CINQ ÉNIGMES POUR LA RENTRÉE

Un bon problème mathématique doit avoir une solution qui ne vient pas toute seule. En voici cinq exemples…

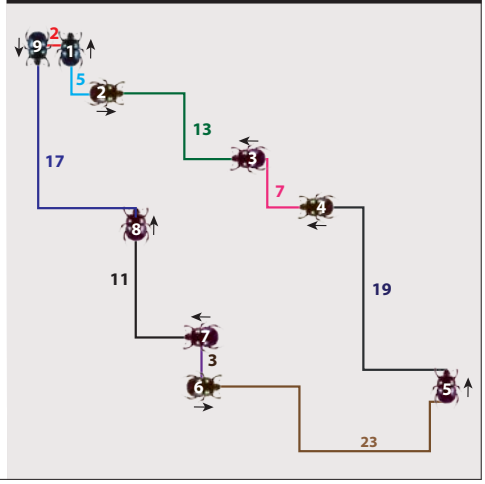
L'AUTEUR

JEAN-PAUL DELAHAYE
professeur émérite à l'université de Lille et chercheur au Centre de recherche en informatique, signal et automatique de Lille (Cristal)

Un de mes professeurs parlait de **démonstration «âne-qui-trotte»** pour désigner les démonstrations qu'on mène en appliquant les définitions de base et en opérant quelques calculs et déductions faciles, n'exigeant aucun effort d'imagination. À l'opposé, les situations que préfèrent les mathématiciens sont celles où les techniques usuelles échouent et où il faut contourner le problème, le prendre par surprise, introduire des éléments qui n'ont en apparence aucun rapport avec l'énoncé et qui brusquement dénouent les difficultés.

De nombreux lecteurs m'ont écrit à la suite de l'article du mois de février où je présentais sept situations miraculeuses propres à réjouir les amateurs de mathématiques de toutes catégories. Puisque ces petits miracles ont intrigué et amusé, en voici cinq autres exposés sous la forme d'énigmes.

1 LES NEUF SCARABÉES



ÉNIGME 1: NEUF SCARABÉES ET DES NOMBRES PREMIERS

On place neuf scarabées sur un circuit, les écarts entre deux scarabées consécutifs, mesurés en mètres le long du circuit, étant l'un des neuf premiers nombres premiers 2, 3, 5, 7, 11, 13, 17, 19 et 23. L'ordre est quelconque et chacun des nombres apparaît une fois exactement. Si l'on fixe arbitrairement le scarabée considéré comme premier, il y a par exemple un écart de 5 mètres entre le premier et le deuxième (en tournant dans le sens horaire), de 13 mètres entre le deuxième et le troisième, de 7 mètres entre le troisième et le quatrième, puis 19, 23, 3, 11, 17 et 2 (entre le dernier et le premier).

Au départ, chaque scarabée choisit au hasard s'il ira, à 1 mètre par minute, dans le sens des aiguilles d'une montre ou dans le sens inverse. Quand deux scarabées se rencontrent, ils font instantanément demi-tour. On suppose que la taille des scarabées est négligeable. Au bout de 50 minutes, après de multiples rencontres et demi-tours des neuf scarabées, on note leurs positions et les écarts qui les séparent. Les neuf écarts sont encore les neuf premiers nombres premiers! Comment expliquer ce miracle arithmétique?

Solution: Notons que le circuit a une longueur de 100 mètres, car 2+3+5+7+11+13+17+19+23=100. Si A est un point du circuit, appelons «point opposé à A» le point B situé à 50 mètres sur le circuit, c'est-à-dire le point à égale distance de A que l'on circule dans le sens horaire ou dans le sens antihoraire.

Imaginons que chaque scarabée porte un drapeau (comme pour l'un des problèmes de février) et que lorsque deux scarabées se rencontrent, ils échangent leurs drapeaux. Chaque drapeau tournera toujours dans le même sens à la vitesse de 1 mètre par minute et, à chaque instant, chaque scarabée portera un seul drapeau.

En cinquante minutes, chaque drapeau aura donc parcouru 50 mètres, ce qui est la moitié exactement de la longueur totale du circuit. Il sera donc arrivé au point opposé à son point de départ. Les positions des scarabées sont les mêmes que les positions des drapeaux, car chaque scarabée, même s'il a changé de drapeau, porte exactement un drapeau. Si le circuit était circulaire, le dessin de leurs positions serait le symétrique par rapport au centre du cercle du dessin initial des positions, et donc les écarts entre scarabées consécutifs seraient les mêmes qu'au départ, c'est-à-dire les neuf premiers nombres premiers. Ces nombres apparaissent dans le même ordre qu'au départ à la condition de tourner dans le sens des aiguilles d'une montre et de partir du scarabée situé au point opposé à celui où se trouvait le premier scarabée dans la description initiale. Que le circuit ne soit pas circulaire ne change pas cette propriété des écarts, qui ne dépend que de la notion de point opposé, et les écarts entre scarabées au bout de 50 minutes sont bien les neuf premiers nombres premiers.

Bien sûr, l'information que les distances sont des nombres premiers n'a aucune importance et constitue un piège: seule leur somme 100 (double de 50) intervient dans la solution.

Notons aussi que ce qui se produit au bout de 50 minutes se produit aussi pour 100 minutes, 150 minutes, etc. mais qu'entre ces moments particuliers, les écarts entre scarabées n'ont pas de raison d'être des nombres premiers.

ÉNIGME 2: DES PAVAGES HEXAGONAUX IMPOSSIBLES

En utilisant des copies des formes A et B (*voir l'illustration 2*), il faut recouvrir parfaitement les figures F_1, F_2, F_3, ou montrer que c'est impossible (les raisonnements d'impossibilité sont importants en mathématiques et on peut les rechercher pour s'entraîner).

On cherche donc à paver F_1, F_2 et F_3 à l'aide des triples hexagones A et B dont on dispose d'autant d'exemplaires que souhaité.

Pour la première forme F_1, c'est impossible car elle est composée d'un nombre d'hexagones (26) qui n'est pas un multiple de 3; or si l'on pave une forme avec A et B, elle sera forcément composée d'un nombre d'hexagones multiple de 3.

Pour la deuxième forme F_2, le nombre d'hexagones (21) est un multiple de 3 et on peut donc envisager de la paver avec des A et des B. C'est pourtant impossible, comme on le voit en raisonnant sur la figure G_1. Pour paver la sorte de pointe en haut (*en bleu*), il faut nécessairement utiliser le pavé A. Ce qui reste alors à paver comporte encore deux sortes de pointes (*en rouge*) qui exigent à nouveau l'utilisation du pavé A, deux fois. Ce qui reste exige à nouveau deux fois la forme A (*en jaune*). Ce qui reste alors (*en vert*) est clairement impossible à paver avec A et B. Le raisonnement s'est déroulé rigoureusement en ne laissant aucune possibilité inexplorée: paver F_2 avec des A ou B est impossible.

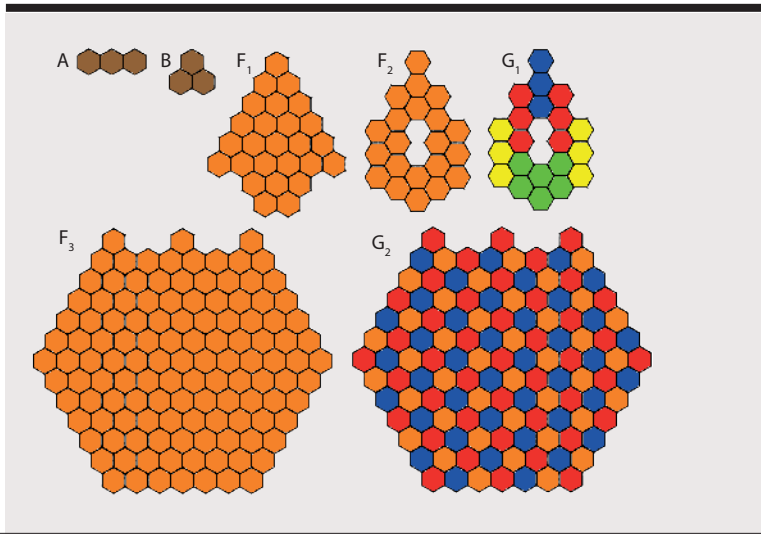
La troisième forme F_3 est elle aussi impossible à paver avec des A ou B, mais c'est moins évident. Comment le démontrer?

Solution: La méthode utilisée pour la forme F_1 ne marche pas, car F_3 contient 123 hexagones, et 123 est multiple de 3. On peut essayer et raisonner en utilisant un argument du même type que celui mené pour F_2. J'ignore si cette méthode aboutit, mais si c'est le cas cela doit être assez compliqué, car plusieurs positionnements des pièces A et B sont possibles quel que soit le point de départ envisagé pour le pavage. Une chose est certaine, la méthode suivante, à l'aide d'un coloriage, est plus rapide. Elle utilise un élément qui n'apparaît pas dans l'énoncé: on colorie le dessin avec trois couleurs comme sur la figure G_2.

On note alors que, en plaçant n'importe où sur ce coloriage une forme A ou B, cette forme couvre nécessairement exactement un hexagone bleu, un rouge et un orange. Si l'on pouvait paver F_3 avec des A et des B, cela impliquerait >

PAVAGES HEXAGONAUX

2



Le dernier ouvrage de J.-P. Delahaye: ***Mathématiques et mystères***, une sélection de ses chroniques parues dans *Pour la Science* (Belin, 2016).

> que F_3 possède autant d'hexagones de chaque couleur. Or F_3 n'a pas le même nombre de pavés de chaque couleur: il y en a 43 de couleur rouge, 40 de couleur bleue et 40 de couleur orange. Elle est donc impossible à paver avec des A et des B.

ÉNIGME 3: SE CONNAÎTRE OU S'IGNORER

Soit k un entier positif. Lorsque n est assez grand, on peut être certain que dans toute assemblée de n personnes, il y en a k qui se connaissent mutuellement, ou alors k qui ne se connaissent pas du tout les unes les autres. Il est intéressant de connaître le plus petit entier n, noté $R(k)$, qui assure cette propriété.

Comme dans l'énigme précédente, nous allons rencontrer une impossibilité; elle est ici encore plus étonnante. Lorsque 6 personnes se rencontrent, alors nécessairement 3 d'entre elles se connaissent mutuellement (a et b se connaissent, b et c se connaissent, a et c se connaissent) ou 3 d'entre elles ne se connaissent pas (a et b ne se connaissent pas, b et c ne se connaissent pas, a et c ne se connaissent pas). On montre cela par le raisonnement (*voir plus loin dans le texte*) ou en écrivant un programme qui examine tous les cas possibles, qui sont en nombre fini (il y a précisément $2^{15}=32768$ graphes à examiner, les personnes étant représentées par des nœuds et leur connaissance mutuelle par des arêtes). Avec moins de 6 personnes, la propriété n'est plus vraie. Avec plus de 6 personnes, la propriété est bien sûr toujours vraie. On dit que le nombre de Ramsey pour $k=3$ vaut 6, et on écrit $R(3)=6$. Pour $k=4$, le nombre de Ramsey est 18: $R(4)=18$. Vous allez être très surpris concernant $R(5)$, le nombre de Ramsey pour $k=5$. Pourquoi?

Solution: La surprise n'est pas que le nombre $R(5)$ n'existe pas ou qu'il soit très grand. La surprise est que personne aujourd'hui ne connaît ce nombre. On sait juste qu'il est compris entre 43 et 48. L'idée d'énumérer par exemple tous les graphes à 43 nœuds pour savoir si 43 convient ou pas est difficile à mettre en œuvre, même avec les plus puissants ordinateurs, car il y en a trop. En effet, il existe $2^{43\times21}$ graphes possibles ayant 43 nœuds, nombre supérieur à 6×10^{271}, or les calculs les plus importants menés pour résoudre des problèmes (par exemple pour casser des systèmes de chiffrement cryptographique) ne comportent au mieux que 10^{21} ou 10^{22} opérations élémentaires, ce qui est très inférieur au nombre en question ici.

On a longtemps disposé uniquement du majorant 49. Ce n'est que récemment que l'on a gagné une unité et que l'on est certain que $R(5)\leq48$. Ce progrès est dû à un travail associant des raisonnements et des calculs massifs par ordinateur menés à leur terme en avril 2017 par Vigleik Angeltveit et Brendan McKay de l'université australienne à Canberra (*voir* https://arxiv.org/pdf/1703.08768.pdf).

Au sujet de ces nombres si faciles à définir et pourtant si difficiles à calculer, le mathématicien hongrois Paul Erdős s'amusait à faire comprendre qu'on ne pourrait jamais aller très loin dans la connaissance des $R(n)$ en racontant l'histoire suivante:

«Si des extraterrestres bien plus puissants que nous arrivent sur Terre et nous demandent la valeur de $R(5)$ sous la menace d'une destruction totale de la planète, alors il faudra enrôler tous nos ordinateurs et tous nos mathématiciens pour calculer ce nombre. En revanche, s'ils nous demandent $R(6)$, nous n'aurons pas d'autres choix que de tenter de les anéantir.»

Si on se limite à la première partie de l'histoire (l'exigence de calculer $R(5)$), il se peut que l'on soit, même sans menace extraterrestre, capable d'y arriver un jour prochain. En effet, de très gros efforts de calcul ont été entrepris pour trouver des graphes à 43 nœuds qui ne contiennent ni sous-ensemble de 5 nœuds sans lien, ni sous-ensemble de 5 nœuds tous liés. De tels graphes prouveraient que $R(5)>43$. Ne pas en trouver suggère que $R(5)=43$ (sans bien sûr que cela puisse être considéré comme une preuve).

Ces recherches infructueuses font cependant espérer que, associé à quelques progrès dans les raisonnements sur ces graphes, on pourrait prochainement prouver définitivement que $R(5)=43$. Si Erdős était vivant, il faudrait donc qu'il envisage de reformuler son histoire... et moi l'énigme proposée ici. Cela serait facile, car, par exemple concernant $R(6)$, on sait seulement qu'il est compris entre 102 et 165. Pour $R(10)$, notre ignorance est sidérante: on sait seulement qu'il est compris entre 798 et 23556 (*voir le tableau de la figure 3*). Sur ces questions, voir l'article de S. Radziszowski dans la bibliographie.

Si le calcul massif est parfois indispensable pour calculer des nombres de Ramsey, le raisonnement n'est pas interdit, et c'est peut-être parce qu'on ne le maîtrise pas bien qu'on doit faire appel aux ordinateurs. À titre d'exemple, voici une démonstration que $R(3)=6$.

Soit une réunion de 6 personnes, parmi lesquelles Alain. Ou bien Alain connaît au moins trois d'entre elles (*cas 1*), ou bien c'est le

3 LES NOMBRES DE RAMSEY DE 1 À 10

k	1	2	3	4	5	6	7	8	9	10
R(k)	1	2	6	18	Entre 43 et 48	Entre 102 et 165	Entre 205 et 540	Entre 282 et 1870	Entre 565 et 6588	Entre 798 et 23556

contraire et il ne connaît pas au moins trois d'entre elles (*cas 2*).

Cas 1. Alain connaît au moins trois autres personnes. Examinons alors les relations que peuvent entretenir les trois connaissances d'Alain entre elles. Si deux d'entre elles se connaissent, alors ces deux personnes et Alain forment un ensemble de trois personnes qui se connaissent. On a obtenu ce qu'on attendait. On peut donc supposer que les trois connaissances d'Alain sont étrangères l'une à l'autre. Dans ce cas, elles constituent trois personnes de l'assemblée qui ne se connaissent pas, on a donc encore obtenu ce qu'on voulait.

Cas 2. Alain ne connaît pas au moins trois des autres personnes. On raisonne comme dans le premier cas, en inversant «connaître» et «ne pas connaître».

Pour voir que 5 personnes ne sont pas suffisantes pour que la propriété «3 se connaissent ou 3 ne se connaissent pas» soit toujours vérifiée, il suffit de considérer la situation suivante: A connaît B, qui connaît C, qui connaît D, qui connaît E, qui connaît A et rien d'autre.

ÉNIGME 4: RENOMMER LES NŒUDS D'UN GRAPHE

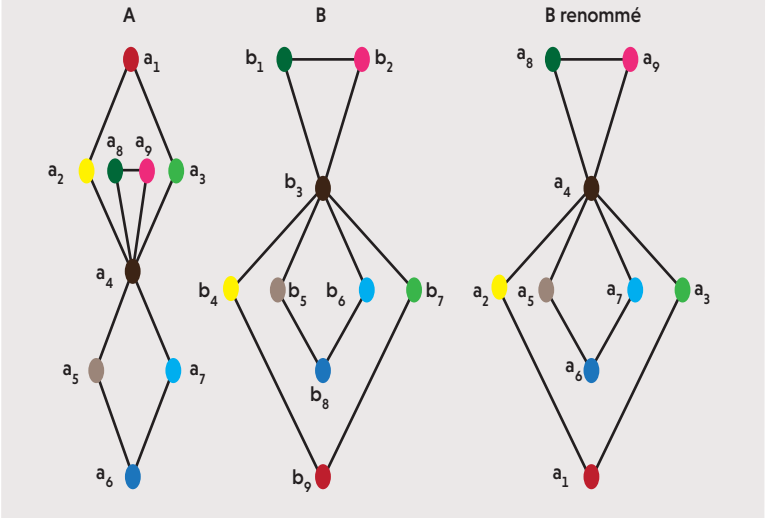
Je dispose de deux très grands graphes notés A et B. Je sais qu'ils sont identiques aux appellations des nœuds près, c'est-à-dire qu'en changeant les noms des nœuds du second par des noms de nœuds du premier et en les plaçant correctement, alors les arêtes des deux graphes sont les mêmes.

Dit autrement, si les arêtes étaient de parfaits élastiques et si je pouvais déplacer les nœuds du second graphe, je pourrais faire coïncider parfaitement les deux graphes (*voir la figure 4*). Lorsque les graphes sont très grands, ces mises en coïncidence sont difficiles à trouver, ce qui fait que l'on peut utiliser la connaissance d'une telle mise en coïncidence comme méthode d'authentification.

Supposons que j'aie eu beaucoup de mal à trouver cette mise en coïncidence par changement des noms, et que mon ami Jacques, qui trouve intéressant le changement des noms qui provoque la mise en coïncidence, souhaite me l'acheter. Il n'a pas confiance en moi car je l'ai escroqué dans une précédente affaire. Il veut que je lui prouve que je dispose de cette mise en coïncidence avant de me l'acheter. Je n'ai pas non plus confiance en lui car lui aussi m'a escroqué récemment (nous ne sommes d'ailleurs plus vraiment amis...). Je ne veux donc pas lui communiquer la moindre information sur la mise en coïncidence dont je dispose car cela pourrait l'aider à la trouver et il ne me l'achèterait pas. Je veux en revanche lui prouver que je connais ce changement des noms du graphe B. Comment mener une telle opération qui semble logiquement impossible?

4

MISE EN COÏNCIDENCE DE GRAPHES



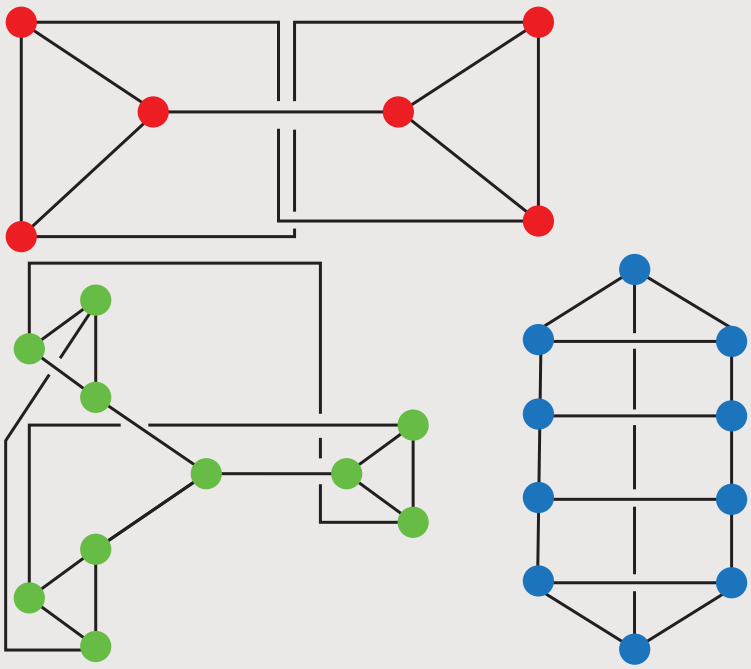
Solution: Le problème est classique et sert souvent comme exemple de «preuve à divulgation nulle de connaissance», un type de protocole utile en cryptographie. Quand deux graphes sont identiques aux noms près des nœuds, on dit qu'ils sont isomorphes, mais nous continuerons à parler simplement de «mise en coïncidence». Voici comment je persuade Jacques.

(a) Je dessine un autre graphe C en changeant les noms des nœuds de A, avec des noms différents de ceux utilisés pour A et B. Je fais bien attention de refaire le dessin en déplaçant les nœuds pour que Jacques ne puisse pas tirer d'informations de la disposition de C. Je le présente à Jacques.

(b) Jacques m'indique alors librement A ou B (éventuellement, il tire à pile ou face pour choisir).

(c) S'il m'indique A, je lui fournis les changements des noms qui transforment C en A. Cela m'est facile, puisque c'est moi qui ai construit C à partir de A. Jacques vérifie que ce changement des noms transforme bien C en A.

(d) S'il m'indique B, alors je lui indique un changement des noms des nœuds de C qui le transforme en B. J'obtiens ce changement en changeant d'abord les noms de C en ceux de A (par exemple c_1 devient a_8, etc.), puis en utilisant la mise en coïncidence que j'ai calculée et que je veux lui vendre pour changer les noms de A en ceux de C (a_8 devient par exemple b_7, etc.). Je lui indique le résultat final de ce double changement des noms (c_1 devient b_7, etc.) qui >



GRAPHES LABYRINTHIQUES

5

> bien sûr définit une mise en coïncidence parfaite entre C et B. Jacques vérifie que c'est bien une mise en coïncidence.

(e) En faisant cela une seule fois, quelqu'un ayant de la chance, mais qui ne connaît pas le bon changement des noms entre A et B, peut répondre de façon satisfaisante: il choisit C en décidant de le mettre en coïncidence avec A et Jacques par chance demande A, ou il choisit C en le mettant en coïncidence avec B et par chance Jacques demande B. Avec une probabilité de 1/2, quelqu'un ne connaissant pas le bon changement de noms entre A et B trompera Jacques.

(f) En revanche, si on opère deux fois ce jeu et que je ne connais pas le bon changement des noms entre A et B, je ne tromperai Jacques qu'une fois sur quatre (il faut que deux fois de suite je gagne à un jeu où j'ai une chance sur deux de gagner). Si l'on recommence le jeu 10 fois, je tromperai Jacques avec une probabilité 1/1024 ($1024=2^{10}$). Etc.

(g) En opérant le jeu autant que Jacques le souhaitera et en réussissant à chaque fois, Jacques finira par être certain que je dispose bien d'un bon changement de noms entre A et B.

(h) Pourtant, même en faisant le jeu 1000 fois, il n'aura rien appris, car les graphes C que j'utilise à chaque fois et pour lesquels je réponds ne lui apprennent qu'un rapport entre A et C ou entre B et C, ce qui ne dit rien sur les rapports entre A et B.

Jacques se décidera à m'acheter ma mise en coïncidence de A et B.

Ce type de protocoles sert à organiser des systèmes d'authentification. Si je choisis moi-même les deux grands graphes A et B en les prenant isomorphes et en les rendant publics, je pourrai m'authentifier vis-à-vis de tout interlocuteur sans jamais affaiblir la méthode, puisque les échanges envisagés dans le protocole ne laissent échapper aucune information sur l'isomorphisme que j'ai choisi, et que je suis le seul à connaître (*voir la bibliographie*).

L'isomorphisme de graphes est un problème délicat dont on a du mal à connaître la classe de complexité. Récemment en 2015, puis en 2017 après s'être rétracté, László Babai, un spécialiste réputé de ces questions, a annoncé disposer d'une démonstration que le problème de l'isomorphisme de graphes était à peu de chose près un problème qu'on peut résoudre en temps polynomial, c'est-à-dire assez rapidement. Si c'était confirmé, alors mon ancien ami Jacques risque de ne plus vouloir m'acheter la mise en coïncidence que nous étions en train de négocier.

ÉNIGME 5: NE PAS SE PERDRE DANS UN LABYRINTHE

On se donne un graphe dont chaque nœud possède exactement 3 arcs (ou arêtes) incidents. On pourrait parler de labyrinthe où 3 chemins exactement se rencontrent à chaque carrefour. Le graphe n'est pas nécessairement planaire (représentable sur un plan sans que les arcs se croisent), mais en chaque nœud, les trois arcs incidents sont placés dans un même plan horizontal, de façon que lorsqu'on arrive à un nœud par l'un des arcs, il y a un arc à droite et un arc à gauche clairement identifiables.

Quelques exemples de tels graphes sont donnés par la figure 5. On peut les disposer sur un plan en acceptant quelques ponts ou tunnels. Cela permet, quand on parcourt de tels graphes et qu'on arrive à un carrefour, de désigner sans ambiguïté l'arc de droite et l'arc de gauche. Les stratégies de parcours «prendre toujours à droite» ou «prendre alternativement à droite et à gauche» sont des stratégies qui vous ramènent à votre point de départ. Il faut le démontrer!

Premier problème. Vous êtes posé sur un arc du graphe et vous avancez en utilisant la méthode suivante: à chaque fois que vous arrivez à un nouveau nœud, vous choisissez l'arc de droite. Prouvez qu'en avançant ainsi, sans jamais revenir en arrière, vous retournerez nécessairement à votre arc de départ.

Deuxième problème. Vous êtes posé sur un arc du graphe et vous avancez en utilisant une méthode un peu plus compliquée: à chaque fois que vous arrivez à un nouveau nœud, vous choisissez alternativement l'arc de droite ou l'arc de gauche. Prouvez à nouveau que vous serez inévitablement ramené à votre arc de départ.