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

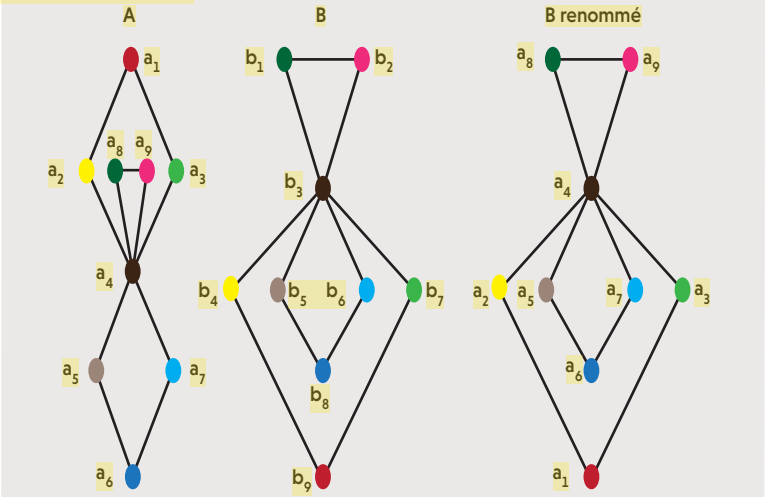
Je dispose de deux très grands graphes notés A et B. Je sais qu'ils sont identiques aux appellations des nœuds près, c'est-à-dire qu'en changeant les noms des nœuds du second par des noms de nœuds du premier et en les plaçant correctement, alors les arêtes des deux graphes sont les mêmes.

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



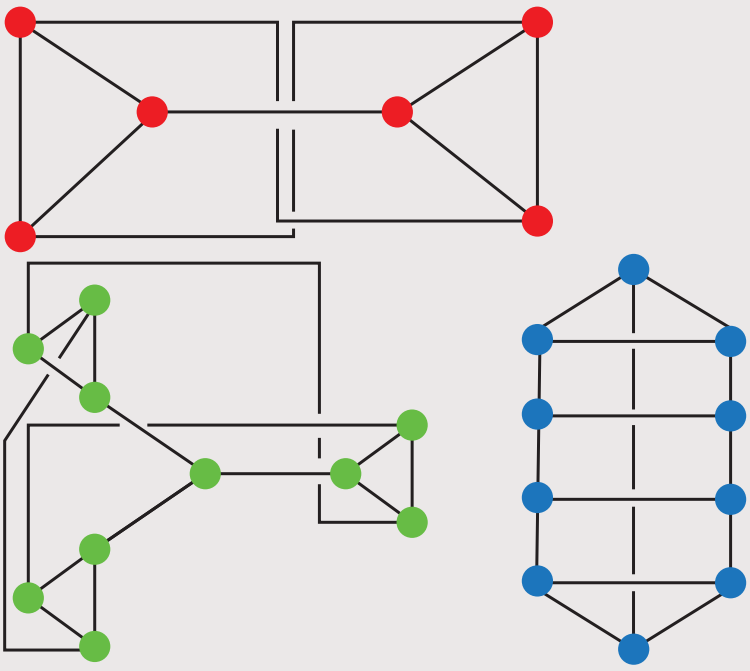
Solution: Le problème est classique et sert souvent comme exemple de «preuve à divulgation nulle de connaissance», un type de protocole utile en cryptographie. Quand deux graphes sont identiques aux noms près des nœuds, on dit qu'ils sont isomorphes, mais nous continuerons à parler simplement de «mise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