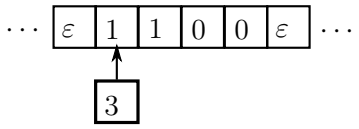
Semaine 4 : Série d'exercices sur la théorie du calcul [Solutions]

1 Machine de Turing

— La machine termine comme ceci :



— Voici une version possible :

ajoute 1
entrée : *écriture binaire d'un entier naturel n* sortie : *écriture binaire de* $n+1$

Tant que caractère lu est '1'
  écrire '0'
  déplacer la tête de lecture à gauche
écrire '1'
déplacer la tête de lecture à gauche
Tant que caractère lu n'est pas 'ε'
  déplacer la tête de lecture à gauche
déplacer la tête de lecture à droite

— Elle ajoute 1 (addition) à un nombre écrit en binaire...
...comme vous allez le voir dans le cours de cette semaine (réflexion préparatoire).

2 Théorie du calcul

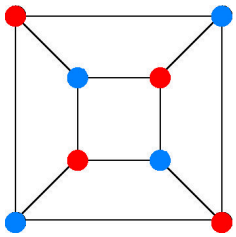
1. — Le problème du tri appartient à P car le meilleur algorithme associé est en $\Theta(n \log n)$. On peut aussi citer le problème de la recherche d'une valeur dans une liste ($\Theta(\log n)$ si la liste est triée et $\Theta(n)$ sinon) ou encore les problèmes de plus court chemin ($\Theta(n)$ à $\Theta(n^3)$ en fonction de ce que l'on fixe (ville de départ, d'arrivée, aucune ou les deux)).
   — La 3-coloration de graphes ou le problème du voyageur de commerce sont décidables, mais leur meilleure complexité connue est exponentielle. De ce fait, on ne sait pas à l'heure actuelle s'ils appartiennent à P. Mais on peut même affirmer que si NP est différent de P, alors ils n'appartiennent pas P [1].
   — La 3-coloration de graphes ou le problème du voyageur de commerce répondent aussi à cette définition.
2. Un algorithme ayant un ordre de complexité important n'est pas pour autant un algorithme difficile à comprendre pour un être humain. La « complexité » mesurée en algorthmique porte sur la durée d'exécution (temps) et l'espace de stockage pour exécuter l'algorithme quand la taille du problème devient grande.

1. On dit que la 3-coloration de graphes est un problème NP-complet.

3. La paire de propositions n'est pas décidable ; on ne peut pas dire si elle est vraie ou fausse. Cela est du au fait que chaque proposition se contredit mutuellement ; c'est une forme d'autoréférence croisée.
4. Seule l'affirmation a) est vraie.

3 Coloriage de graphes

a) Pour le graphe de gauche, la réponse est oui :



Pour celui de droite, la réponse est non (voir **b)** pour une explication).

b) L'algorithme est le suivant : on part d'un sommet (n'importe lequel), qu'on colorie d'une couleur (disons vert). Après cela, on colorie tous ses voisins de l'autre couleur (disons rouge), puis on essaye de colorier tous les voisins des voisins à nouveau en vert, etc. Si en procédant ainsi, on se retrouve à un moment donné avec deux sommets voisins de même couleur, alors on sait qu'un coloriage de tout le graphe avec seulement deux couleurs n'est pas possible. Si par contre, on arrive jusqu'au bout sans problème, alors on a trouvé une solution au problème.

c) Le nombre d'opérations à effectuer pour exécuter l'algorithme ci-dessus est le suivant : au pire, on doit parcourir tous les n sommets du graphe, et à chaque sommet, on doit vérifier qu'aucun des voisins n'a déjà été colorié dans la même couleur que celle qu'on est en train d'utiliser pour colorier le sommet. Comme chaque sommet peut avoir jusqu'à $n-1$ voisins (ce sera le cas pour certains sommets dans certains graphes), on risque donc au pire d'effectuer $\mathcal{O}(n^2)$ opérations en tout. Bien sûr, il se peut qu'on puisse conclure plus vite que ça, mais on est sûr qu'on ne fera pas pire et cela nous suffit. En effet, le fait qu'on n'ait besoin au pire de $\mathcal{O}(n^2)$ opérations [2] pour résoudre le problème suffit pour conclure que le problème du coloriage d'un graphe avec deux couleurs est dans la classe P (c'est un problème soluble en un temps polynomial en le nombre de variables).

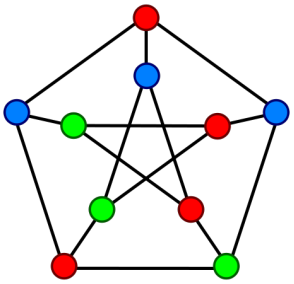
d) Pour vérifier si un coloriage donné avec k couleurs fonctionne, on parcourt simplement tous les sommets du graphe, et pour chacun des sommets, on vérifie qu'aucun de ses voisins n'est colorié de la même couleur que le sommet lui-même. Comme il y a n sommets et que chacun des sommets peut avoir au pire $n-1$ voisins, le nombre total d'opérations nécessaires pour cette vérification est à nouveau en $\mathcal{O}(n^2)$. Le problème du coloriage d'un graphe avec k couleurs est donc dans la classe NP (c'est un problème tel que si on nous donne une solution du problème, alors il est possible de vérifier en un temps polynomial en le nombre de variables si cette solution est correcte ou non).

e*) Sans indication de départ, trouver un coloriage avec trois couleurs qui fonctionne pour un graphe donné est a priori (beaucoup) plus compliqué. Bien sûr, s'il se trouve qu'un coloriage avec deux couleurs fonctionne, comme dans le cas du graphe de gauche, alors automatiquement on sait dans ce cas qu'un

2. Pour rappel, la notation $\mathcal{O}(\cdot)$ inclut toutes les complexités inférieures, nous n'avons **pas** besoin ici de la plus petite de ces complexités. En réalité, cet algorithme est en $\Theta(n)$, mais savoir qu'il est en $\mathcal{O}(n^2)$ nous suffit pour conclure ici.

coloriage avec trois couleurs fonctionne également (il suffit de remplacer la couleur d'un des sommets avec la troisième couleur, par exemple) ; en fait, beaucoup de coloriages avec trois couleurs fonctionnent dans ce cas.

Par contre, si aucun coloriage du graphe avec deux couleurs ne fonctionne (comme dans le cas du graphe de droite), alors tout se complique pour le cas de trois couleurs. Il se trouve que pour le graphe de droite, une tel coloriage existe : (image page suivante)



Comment le trouver ? (comment l'avez-vous trouvé vous-même ?) On peut bien sûr essayer en tâtonnant et espérer avoir de la chance... On peut aussi essayer toutes les possibiliés, comme suggéré dans l'énoncé de l'exercice, mais le nombre d'opérations nécessaires sera alors de 3^n, donc exponentiel en le nombre de variables... Est-il possible de faire mieux ? A l'heure actuelle, la réponse à cette question est : on ne sait pas s'il existe un algorithme capable de résoudre ce problème en un temps polynomial en n (ceci reviendrait à prouver que P=NP).

4 Dénombrabilité

a) Chaque client déjà présent se déplace dans la chambre portant un numéro supérieur d'une unité à celle qu'ils occupent actuellement. cela libère la chambre 1 pour le nouveau client.

b) Chaque client actuel se déplace à la chambre portant le numéro qui est le double de celui de sa chambre actuelle. On peut ainsi utiliser l'infinité des numéros impairs pour les passagers du bus.

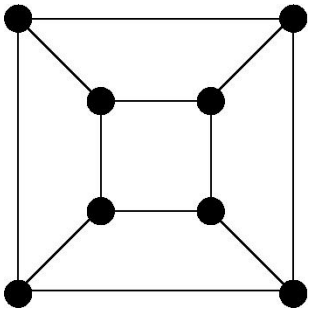
c) Plus difficile, il faut s'inspirer du dénombrement de paires d'entiers pour généraliser la partie 2. Si on imagine que les bus sont alignés sur un parking (un par ligne) on peut imaginer que les passagers de chaque bus apparaissent dans des colonnes (un par colonne). Même avec un nombre infini de lignes et de colonnes, on peut construire un parcours de cette grille en logeant les paires (bus,passager) de même somme car il y a toujours un nombre fini de paires pour une somme donnée. On commence par la somme valant 2 (bus 1, passager 1), puis valant 3 (bus 1, passager 2) et (bus 2, passager 1) etc. (que l'on loge dans les chambres de numéros impairs comme dans l'exercice précédent).

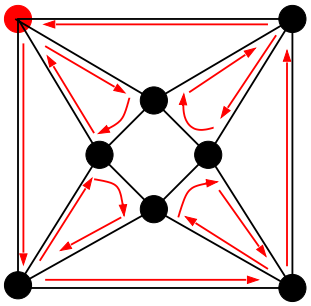
Pour aller plus loin...

5 Chemins eulériens et hamiltoniens

5.1 Chemins eulériens

Il n'existe pas de chemin eulérien qui parcourt le graphe de gauche. Par contre, il en existe un dans le graphe de droite (partant et revenant au sommet en haut à gauche) :



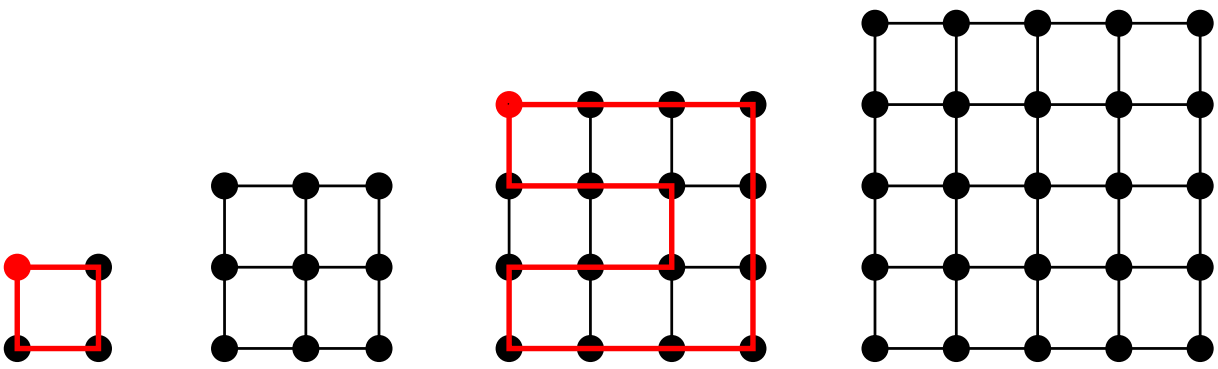


On observe que dans le graphe de gauche, un nombre impair d'arêtes (plus précisément 3) partent de chaque sommet (on dit que le *degré* de chaque sommet est impair). En y réfléchisssant un peu, on peut voir que même si un seul sommet d'un graphe a un degré impair, alors il n'y aura pas de chemin eulérien qui parcourt ce graphe. On peut aussi montrer (mais c'est plus difficile) que dans un graphe dont tous les sommets ont un degré pair, il est toujours possible de trouver un chemin eulérien qui parcourt le graphe.

Ceci nous donne une règle simple pour répondre à la question posée dans l'énoncé : étant donné un graphe avec n sommets, il suffit de calculer le degré de chaque sommet du graphe ; si tous les degrés sont pairs, il existe un chemin eulérien dans le graphe, sinon, il n'en existe pas. Vu que chaque sommet est relié au plus à $n-1$ autres sommets, ce décompte des degrés demande au plus $n(n-1) \in \Theta(n^2)$ opérations. Le problème de trouver un chemin eulérien dans un graphe est donc dans la classe P.

5.2 Chemins hamiltoniens

Parmi les quatre graphes ci-dessous, seuls le premier et le troisième ont un chemin hamiltonien :



Tous ces graphes ont pourtant une structure très similaire (ce sont tous des grilles) ; l'existence ou la non-existence d'un chemin hamiltonien dépend essentiellement de détails subtils. En général, on ne connaît malheureusement pas de règle simple qui permette de décider de l'existence ou non d'un chemin hamiltonien dans un graphe. Des critères ont été trouvés pour *certains* types de graphes : par exemple, si chaque sommet est au moins de degré $n/2$, alors il existe un chemin hamiltonien dans le graphe. Mais un critère simple et général manque encore [3].

La complexité du problème est donc grande a priori : si on veut tester tous les chemins possibles, on devra tester (dans le pire des cas) $n \cdot (n-1) \cdot (n-2) \cdots 3 \cdot 2 \cdot 1 = n!$ possibilités, c'est-à-dire un nombre exponentiel de chemins. Par contre, si on se voit proposer un chemin, il est possible de vérifier en un temps polynomial en n si celui-ci est hamiltonien ou non. Le problème de trouver un chemin hamiltonien dans un graphe est donc dans la classe NP.

Pour le fun...

La seule solution est :

La longueur de cette phrase est de **soixante et un** caractères.

Avec les espaces, nous avons en effet déjà 47 caractères. Il nous faut donc chercher au dessus de 47.

Par ailleurs, l'écriture en lettres d'un nombre croissant nettement moins vite que le nombre lui-même, il est certain que nous n'aurons pas de solution au dessus de, disons, 69 (déjà 9 caractères manquants).

Pour les nombres entre deux, regardons combien de caractères leur écriture ajoute à la phrase :

		et un	-deux	-trois	-quatre	-cinq	-six	-sept	-huit	-neuf
		6	5	6	7	5	4	5	5	5
quarante								13	13	13
cinquante	9	15	14	15	16	14	13	14	14	14
soixante	8	14	13	14	15	13	12	13	13	13

et si l'on soustrait l'écart à 47 (on cherche les 0) :

		et un	-deux	-trois	-quatre	-cinq	-six	-sept	-huit	-neuf
quarante								13	12	11
cinquante	6	11	9	9	9	6	4	4	3	2
soixante	–5	**0**	–2	–2	–2	–5	–7	–7	–8	–9

Pour l'amour des maths...

— Nous avons en effet montré en cours que $\mathbb{N}^2$ est en bijection avec $\mathbb{N}$ (c.-à-d. dénombrable). Or $\mathbb{Q}^+$ (rationnels positifs) est en bijection avec un sous-ensemble de $\mathbb{N}^2$ (écriture sous forme de fraction irréductible), donc $\mathbb{Q}^+$ est dénombrable ; idem pour $\mathbb{Q}^-$ et donc pour $\mathbb{Q}$ tout entier (même démonstration que pour $\mathbb{Z}$ dans le cours).

3. Du reste, trouver un tel critère reviendrait à nouveau à prouver que P=NP !

— La même démonstration que la non-dénombrabilité des fonctions booléeenes peut être faite pour l'écriture (binaire ou même décimale) de tous les nombres réels entre 0 et 1 (« diagonale de Cantor ») : l'intervalle $[0, 1]$ n'est donc pas dénombrable.
— $\mathbb{R}$ contenant cet intervalle n'est donc pas non plus dénombrable.
— $\mathbb{R}\backslash\mathbb{Q}$ n'est donc pas dénombrable (puisque $\mathbb{Q}$ l'est et que $\mathbb{R}$ tout entier ne l'est pas).