> 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

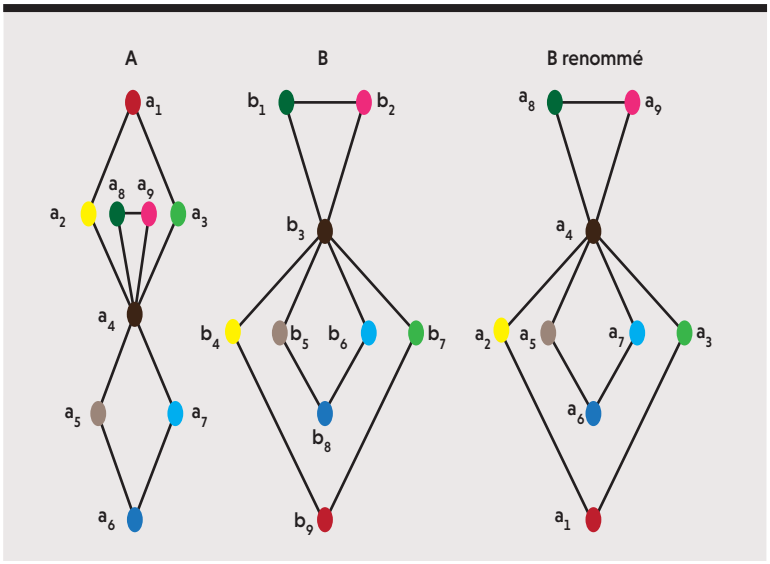
Je dispose de deux très grands graphes notés A et B. Je sais qu'ils sont identiques aux appellations des nœuds près, c'est-à-dire qu'en changeant les noms des nœuds du second par des noms de nœuds du premier et en les plaçant correctement, alors les arêtes des deux graphes sont les mêmes.

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 >