Road coloring problem

Jérémie Dumas

8 décembre 2010

Résumé

On s'intéresse dans ce qui suit à la question de la synchronisation d'automate, également connu en anglais sous le nom de *Road Coloring problem*. La question est la suivante : étant donné un automate $\mathcal{A}$ fini déterministe complet, est-il possible de ré-étiqueter les lettres sur les arêtes de sorte que $\mathcal{A}$ possède un mot synchronisant, i.e. qui enbbvoie n'importe quel état de $\mathcal{A}$ vers un seul et même état v ?

On donnera des conditions nécessaires et suffisantes à l'existence d'une telle configuration, avec une démonstration dans le cas eulérien (le cas général étant devenu un théorème depuis peu [Tra09]). On présentera également des bornes sur la longueur d'un mot synchronisant, ainsi qu'un algorithme de reconnaissance des automates synchronisables (possédant un mot synchronisant).

Table des matières

Introduction

La question de l'existence d'une coloration synchronisante pour un graphe donné est restée pendant longtemps une conjecture, dont la démonstration a été publiée en 2009 dans un journal [Tra09]. Cette démonstration, pourtant assez courte, repose sur des idées déjà établies dans de précédents travaux. Notez que l'on parle aussi bien de coloration synchronisante d'un graphe que d'étiquetage d'automate fini déterministe complet.

Une idée derrière la notion de synchronisation est de produire un automate robuste aux erreurs : imaginons qu'on lui fournisse une entrée invalide, et qu'on se retrouve dans un état quelconque, inconnu. Alors s'il existe un mot synchronisant, on sait que l'on peut appliquer les instructions correspondantes et qu'à la fin l'automate se retrouvera toujours dans un même état connu v. D'autres applications sont envisageables : si on modélise une carte routière par un graphe orienté, peut-on donner une même série de directions à suivre qui permette à n'importe qui sur la carte de se retrouver ensuite en une même ville donnée ?

D'autres questions qui vienent naturellement après la question de l'existence concerne la longueur minimale d'un mot synchronisant. Jan Černý conjecture en 1964 que la longueur d'un tel mot est bornée par $(n-1)^2$, où n est le nombre de sommets du graphe. Il a montré que cette borne est atteinte, et on connait maintenant des preuves pour certains cas particulier. Mais le problème général reste ouvert.

1 Généralités

1.1 Notations

1.1.1 Graphes

Commençons par introduire les notations utilisées. On notera $G = (V, E)$ un graphe orienté possédant éventuellement des arcs multiples et des boucles (E est donc un multiensemble). On notera $e : v \to u$ si $e = (v, u) \in E$, et $n = |V|$, où $|\cdot|$ désigne le cardinal d'un ensemble (ou multiensemble).

G est dit *fortement connexe* si pour tout $u, v \in V$, il existe un chemin de u à v (on notera alors $u \rightsquigarrow v$). Si $v \in V$, on note $\mathcal{N}^+(v)$ (resp. $\mathcal{N}^-(v)$) son voisinage sortant (resp. entrant). On notera également $d^+(v)$ (resp. $d^-(v)$) son degré sortant (resp. entrant). Notez que l'on n'a pas forcément $d^+(v) = |\mathcal{N}^+(v)|$, du fait de la présence d'arcs multiples.

Un *circuit* dans un graphe orienté est un chemin (une séquence d'arcs) $v \rightsquigarrow v$. La longueur d'un chemin α (resp. circuit) est le nombre d'arcs qui composent ce chemin (resp. circuit), et sera noté $l(\alpha)$. On dira qu'un graphe G est *apériodique* si le pgcd des longueurs de ses circuits vaut 1. Ce pgcd est aussi appelé *cyclicité* de G. On notera enfin L_G l'ensemble des circuits d'un graphe G.

On dira enfin que G est *admissible* (ou k-admissible) si tous ses sommets ont le même degré sortant k. Si de plus tous les sommets ont un degré sortant égal à leur degré entrant $d^+(v) = d^-(v)$, on dit que le graphe (fortement connexe) est eulérien.

Propriété 1. *Un graphe eulérien possède un circuit passant une et une seule fois par chaque arc de G.*

Si G est k-admissible, alors il est possible de colorier les arcs de G de sorte que deux arcs issus d'un même sommet v aient des couleurs différentes $\forall e, f \in E, e : v \to p, f : v \to q, e \neq f \Rightarrow c(e) \neq c(f)$. Une telle coloration sera appelée une coloration propre des arcs. Dans ce qui suit on ne considérera que des graphes orientés admissibles fortement connexes.

1.1.2 Automates

Soit $\mathcal{A} = (V, \Sigma, \delta)$ un automate fini déterministe complet (abrégé en AFDC), sans état initial ni état final. V est l'ensemble des états de $\mathcal{A}$, $\Sigma = \Sigma_k = \{1 \dots k\}$ désigne l'alphabet et $\delta : V \times \Sigma \to V$ la fonction de transition, abrégée en $\delta_a(x)$ si $(x, a) \in V \times \Sigma$. Si $w = a_1 \dots a_m \in \Sigma^+$ est un mot et $x \in V$, on notera $\delta_w(x) = \delta_{a_2 \dots a_m}(\delta_{a_1}(x))$ défini par induction sur $|w|$ longueur de w. On étend encore la notation au cas où $S \subseteq V$ en notant $\delta_w(S) = \cup_{x \in S} \delta_w(x)$. Enfin on notera $\delta_w^{-1}(S) = \{x, \delta_w(x) \in S\}$ l'image réciproque de S selon δ_w.

À un AFDC $\mathcal{A}$ donné on associe canoniquement un graphe orienté $G = (V, E)$ avec $E = \{\!\{(x, y), y = \delta_a(x), a \in \Sigma\}\!\}$. On fera souvent l'amalgame entre l'automate et son graphe associé. De même on peut définir un AFDC $\mathcal{A}$ à partir d'un graphe G et d'une coloration propre c (que l'on confondra avec δ, en posant $\delta_a(x) = y$ ssi $e : x \to y \in E$ et $c(e) = a$).

1.2 Énoncé du théorème

Soit un AFDC $\mathcal{A}$. Un mot w est dit *synchronisant* si $|\delta_w(V)| = 1$, i.e. w envoie n'importe quel état de $\mathcal{A}$ sur un seul état $s \in V$. On dit alors que $\mathcal{A}$ est *synchronisé* en s. On dit aussi qu'un graphe G est *synchronisable* s'il existe un étiquetage de ses arcs tel que l'automate obtenu soit synchronisé en un certain sommet v. Cela correspond aussi à trouver un ré-étiquetage d'un AFDC $\mathcal{A}$ (donné par une nouvelle fonction de transition δ').

On peut alors formuler le théorème du *Road Coloring* comme suit :

Theorème 1. *[Tra09] Soit G un graphe admissible fortement connexe. Alors G est synchronisable si et seulement si G est apériodique.*

L'implication *synchronisable* $\Rightarrow$ *apériodique* est la plus facile (partie 2). On donnera une démontration de la réciproque dans le cas eulérien uniquement (partie 3).

2 Graphes apériodiques

2.1 Une condition nécessaire

Afin de démontrer la première implication du théorème du *Road Coloring*, on utilise une caractérisation des graphes apériodiques.

On dit qu'un graphe $G = (V, E)$ est *cyclique* si on peut partitionner V en $d \geqslant 2$ ensembles $V_0 \dots V_{d-1}$ tels que $\forall (x, y) \in E, \exists i, x \in V_i, y \in V_{i+1 \mod d}$ (les seules arcs sont entre un ensemble de type V_i et $V_{i+1 \mod d}$). Voir figure 1.

Propriété 2. *Soit G fortement connexe. Alors G est cyclique si et seulement si G est périodique.*

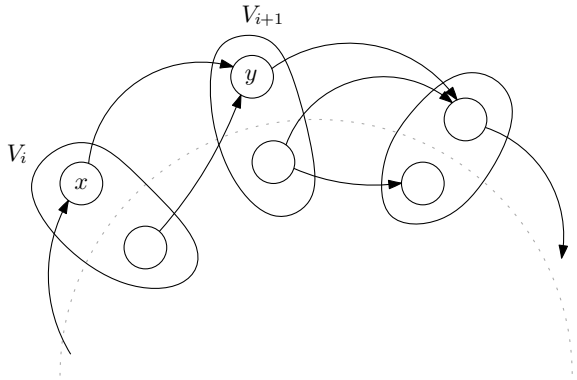

FIGURE 1 – Exemple de décomposition de V

Démonstration. $\Rightarrow$ Assez clairement, si G est cyclique d'ordre d, alors tout circuit α a un nombre d'arc multiple de d. De fait d divise la longueur de n'importe quel cycle de G, d'où d divise leur pgcd.

$\Leftarrow$ Dans l'autre sens, appelons $d = pgcd(L_G) \geqslant 2$ le pgcd des longueurs des circuits de G. Commençons par un petit lemme :

Lemme 1. *Soient $x, y \in V$. Si α_1 et α_2 sont deux chemins possibles de x à y, alors $l(\alpha_1) \equiv l(\alpha_2)\ [d]$.*

En effet, G étant fortement connexe, il existe aussi $\alpha : y \rightsquigarrow x$. Or $\alpha_1\alpha$ est un cycle, donc $l(\alpha_1) + l(\alpha) \equiv l(\alpha_1\alpha) \equiv 0\ [d]$. De même pour α_2. On en déduit que $l(\alpha_1) \equiv l(\alpha_2) \equiv -l(\alpha)\ [d]$.

On peut alors définir une relation d'équivalence sur V par $x \sim y \Leftrightarrow l(\alpha_{x,y}) \equiv 0\ [d]$, où $\alpha_{x,y}$ est un chemin quelconque de x vers y. Il est facile de voir que $\sim$ est réflexive, symétrique et transitive. Notons que cette relation induit au plus d classes d'équivalences différentes.

Considérons maintenant un cycle c quelconque de G, qui commence par $v_0 \dots v_{d-1} \dots$ (il contient au moins d sommets, car $d \mid l(c)$). Chaque v_i pour $0 \leqslant i \leqslant d-1$ appartient à des classes d'équivalence différentes pour $\sim$ (car ils définissent des chemins de v_0 à v_i de longueur $i < d$). On a donc trouvé d classes d'équivalence différentes $V_0 \dots V_{d-1}$ avec $v_i \in V_i$.

On voit finalement que si $(x, y) \in E$, avec $x \in V_i$, alors $y \in V_{i+1 \mod d}$. En effet, par construction des V_j on a au moins un arc (u, v) avec $u \in V_i$ et $v \in V_{i+1 \mod d}$. G étant fortement connexe, on considère alors un chemin $v \rightsquigarrow u \rightsquigarrow x \rightsquigarrow y$; on voit que $l(v \rightsquigarrow u) \equiv -1\ [d]$, $l(u \rightsquigarrow x) \equiv 0\ [d]$, et $l(x \rightsquigarrow y) = 1\ [d]$. On a donc bien $l(v \rightsquigarrow y) \equiv -1 + 0 + 1 = 0\ [d]$, d'où $v \sim y$ et $y \in V_{i+1 \mod d}$. □

On en déduit alors la première implication :

Propriété 3. *Si G fortement connexe possède est synchronisable, alors G est apériodique.*

Démonstration. Raisonnons par contraposée. Supposons G périodique. Alors d'après la propriété 2 il est cyclique et possède une décomposition $V_0 \dots V_{d-1}$ avec $d \geqslant 2$. On voit donc que pour tout mot $w \in \Sigma^+$ et tout étiquetage δ, si

$u \in V_i$ et $v \in V_j$ avec $i \neq j$, on aura forcément $\delta_w(u) \in V_{i+|w| \mod d} = A$ et $\delta_w(v) \in V_{j+|w| \mod d} = B$, avec $A \neq B$. D'où $\forall w, \delta$, on a $\delta_w(V) \neq \{x\}$: il n'existe aucune coloration propre qui possède un mot synchronisant. □

2.2 Algorithme de reconnaissance

2.2.1 Présentation

On donne maintenant un algorithme présenté dans [JS96] qui permet de tester si un graphe fortement connexe est apériodique ou non. L'algorithme utilise la caractéristation 2 ainsi que le lemme 1. L'idée générale est de faire un parcours (en largeur) de G, de construire un arbre à partir de ce parcours, et ensuite de calculer le pgcd d'un ensemble de valeur calculées grâce à un tel parcours. On montre alors que ce pgcd est bien la cyclicité de G.

Plus précisément, considérons un parcours en largeur (BFS) du graphe G à partir de i_0. Cela nous donne un arbre couvrant $T \subseteq E$. Pour $i \in V$, on définit son niveau $level(i)$ comme étant la longueur de l'unique chemin de i_0 à i dans T (c'est la distance à i_0). Assurément deux sommets sur un même niveau sont dans la même classe d'équivalence pour $\sim$ d'après la propriété 2. Reste à chercher quels niveaux regrouper dans une même classe pour obtenir $d = pgcd(L_G)$.

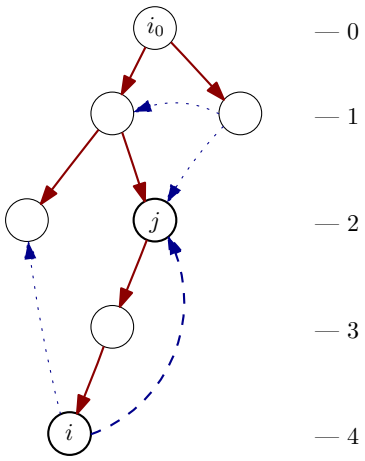

FIGURE 2 – Calcul de $val(i, j)$ à une étape de l'algorithme

Définissons maintenant une valuation sur les arcs $e = (i, j)$. On pose donc $val(e) = level(i) - level(j) + 1 \geqslant 0$ (on a $level(j) \leqslant level(i) + 1$ par construction de T via un BFS). On voit aussi que pour $e \in T$, on a $val(e) = 0$. Et si $e \notin T$, deux cas se présentent (cf. figure 2) :

- j est un ancêtre de i dans T. Alors l'arc (i, j) crée un cycle $\alpha : j \rightsquigarrow i \to j$. Dans ce cas on doit avoir $d \mid l(\alpha) = level(i) - level(j) + 1$.
- j n'est pas sur le chemin de i_0 à i dans T, ce qui nous donne deux chemins différents $\alpha_1 : i_0 \rightsquigarrow j$ via T, et $\alpha_2 : i_0 \rightsquigarrow_T i \to j$. D'après le lemme 1 cela implique que $l(\alpha_1) = level(j) \equiv l(\alpha_2) = level(i) + 1$ $[d]$.

Dans tous les cas, on doit avoir, si $val(e) > 0$, $d \mid val(e)$. Notons alors $g = pgcd\{val(e), val(e) > 0\}$. On a déjà $d \mid g$. Il reste donc à montrer que $g \mid d$ également pour obtenir le résultat voulu.

2.2.2 Correction de l'algorithme

Soit $\alpha : x_0, \dots x_k$ un chemin dans G. On étend la notion de valuation en posant $val(\alpha) = \sum_{s=0}^{k-1} val(x_s, x_{s+1})$. Mais par définition de $val(x_s, x_{s+1})$, on voit bien que $val(\alpha) = level(x_0) - level(x_s) + l(\alpha)$. En particulier si α est un circuit, on a donc $val(\alpha) = level(x_0) - level(x_0) + l(\alpha) = l(\alpha)$. Il s'en suit que $l(\alpha) = val(\alpha) = \sum\{val(e), e \in \alpha, val(e) \neq 0\}$. Or chaque élément de cette somme est positif et divisible par g, d'où $g \mid l(\alpha)$.

On vient de montrer que g divisait la longueur de n'importe quel circuit de G, donc qu'il divise leur pgcd d. Cela achève de montrer la correction de l'algorithme, qui se contente de renvoyer g.

2.2.3 Synthèse, complexité

Notons que l'algorithme présenté s'applique dans le cas où G est fortement connexe. Dans le cas général on peut s'y ramener en calculant les composantes fortement connexes de G, puis en appelant l'algorithme sur chacune de ces composantes. Finalement, l'algorithme peut être décrit assez simplement :

Programme 1 Reconnaissance des graphes apériodiques

Entrée : G orienté fortement connexe.
Sortie : $pgcd(L_G)$ la cyclicité de G.

```
1:  g ← 0 // Valeur par défaut
2:  level ← BreadthFirstSearch(G, v_0) // Pour v_0 quelconque
3:  Pour (i, j) ∈ E faire
4:     val ← level(i) − level(j) + 1
5:     Si val > 0 alors
6:        Si g = 0 alors // Initialisation du pgcd
7:           g ← v
8:        Sinon // Mise à jour
9:           g ← PGCD(val, g)
10:       Fin Si
11:    Fin Si
12: Fin Pour
13: Retourner g
```

Complexité Si $G = (V, E)$ avec $n = |V|$ et $m = |E|$, alors *BreadthFirstSearch* a une complexité $\mathcal{O}(n+m)$. Ensuite, le théorème de Lamé nous donne une borne $\mathcal{O}(\log(t))$ sur le nombre d'itération de l'algorithme d'Euclide pour le calcul du pgcd de deux nombres $a, b \leqslant t$. Or ici $\forall e, val(e) \leqslant n$. D'où, avec la méthode naïve de calcul de pgcd de $k \leqslant m$ nombres présentée ici, l'algo a un coût $\mathcal{O}(m \log(n))$.

Dans le cas général, on peut également calculer les composantes fortement connexes d'un graphe G en temps $\mathcal{O}(n+m)$ (algorithme de Kosaraju ou Tarjan par exemple). Finalement la complexité temporelle de l'algorithme de reconnaissance est donc $\mathcal{O}(n + m \log(n))$.

3 Cas des graphes eulériens

3.1 Généralités

On rappelle qu'un graphe orienté est dit eulérien s'il est fortement connexe et que ses sommets vérifient $d^+(v) = d^-(v)$ (il s'agit plutôt d'une caractérisation mais peu importe). On va démontrer dans cette section qu'un graphe eulérien admissible possède une coloration synchronisante. Commençons par établir le lemme suivant :

Lemme 2. *Soit G orienté dont les sommets ont le même degré sortant et entrant k fixé. Alors on peut colorer les arcs de G avec k couleurs de sorte les arcs sortants (resp. entrants) d'un sommet soient tous de couleurs différentes.*

Remarque. On dira qu'une telle coloration est totalement non synchronisante. En effet, pour chaque mot $w \in \Sigma$, δ_w induit une permutation des sommets.

Démonstration. On transforme notre graphe $G = (V, E)$ où $V = \{v_1, \dots, v_n\}$ en un graphe bipatie *non-orienté* $G' = (X \sqcup Y, E')$ avec $X = \{x_1, \dots, x_n\}$, $Y = \{y_1, \dots, y_n\}$, et tel que $\{x_i, y_j\} \in E'$ ssi $(v_i, v_j) \in E$. G étant eulérien, tous les sommets de G' ont le même degré k par construction (figure 3).

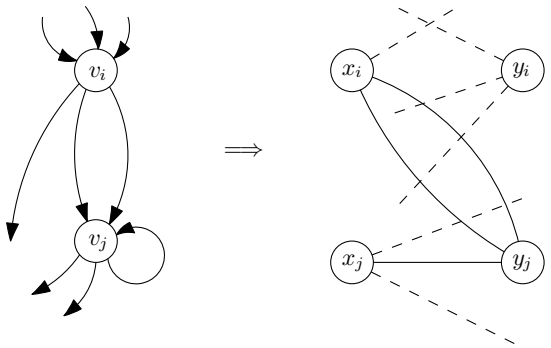

FIGURE 3 – La transformation de G orienté en G' biparti non orienté

En appliquant le théorème de Hall à G', on sait qu'il existe un couplage des arêtes de G' saturant X. Et comme $|X| = |Y|$ il s'agit d'un couplage parfait. Pour montrer que G' vérifie les conditions du théorème de Hall, on montre par récurrence sur $|S|$ que si $S \subseteq X$, alors $|S| \leqslant |\mathcal{N}(S)|$. Supposons l'hypothèse vraie pour $|S| \leqslant p$ fixé. Soit $S = \{x\} \cup S'$ de cardinal $p+1$. Deux cas possibles :

- $|S'| < |\mathcal{N}(S')|$. Auquel cas on peut ajouter x on aura encore $|S| \leqslant |\mathcal{N}(S')|$.
- $|S'| = |\mathcal{N}(S')|$. Comme tous les sommets ont le même degré k, le graphe induit par $S' \cup \mathcal{N}(S')$ a également tous ses sommets de degré k. Cela signifie qu'il n'y a pas d'arêtes dans G' reliant un sommet de $\mathcal{N}(S')$ à un sommet de $X \backslash S'$. Ainsi les voisins de x ne sont pas dans $\mathcal{N}(S')$ et on aura toujours $|S| \leqslant |\mathcal{N}(S)|$.

On peut donc appliquer le théorème de Hall et exhiber M couplage parfait. Les arêtes de M correspondent alors à un circuit de G passant par tous les sommets une et une seule fois. Colorons-les avec la couleur k et retirons ces arcs de G : on obtient un sous-graphe G_1, eulérien lui aussi, car tous ses sommets ont un degré entrant et sortant égal à $k-1$. Par récurrence on peut donc exhiber

une coloration totalement non synchronisante de G_1 avec $k-1$ couleurs, qu'il est facile de compléter pour colorer G.

□

3.2 Taille des sous-ensembles synchronisés

On établit ici quelques résultats intermédiaires relatifs aux sous-ensembles synchronisés de G. Les notions ont été introduites dans [Fri90] et reprises ensuite dans [Kar03] pour le cas des graphes eulériens. On considère un AFDC $\mathcal{A}$; un sous-ensemble synchronisé est un ensemble $S \subseteq V$ pour lequel il existe $w \in \Sigma^+$ tel que $\delta_w(S) = \{x\}$.

Notons θ la taille maximum d'un sous-ensemble synchronisé pour $\mathcal{A}$. Dans le cas eulérien, tout sommet possède k arcs entrants. On remarque que l'on a donc, pour tout sous-ensemble S, la propriété $\sum_{a\in\Sigma} \delta_a^{-1}(S) = k|S|$. On a donc une pour si S un ensemble synchronisé de taille maximum, on a une somme de k élements tous $\leqslant \theta$. D'où $|\delta_a^{-1}| = \theta$ pour tout a. On étends facilement le résultat à $w \in \Sigma^+$, ce qui signifie que pour tout ensemble S synchronisé de taille maximum, et tout mot $w \in \Sigma^+$, alors $\delta_w^{-1}(S)$ est aussi un ensemble synchronisé (a). On peut maintenant établir le lemme suivant :

Lemme 3. *Soit $\mathcal{A}$ un AFDC. Alors il existe une partition de ses sommets en sous-ensembles synchronisés par un même mot w.*

Démonstration. Ce résultat plus général est présenté dans [Fri90]. On donne ici une démonstration dans le cas eulérien en se basant sur les remarques faites précédemment. Considérons une famille $S_1, \ldots, S_p$ d'ensembles de tailles maximum θ synchronisés par un même mot w. Ces ensembles sont envoyés chacun sur un état différent de $\mathcal{A}$ en appliquant w (sinon on aurait trouvé un nouvel ensemble synchronisé de taille strictement supérieure à θ), ils sont donc disjoints.

Supposons que les S_i ne recouvrent pas tout V. On choisit alors un sommet $x \in V - \cup_i S_i$. Notons $y_i = \delta_w(S_i)$ pour $1 \leqslant i \leqslant p$. On a en particulier $\delta_w(x) \neq y_i$ pour tout i. Comme G est fortement connexe, il existe un mot u tel que $\delta_u(y_1) = x$. Considérons alors les ensembles synchronisés par wuw : il y a déjà les $\delta_{wu}^{-1}(S_i)$ pour $1 \leqslant i \leqslant p$, qui sont envoyés sur les y_i. Mais on a aussi S_1, car $\delta_{wuw}(S_1) = \delta_{uw}(y_1) = \delta_w(x) \neq y_i$ pour tout i. On a donc exhibé $p+1$ ensembles synchronisés disjoints de taille maximum.

En répétant le processus jusqu'à ce que les S_i recouvrent V, on obtient bien une partition de l'ensemble des sommets en sous-ensembles synchronisés de taille maximum. □

La démonstration dans se généraliste aux graphes non-eulériens en introduisant une pondération rusée sur les sommets. Si M désigne la matrice d'adjacence d'un graphe $k-admissible$, alors on montre que M admet un vecteur propre à gauche $\omega \neq 0$ tel que $\omega M = k\omega$. On choisit ω à coefficients entiers premiers entre eux. On associe alors à un sommet $v_i \in V$ le poids ω_i. La remarque (a) s'applique encore en remplaçant "taille maximum" par "poids maximum" : si S est un ensemble synchronisé de poids maximum, alors $\delta_a^{-1}(S)$ aussi, et ce pour tout $a \in \Sigma$. La preuve de 3 reste quant à elle inchangée.

3.3 Paires stables, classes d'équivalence

[IKK02] introduit la notion de paire sable, dont on se servira pour la démonstration du théorème du *Road Coloring*dans le cas eulérien. Si $\mathcal{A}$ est un AFDC et x, y sont deux états de $\mathcal{A}$, on dit que $\{x, y\}$ est une paire stable si pour tout mot $u \in \Sigma^*$, il existe $w \in \Sigma^*$ tel que $\delta_{uw}(x) = \delta_{uw}(y)$. On notera alors $x \equiv y$.

Propriété 4. *La relation $\equiv$ est une congruence.*

Démonstration. $\equiv$ est trivialement symétrique et réflexive. Pour la transitivité, il suffit de voir que si $x \equiv y$ et $y \equiv z$ et si $u \in \Sigma^*$, alors il existe $w \in \Sigma^*$ tel que $\delta_{uw}(x) = \delta_{uw}(z)$. En effet on a déjà $\delta_{uw_1}(x) = \delta_{uw_1}(y)$ pour un certain $w_1 \in \Sigma^*$, et de même $\delta_{uw_1w_2}(y) = \delta_{uw_1w_2}(z)$ pour un certain $w_2 \in \Sigma^*$. On voit alors que $w = w_1w_2$ convient. Enfin, si $x \equiv y$, on a également $\delta_a(x) = \delta_a(y)$ pour tout $a \in \Sigma$. D'où $\equiv$ est bien une congruence. □

Les classes d'équivalences pour $\equiv$ sont appelées les *classes de stabilité* de $\mathcal{A}$. On peut alors définir l'automate quotient $\mathcal{F} = (\mathcal{A}/\equiv) = (\mathcal{C}_V, \Sigma, \delta)$ dont les états sont les classes de stabilité. La fonction de transition est bien définie pour $\mathcal{F}$, car $\equiv$ est une congruence.

Quelques remarques avant de continuer : supposons que l'on trouve une coloration synchronisante (un ré-étiquetage) pour l'automate $\mathcal{F}$, alors on peut en déduire une coloration synchronisante pour $\mathcal{A}$. En effet, un ré-étiquetage de $\mathcal{F}$ induit un ré-étiquetage $\mathcal{A}'$ de $\mathcal{A}$ qui respecte les classes d'équivalence (i.e. si x, y est stable dans $\mathcal{A}$, la paire reste stable dans $\mathcal{A}'$). Si de plus la coloration est synchronisante pour $\mathcal{F}$, alors $\mathcal{F}$ ne possède qu'une seule classe d'équivalence pour $\equiv$. D'où $\mathcal{A}'$ est synchronisé.

L'automate quotient est également fortement connexe et apériodique (facile à voir avec la caractérisation 2). Ainsi pour montrer que tout AFDC eulérien fortement connexe et apériodique est synchonisable, on peut raisonner par induction. En effet, pour synchroniser $\mathcal{A}$, il suffit de trouver une paire stable dans $\mathcal{A}$ pour se ramener à un automate quotient eulérien $\mathcal{F}$ possédant un nombre d'états strictement inférieur.

Theorème 2. *Tout graphe admissible eulérien fortement connexe et apériodique possède une coloration synchronisante.*

Démonstration. Si $|V| = 1$, c'est trivial. Supposons maintenant le théorème vrai pour les graphes admissibles eulérien fortement connexe et apériodique possédant strictement moins de n sommets. Soit G un graphe vérifiant ces propriétés mais avec $|V| = n > 1$. D'après les remarques faites précédemment, il suffit d'exhiber une paire de sommet stable pour une certaine coloration propre δ, et d'utiliser l'hypothèse de récurrence.

Commençons par utiliser une coloration totalement non synchronisante δ (qui existe d'après le lemme 2). Soit x qui possèdent deux arcs sortants vers des sommets différents $\delta_a(x) \neq \delta_b(x)$, où $a, b \in \Sigma$ (existe sinon le graphe serait périodique). Notons $y = f_a(x)$ et $z = f_b(x)$. Échangeons les couleurs a et b sur les arcs $x \to y$ et $x \to z$. Alors z possèdent deux arcs entrants de couleur a, et y deux arcs entrants de couleurs b. Or tous les autres sommets possèdent exactement un arc entrant de couleur a (resp. b).

Ainsi, pour tout $S \subseteq V$, si $z \in S$ et $y \notin S$, alors $|\delta_a^{-1}(S)| > S$. De même si $z \notin S$ et $y \in S$, alors $|\delta_b^{-1}(S)| > S$. De fait, si S est un ensemble synchronisé de

taille maximum, alors soit il contient y et z, soit il ne contient aucun des deux (car sinon $\delta_a^{-1}(S)$ ou $\delta_b^{-1}(S)$ serait de cardinal strictement supérieur ...).

On considère maintenant une partition de V en sous-ensembles $S_1 \dots S_p$ de taille maximum synchronisés par un même mot w. Alors y et z appartiennent à un même ensemble synchronisé S_{i_0}, ce qui veut dire que w synchronise y et z. Maintenant, pour tout mot $u \in \Sigma$, on a encore $\delta_{uw}(y) = \delta_{uw}(z)$, car les $\delta_u^{-1}(S_i)$ forment toujours une partition de V en ensembles synchronisés de taille maximale, donc $y, z \in \delta_u^{-1}(S_{i_1})$ pour un autre i_1 éventuellement $\neq i_0$.

Reste à montrer que l'automate quotient $\mathcal{F} = (\mathcal{A}/\equiv)$ est toujours eulérien. C'est à dire que toute classe $\mathcal{C}$ possède k arcs entrants. Pour les classes qui ne contiennent pas y et z, c'est facile : il y a toujours k arcs entrants, tous de couleurs différentes. Et comme $y \equiv z$, la dernière classe a encore des arcs entrants de couleur a (venant de z), et des arcs entrants de couleur b (venant de y). On applique la récurrence à $\mathcal{F}$ qui est un AFDC eulérien, fortement connexe et apériodique : on en déduit une coloration synchronisante pour $\mathcal{A}$. □

3.4 Extension au cas général : un théorème récent

Dans le cas général, cette démonstration ne fonctionne pas, car on utilise une coloration totalement synchronisante pour trouver notre paire stable. Sans pour autant détailler la démonstration générale de [Tra09], on peut quand même en donner l'idée générale. Pour trouver une paire stable dans un graphe vérifiant les bonnes hypothèses, on distingue deux cas. D'abord, s'il existe un sommet p étant le seul voisin sortant de deux sommets différents q et r (tous les arcs sortant de q et r entrent dans p), alors il est facile de voir que $\{q, r\}$ est une paire stable.

Sinon, il n'existe aucun sommet étant le seul voisin sortant de deux autres sommets de G. On introduit alors la notion de *sous-graphe couvrant* de G. $\Gamma \subseteq G$ est un sous-graphe couvrant de G s'il contient tous les sommets V, et que chaque sommet de Γ possède un seul arc sortant. Une remarque importante est qu'un tel sous-graphe consiste en une union de circuits disjoints et d'arbres enracinés en des sommets d'un circuit (où *arbre* désigne ici un sous-arbre maximal de Γ, enraciné en un sommet d'un circuit de Γ, et ne possédant aucun arc en commun avec les circuits de Γ), cf. figure 4.

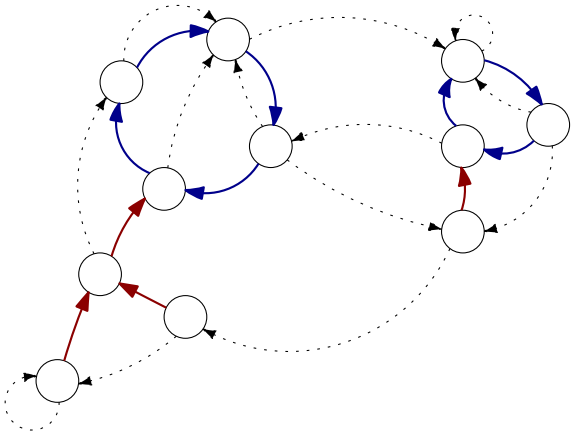

FIGURE 4 – Exemple de sous-arbre couvrant, avec les arbres correspondants.

On définit aussi le niveau d'un sommet v comme étant 0 si v appartient à un cycle de Γ, et sa distance à la racine l'arbre le contenant sinon. On peut alors énoncer le lemme principal de l'article [Tra09], sur lequel repose sa démonstration du théorème du *Road Coloring*.

Lemme 4. *Si G orienté est admissible, fotement connexe et apériodique, alors G possède un sous-graphe couvrant Γ tel que tous les sommets de niveau maximal appartiennent à un seul arbre non trivial.*

4 Conjecture de Černý

4.1 Un problème ouvert

On sait maintenant dans quelles conditions on peut trouver un mot synchronisant w pour G. Une question qui vient naturellement concerne donc la longueur minimale d'un mot synchronisant. Černý dans son papier originel [Če64] que la plus petite longueur d'un mot synchronisant est inférieure à $(n-1)^2$, où n est le nombre de sommets du graphe. Il montre aussi que cette borne est optimale en exhibant une classe de graphes qui ne possèdent pas de mots synchronisants de longueur inférieure à $(n-1)^2$.

La question dans le cas général demeurre un problème ouvert, même si des bornes plus élevées (cubique) existent à ce jour. On peut donner cependant une preuve pour le cas eulérien, qui nous donnera même une borne un peu meilleure, d'au plus $(n-1)(n-2)+1$.

4.2 Le cas eulérien

La démonstration de la conjecture de Černý dans le cas des graphes eulériens fait appel à des propriétés d'algèbre linéaire. On se donne un graphe G synchronisable avec sa coloration synchronisante δ. On identifie les sommets de V avec la base canonique de $\mathbb{R}^n$, vu comme un espace vectoriel de dimension n. Un ensemble $S \in V$ est donc représenté par un vecteur $vecS$ de $\mathbb{R}^n$, somme d'éléments de V. L'application δ_a^{-1}, pour $a \in \Sigma$, peut aussi être vue comme un

endomorphisme de $\mathbb{R}^n$, définie sur les vecteurs de base V. La notation étendue $\delta_a^{-1}(\vec{S})$ coïncide bien avec la nouvelle définition de δ_a^{-1} par linéarité. On étend encore une fois la notation à $\delta_w^{-1} = \delta_a^{-1} \circ \delta_{w'}^{-1}$ si $w = aw' \in \Sigma^+$. Un mot w est donc synchronisant ssi δ_w^{-1} envoie au moins un vecteur de base sur $e = (1, \dots, 1)$.

Si $\forall x \in \mathbb{R}^n$, on définit son poids $|x| = \langle x|e\rangle = \sum_i x_i$. Notons que si $S \subseteq V$, $|\vec{S}|$ correspond bien au cardinal de S. Le graphe G étant k-admissible eulérien, on a donc, pour tout $x \in \mathbb{R}^n$:

$$\sum_{a\in\Sigma} |\delta_a^{-1}(x)| = k|x| \tag{1}$$

Notons que cette équation est vraie quand G est k-admissible, pas seulement eulérien. Il suffit de remplacer dans la définition de $\langle x|e\rangle$ le vecteur e par $\omega \neq 0$ un vecteur propre à gauche de la matrice d'adjacence (pour la valeur propre k), et où les coefficients de ω sont entiers et premiers entre eux.

Démonstration. L'équation (1) s'exprime bien en terme de matrices dans le cas général où G est k-admissible et les sommets pondérés. Notons M la matrice d'adjacence de G (dont les coefficients ne valent pas forcément 1, du fait des arcs multiples), et Δ_a^{-1} la matrice de l'endomorphisme δ_a^{-1} (pas forcément inversible). On a, pour $X \in \mathbb{R}^n$, $\sum_{a\in\Sigma} \Delta_a^{-1} X = MX$. En notant $W = \omega$ défini précédemment, on a donc :

$$\begin{aligned}
\sum_{a\in\Sigma} |\delta_a^{-1}(x)| &= \sum_{a\in\Sigma} (\Delta_a^{-1} X)^{\mathrm{T}} \cdot W \\
&= X^{\mathrm{T}} \cdot (\sum_{a\in\Sigma} \Delta_a^{-1})^{\mathrm{T}} \cdot W \\
&= X^{\mathrm{T}} M^{\mathrm{T}} W = X^{\mathrm{T}} \cdot kW \\
&= k\langle X|W\rangle = k|x|
\end{aligned}$$

□

On remarque finalement que si $x \in \mathbb{R}^n$, alors soit $\forall a \in \Sigma, |\delta_a^{-1}(x)| = |x|$, soit $\exists a \in \Sigma, |\delta_a^{-1}(x)| > |x|$. De fait, si $|\delta_w^{-1}(x)| \neq |x|$ pour $w \in \Sigma^+$, on peut alors construire un mot u de même longueur que w qui vérifie $|\delta_u^{-1}(x)| > |x|$. Notre but va être maintenant de trouver une borne supérieur pour le plus petit mot u ayant cette propriété.

Considérons pour cela l'ensemble $Z_0 = \{x \in \mathbb{R}^n, |x| = 0\}$, espace vectoriel de dimension $(n-1)$. Soit $Z_1 = \{(r, \dots, r), r \in \mathbb{R}^n)\}$ la droite vectorielle engendrée par $\vec{V}$. Z_0 et Z_1 sont deux espaces supplémentaires, c'est à dire que $\forall x \in \mathbb{R}^n, \exists!(x_0, x_1) \in Z_0 \times Z_1, x = x_0 + x_1$. On remarque maintenant que pour tout mot $w \in \Sigma^+$ et tout $x_1 \in Z_1$, on a $\delta_w^{-1}(x_1) = x_1$. Il s'ensuit que :

$$\delta_w^{-1}(x_0) \notin Z_0 \Leftrightarrow |\delta_w^{-1}(x_0)| \neq |x_0| = 0 \Leftrightarrow |\delta_w^{-1}(x)| \neq |x| \tag{2}$$

$$\Leftrightarrow \exists u, |u| = |w|, |\delta_u^{-1}(x)| > |x| \tag{3}$$

Établissons encore quelques résultats intermédiaires :

Lemme 5. *Soit U un sous-espace vectoriel de $\mathbb{R}^n$ et soit $x \in U$. Soit Σ alphabet fini avec pour tout $a \in \Sigma$, φ_a un endomorphisme de $\mathbb{R}^n$. Pour $w = a_1 \dots a_p \in \Sigma^*$, on définit $\varphi_w = \varphi_{a_1} \circ \dots \circ \varphi_{a_p}$. Alors s'il existe un mot w tel quel $\varphi_w(x) \notin U$, il existe un tel mot de longueur $\leqslant \dim U$.*

Démonstration. On définit $U_0 \subseteq U_1 \subseteq \dots$ où U_i est l'espace vectoriel engendré par $\{\varphi_w(x), w \in \Sigma^* \wedge |w| \leqslant i\}$. Si $U_i = U_{i+1}$ pour un certain i, on obtient que $U_i = U_j$ pour tout $j \geqslant i$. En effet, $U_{i+1} = \sum_{a\in\Sigma} \varphi_a(U_i)$, donc dire que $U_i = U_{i+1}$ signifie (en regardant les dimensions) que $\varphi_a(U_i) \subseteq U_i$. On en déduit bien $U_{i+2} = \sum_a \varphi_a(U_{i+1}) = \sum_a \varphi_a(U_i) = U_i$, et le résultat général par récurrence.

Considérons maintenant le plus petit i tel que $\varphi_w(x) \notin U$ avec $|w| = i$. Cela signifie que $U_{i-1} \subseteq U$ mais $U_i \not\subseteq U$. Alors on a des inclusions strictes $U_0 \subset U_1 \subset \dots \subset U_i$, et $1 = \dim U_0 < \dim U_1 < \dots < \dim U_{i-1} < \dim U_i$. On en conclut que $i \leqslant \dim U_{i-1} \dim U$. □

Lemme 6. *Soit $\mathcal{A}$ un automate synchronisé. Soit $x \in \mathbb{R}^n, x \notin Z_1$. Alors il existe $w \in \Sigma^*$ de longueur $\leqslant n-1$ tel que $|\delta_w^{-1}(x)| > |x|$*

Démonstration. On décompose $x = x_0 + x_1$ avec $x_0 \in Z_0$ et $x_1 \in Z_1$. D'après la relation (3), il nous suffit de trouver un mot w tel que $\delta_w^{-1}(x_0) \notin Z_0$ et de longueur $\leqslant n-1$. Commençons par chercher tel mot sans la condition $|w| \leqslant n-1$.

On écrit $x_0 = \lambda_i v_i + \sum_{j\neq i} \mu_j v_j$, où les $v_j \in V$ sont les vecteurs de la base canonique, et avec $\lambda_i \neq 0$. Considérons alors w un mot synchronisant qui envoie les états de $\mathcal{A}$ sur v_i : $\delta_w^{-1}(v_i) = e = (1, \dots, 1)$. On a forcément $\delta_w^{-1}(v_j) = 0$ pour $j \neq i$ (sinon, si la p-ième coordonnée est non nulle cela signifie que $\delta_w(v_p) = v_j$, ce qui est impossible car w synchronise sur v_i). On en déduit :

$$\begin{aligned}\delta_w^{-1}(x_0) &= \lambda_i \delta_w^{-1}(v_i) + \sum_{j\neq i} \mu_j \delta_w^{-1}(v_j) \\ &= \lambda_i e + 0 \in Z_1\end{aligned}$$

Maintenant que l'on a un mot w tel que $\delta_w^{-1}(x_0) \notin Z_0$, on utilise le lemme 5 avec $\varphi_a = \delta_a^{-1}$ et $U = Z_0$. On obtient alors un autre mot w' qui vérifie $\delta_w^{-1}(x_0) \notin Z_0$ et $|w'| \leqslant \dim Z_0 = n-1$. Ce qui donne bien $|\delta_{w'}^{-1}(x)| > |x|$ □

Ce dernier lemme nous permet enfin de démontrer la conjecture de Černý dans le cas d'un graphe eulérien.

Theorème 3. *Si $\mathcal{A}$ est un AFDC synchronisé et si son graphe sous-jacent est eulérien, alors il existe un mot synchronisant w de longueur $\leqslant (n-2)(n-1)+1$.*

Démonstration. Considérons un sous-ensemble strict $S \subset V$. On a en particulier $\vec{S} \notin Z_1$. D'après le lemme 6, il existe alors w de longueur $\leqslant n-1$ tel que $|\delta_w^{-1}(\vec{S})| \geqslant |\vec{S}| + 1$. En répétant le processus i fois, avec $|\vec{S}| + i \leqslant |\vec{V}|$, on obtient que $|\delta_{w'}^{-1}(\vec{S})| \geqslant |\vec{S}| + i$, avec $|w'| \leqslant i \times (n-1)$. On prend alors $i = |V| - |S|$, ce qui nous donne bien $|w'| \leqslant (|V| - |S|) \times (n-1)$.

Choisissons maintenant un sommet v tel que $S = \delta_a^{-1}(v)$ contienne deux arcs entrants étiquetés par la même couleur a (existe car sinon la coloration ne serait pas synchronisante). On applique le raisonnement du paragraphe précédent : on

obtient un mot w de longueur $\leqslant (|V|-|S|)(n-1) \leqslant (n-2)(n-1)$ (car $|S| \geqslant 2$) et tel que $\delta_w^{-1}(\vec{S}) = \vec{V}$. On conclut car wa est alors un mot synchronisant et il est de longueur $\leqslant (n-2)(n-1)+1$. □

Conclusion

Finalement dans ce rapport, on a montré une première implication du théorème du *Road Coloring*, sa réciproque dans le cas des graphes eulériens. On a aussi montré la conjecture de Černý dans le cas des graphes eulériens toujours. En enfin n'oublions pas l'algorithme de reconnaissance des graphes apériodiques.

On peut également conclure en soulignant la multiplicité des outils utilisés. En effet, l'algèbre linéaire montre encore une fois combien elle peut aider sur des questions de graphes ou d'automates. De plus le problème de la synchronisation a des applications dans bien des situations comme on l'a évoqué en introduction de cette synthèse. De plus la question de l'apériodicité fait aussi le lien avec l'étude des chaînes de Markov, quand on se pose la question de la convergence notamment.

Références

[Fri90] Joel Friedman. On the road coloring problem. *Proceedings of the American Mathematical Society*, 110(4) :1133 – 1135, 1990.

[IKK02] Karel Culik II, Juhani Karhumäki, and Jarkko Kari. A note on synchronized automata and road coloring problem. *International Journal of Foundations of Computer Science*, 13(3) :459 – 471, 2002.

[JS96] J. P. Jarvis and Douglas R. Shier. Graph-theoretic analysis of finite markov chains. In *Applied Mathematical Modeling : A Multidisciplinary Approach*. Shier, D.R., Wallenius, K.T., 1996.

[Kar03] Jarkko Kari. Synchronizing finite automata on eulerian digraphs. *Theoretical Computer Science*, 295(1-3) :223 – 232, 2003.

[Tra09] Avraham Trahtman. The road coloring problem. *Israel Journal of Mathematics*, 172 :51–60, 2009.

[Če64] Jan Černý. Poznámka k homogénnym eksperimentom s konecnými automatami. *Matematicko-fyzikálny Časopis Slovenskej Akadémie Vied*, 14 :208 – 216, 1964. (in Slovak).