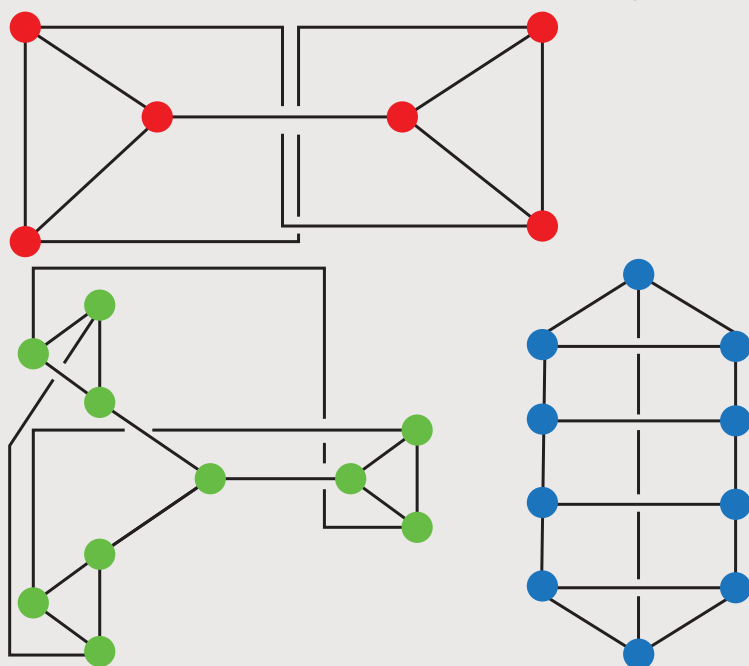




GRAPHES LABYRINTHIQUES

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.