Coloriage secret

Émile Larroque

mai 2024

Niveau de l'activité : classe de terminale (éventuellement classe de première)
Durée de l'activité : 1 h 30 environ

Résumé Il s'agit de faire s'approprier aux élèves une procédure permettant à un *prouveur* de convaincre un *vérificateur* que lui, le prouveur, connaît un secret, sans pour autant rien révéler de ce secret au vérificateur, de sorte notamment que le vérificateur ne puisse pas ultérieurement se faire passer pour le prouveur. Ce type de procédure est ce qu'on appelle une *preuve à divulgation nulle de connaissance* (ou *preuve zero-knowledge*, ZKP) et constitue un outil fondamental et omniprésent de la cryptographie moderne. L'exemple de ZKP pris dans cette activité concerne le 3-coloriage de graphe.

Au sein de leur groupe, les élèves incarnent alternativement les différents rôles / points de vue (rôle de prouveur, rôle de vérificateur, point de vue omniscient) dans différents contextes (prouveur honnête, prouveur malhonnête) développant une intuition de ce qui se joue.

Table des matières

1 Le jeu de rôle et les clefs d'explication pour l'enseignant·e **2**
1.1 La table et les joueurs . . . 2
1.2 Prouver sans divulguer de connaissance . . . 2
1.2.1 Principe général . . . 2
1.2.2 Procédure probabiliste . . . 3
1.2.3 Répéter pour convaincre . . . 3

2 L'activité **4**
2.1 S'approprier le jeu de rôle (15 min) . . . 4
2.2 Divulgation nulle de connaissance (30 min) . . . 4
2.3 Argument probabiliste (30 min) . . . 5
2.4 Conclusion (5 à 10 min) . . . 6

3 Notions d'informatique abordées et compléments théoriques **8**

A Aide de jeu à afficher sur le paravent **9**

B Batterie de graphes et de 3-coloriages **9**

1 Le jeu de rôle et les clefs d'explication pour l'enseignant·e

1.1 La table et les joueurs

Sur la table, un paravent sépare :
— d'un côté ce que voit le prouveur : un graphe 3-colorié à n sommets,
— d'un autre côté ce que voit le vérificateur : le même graphe, dont les sommets ne sont pas coloriés.

Définition 1 (graphe, 3-coloriage). *Un* graphe *est un ensemble fini de* sommets*, dont certaines paires de sommets distincts sont reliées par une* arête.

Un coloriage *consiste à affecter à chaque sommet une couleur. Un* 3-coloriage *est un coloriage qui respecte deux contraintes :*
— *le coloriage utilse au plus 3 couleurs : rouge, vert et bleu, notées r, v et b*
— *deux sommets reliés sont toujours de couleur différentes.*

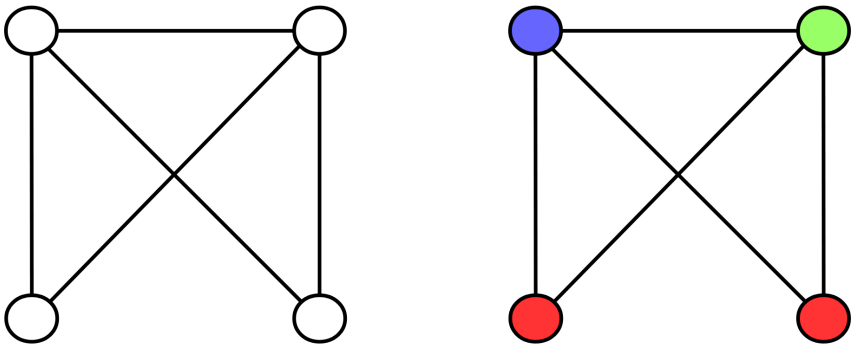


Figure 1 – Un graphe et ce même graphe 3-colorié.

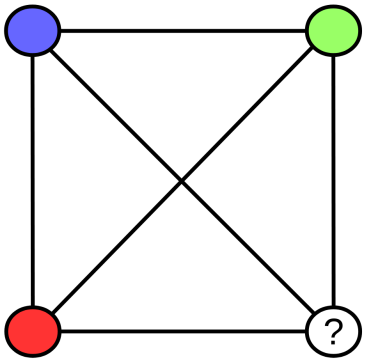


Figure 2 – Le graphe complet à 4 sommets n'est pas 3-coloriable.

Le secret du prouveur, c'est le 3-coloriage du graphe que lui seul voit.

1.2 Prouver sans divulguer de connaissance

1.2.1 Principe général

Pour convaincre le vérificateur qu'il connaît un 3-coloriage, le prouveur met en place une procédure telle que :

— cas honnête : si le prouveur connaît un 3-coloriage du graphe et suit la procédure prévue, alors ce que le vérificateur observe se résume à une variable aléatoire uniforme sur l'ensemble des paires de couleurs différentes : $X \hookrightarrow \mathcal{U}(\{(r;v);(r;b);(v;r);(v;b);(b;r);(b;v)\})$
— cas malhonnête : si le prouveur ne connaît pas de 3-coloriage du graphe, alors il y a une probabilité d'au moins $\frac{1}{n^2}$ que ce qu'observe le vérificateur soit une paire de couleurs identiques : $\mathbb{P}[X \in \{(r;r);(v;v);(b;b)\}] \geq \frac{1}{n^2}$.

La bonne intuition Dans le cas honnête, puisque le vérificateur observe une variable alétoire dont la distribution est connue à l'avance, dit autrement dont la distribution ne dépend pas du secret, alors le vérificateur n'apprend *rien* du secret !

1.2.2 Procédure probabiliste

La procédure se déroule en 4 étapes.

Le prouveur derrière le paravent Le prouveur dispose de cartes dont le recto porte une couleur et les verso sont indiscernables. Le prouveur tire aléatoirement une des 6 permutations possibles des couleurs, la garde secrète et prépare les cartes de couleur pour l'étape suivante.

Engagement devant le paravent Sur le graphe non colorié du vérificateur, le prouveur pose une carte face cachée sur chaque sommet. Il a ainsi posé un coloriage face caché. Dans le cas honnête (où le prouveur connaît un 3-coloriage) les couleurs des cartes correspondent aux couleurs du 3-coloriage secret, sauf que ces couleurs ont été permutées conformément à la permutation tirée à l'étape précédente. Le coloriage face caché est alors un 3-coloriage.

Défi du vérificateur Le vérificateur désigne une arête de son choix sur le graphe.

Révélation du prouveur Le prouveur révèle les deux cartes aux extrêmités de l'arête. Si les deux couleurs sont identiques, alors le prouveur vient d'être démasqué par le vérificateur : il est malhonnête, le coloriage face caché n'est pas un 3-coloriage !

1.2.3 Répéter pour convaincre

Le risque pris par un prouveur malhonnête Si le vérificateur choisit l'arête défi uniformément aléatoirement, alors il est sûr qu'un prouveur malhonnête a une probabilité d'au moins $\frac{1}{n^2}$ de se faire démasquer.

Répéter est très risqué En effectuant cette procédure, un prouveur honnête ne prend aucun risque de révéler son secret, mais un prouveur malhonnête prend un risque d'être démasqué. En répétant la procédure, un prouveur malhonnête finirait donc par être démasqué.

De plus, connaissant un minorant du risque d'être démasqué pris par un prouveur malhonnête ($\frac{1}{n^2}$) le vérificateur peut exiger un nombre de répétitions lui garanissant 10 chances contre 1 de démasquer un éventuel prouveur malhonnête, ou 100 chances contre 1, ou 1 000 000 de chances contre 1 s'il le veux.

Répéter ne révèle rien Parce que répéter la procédure, c'est aussi à chaque fois répéter le tirage de la permutation aléatoire, alors les observations X_1, X_2, X_3 etc. que le vérificateur fait à chaque répétition sont indépendantes identiquement distribuées. Ainsi, la distribution de ce qu'observe le vérificateur est connue à l'avance, et donc indépendante du secret : $(X_1;\ldots;X_k) \hookrightarrow \mathcal{U}(\{(r;v);(r;b);(v;r);(v;b);(b;r);(b;v)\}^k)$ (où k est le nombre de répétitions).

2 L'activité

Les élèves sont répartis par groupes d'environ 6 élèves, en îlots, avec le matériel nécessaire pour chaque îlot.

Matériel pour un îlot :

- un paravent (à fabriquer) : rectangle de carton maintenu vertical, sur lequel afficher l'aide de jeu (Annexe A)
- 10 jetons (ou petites cartes) de chaque couleur (rouge, vert, bleu) dont le dos est identique (jetons non distinguables lorsque face cachée) et qui pour des raisons d'accessibilité ne sont pas distingués que par une couleur mais aussi par une lettre (R, V, B) ou un symbole.
- un dé à 6 faces
- pour chaque graphe qu'on utilise, une paire de feuilles graphe colorié / graphe non colorié (Annexe B)

2.1 S'approprier le jeu de rôle (15 min)

L'introduction présente l'enjeu de l'activité – réaliser une procédure permettant de convaincre un vérificateur qu'on connait un secret, sans rien révéler de ce secret – pour attiser la curiosité des élèves. Elle situe brièvement l'importance des preuves à divulgation nulle de connaissance pour la cryptographie.

Pour familiariser les élèves avec la procédure, on la présente étape par étape tout en la leur faisant réaliser pas à pas. Il s'agit du cas honnête où le prouveur dispose d'un 3-coloriage. Cette présentation n'explicite pas les proprétés de la procédure (non divulgation de connaissance, risque pris par un prouveur malhonnête) qui seront abordées dans la suite de l'activité.

Durant cette phase, les élèves adoptent tous le point de vue omniscient et réalisent une à trois répétitions supplémentaire, afin d'être rôdés et de permettre à l'enseignant·e de passer répondre aux questions dans les groupes.

2.2 Divulgation nulle de connaissance (30 min)

Au sein d'un groupe d'élèves, 2 commencent en position de prouveur et les autres en position de vérificateur. Le côté prouveur reçoit un graphe 3-colorié et le côté vérificateur le même graphe non colorié (Annexe B).

Les groupes d'élève sont indépendants, donc on peut donner le même graphe à tous les groupes (ce qui facilite aussi le dialogue lors de la mise en commun).

Expérimentation (10 min) Les élèves réalisent la procédure de multiples fois. On donne comme objectif au côté vérificateur de trouver un 3-coloriage du graphe en obtenant des informations via la procédure. Il leur est pour cela recommandé de prendre en note tous les résultats et d'élaborer au fur et à mesure au brouillon leurs hypothèses et leur stratégie. (Par ailleurs, la taille du graphe est dissuasive pour la stratégie consistant à essayer de trouver directement un 3-coloriage sans obtenir d'information via le prouveur.)

Cependant, comme vue dans les clefs d'explication pour l'enseignant·e, il n'est pas possible d'obtenir de l'information sur le coloriage par la procédure et il s'agit en fait pour les élèves de s'en faire une première idée par la pratique.

De plus, il est possible pour les élèves de quitter (définitevement) le rôle de vérificateur, pour passer en observateur en adoptant alors un point de vue omniscient. L'élève peut se lever et circuler autour de l'ilôt, d'un côté et de l'autre du paravent. La consigne est donnée qu'il reste au moins un ou deux vérificateurs.

Mise en commun et explications (15 min) On met en commun en classe entière les expériences de chacun des groupes : stratégies, interrogations, etc. Il s'agit de faire émerger l'idée que la procédure ne révèle rien sur le secret au côté vérificateur.

La mise en commun et les explications complémentaires doivent expliciter les points suivants :

- Ce que le vérificateur observe lors d'une répétition se résume à une variable aléatoire uniforme sur l'ensemble des paires de couleurs différentes : $X \hookrightarrow \mathcal{U}(\{(r;v);(r;b);(v;r);(v;b);(b;r);(b;v)\})$. Il faut pour cela expliquer qu'une distribution (les paires de couleurs de sommets voisins) composée par une distribution uniformément aléatoire (la permutation des (paires de) couleurs) donne une distribution uniformément aléatoire.
- Puisque le vérificateur observe une variable alétoire X dont la distribution est connue à l'avance, dit autrement dont la distribution ne dépend pas du secret, alors le vérificateur n'apprend *rien* du secret !
- Les observations X_1, X_2, X_3 etc. que le vérificateur fait à chaque répétition sont indépendantes identiquement distribuées. Cela garantit que la distribution de ce qu'observe le vérificateur soit connue à l'avance, et donc indépendante du secret : $(X_1;\ldots;X_k) \hookrightarrow \mathcal{U}(\{(r;v);(r;b);(v;r);(v;b);(b;r);(b;v)\}^k)$ (où k est le nombre de répétitions).

Revoir sous un jour nouveau (5 min) On laisse les élèves poursuivre avec encore deux répétitions pour leur permettre de voir la divulgation nulle de connaissance qui était à l'œuvre depuis le début. À la fin, on révèle exceptionnellement tout le coloriage de face caché à face visible : il y a effectivement un 3-coloriage, là, sous le nez du vérificateur pendant la procédure, mais celui-ci n'apprend rien dessus !

2.3 Argument probabiliste (30 min)

Les deux élèves du groupe étant restés le plus longtemps dans le rôle de vérificateur forment maintenant le côté prouveur, et les autres le côté vérificateur.

Consigne et mise en place (5 min) « On va recommencer avec un autre graphe. Mais cette fois-ci, dans certains groupes, le côté prouveur ne recevra en fait pas la solution du problème de 3-coloriage. Ils n'auront que le graphe non colorié. Ils auront pour but de convaincre les vérificateurs qu'ils connaissent un 3-coloriage… alors qu'ils n'en connaissent pas. Ce seront des usurpateurs !

L'objectif des vérificateurs est de déterminer si les prouveurs sont des usurpateurs ou s'ils connaissent effectivement un 3-coloriage. Pour cela, si on leur révèle une paire de couleurs identiques, c'est terminé, les usurpateurs sont démasqués.

Donc à chaque répétition, les usurpateurs vont essayer de placer un coloriage face cachée qui soit le moins mauvais possible (avec le plus d'arêtes dont les extrêmités sont de couleurs différentes) ou dont les parties incorrectes sont sur des arêtes qu'ils pensent que les vérificateurs ne vont probablement pas choisir.

Donc les vérificateurs aussi, réfléchissez bien à votre stratégie !

Dernier point pour les vérificateurs. Comme la fois d'avant, vous pouvez à tout moment décider d'arrêter d'être vérificateur et passer en simple observateur de la situation, pour voir derrière le paravent et mieux comprendre ce qui se passe.

Attention pour les usurpateurs : si vous êtes trop lents ou que vous avez l'air de vous emmêler, vous allez vite être suspects. Concrètement, vous disposez du temps que ça prend normalement d'appliquer la permutation. D'ailleurs, n'oubliez pas de lancer le dé même s'il ne vous sert à rien, ça serait dommage d'être démasqués pour si peu !

Maintenant, avant de distribuer les nouveaux graphes, on va laisser 2 min aux prouveurs de chaque groupe pour se concerter et choisir comment ils vont procéder si jamais ils se retrouvent en position d'usurpateur. »

Une fois la consigne donnée, on distribue en fait un graphe non colorié à tous les prouveurs : ils sont tous usurpateurs. De plus, le graphe distribué n'est pas 3-coloriable, si bien que l'enseignant·e est sûr·e que les usurpateurs en vont pas trouver de 3-coloriage à la volée.

On a quelques graphes en réserve pour pouvoir relancer un groupe dont les usurpateurs se feraient trop vite démasquer.

Expérimentation (10 min) Les élèves réalisent la procédure de multiples fois. On s'arrête quand les usurpateurs ont été démasqués par l'observation d'une paire de mêmes couleurs dans deux groupes.

Pour une classe de 35 élèves, on fait 6 groupes. Avec des graphes de 15 arêtes, ça fait qu'en 6 répétions on passe sous les 10% de probabilité qu'aucun usurpateur n'ait été démasqué (si le côté vérificateur choisit aléatoirement et que les usurpateurs arrivent à n'avoir qu'un seul conflit dans leur coloriage, donc c'est une estimation à la hausse).

Une fois qu'un groupe a démasqué ses usurpaeurs, on les fait réfléchir ensemble sur la stratégie à adopter pour le côté vérificateur.

Mise en commun et explications (15 min) On met en commun en classe entière les expériences de chacun des groupes : stratégies, interrogations, etc. Il s'agit de faire émerger l'idée que la procédure finira par démasquer un éventuel usurpateur… pour peu que le vérificateur tire l'arête défi au hasard.

La mise en commun et les explications complémentaires doivent expliciter les points suivants :

- **Risque pris par un prouveur malhonnête :**
  - Par définition un prouveur malhonnête ne connait pas de 3-coloriage, donc le coloriage qu'il place face cachée comporte au moins une arête monochromatique.
  - Si le vérificateur choisit l'arête défi uniformément aléatoirement, alors il est sûr qu'un prouveur malhonnête prend un risque d'au moins $\frac{1}{a}$ de se faire démasquer (où a désigne le nombre d'arêtes du graphe).
- **Garantie pour le vérificateur :**
  - En répétant la procédure, un prouveur malhonnête finirait donc par être démasqué.
  - De plus, connaissant un minorant du risque d'être démasqué pris par un prouveur malhonnête ($\frac{1}{a}$), le vérificateur peut exiger un nombre de répétitions lui garanissant 10 chances contre 1 de démasquer un éventuel prouveur malhonnête, ou 100 chances contre 1, ou 1 000 000 de chances contre 1 s'il le veux.
  - Éventuellement, on peut faire remarquer que dans le cas d'un usurpateur, la probabilité d'échouer à le démasquer décroît géométriquement avec le nombre de répétitions : diviser par 2 cette probabilité demande d'ajouter un nombre forfaitaire de répétitions.

2.4 Conclusion (5 à 10 min)

Structure du présent exemple Finalement, pour convaincre le vérificateur qu'il connaît une solution secrête à un problème, le prouveur met en place une procédure telle que :

- **non divulgation de connaissance** : si le prouveur connaît une solution secrête et suit la procédure prévue, alors ce que le vérificateur observe se résume à une variable aléatoire qui suit une distribution donnée, connue à l'avance et indépendante du secret
- **preuve probabiliste** : si le prouveur ne connaît pas de solution, alors le vérificateur peut s'en apercevoir avec probabilité p ; p pouvant être décidée à l'avance et arbitrairement proche de 1.

C'est ce qu'on appelle une preuve à divulgation nulle de connaissance, ou preuve zero-knowledge.

Usage en cryptographie Pour un usage en cryptographie, et donc à distance, il faut imaginer que les jetons face cachée sont plutôt sous clef dans un coffre et que retourner un jeton correspond plutôt au fait pour le

prouveur d'envoyer la clef permettant d'ouvrir le coffre.

Les preuves zero-knowledge sont à la base de la cryptographie moderne. Un exemple simple d'usage est l'authentification en linge : je peux montrer que je suis bien la personne qui connait un 3-coloraige du graphe affiché sur le profil de cette célébrité.

En pratique, on utilise des preuves zero-knowledge moins gourmandes en calcul que le 3-coloriage de graphe.

Ouverture Même si c'est difficile de trouver un 3-coloriage, ce n'est pas impossible. Il faut donc changer régulièrement de paire graphe 3-coloriable, 3-coloriage. Heureusement c'est assez facile de générer un graphe 3-colorié : on tire au hasard la couleur du prochain sommet qu'on rajoute, puis on tire au hasard parmi les sommets de couleur différente ceux qui lui seront relié, puis on recommence.

3 Notions d'informatique abordées et compléments théoriques

Théorie des graphes La théorie des graphes est omniprésente en informatique. Elle permet de formuler des problèmes d'une façon simple, qui se prête à une étude mathématique. Au-delà de son utilité pour la modélisation, il s'agit d'un outil d'abstraction puissant permettant de concevoir et de décrire des situations variées.

Faire manipuler des graphes aux élèves comme dans cette activité leur sera utile dans leurs apprentissages ultérieurs d'informatique.

Théorie de la complexité Le *problème de 3-coloriage* prend en entrée un graphe et en sortie indique si il est 3-coloriable ou non. Le problème de 3-coloriage est NP-complet. Concrètement, il fait consensus de conjecturer qu'il n'existe pas d'algorithme résolvant ce problème qui demande un nombre d'opération polynomial en la taille du graphe en entrée. Casser un secret consistant en un 3-coloriage est en ce sens conjecturé difficile.

Inversement, effectuer la procédure présentée ici pour atteindre un argument à un contre h pour h fixé (par exemple 1 000 000) demande un nombre d'opération seulement polynomial en la taille du gaphe. De même, générer un graphe 3-colorié de taille n est polynomial en n. Ainsi, générer des 3-coloriages secrets et réaliser de telles preuves zéro-knowledge pour mettre en place des protocoles cryptographiques est relativement facile (pour les agents honnêtes qui respectent le protocole).

De façon générale en cryptographie, on montre qu'un protocole cryptographique (chiffrement, authentification etc.) est sécurisé en le paramétrant par un nombre n appelé paramètre de sécurité et en montrant que casser le protocole demande exponentiellement plus (en n) de ressources calculatoires que ce qui est nécessaire pour les agents qui l'utilise honnêtement. Ces preuves reposent le plus souvent sur des conjectures consensuelles de théorie de la complexité.

Les preuves zero-knowledge dans la communication scientifique Les preuves zero-knowledge sont un sujet particulièrement peu vulgarisé, surtout en français. Lorsqu'elles le sont, c'est souvent de façon peu approfondie au détour d'un intérêt pour les cryptomonnaies.

Cet état de la communication scientifique sur ce sujet ne rend pas compte de son importance. D'une part, les preuves zero-knowledge sont au fondement de la cryptographie moderne, ce que ne sont pas d'autres sujets plus vulgarisés de cryptographie comme le code de César ou la machine Enigma. D'autre part, comme témoin de leur importance, Shafi Goldwasser, co-inventrice des preuves zero-knowledge dans les années 1985, du fait de l'importance de ces travaux (et d'autres) a reçu le Prix Turing (équivalent en informatique du Prix Nobel) en 2012.

Pour s'approprier facilement les preuves zero-knowledge, on rapporte néanmoins une vidéo francophone de vulgarisation de grande qualité de décembre 2023 : https://www.youtube.com/watch?v=OSdcnoAmohs. Dans le cadre de cette activité, elle peut servir à l'enseignant·e à avoir une compréhension plus poussée du sujet. Elle peut aussi être indiquée aux élèves comme contenu pour approfondir.

Ci-dessous on trouve :
— l'Annexe A qui présente l'aide de jeu
— l'Annexe B qui présente les graphes
— suivi de l'ensemble de ce qu'il y a à imprimer pour un groupe
  — deux exemplaires de l'aide de jeu, un pour chaque côté du paravent
  — pour chaque graphe 3-coloriable, la version 3-coloriée à donner au côté prouveur et la version non coloriée à donner au côté vérificateur
  — pour chaque graphe non 3-coloriable, deux exemplaires non coloriés à donner l'un au côté prouveur et l'autre au côté vérificateur.
  — **Attention :** on conseille d'imprimer de façon non assemblée de sorte à facilement former des paquets de feuille à distribuer au fur et à mesure de l'activité.

A Aide de jeu à afficher sur le paravent

L'aide de jeu résume graphiquement la procédure de preuve zero-knowledge en présentant ce qui se passe lors d'une répétition. Elle vise notamment à rendre clair qu'à chaque répétition la permutation des couleurs doit être tirée à nouveau.

B Batterie de graphes et de 3-coloriages

Les graphes données ci-après dans les éléments à imprimer sont de deux types : les graphes 3-coloriables (fournis avec et sans 3-coloriage) et les graphes non 3-coloriables. Imprimés en taille A4, les graphes sont d'une taille adaptée pour utiliser des jetons de la taille de ceux qu'on trouve dans un jeu othello par exemple.

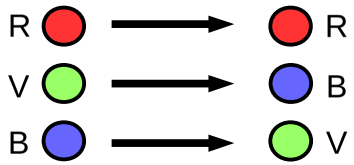
Pour refaire l'activité avec d'autres graphes, on conseille les critères suivants :
— graphe 3-coloriable :
  — taille suffisamment grande pour dissuader la recherche de 3-coloriage par les vérificateurs
  — graphe sans triangle pour éviter les déductions simples de triplets de sommets devant être de couleur différente : c'est important pour éviter que des élèves du côté vérificateur aient l'impression de progresser dans leur découverte du coloriage secret et surtout éviter qu'iels aient l'impression d'avoir obtenu des informations sur le coloriage via la procédure de preuve zero-knowledge
— graphe non 3-coloriable :
  — taille suffisamment petite pour que la probabilité soit assez grande que dans un groupe les vérificateurs démasquent les prouveurs usurpateurs
  — graphe sans triangle pour éviter les déductions simples de triplets de sommets devant être de couleur différente : c'est important pour que les prouveurs usurpateurs ne se rendent pas compte (rapidement) que le graphe n'est pas 3-coloriable (ou, si on décide plutôt de les lancer sur un graphe 3-coloriable, pour qu'ils n'arrivent pas à trouver un 3-coloriage et cessent alors d'être usurpateur).

Tous les graphes donnés dans les éléments à imprimer sont sans triangle. Le premier graphe non 3-coloriable est le graphe de Perteson. Il s'agit d'un exemple de petite taille de graphe sans triangle non 3-coloriable.

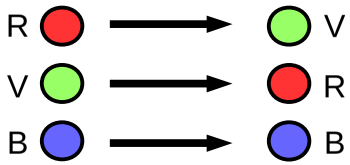
ÉTAPE 1 : prouveur

tire le dé – change les couleurs – pose face cachée

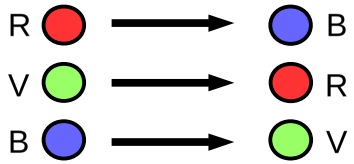
1



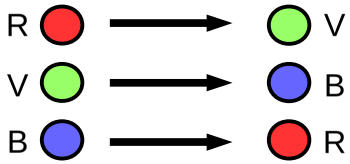
2



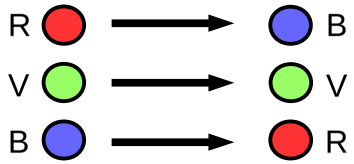
3



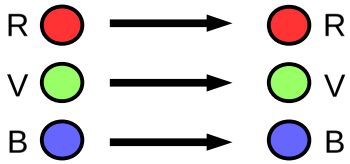
4



5

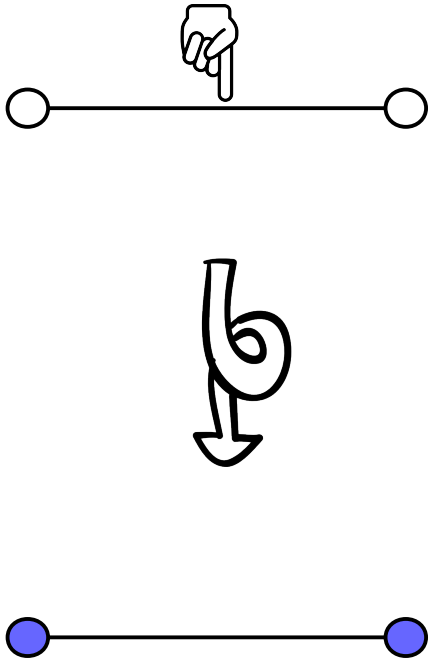


6



ÉTAPE 2 : vérificateur

choisi une arête pour défier le prouveur – le prouveur révèle les extrêmités

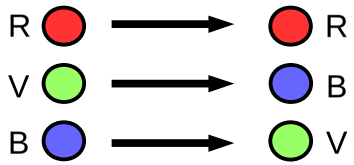


même couleur
=
prouveur a perdu

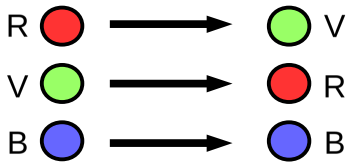
ÉTAPE 1 : prouveur

tire le dé – change les couleurs – pose face cachée

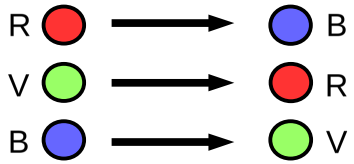
1



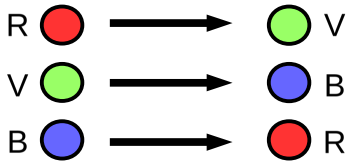
2



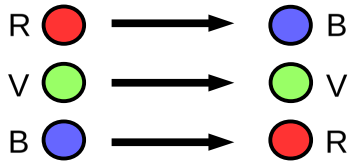
3



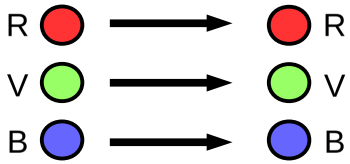
4



5

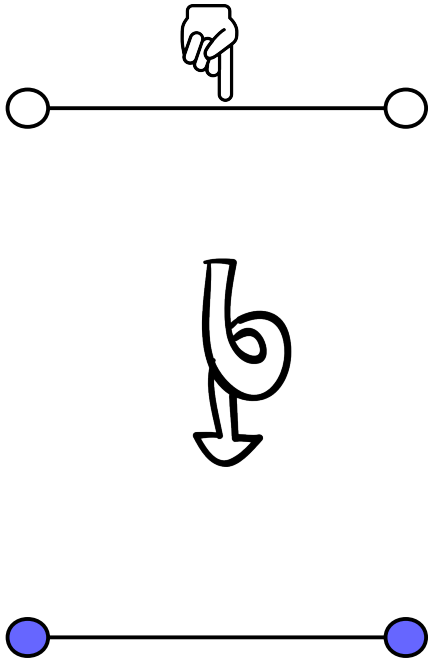


6



ÉTAPE 2 : vérificateur

choisi une arête pour défier le prouveur – le prouveur révèle les extrêmités



même couleur
=
prouveur a perdu