chaque étape du calcul, où il s'agit de lire une lettre a à partir d'un état q, il existe exactement un unique état q' tel que $(q, a, q') \in T$ donc on effectue la prochaine étape à partie de q' nécessairement et ce jusqu'à épuisement des lettres de w.
Ainsi, de proche en proche on construit un unique calcul sur w. Il est impossible d'en construire un autre.
L'existence découle du caractère complet de l'automate et l'unicité du caractère déterministe.

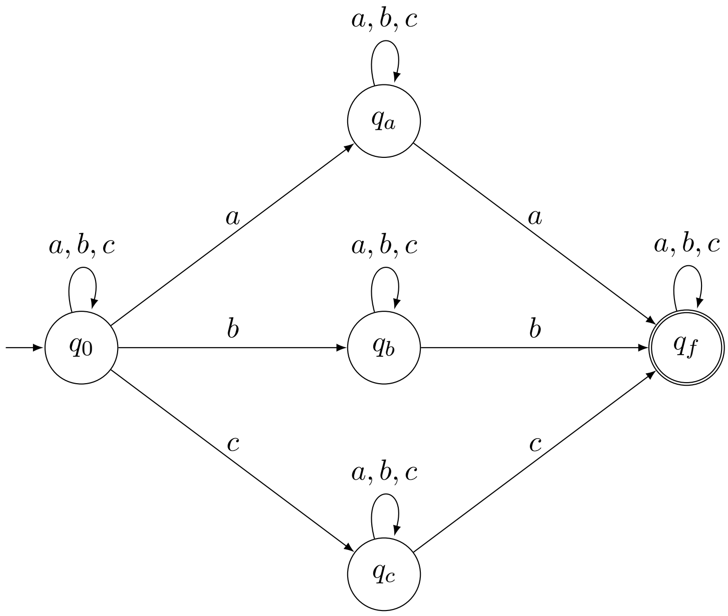
Question 3.5. Si $w = w'$ alors il existe un unique calcul de $\mathcal{B}$ sur $w = w'$ qui aboutit à un unique état $q_w = q_{w'}$.
Réciproquement si $q_w = q_{w'}$ alors pour tout $v \in \Sigma*$ on a $q_{wv} = q_{w'v}$ en concaténant les calculs de w ou w' et le calcul de v (unique par la question précédente).
Ainsi $wv \in L_n$ si et seulement si $w'v \in L_n$.
On pose $w = a_1....a_n$ et $w' = b_1...b_n$.
Soit $v = c_1...c_p$ de longueur $0 \leq p < n$ un entier, alors $wv = a_1...a_nc_1...c_p$ et $w'v = a_1...a_nc_1...c_p$.
$wv \in L_n$ si et seulement si $w'v \in L_n$ donc $a_{p+1} = b_{p+1}$ qui est la n-ième lettre en partant de la fin.
Ceci est vrai pour tout $0 \leq p < n$ donc $w = w'$.

Question 3.6. Supposons par l'absurde qu'il existe un automate $\mathcal{C}$ reconnaissant L_n complet et déterministe à moins de 2^n états.
Par le principe des tiroirs, il existe deux mots de longueur n ($|\Sigma^n| = 2^n$), w et w' tel que $q_w = q_{w'}$. Ainsi, par la question précédente, $w = w'$ CONTRADICTION.

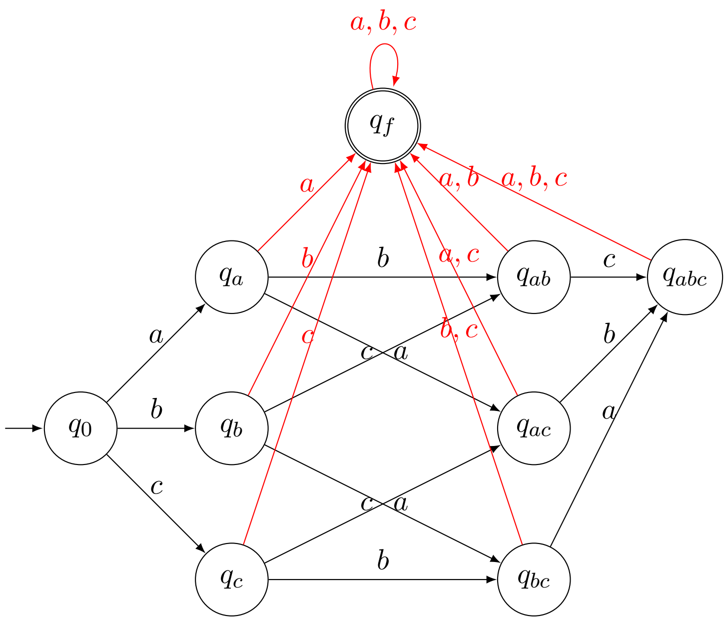
4 Concision des automates ambigus

Question 4.1.

(i)



(ii) On construit un automate déterministe donc non ambigu : chaque état conserve en mémoire les lettres déjà rencontrées.



Question 4.2. De la même façon que dans la question précédente, on peut construire un automate tel que :

— $Q = \{q_0, q_f\} \cup \{q_\sigma, \sigma \in \Sigma\}$

— $F = \{q_f\}$

— $I = \{q_0\}$

— $T = \{(q,\sigma,q) | q \in Q, \sigma \in \Sigma\} \cup \{(q_0,\sigma,q_\sigma, \sigma \in \Sigma\} \cup \{(q_\sigma,\sigma,q_f), \sigma \in \Sigma\}$

Cet automate a $n+2$ état et reconnaît bien K_n. Un mot est reconnu s'il existe un calcul entrant et sortant d'un q_σ : pour cela il faut et il suffit que σ apparaisse deux fois dans le mot.

Question 4.3. De même, on s'inspire de la construction pour K_3 :

— $Q = \{q_f\} \cup \{q_X, X \subset \Sigma\}$

— $F = \{q_f\}$

— $I = \{q_\emptyset\}$

— $T = \{(q_X,\sigma,q_{X\cup\{\sigma\}}) | X \subset \Sigma, \sigma \notin X\} \cup \{(q_X,\sigma,q_f) | X \subset \Sigma, \sigma \in X\} \cup \{(q_f,\sigma,q_f) | \sigma \in \Sigma\}$

Cet automate a $2^n + 1$ états et reconnaît bien K_n. Il est déterministe donc non ambigu. Chaque état conserve en mémoire les lettres déjà rencontrées et à la lecture d'une lettre déjà rencontrée, on rejoint l'état final.

Question 4.4. (i) Le calcul acceptant de uv est de la forme $q_0q_1...q_{u,v}...q_f$.
Le calcul acceptant de uv est de la forme $q_0q'_1...q_{u',v'}...q'_f$.
En concaténant le début du premier et la fin du second, on a $q_0q_1...q_{u,v}...q'_f$ un calcul acceptant de $u\cdots v'$ qui appartient bien à K_n.
En concaténant le début du second et la fin du premier, on a $q_0q'_1...q_{u',v'}...q_f$ un calcul acceptant de $u'\cdots v$ qui appartient bien à K_n.

(ii) L'égalité $q_{u,v} = q_{u,v'} = q_{u',v} = q_{u',v'}$ découle des calculs (uniques) mis en avant dans la question (i).

Question 4.5. Soit $n \geq 2$, $s^n = s^{n-1}, s^{n-1} \cdot \alpha_n$. D'après la remarque s^{n-1} contient 2^{n-1} éléments.
Ainsi $s_{i+2^{n-1}} = s_i \cdot \alpha_n$ pour $0 \leq i \leq 2^{n-1} - 1$.
Pour $0 \leq i \leq 2^{n-1} - 1$ et $0 \leq j \leq 2^{n-1} - 1$, on a :

$$M_n[i,j] = M_{n-1}[i,j] = \begin{cases} 1 & \text{si } s_i \text{ et } s_j \text{ ont une lettre en commun} \\ 0 & \text{sinon} \end{cases}$$

$$M_n[i+2^{n-1},j] = \begin{cases} 1 & \text{si } s_i\cdot\alpha_n \text{ et } s_j \text{ ont une lettre en commun} \\ 0 & \text{sinon} \end{cases} = M_n[i,j]$$

$$M_n[i,j+2^{n-1}] = \begin{cases} 1 & \text{si } s_i \text{ et } s_j\cdot\alpha_n \text{ ont une lettre en commun} \\ 0 & \text{sinon} \end{cases} = M_n[i,j]$$

car α_n n'apparaît pas dans s^{n-1}.

$$M_n[i+2^{n-1},j+2^{n-1}] = \begin{cases} 1 & \text{si } s_i\cdot\alpha_n \text{ et } s_j\cdot\alpha_n \text{ ont une lettre en commun} \\ 0 & \text{sinon} \end{cases} = 1$$

D'où le résultat attendu.

Question 4.6. Si $s_i \cdots s_j \in K_n$ alors s_i et s_j partagent une lettre puisqu'une lettre apparaît deux fois dans le mot et s_i et s_j sont par construction des mots sans répétition.
Ainsi $M_n[i,j] = 1$.
Réciproquement, si $M_n[i,j] = 1$, alors s_i et s_j partagent une lettre donc elle se répète dans $s_i \cdots s_j \in K_n$.

Question 4.7. Montrons le résultat proposé dans l'indication. Soit u_j la j-ième colonne de M_n pour $0 \leq j \leq 2^n - 1$.
Soit $0 \leq i \leq 2^n - 1$, alors si $M_n[i,j] = u_j[i] = 1$, alors il existe $q \in Q$ tel que $q = q_{s_i,s_j}$ et $v_q[i] = 1$.
On a donc $u_j[i] \leq \sum_{\substack{q \in Q \\ \exists i, q = q_{s_i,s_j}}} v_q[i]$

Par ailleurs, soit q, q' distinct dans Q tel qu'il existe i, i' tel que $q = q_{s_i,s_j}$ et $q' = q_{s_{i'},s_j}$.
On a $v_q[i] = 1$ et $v_{q'}[i'] = 1$.
Supposons par l'absurde que $v_{q'}[i] = 1$ et ainsi $\sum_{\substack{q \in Q \\ \exists i, q = q_{s_i,s_j}}} v_q[i] \geq 2$. On a alors $j' < 2^n$ tel que $q' = q_{s_i,s_{j'}}$ et d'après la question 4.4, on a $q' = q_{s_{i'},s_j} = q_{s_i,s_{j'}} = q_{s_i,s_j} = q$
CONTRADICTION.

Ainsi on a bien pour tout i, $u_j[i] = \sum_{\substack{q \in Q \\ \exists i, q = q_{s_i,s_j}}} v_q[i]$ puisque cette quantité vaut 1 si et seulement si il existe un unique q tel que $q = q_{s_i,s_j}$.
Donc $u_j = \sum_{\substack{q \in Q \\ \exists i, q = q_{s_i,s_j}}} v_q$.
Ainsi la famille des v_q permet d'obtenir la famille des u_j colonnes de M_n par combinaison linéaire.

En supposant le résultat de la question précédente déjà connu, on obtient l'égalité par égalité de dimension car $v_q[0] = 0$ car $s_0 = \varepsilon$ pour tout q donc l'espace engendré est de dimension au plus $2^n - 1$. Et on a l'espace engendré par les colonnes u_j est de dimension $2^n - 1$.

Question 4.8. Montrons le résultat par récurrence.
On a $M_0 = (0)$ de rang 0, M_1 de rang 1 et M_2 de rang 3 très clairement sur l'exemple.
De plus, la première ligne et la première colonne sont nulles. La dernière ligne contient un 0 puis que des 1.
On suppose donc que M_{n-1} est de rang $2^{n-1} - 1$.
En appliquant une sorte de pivot de Gauss par bloc, on obtient

$$rg \begin{pmatrix} M_{n-1} & M_{n-1} \\ M_{n-1} & \mathbf{1}_{n-1} \end{pmatrix} = rg \begin{pmatrix} M_{n-1} & \mathbf{0}_{n-1} \\ \mathbf{0}_{n-1} & \mathbf{1}_{n-1} - M_{n-1} \end{pmatrix} = rg(M_{n-1}) + rg(\mathbf{1}_{n-1} - M_{n-1})$$

On a $rg(\mathbf{1}_{n-1} - M_{n-1}) = 2^{n-1}$. En effet, en soustrayant la première colonne à toutes les autres et en les multipliant par (-1) on reconnaît les $2^{n-1} - 1$ colonnes libres de M_{n-1}. Elles finissent toutes par 0, donc la première colonne finissant par un 1 est bien hors de l'espace engendré.
On en déduit $rg(M_n) = rg(M_{n-1}) + 2^{n-1} = 2^n - 1$

Question 4.9. Supposons par l'absurde que $\mathcal{A}$ contiennent strictement moins de $2^n - 1$ états q tels que $v_q \neq 0$. Alors, l'espace engendré par les v_q est de dimension au plus $2^n - 2$. Or il est égal à l'espace engendré par les colonnes de M_n de dimension $2^n - 1$.
CONTRADICTION.

Question 4.10. Soit q tel que $v_q \neq 0$, alors il existe i, j tel que $q = q_{s_i,s_j}$, en particulier depuis q il existe un calcul $q...q_f$ avec $q_f \in F$.

Si $q \in I$, alors $s_j \in K_n$, ce qui est impossible car s_j est sans répétition.
Si $q \in F$, alors $q_0...q$ est un calcul de s_i acceptant et $s_i \in K_n$, ce qui est impossible car s_i est sans répétition.
Ainsi, $q \notin I$ et $q \notin F$.

Question 4.11. $\mathcal{A}$ contient au moins un état final, un état initial tels que $v_q = 0$ et $2^n - 1$ états tels que $v_q \neq 0$ soit au moins $2^n + 1$ états.