Devoir maison n°5

Corrigé

⋆ ⋆ ⋆

1 Machines synchronisées

Question 1 Sur une machine à un seul état q, les transitions sont exactement les $\delta(q,a) = q$ pour $a \in \Sigma$, et on en déduit que tous les mots sont synchronisants.

Question 2 On remarque que si $|u| \equiv 0[2]$, alors $\delta^*(q_i,u) = q_i$ et si $|u| \equiv 1[2]$, alors $\delta^*(q_i,u) = q_{1-i}$ (ce résultat se prouve aisément par récurrence). On en déduit que pour tout mot u, $\delta^*(q_0,u) \neq \delta^*(q_1,u)$, donc qu'il n'existe pas de mot synchronisant.

Question 3 On remarque que la lecture d'un a emmène à l'état q_1 ou l'état q_2. De plus, la lecture de da depuis l'un de ces deux états emmène nécessairement vers l'état q_1. On en déduit que ada est un mot synchronisant pour M_2. D'autres mots peuvent convenir, comme bca, bdb, aca, bcb, acb, adb.

Question 4 On calcule une transition tant qu'on n'est pas arrivé sur le caractère de fin du mot `u`. On utilise la fonction `code` pour passer d'un caractère à un entier dans le bon intervalle.

```
int delta_etoile(machine M, int q, char* u){
    for (int i=0; u[i] != '\0'; i++){
        q = M.delta[q][code(u[i])];
    }
    return q;
}
```

Question 5 Il faut tester pour chaque état que la lecture du mot emmène vers un unique état. Pour cela, on fait le calcul depuis l'état 0, puis on utilise une boucle pour vérifier que l'image depuis chaque autre état mène bien au même état.

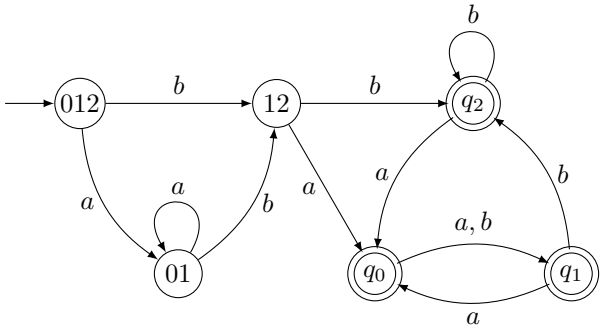
```
bool synchronisant(machine M, char* u){
    int p = delta_etoile(M, 0, u);
    for (int q=1; q<M.Q; q++){
        if (delta_etoile(M, q, u) != p) return false;
    }
    return true;
}
```

Question 6 On remarque que s'il existe un mot synchronisant u pour M, tel que $\forall q \in Q$, $\delta^*(q,u) = q_0$, alors $\widehat{\delta}^*(Q,u) = \{q_0\}$. On en déduit qu'il existe un mot synchronisant pour M si et seulement si un singleton est accessible depuis l'état $Q \in \widehat{Q}$ dans $\widehat{M}$.

Question 7 On définit l'automate déterministe $(\widehat{Q}, \Sigma, \widehat{\delta}, Q, \{\{q\} | q \in Q\})$. D'après la proposition précédente, cet automate reconnaît bien l'ensemble de tous les mots synchronisants de M. On en déduit que $LS(M)$ est reconnaissable.

Question 8 On détermine l'automate des parties sous forme de tableau, puis on le représente en enlevant les états non utiles (l'état initial étant Q) :

	a	b
$\{q_0, q_1, q_2\}$	$\{q_0, q_1\}$	$\{q_1, q_2\}$
$\{q_0, q_1\}$	$\{q_0, q_1\}$	$\{q_1, q_2\}$
$\{q_1, q_2\}$	$\{q_0\}$	$\{q_2\}$
$\{q_0\}$	$\{q_1\}$	$\{q_1\}$
$\{q_1\}$	$\{q_0\}$	$\{q_2\}$
$\{q_2\}$	$\{q_0\}$	$\{q_2\}$



Notons qu'on peut simplifier cet automate en fusionnant q_0, q_1 et q_2 d'une part et 012 et 01 d'autre part.

2 Existence de mot synchronisant

2.1 Machine des paires

Question 9 On a nécessairement $|\delta^*(Q, u_0)| \geqslant |\delta^*(Q, u_1)| \geqslant \ldots \geqslant |\delta^*(Q, u_r)| = 1$. En effet la machine étant déterministe, en lisant un mot depuis un état, on ne peut atteindre qu'un seul état. En lisant un mot depuis un ensemble d'états, le nombre d'états atteignables ne peut que diminuer (en cas de collisions). De plus, comme $u = u_r$ est synchronisant, $|\delta^*(Q, u_r)| = 1$.

Question 10 Le sens direct est le plus simple, car $u_{p,q} = u$ convient (u est synchronisant).

Réciproquement, définissons les suites :

- $u_0 = v_0 = \varepsilon$ et $Q_0 = Q$;
- pour $i \in \mathbb{N}$, si $|Q_i| = 1$, alors on s'arrête, sinon, il existe deux états p et q de Q_i et un mot $u_{i+1} = u_{p,q}$ tel que $|Q_{i+1}| = |\delta^*(Q_i, u_{i+1})| < |Q_i|$. On pose alors $v_{i+1} = v_i u_{i+1}$.

La suite des $(|Q_i|)$ est strictement décroissante et minorée par 1, donc à partir d'un rang $j < n$, on a $|Q_j| = 1$, donc le mot v_j est synchronisant (car $Q_j = \delta^*(Q_0, v_j)$ par définition des suites et de δ^*).

Question 11 Il s'agit ici de coder un parcours en profondeur depuis un état de $\widetilde{M}$ afin de déterminer s'il est possible d'atteindre un singleton. On code pour cela une fonction auxiliaire récursive qui prend en plus un tableau de booléens de taille $\widetilde{n}$ permettant de déterminer si un état a déjà été vu ou non. La fonction renvoie un booléen qui vaut `true` si et seulement si le parcours a permis d'atteindre un état singleton depuis $\{p, q\}$ en passant par des sommets non vus.

```
bool DFS(machine M, int* vus, int p, int q){
    if (p == q) return true;
    int X = phi(p, q);
    if (!vus[X]){
        vus[X] = true;
        for (int i=0; i<M.Sigma; i++){
            int pi = M.delta[p][i];
            int qi = M.delta[q][i];
            if (DFS(M, vus, pi, qi)) return true;
        }
    }
    return false;
}
```

Dès lors, la fonction principale consiste juste à créer le tableau de booléens et à déterminer la valeur de retour pour un appel à `DFS`.

```
bool paire_synchronisee(machine M, int p, int q){
    int nt = (M.Q * (M.Q + 1)) / 2;
    int* vus = malloc(nt * sizeof(vus));
    for (int X=0; X<nt; X++) vus[X] = false;
    bool b = DFS(M, vus, p, q);
    free(vus);
    return b;
}
```

Question 12 On lance un appel à la fonction précédente pour chaque paire d'états. Si l'un des appels renvoie `false`, la machine n'est pas synchronisée. Sinon, elle l'est.

```
bool synchronisee(machine M){
    for (int p=0; p<M.Q; p++){
        for (int q=p+1; q<M.Q; q++){
            if (!paire_synchronisee(M, p, q)) return false;
        }
    }
    return true;
}
```

Question 13 La fonction `paire_synchronisee` consiste à faire un parcours en profondeur, donc de complexité linéaire en nombre d'arêtes + nombre de sommets, soit $\mathcal{O}(|Q|^2|\Sigma)$. On l'appelle autant de fois qu'il y a de paires, c'est-à-dire $\binom{|Q|}{2}$ fois. La complexité totale est donc en $\mathcal{O}(|Q|^4|\Sigma|)$.

Question 14 Au lieu de faire autant de parcours qu'il y a de paires, on peut ne faire qu'un seul parcours, mais dans l'automate transposé (où on a retourné toutes les transitions). L'idée est alors de faire un parcours depuis tous les états singletons puis de vérifier qu'on a atteint tous les autres états. Comme il s'agit d'un seul parcours, on aurait bien une complexité en $\mathcal{O}(|Q|^2|\Sigma|)$.

2.2 Bornes sur les mots synchronisants

Question 15 On commence par montrer qu'une paire d'états $\{p, q\} \subseteq Q$ peut toujours être synchronisée par un mot $u_{p,q}$ de longueur $\leqslant \binom{n}{2}$. En effet, dans la machine $\widetilde{M}$, un chemin élémentaire de $\{p, q\}$ à un singleton comporte au plus $\binom{n}{2} + 1$ états (les $\binom{n}{2}$ paires et un singleton en dernier état). Le mot lu le long de ce chemin

est bien un mot synchronisant $\{p, q\}$.

De plus, en reprenant les notations de la question 10, chaque mot u_i pour $i > 0$ est un mot synchronisant une paire, et le mot synchronisant construit est la concaténation d'au plus $n-1$ des u_i, donc est de taille $\leqslant (n-1)\binom{n}{2} = \frac{n(n-1)^2}{2}$.

Question 16 Montrons que $u = a(b^{n-1}a)^{n-2}$ est un mot synchronisant pour $\mathcal{C}_n$, en considérant les $\delta^*(Q, u_i)$, pour u_i certains préfixes de u bien choisis. Posons, pour $i \in [\![0, n-2]\!]$, $u_i = a(b^{n-1}a)^i$. Montrons par récurrence sur i que $\delta^*(Q, u_i) = \{1, 2, \ldots, n-i-1\}$.

- pour $i = 0$, par définition de δ, on a bien $\delta^*(Q, u_0) = \delta(Q, a) = \{1, \ldots, n-1\}$;
- supposons le résultat vrai pour $i \geqslant 0$ fixé. Sachant que pour $q \in Q$, $\delta(q, b) = (q+1) \bmod n$, on en déduit par une récurrence rapide que $\delta^*(\{1, 2, \ldots, n-i-1\}, b^{n-1}) = \{0, 1, \ldots, n-i-2\}$. Dès lors, $\delta^*(Q, u_{i+1}) = \delta(\delta^*(\delta^*(Q, u_i), b^{n-1}), a) = \delta(\{0, 1, \ldots, n-i-2\}, a) = \{1, 2, \ldots, n-i-2\}$.

On conclut par récurrence. Finalement, $\delta^*(Q, u) = \delta^*(Q, u_{n-2}) = \{1\}$, donc u est synchronisant pour $\mathcal{C}_n$, et est bien de taille $1 + n \times (n-2) = (n-1)^2$.

Question 17 On commence par remarquer que pour $X \subseteq Q$, alors $\delta(X, b) = \{(q+1) \bmod n \mid q \in X\}$, donc $|\Delta(X)| = |\Delta(\delta(X, b))|$. Ainsi, $\alpha = a$.

De plus, $\delta(X, a) = X \setminus \{0\}$. On en déduit les propriétés suivantes :

- $0 \in X$ et $0 \in \Delta(\delta(X, a))$, sinon $\Delta(X) = \Delta(\delta(X, a))$;
- $1 \in \delta(X, a)$, car $\delta(0, a) = 1$, donc $1 \notin \Delta(\delta(X, a))$;
- en combinant les deux points précédents, $\Delta(\delta(X, a)) = \{n-j, n-j+1, \ldots, n-1, 0\}$.

Finalement, $\Delta(X) = \Delta(\delta(X, a)) \setminus \{0\} = \{n-j, n-j+1, \ldots, n-1\}$.

Question 18 Soit $u = a_1 a_2 \ldots a_k$ un mot synchronisant pour $\mathcal{C}_n$ de taille minimale. Pour $n = 1$, $u = \varepsilon$, de taille $0 = (1-1)^2$, est synchronisant. Pour $n = 2$, ε n'est pas synchronisant (car il y a deux états), mais $u = a$, de taille $1 = (2-1)^2$ est synchronisant. Pour la suite, supposons $n \geqslant 3$.

On commence par remarquer que $a_1 = a$, car $\delta(Q, b) = Q$, donc si bv est synchronisant, alors v aussi. Par minimalité de la taille de u, $a_1 = a$.

Posons, pour $i = 1, \ldots, k$, $X_i = \delta^*(Q, a_1 a_2 \ldots a_i)$. On a $X_1 = \{1, 2, \ldots, n-1\}$ (car $a_1 = a$) et $X_k = \{1\}$ (car u est synchronisant et que 1 est le seul état qui a deux transitions entrantes étiquetées par une même lettre).

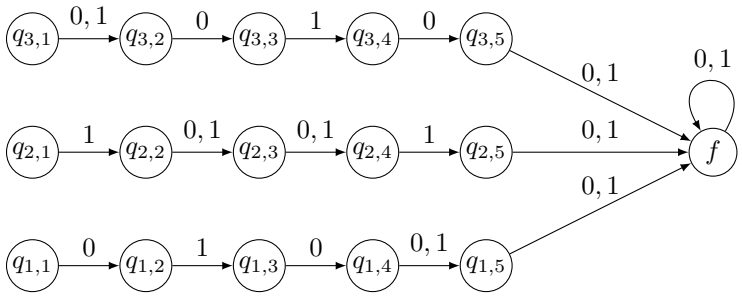
Soit alors $i \in [\![2, k]\!]$ et $j \in [\![1, n-2]\!]$ tels que $|\Delta(X_{i-1})| = j$ et $|\Delta(X_i)| = j+1$. Par la question précédente, $\Delta(X_{i-1}) = \{n-j, n-j+1, \ldots, n-1\}$ et $\Delta(X_i) = \{n-j, n-j+1, \ldots, n-1, 0\}$.

De plus, soit $\ell > 0$ tel que $|\Delta(X_{i+\ell})| = j+2$. Alors $\ell \geqslant n$, car b^{n-1} est le mot le plus court qui peut transformer $\Delta(X_i)$ en $\{n-j-1, n-j, \ldots, n-1\}$ (on applique b $n-1$ fois pour faire « tourner » le « trou » autour de l'automate).

Finalement, $k \geqslant 1 + (n-2) \times n = (n-1)^2$ (il faut augmenter la taille de $\Delta(X_i)$ un total de $n-2$ fois, de 1 à $n-1$).

2.3 Difficulté du mot synchronisant minimal

Question 19 On obtient la machine suivante, à 16 états :



Pour alléger la figure, on a choisi de ne de pas représenter les transitions manquantes, qui doivent pointer vers f.

Question 20 On propose le modèle μ vérifiant $\mu(x_1) = \mu(x_2) = \mu(x_3) = 1$ et $\mu(x_4) = 0$. La première clause est satisfaite par x_1, la deuxième par x_4 et la troisième par x_2. On constate que le mot 1110 est un mot synchronisant.

Question 21 On peut montrer que si u est un mot de taille $\geqslant m+2-k$, alors pour tout i, $\delta^*(q_{i,k}, u) = f$:

- c'est vrai si $k = m+1$ car $\delta(q_{i,m+1}, 0) = \delta(q_{i,m+1}, 1) = f$ et $\delta^*(f, v) = f$ pour tout mot v ;
- si on suppose que c'est vrai pour un certain k, alors c'est vrai pour $k-1$. En effet, si $u = av$, alors $\delta(q_{i,k-1}, a)$ vaut soit $q_{i,k}$, soit f. Dans les deux cas, par hypothèse, la lecture de v amène dans f.

On conclut par récurrence descendante qu'un mot de taille $m+1$ est synchronisant.

On en déduit qu'un mot u de longueur m est synchronisant pour M_φ si et seulement si pour chaque $i \in [\![1, n]\!]$, $\delta^*(q_{i,1}, u) = f$ (car la lecture du mot u depuis n'importe quel autre état amène en f).

Dès lors :

- Supposons que φ est satisfiable et soit μ un modèle de φ. Montrons que le mot $u = \mu(x_1)\mu(x_2)\ldots\mu(x_m)$ est synchronisant. Soient $i \in [\![1, n]\!]$ et $j \in [\![1, m]\!]$, c_i une clause de φ et ℓ_j un littéral x_j ou $\overline{x_j}$ satisfaisant c_i pour μ. On a donc $\mu(\ell_j) = 1$. Par définition de δ, on a $\delta(q_{i,j}, \mu(x_j)) = f$. En effet :
  - si $\ell_j = x_j$, alors $\mu(x_j) = \mu(\ell_j) = 1$ et $\delta(q_{i,j}, 1) = f$ car x_j apparaît dans c_i ;
  - si $\ell_j = \overline{x_j}$, alors $\mu(x_j) = 1 - \mu(\ell_j) = 0$ et $\delta(q_{i,j}, 0) = f$ car $\overline{x_j}$ apparaît dans c_i.

  Si on suppose j minimal tel que ℓ_j est un littéral satisfaisant c_i, alors on a :

  $$\delta^*(q_{i,1}, u) = \delta^*(\delta^*(q_{i,1}, \mu(x_1)\ldots\mu(x_{j-1})), \mu(x_j)\ldots\mu(x_m)) = \delta^*(q_{i,j}, \mu(x_j)\ldots\mu(x_m)) = \delta^*(f, \mu(x_{j+1})\ldots\mu(x_m)) = f$$

  Ce raisonnement pouvant être fait pour tout i (car φ est satisfaite par μ), on en déduit que u est bien synchronisant.
- Supposons que u est un mot synchronisant de longueur inférieure ou égal à m. Remarquons que, f étant un état puits, s'il existe un mot synchronisant u de longueur inférieure ou égale à m, alors pour tout $q \in Q$, $\delta^*(q, u) = f$. Sans perte de généralité, on peut supposer u de longueur exactement m, quitte à rajouter des lettres.

  Posons $u = a_1\ldots a_m$ et définissons la valuation μ par $\mu(x_i) = a_i$. Montrons que μ est un modèle de φ. Soit $i \in [\![1, n]\!]$. Sachant que $\delta^*(q_{i,1}, u) = f$, il existe nécessairement $j \in [\![1, m]\!]$ tel que $\delta(q_{i,j}, a_j) = f$ (sinon $\delta^*(q_{i,1}, u) = q_{i,m+1} \neq f$). Par définition de δ, cela signifie l'une des deux choses :
  - $a_j = 0$ donc $\overline{x_j}$ apparaît dans c_i, et on a $\mu(x_j) = a_j = 0$, donc c_i est satisfaite par μ ;
  - $a_j = 1$ donc x_j apparaît dans c_i, et on a $\mu(x_j) = a_j = 1$, donc c_i est satisfaite par μ.

  Dans tous les cas, c_i est satisfaite par μ, donc μ est un modèle de φ.

Question 22 La construction de la machine M_φ se faisant en temps polynomial, on a montré que `3SAT` $\leqslant_{\mathsf{m}}^{\mathsf{P}}$ `SYNCHRONISANT MINIMAL`. De plus, le problème `SYNCHRONISANT MINIMAL` est dans NP, car un mot u de longueur n est un certificat et on peut vérifier en temps polynomial qu'il est synchronisant.

Attention toutefois, un tel mot u n'est pas nécessairement de taille polynomiale, notamment si n est très grand devant $|Q|$. Pour ce faire, on peut se contenter de considérer un mot de longueur $\min(n, \frac{|Q|(|Q|-1)^2}{2})$ d'après la question 15. On en déduit que le problème est dans NP donc NP-complet.

3 Jeu de synchronisation

Question 23 Il suffit en fait qu'il existe une partie gagnée par 1 pour que M soit synchronisée. Si 1 a une stratégie gagnante, une telle partie existe nécessairement. Soit $a_1, \ldots, a_k$ les lettres choisies par les joueurs lors d'une partie gagnée par 1 et les X_i définis comme dans l'énoncé. Sachant que $X_{i+1} = \delta(X_i, a_{i+1})$, une récurrence rapide permet de montrer que $X_i = \delta^*(X_0, a_1 \ldots a_i)$. Sachant que $X_0 = Q$, pour $u = a_1 \ldots a_k$, on a $X_k = \delta^*(Q, u)$ et $|X_k| = 1$ (car 1 remporte la partie). Le mot u est bien synchronisant pour M.

Question 24 Sens direct : raisonnons par contraposée et supposons qu'il existe $p, q \in Q$ tel que le joueur 1 n'a pas de stratégie gagnante depuis $\{p, q\}$. Ainsi, le joueur 2 a une stratégie gagnante depuis $\{p, q\}$. La stratégie gagnante pour 2 depuis $X = Q$ est alors la suivante : le joueur 2 applique la stratégie gagnante depuis $\{p, q\}$ en ignorant les autres pièces (on suppose que si l'une des pièces initialement sur l'état p ou q se retrouve sur un état en même temps qu'une autre pièce, c'est cette autre pièce qui est enlevée).

Sens réciproque : supposons que le joueur 1 peut gagner depuis toute configuration $\{p, q\} \subseteq Q$. La stratégie gagnante pour 1 depuis Q est la suivante :

> **Tant que** il reste au moins deux états $p \neq q$ qui contiennent une pièce. **Faire**
> Appliquer la stratégie gagnante depuis $\{p, q\}$, jusqu'à ce que les pièces sur p et q se retrouvent sur le même état.

À chaque passage dans la boucle **Tant que**, au moins une pièce est retirée du jeu (peut-être plus). Ainsi, il s'agit bien d'une stratégie gagnante pour 1.

Question 25 Soit $n \geqslant 3$. Montrons qu'il existe, dans $\mathcal{C}_n$, une stratégie gagnante pour 2 depuis la configuration $\{1, 3\}$. Par la question précédente, cela montrera qu'il existe une stratégie gagnante pour 2 depuis $X = Q$.

La stratégie est la suivante :

- pour $X = \{0, 2\}$ ou $X = \{0, n-2\}$, on pose $g(X) = b$;
- sinon, $g(X) = a$.

En effet, avec cette stratégie, le joueur 2 garantit qu'il y aura toujours un état sans pièce entre les deux états qui contiennent une pièce.

Soit f une stratégie pour 1 et $(X_i)_{i \in \mathbb{N}}$ une (f, g)-partie depuis $\{1, 3\}$, dont les lettres sont les $(a_i)_{i \in \mathbb{N}^*}$. Montrons que pour $i \in \mathbb{N}$, $X_i = \{p_i, q_i\}$, avec $p_i - q_i \equiv 2 \bmod n$ (en particulier, $|X_i| > 1$), et $0 \in X_i \Rightarrow i$ est impair (c'est-à-dire que c'est au joueur 2 de jouer).

- la propriété est vraie pour $i = 0$ car $X_0 = \{1, 3\}$;
- supposons la propriété vraie pour $i \in \mathbb{N}$ et distinguons :
  - si c'est au joueur 1 de jouer, comme $0 \notin X_i$, alors si $a_{i+1} = a$, $X_{i+1} = X_i$ vérifie toujours les propriétés, et si $a_{i+1} = b$, alors $X_{i+1} = \{p_i + 1 \bmod n, q_i + 1 \bmod n\}$ vérifie toujours les propriétés ;
  - si c'est au joueur 2 de jouer, si $0 \in X_i$, alors $a_{i+1} = b$ et $X_{i+1} = \{p_i + 1 \bmod n, q_i + 1 \bmod n\}$ vérifie toujours les propriétés (en particulier, $0 \notin X_{i+1}$), sinon, $a_{i+1} = a$ et $X_{i+1} = X_i$ vérifie toujours les propriétés.

On déduit le résultat par récurrence, ce qui montre que la partie est gagnée par le joueur 2.

Question 26 (a) $\Rightarrow$ (c) M étant faiblement acyclique, elle possède un ordre topologique (c'est-à-dire une énumération de $Q = \{q_0, q_1, \ldots, q_{n-1}\}$ telle que $q_i \preccurlyeq q_j \Rightarrow i \leqslant j$). Supposons que q_{n-1} est l'unique puits. Pour $X \subseteq Q$, notons $\min X = q_i$ où $i = \min\{j \in [\![0, n-1]\!] \mid q_j \in X\}$. On a les deux propriétés suivantes :

- pour $a \in \Sigma$, $\min \delta(X, a) \succcurlyeq \min X$, par définition de l'ordre topologique ;
- si $X \neq \{q_{n-1}\}$, il existe $a_X \in \Sigma$, $\min \delta(X, a_X) \succ \min X$, car si $X \neq \{q_{n-1}\}$, $\min X \neq q_{n-1}$, donc possède un voisin qui lui est strictement supérieur (car seul le puits n'a pas d'élément strictement supérieur).

On peut alors montrer par récurrence que la stratégie $f : X \mapsto a_X$ est gagnante pour le joueur 1 (avec $X_{\{q_{n-1}\}}$ choisi de manière quelconque) : à son tour, le joueur 1 pourra faire augmenter strictement l'élément minimal

où il reste une pièce, jusqu'à atteindre q_{n-1} comme unique état avec une pièce.

(b) $\Rightarrow$ (a) M étant faiblement acyclique, elle possède un ordre topologique $(q_0, \ldots, q_{n-1})$. Alors, si M est synchronisée, q_{n-1} est l'unique puits de M (s'il y avait un autre puits, M ne pourrait pas être synchronisée).

(c) $\Rightarrow$ (b) : a déjà été montré à la question 23

Partie Bonus

Question 27 La conjecture de Černý, énoncée en 1964 et toujours un problème ouvert à ce jour, affirme que toute machine synchronisée à n états possède un mot synchronisant de taille inférieure ou égale à $(n-1)^2$. Cette question n'a donc pas de preuve connue !

$\star\star\star$