Faire de maths ... c'est cool !!

J.L. Ramírez Alfonsín

IMAG, Université de Montpellier

Lycée E. Hemingway, Nîmes, 15 mars 2024

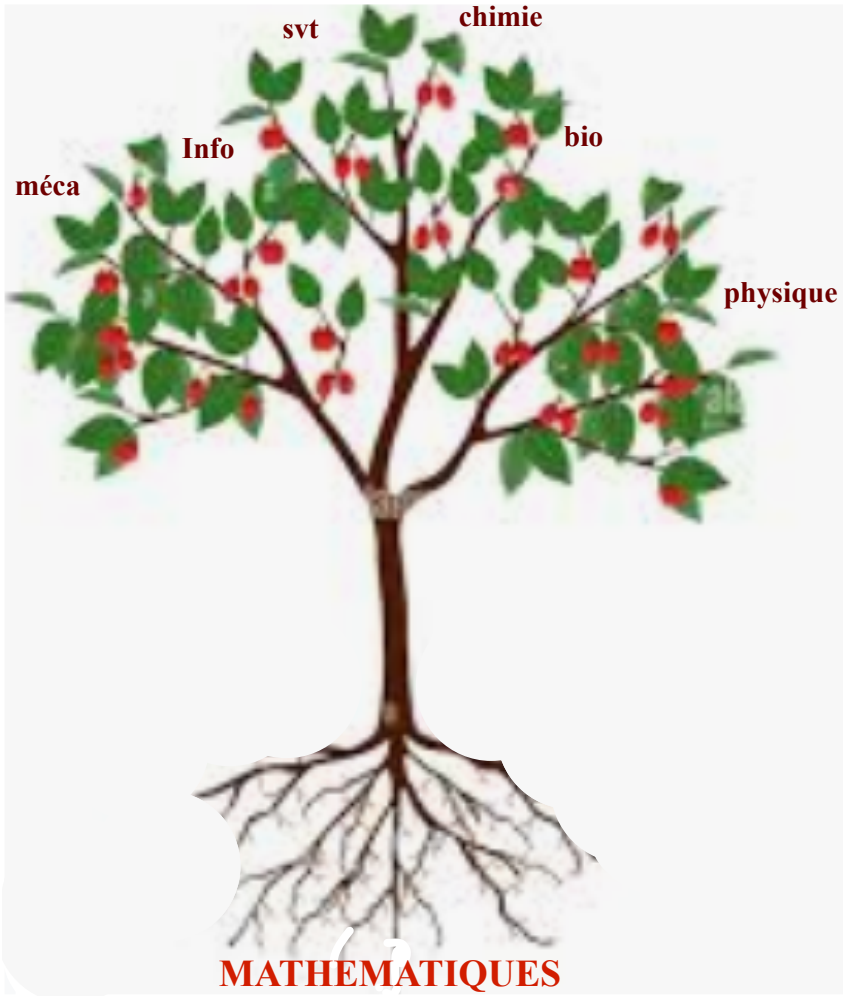
Mathématiques : la mère des sciences !

Interactions des mathématiques avec beaucoup d'autres disciplines.

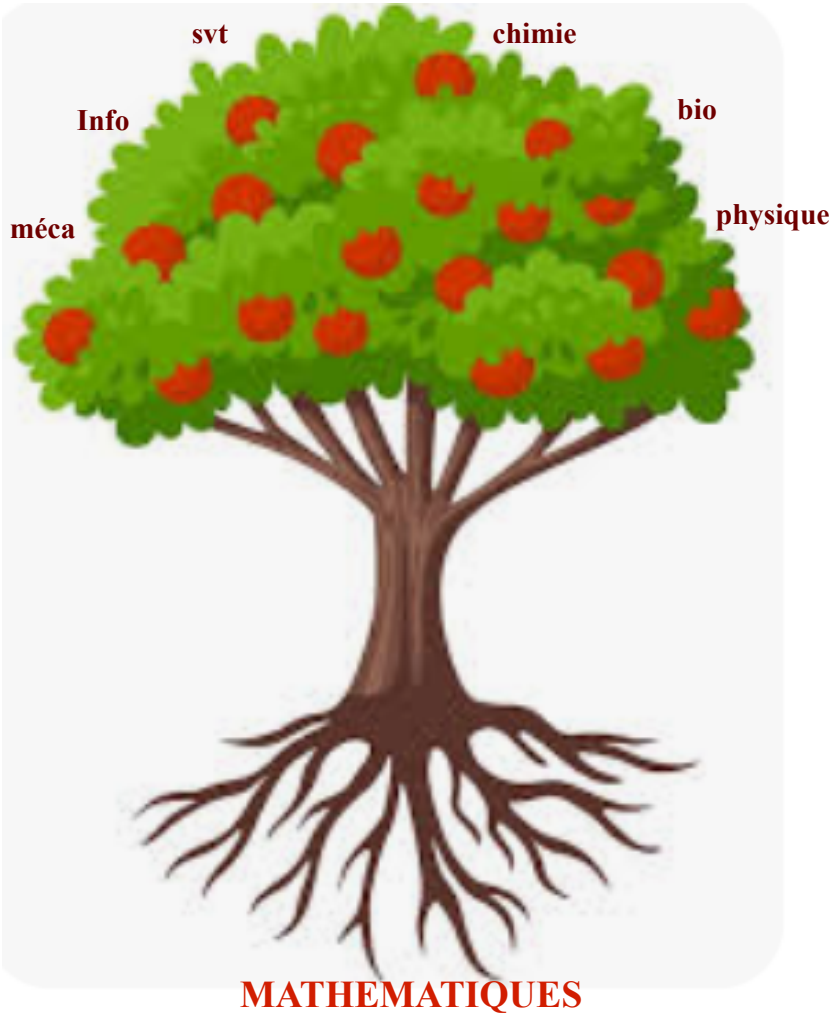
Mathématiques : la mère des sciences !

Interactions des mathématiques avec beaucoup d'autres disciplines.

L'arbre des sciences



L'arbre des sciences



Plus fortes et solides sont les racines, plus les fruits seront abondants !

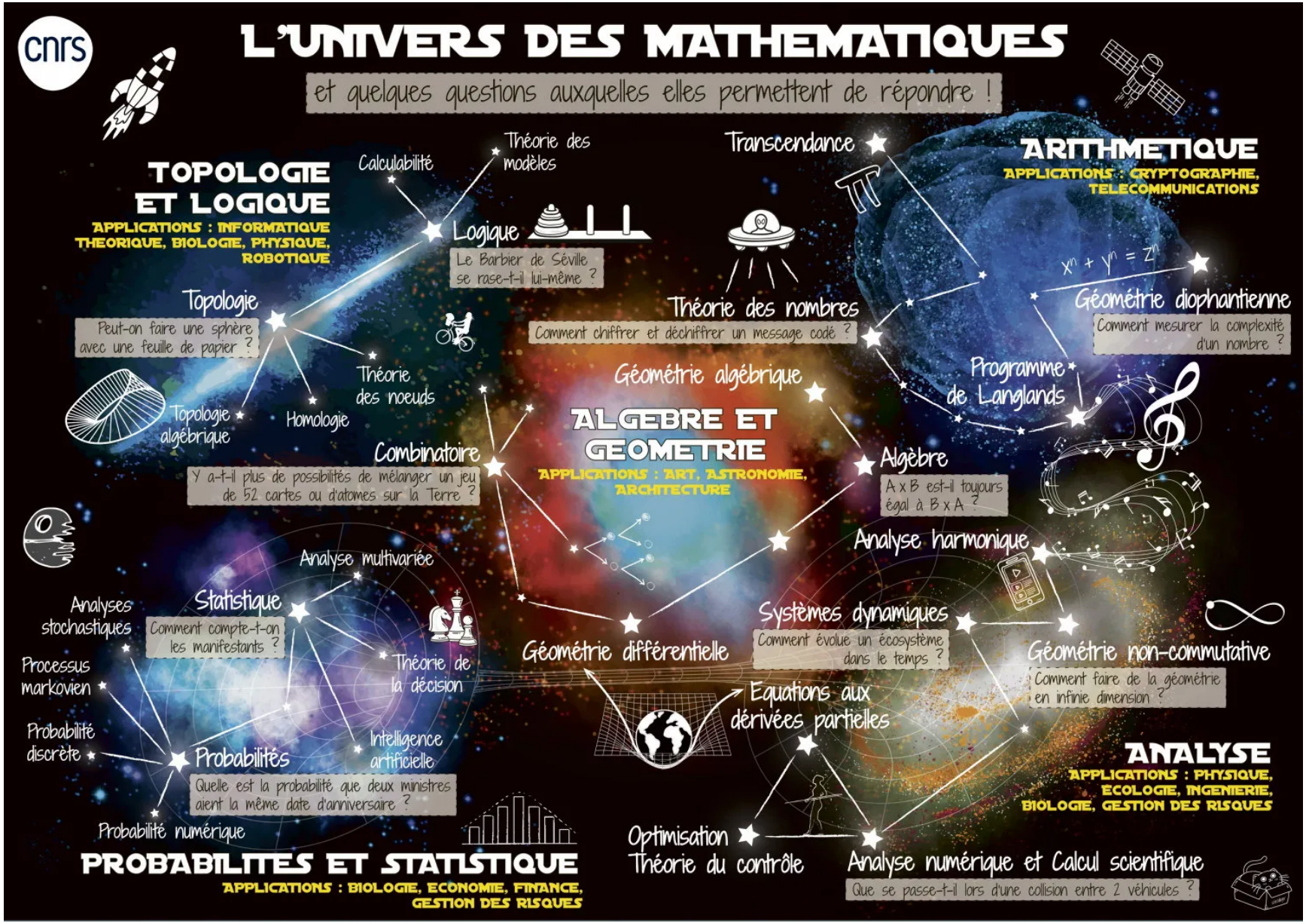
Les Mathématiques : présentes dans tous les secteurs !

Les Mathématiques jouent un rôle grandissant dans la conception et l'élaboration des objets de notre vie quotidienne.

Les Mathématiques : présentes dans tous les secteurs !

Les Mathématiques jouent un rôle grandissant dans la conception et l'élaboration des objets de notre vie quotidienne.

Domaines Mathématiques

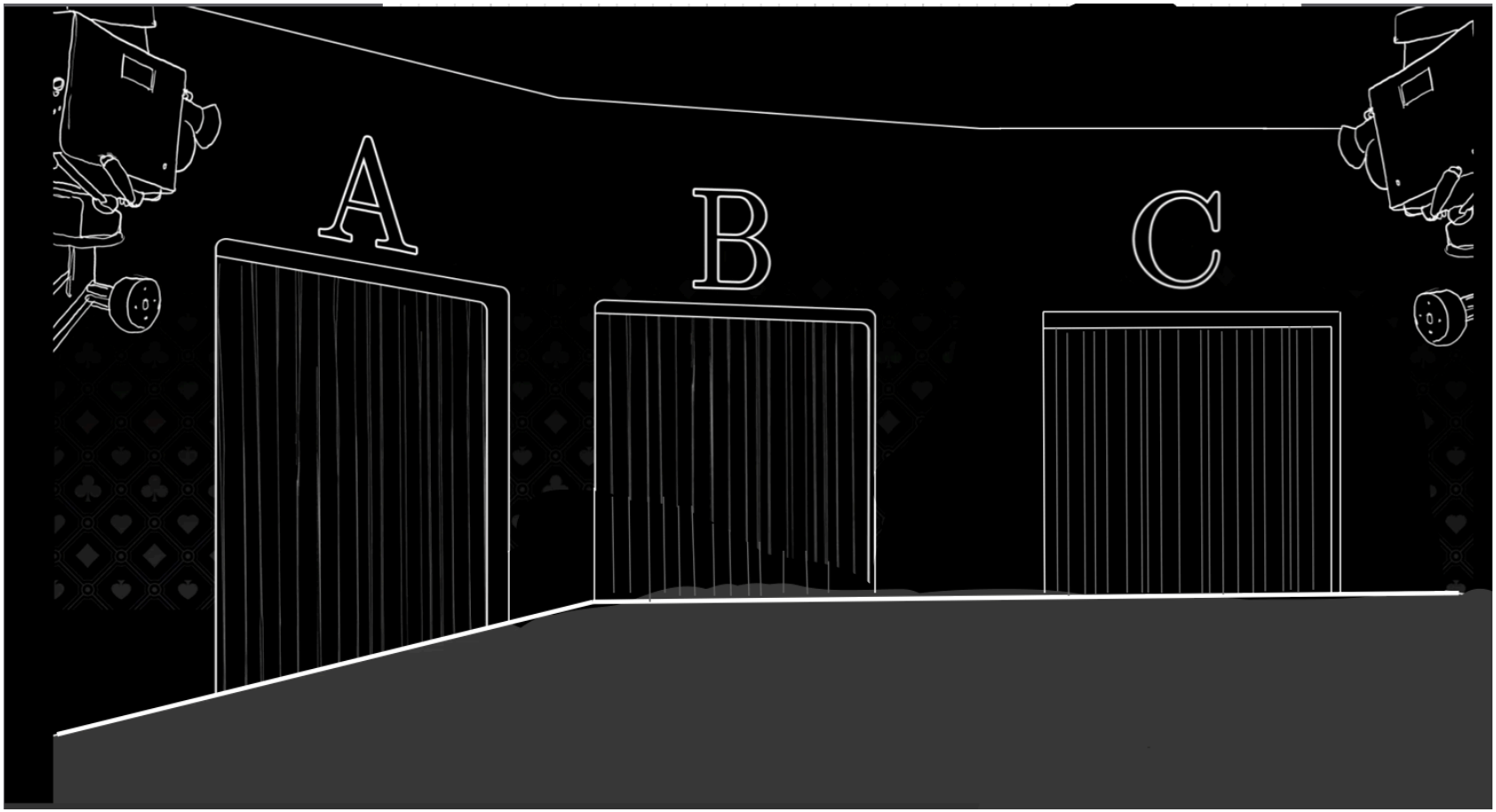


À la recherche de petits bijoux mathématiques perdus

Les maths, c'est pour **toutes** et tous ! !

Je vous présente quelques mathématiciennes remarquables :

1er  : le problème de Monty Hall

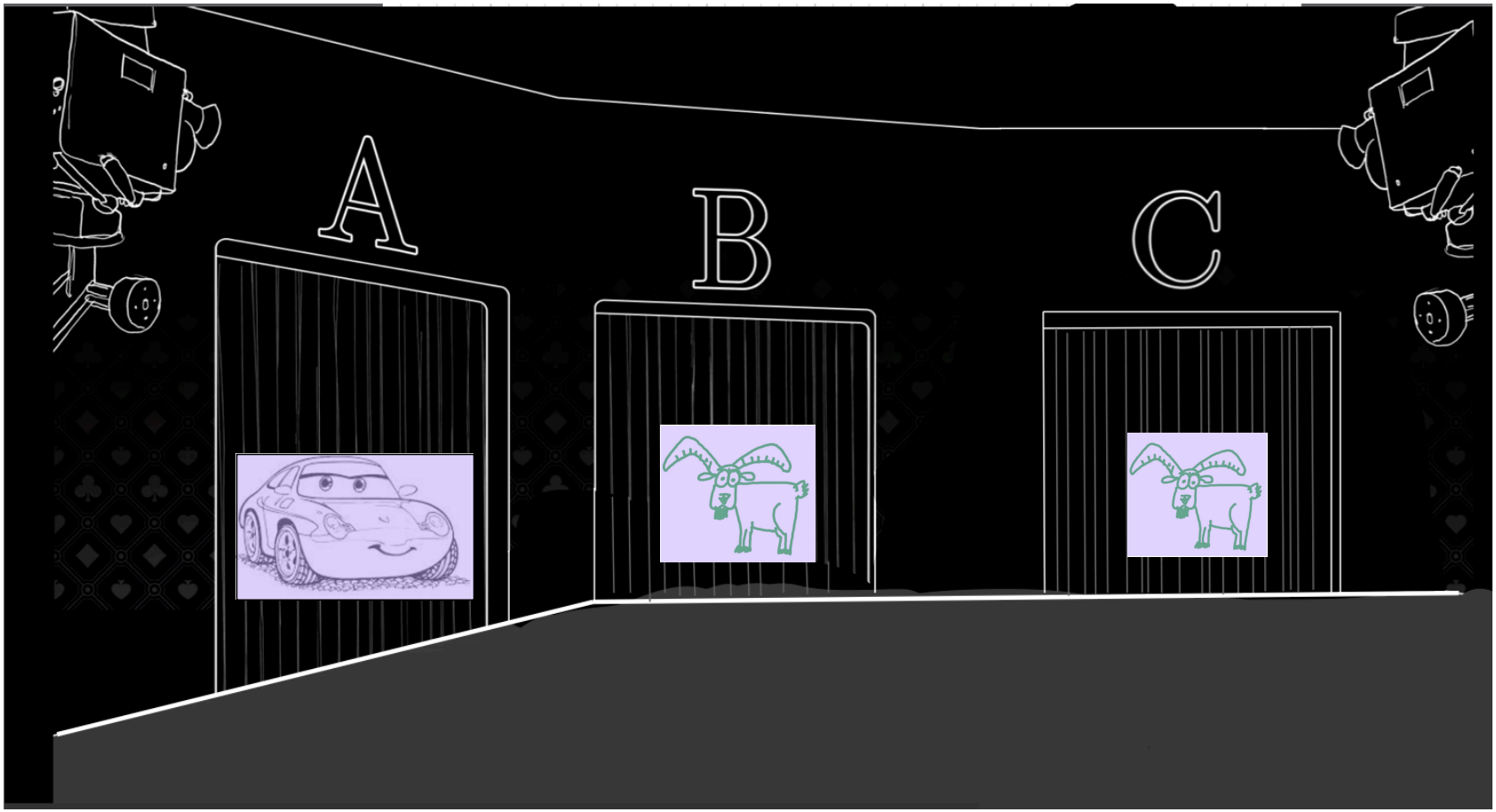


Plateau jeu televisé americain des années 70 (conduit par M. Hall).

(repris de : Voyages au pays des maths

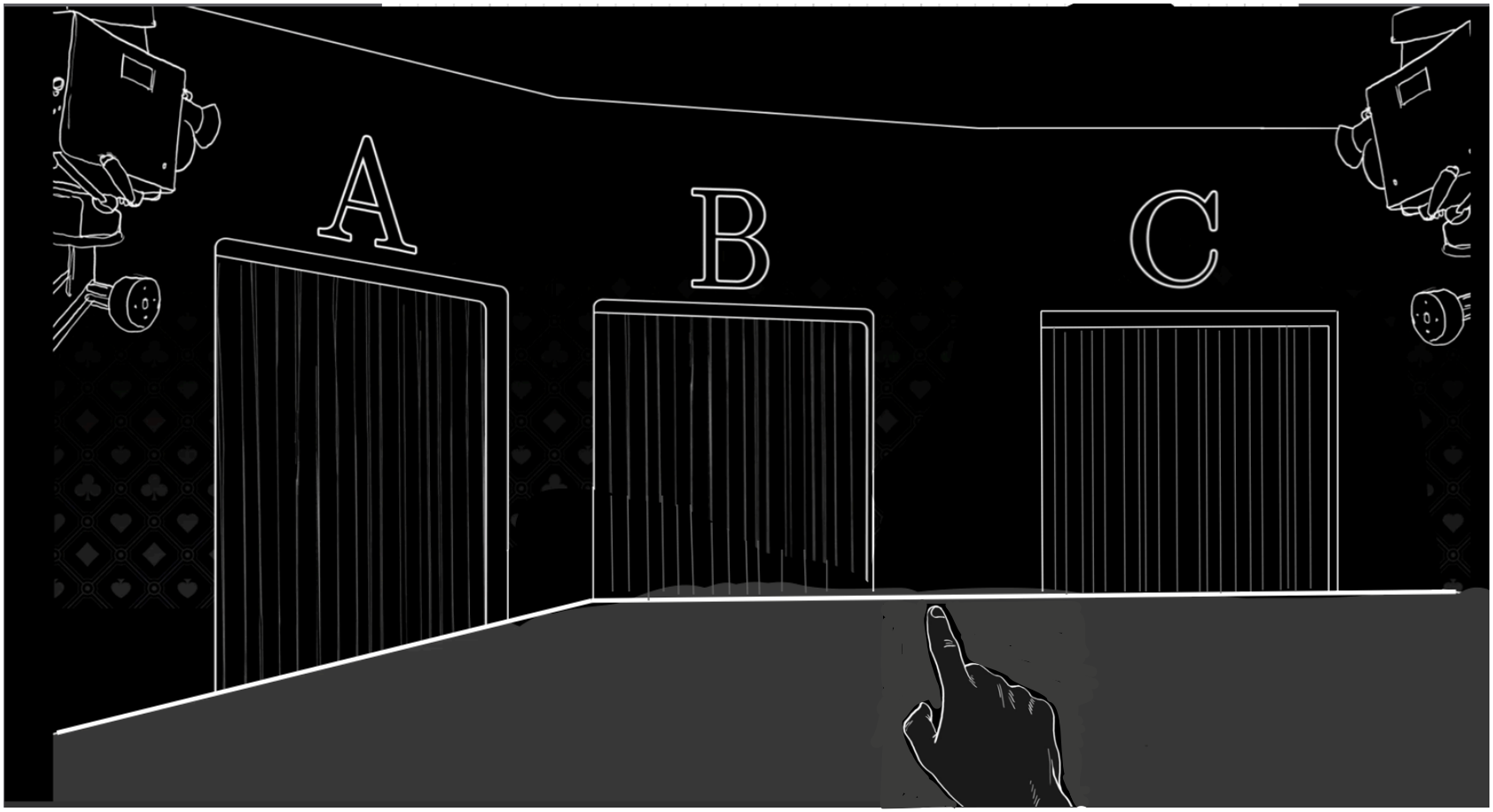
https://www.arte.tv/fr/videos/107398-001-A/voyages-au-pays-des-maths/)

Le problème de Monty Hall



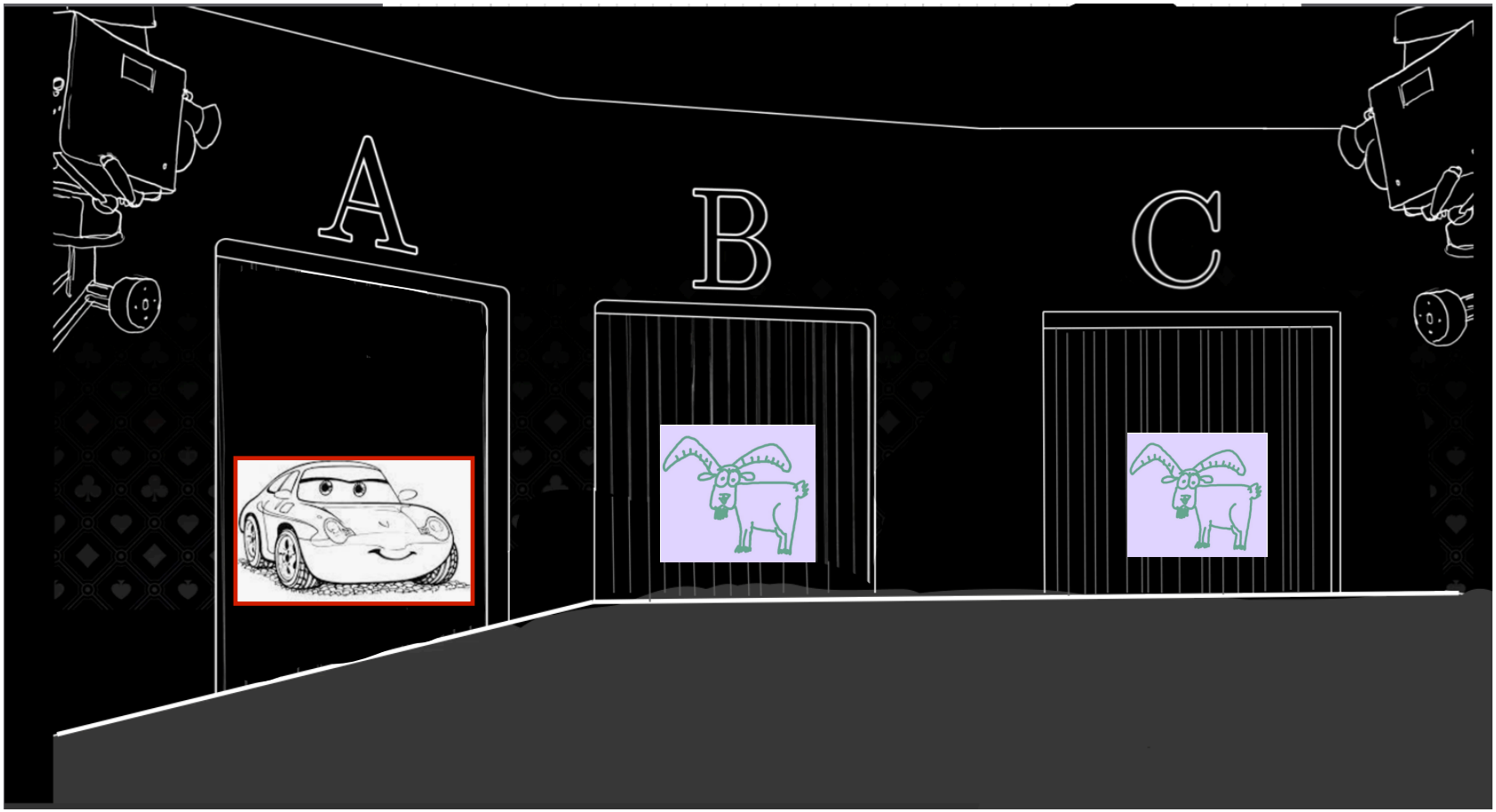
Derrière l'une des portes il y a une voiture et derrière les deux autres portes il y a une chèvre.

Le problème de Monty Hall



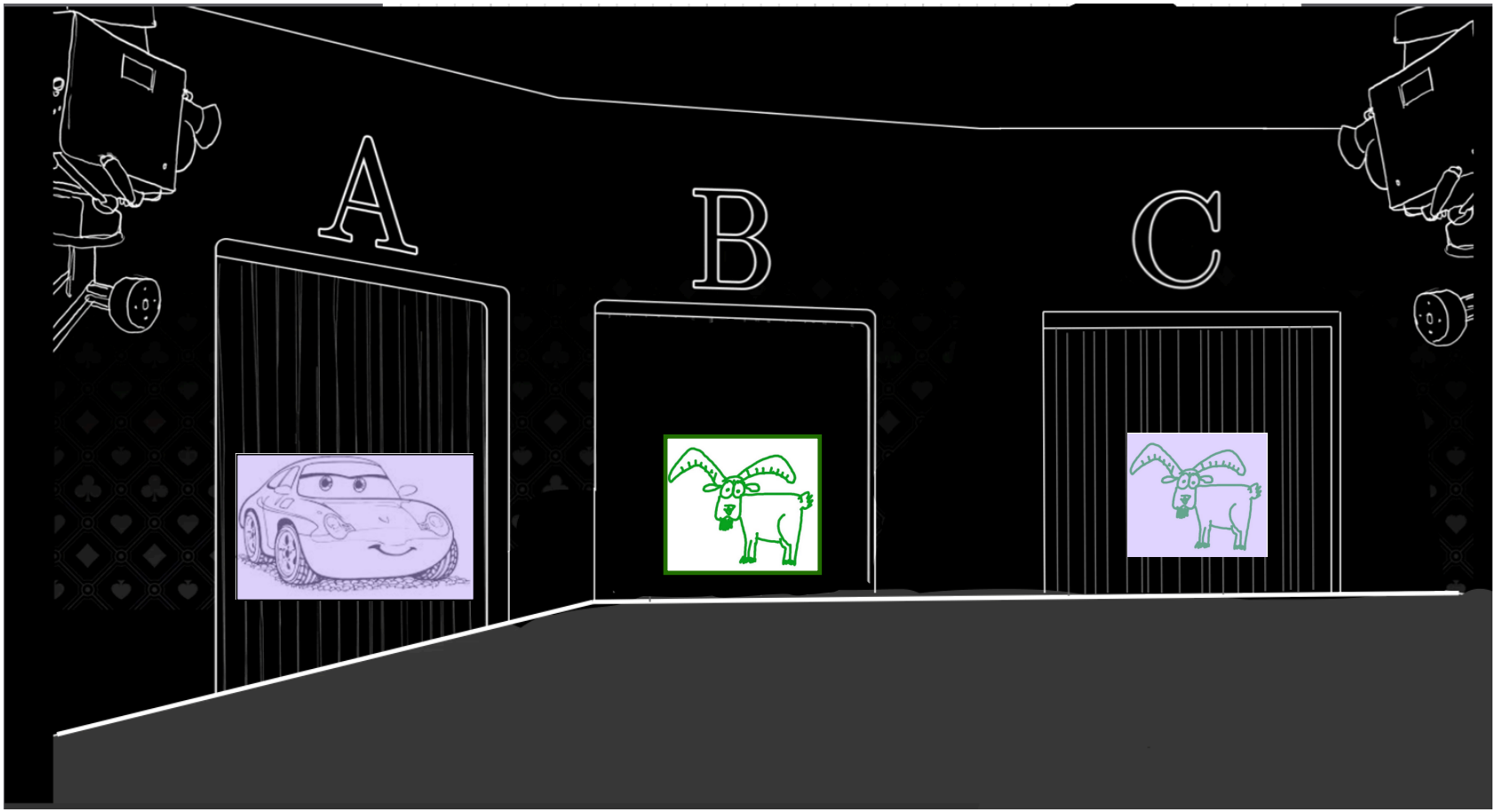
Monty vous demande d'ouvrir une porte.

Le problème de Monty Hall



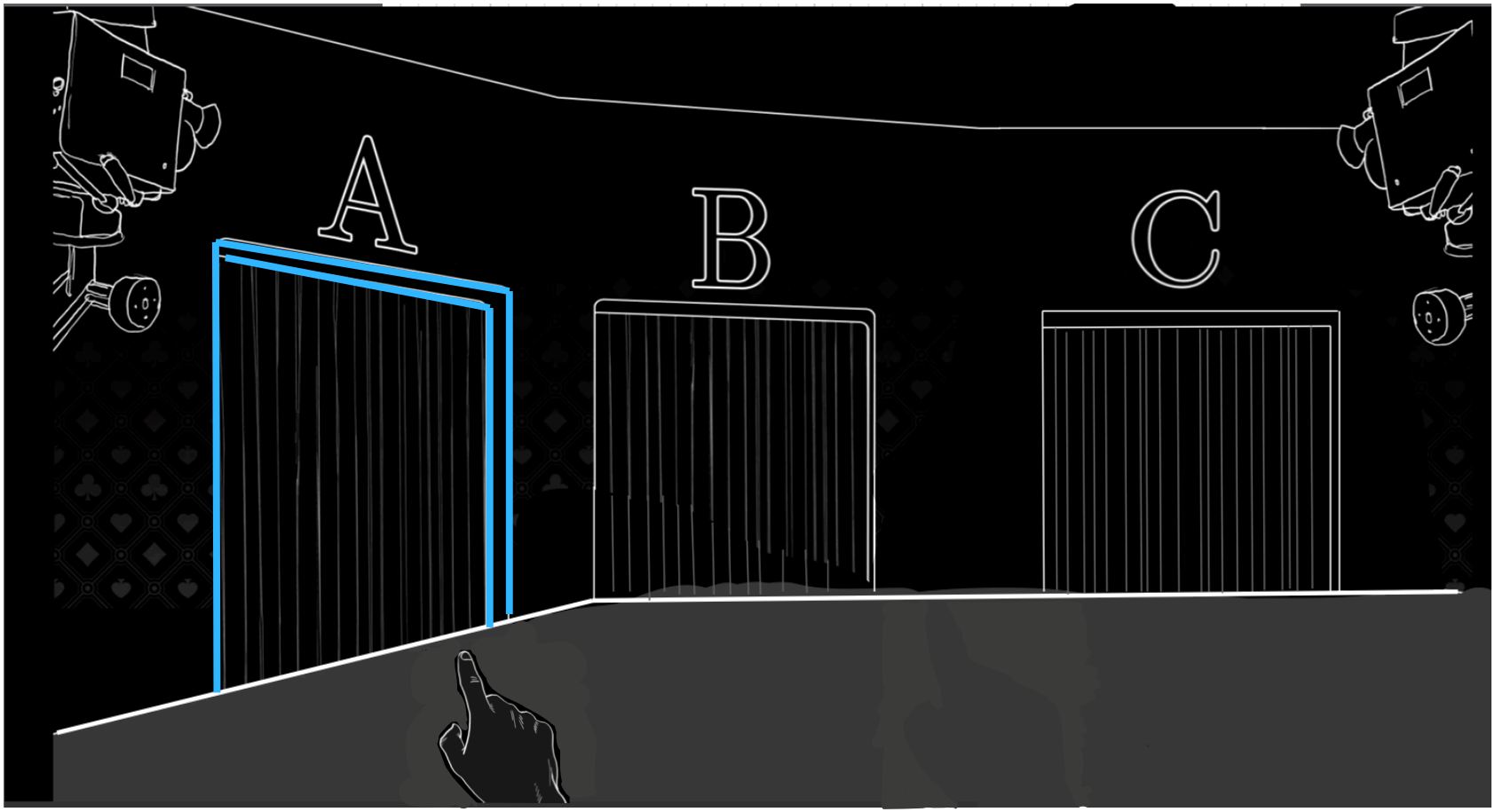
Si vous ouvrez la bonne porte, vous partez avec la voiture.

Le problème de Monty Hall



Sinon, vous partez avec une chèvre. ☹

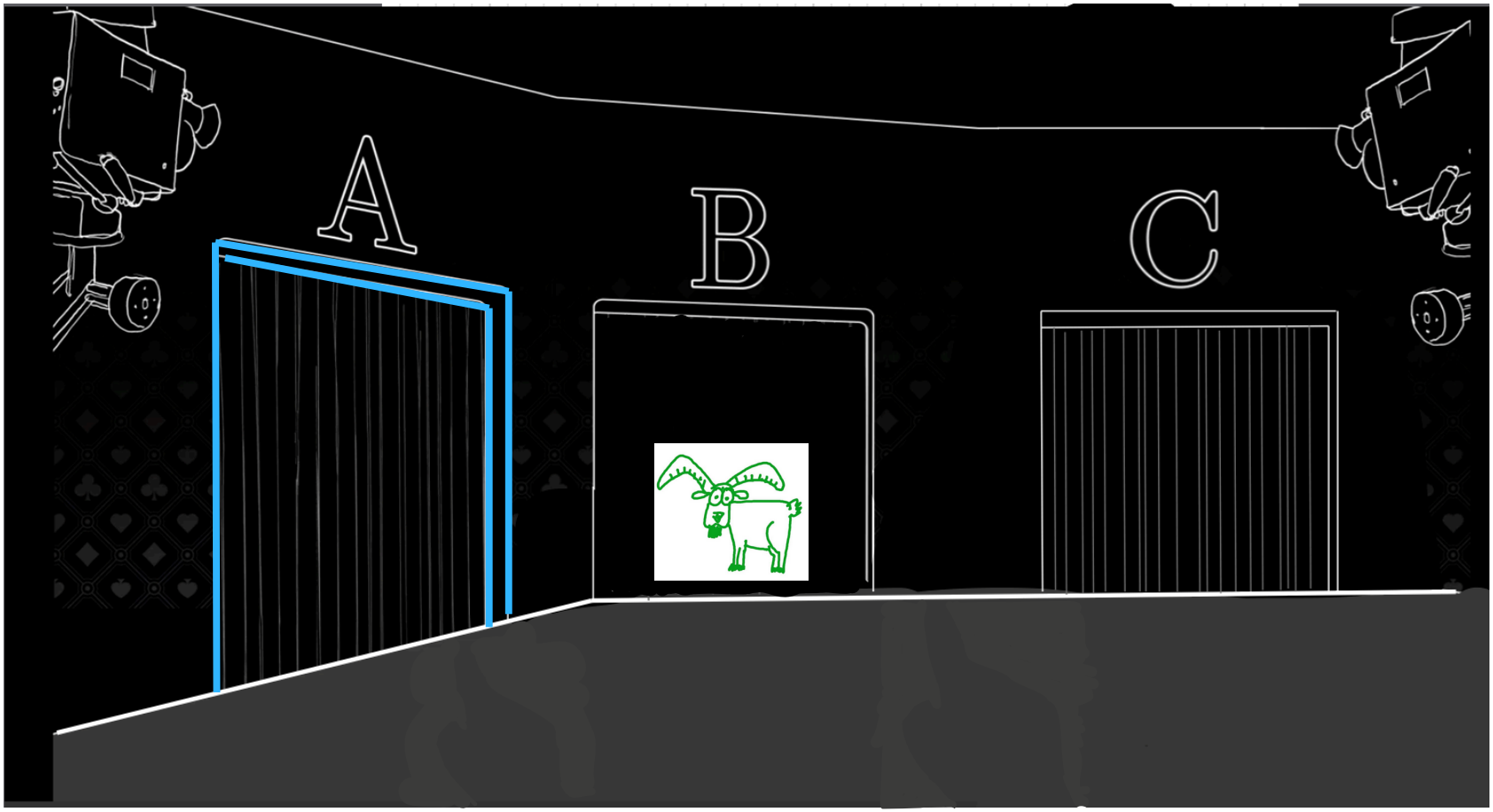
Le problème de Monty Hall



Nous ne savons pas où est la voiture.

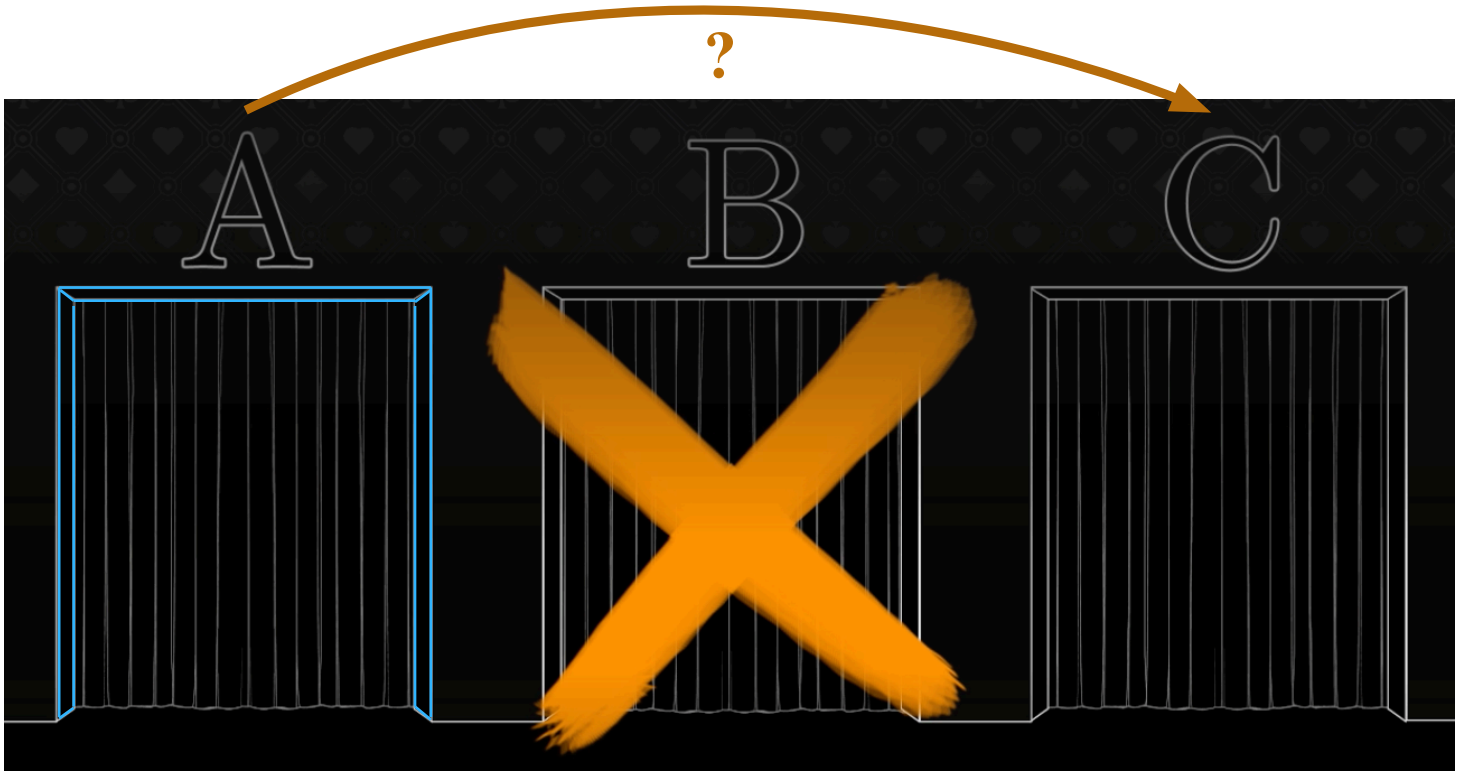
Vous chosissez donc une porte AU HASARD !

Le problème de Monty Hall

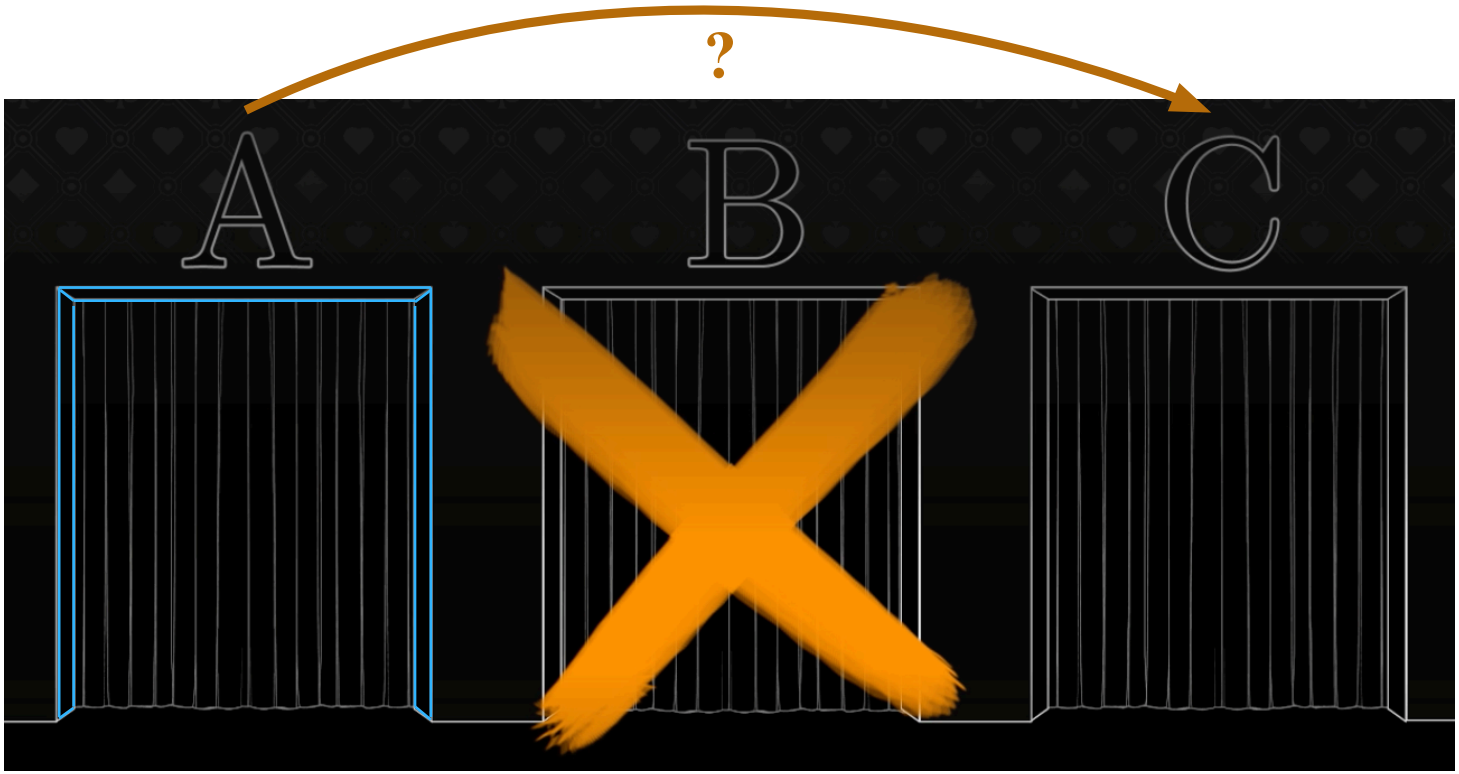


Monty ouvre l'une des deux autres portes où il y a une chèvre et il vous propose de modifier votre choix si vous le souhaitez.

Changeriez-vous votre choix ?

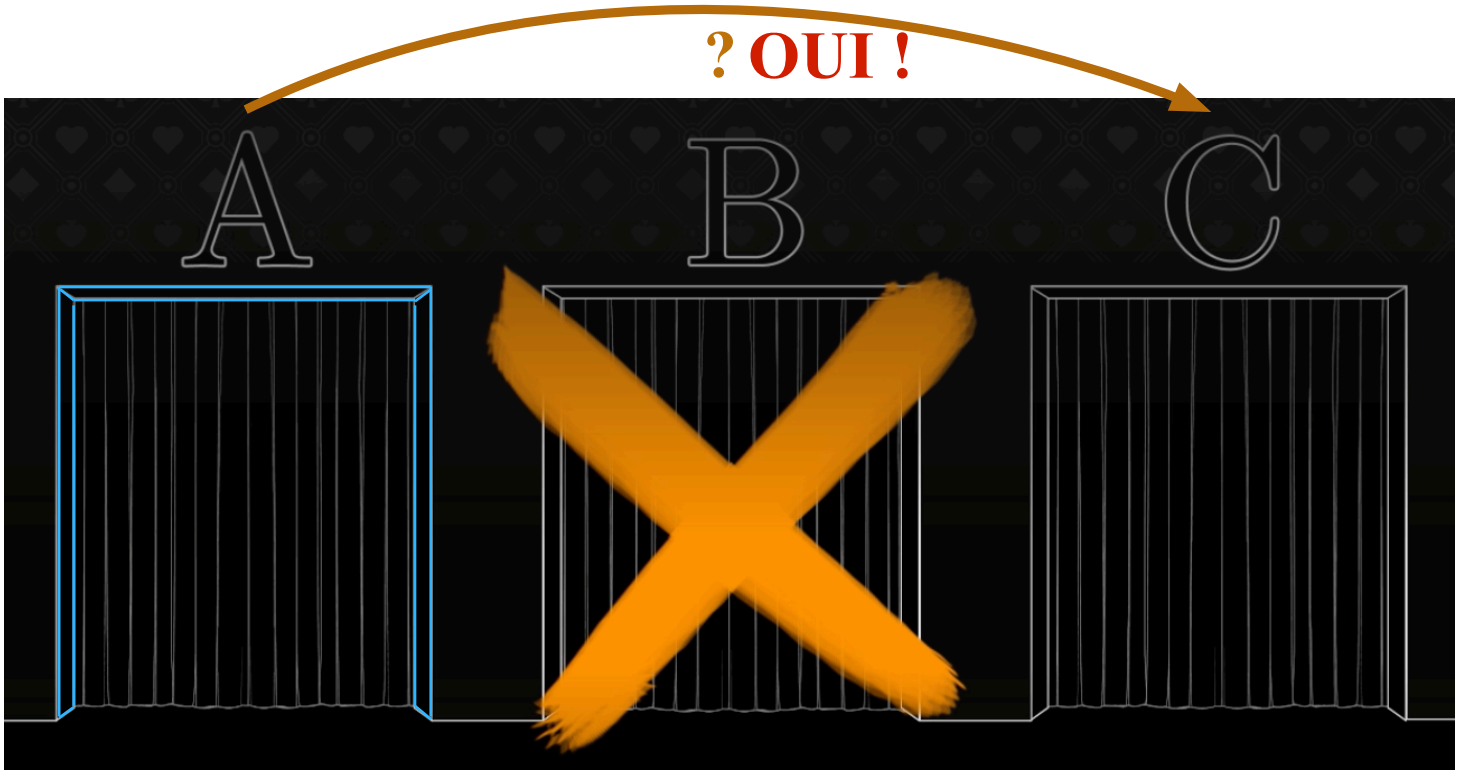


Changeriez-vous votre choix ?



Intuition : j'ai une chance sur deux de trouver la voiture et donc ça ne sert à rien de changer mon choix.

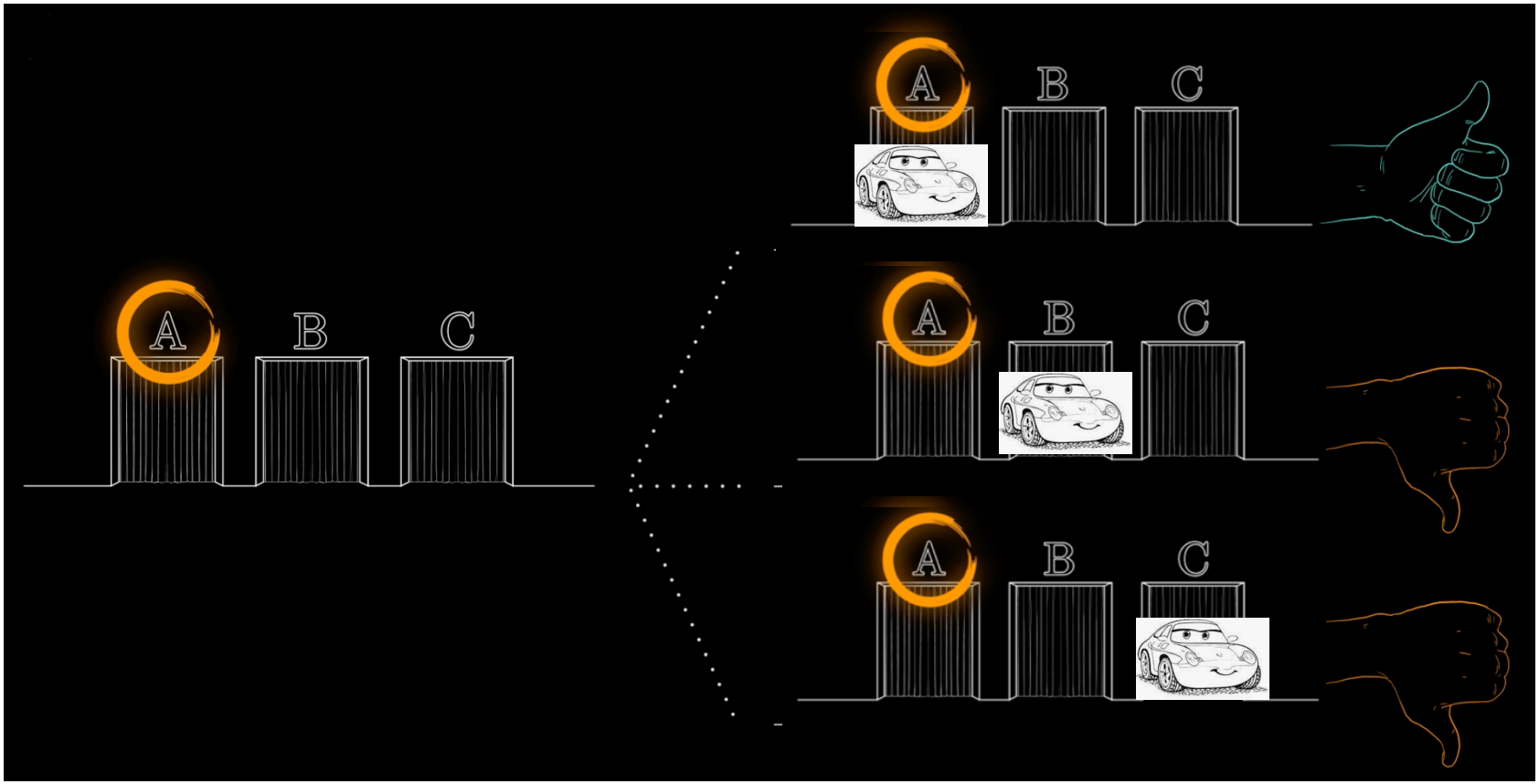
Changerez-vous votre choix ?



Intuition : j'ai une chance sur deux de trouver la voiture et donc ça ne sert à rien de changer mon choix.

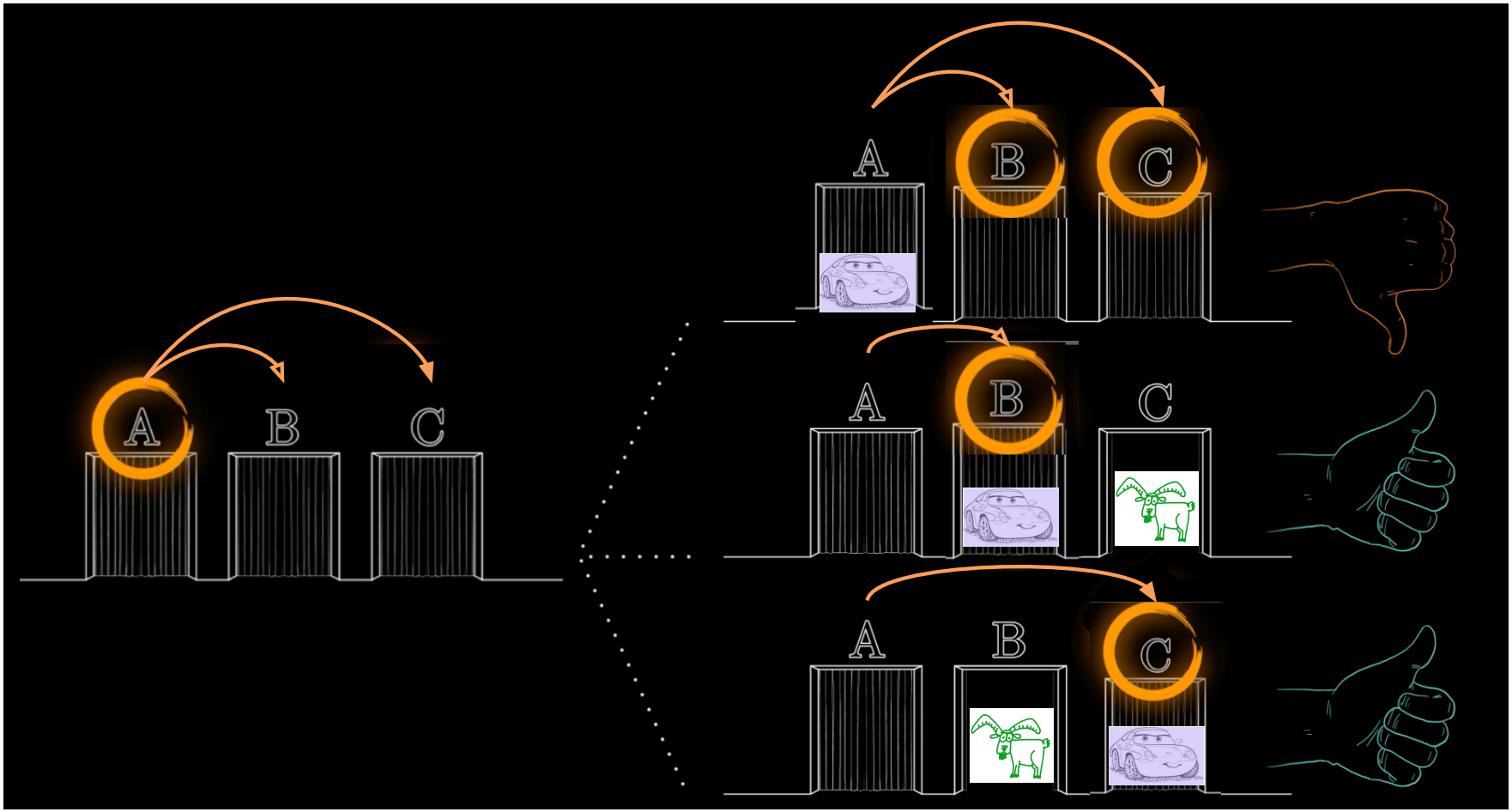
IL FAUT CHANGER VOTRE CHOIX ! !

Si vous ne changez pas



Vous avez une chance sur trois de gagner.

Si vous changez



Vous avez deux chances sur trois de gagner.

Problème de Monty Hall : histoire

Le problème ainsi que la solution ont été présentés pour la première fois par **Marilyn Vos Savant** dans le magazine PARADE rubrique « *Ask Marilyn* ».

Problème de Monty Hall : histoire

Le problème ainsi que la solution ont été présentés pour la première fois par **Marilyn Vos Savant** dans le magazine PARADE rubrique « *Ask Marilyn* ».

Elle a reçuu de milliers de lettres contestataires contre sa solution du problème y compris de la part de mathématiciens reconnus ! ! !

Problème de Monty Hall : histoire

Le problème ainsi que la solution ont été présentés pour la première fois par **Marilyn Vos Savant** dans le magazine PARADE rubrique « *Ask Marilyn* ».

Elle a reçuu de milliers de lettres contestataires contre sa solution du problème y compris de la part de mathématiciens reconnus ! ! ! Certains ont reconnu leur tort et lui en ont fait part.

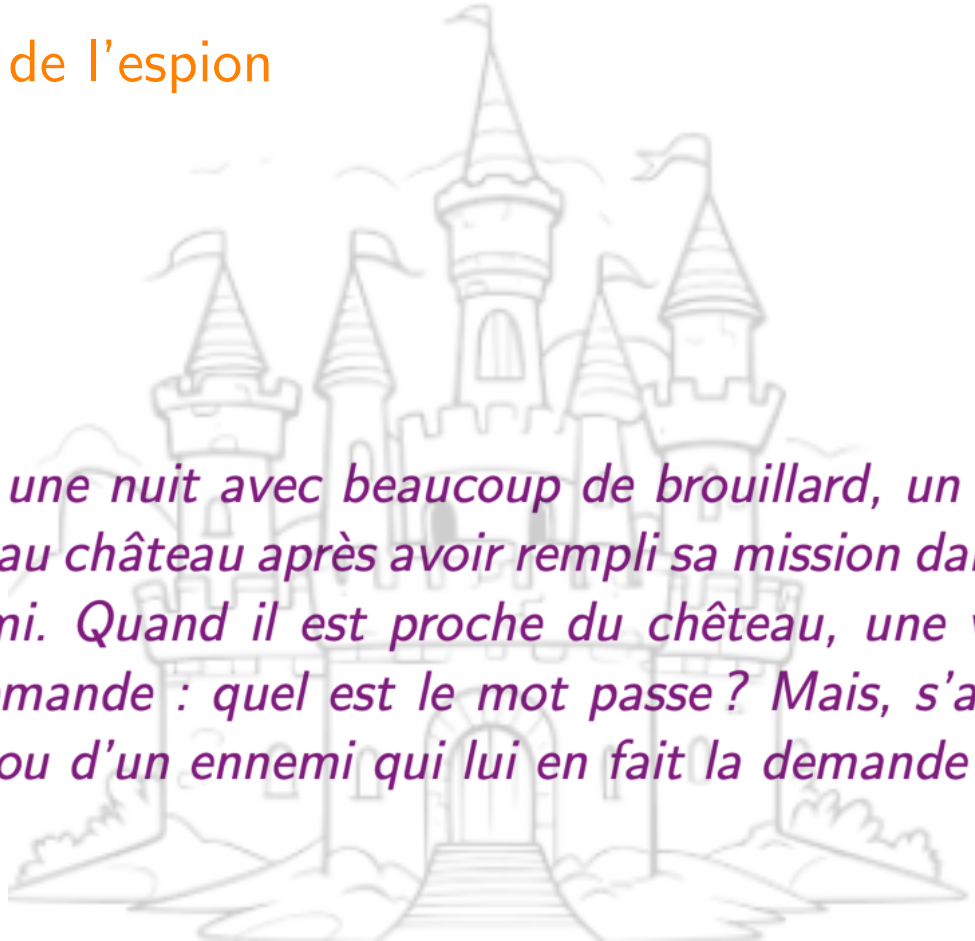
2ème  : preuve à divulgation nulle de connaissance

2ème  : preuve à divulgation nulle de connaissance

Le dilemme de l'espion

2ème  : preuve à divulgation nulle de connaissance

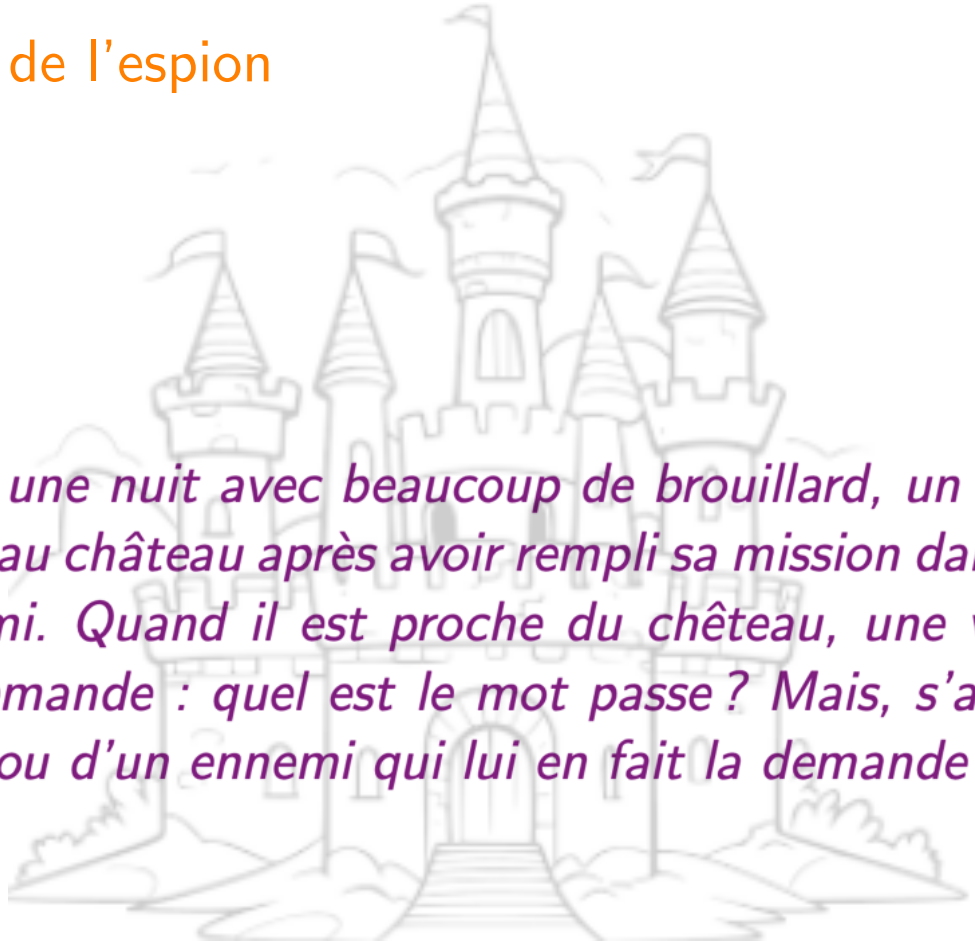
Le dilemme de l'espion



Dans une nuit avec beaucoup de brouillard, un espion revient au château après avoir rempli sa mission dans le camp ennemi. Quand il est proche du chêteau, une voix faible lui demande : quel est le mot passe ? Mais, s'agit-il d'un ami ou d'un ennemi qui lui en fait la demande ?

2ème  : preuve à divulgation nulle de connaissance

Le dilemme de l'espion



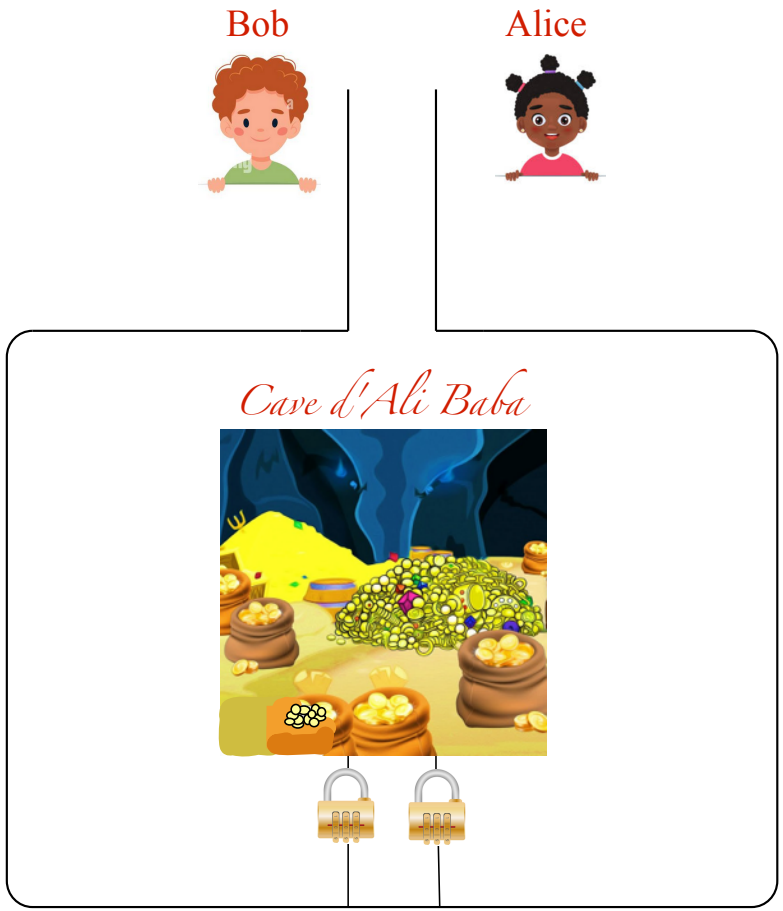
Dans une nuit avec beaucoup de brouillard, un espion revient au château après avoir rempli sa mission dans le camp ennemi. Quand il est proche du chêteau, une voix faible lui demande : quel est le mot passe ? Mais, s'agit-il d'un ami ou d'un ennemi qui lui en fait la demande ?

Une méthode proposée pour communiquer le mot passe dans ce contexte est : preuve à divulgation nulle de connaissance.

La grotte d'Ali Baba (Quisquater et Guillou, 1989)

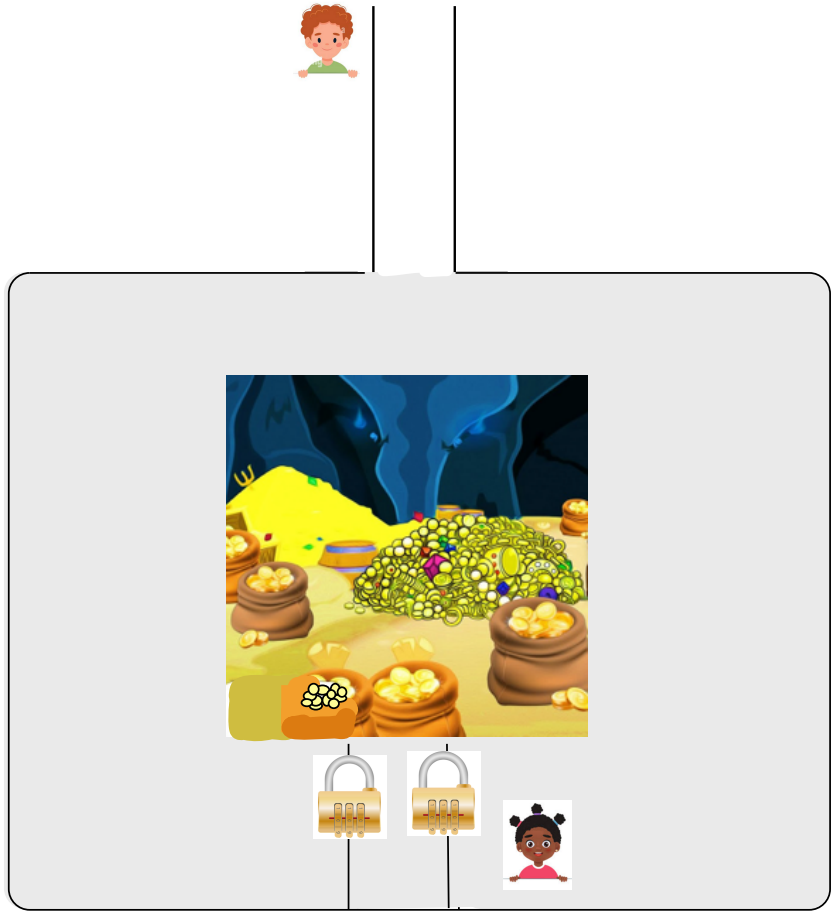
La grotte d'Ali Baba (Quisquater et Guillou, 1989)

ALICE veut prouver à BOB qu'elle connaît le mot magique « *sésame ouvre-toi* » (code du cadena) pour ouvrir la porte de la grotte d'Ali Baba mais ne veut pas que Bob l'apprenne.



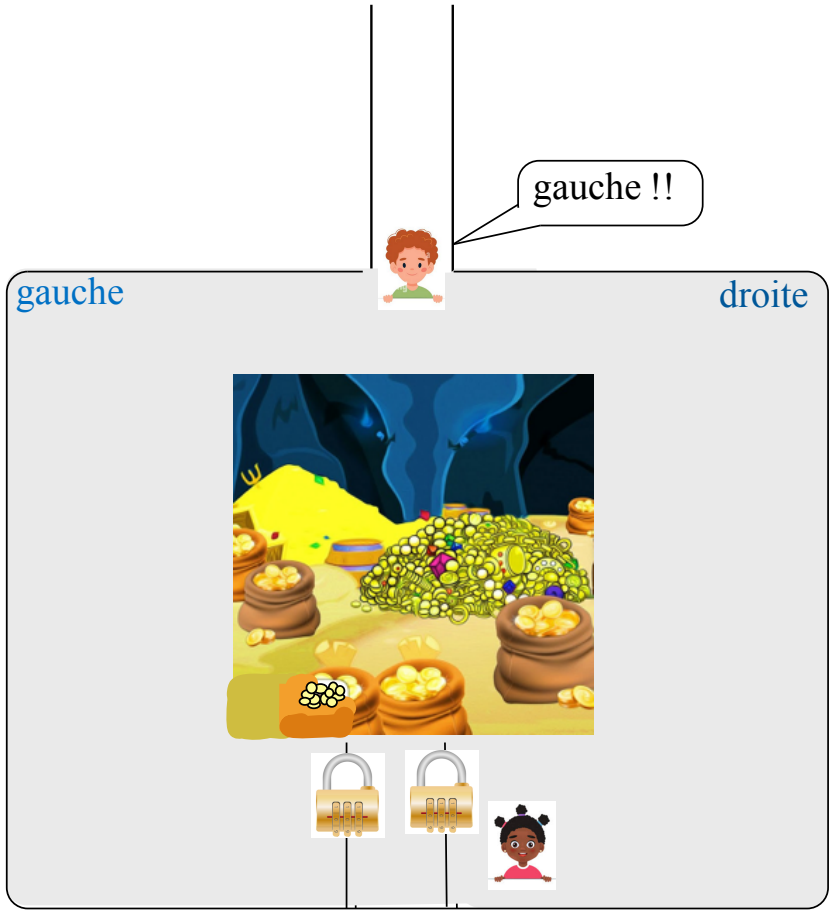
Etape 1

Bob attend à l'entrée de la grotte et ne voit pas à l'intérieur. Alice s'introduit dans la galerie et choisit aléatoirement l'un des chemins (à gauche ou à droite) à la bifurcation.



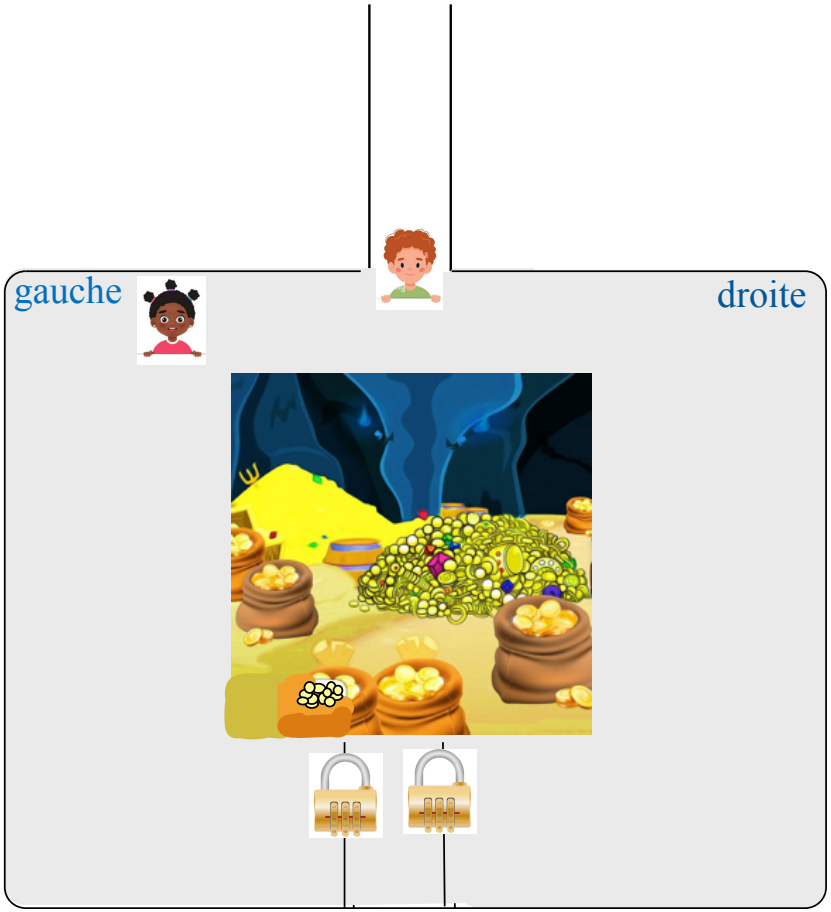
Etape 2

Bob entre dans le tunnel et attend à la bifurcation. Il lance une pièce de monnaie. Selon le côté où tombe la pièce, Bob crie « gauche » ou « droite ».



Etape 3

Alice doit démontrer maintenant qu'elle est en possession de la preuve, elle doit se diriger vers la sortie demandée par Bob.



Analysons ce protocole

- Si Alice connaît bien le mot magique, elle répondra correctement à la requête de Bob.

Analysons ce protocole

- Si Alice connaît bien le mot magique, elle répondra correctement à la requête de Bob.
- Une erreur d'Alice sera considérée comme une preuve de non connaissance. À ce moment, Bob s'arrête et il est assuré qu'Alice ne connaît pas le mot magique.

Analysons ce protocole

- Si Alice connaît bien le mot magique, elle répondra correctement à la requête de Bob.
- Une erreur d'Alice sera considérée comme une preuve de non connaissance. À ce moment, Bob s'arrête et il est assuré qu'Alice ne connaît pas le mot magique.
- Si Alice n'est pas en possession du mot magique, il y a 50 % de chance pour qu'elle commette une erreur.

Analyse du protocole

- Avec N essais de ce protocol (à partir de l'étape 1), la probabilité pour que BOB affirme qu'ALICE possède le secret alors qu'elle ne le possède pas est de $\frac{1}{2^N}$

Analyse du protocole

- Avec N essais de ce protocol (à partir de l'étape 1), la probabilité pour que BOB affirme qu'ALICE possède le secret alors qu'elle ne le possède pas est de $\frac{1}{2^N}$
- Pour N assez grand (disons $N = 100$) il y a de grande chance pour que BOB ne se trompe pas.

Analyse du protocole

- Avec N essais de ce protocol (à partir de l'étape 1), la probabilité pour que Bob affirme qu'Alice possède le secret alors qu'elle ne le possède pas est de $\frac{1}{2^N}$
- Pour N assez grand (disons $N = 100$) il y a de grande chance pour que Bob ne se trompe pas.

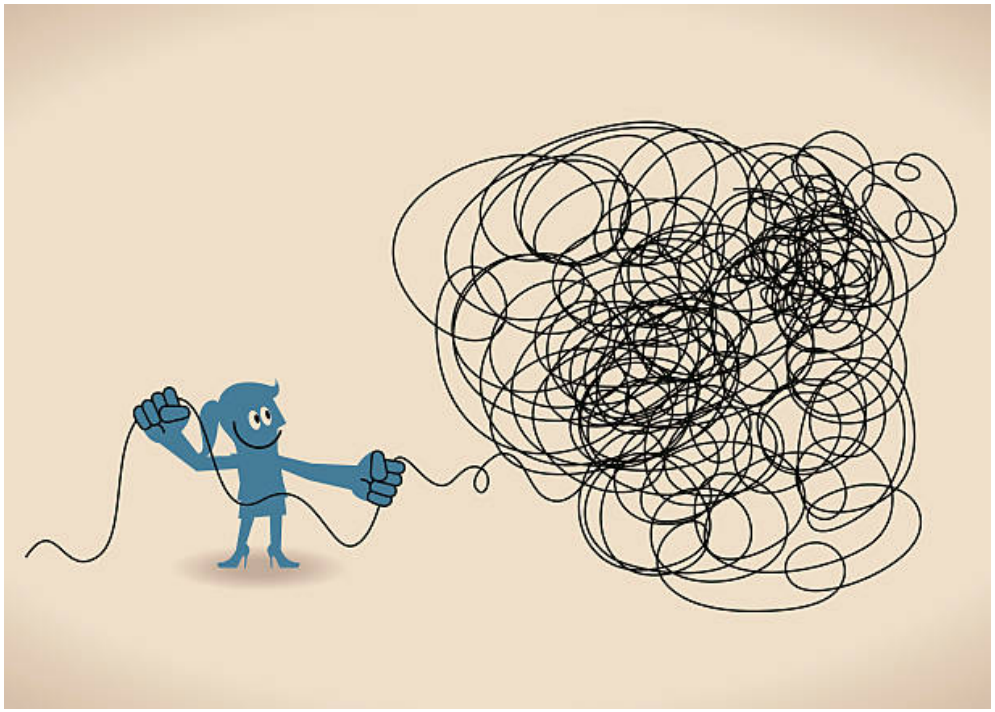
La probabilité qu'un ordinateur soit détruit par une météorite au cours de chaque microseconde de son calcul est au moins égale à $\frac{1}{2^{100}}$ (selon l'hypothèse d'un impact de météorite par millénaire qui détruit au moins 100 m^2 de la surface terrestre).

3ème  : nœud trivial

Petit défi : avez-vous déjà essayé de démêler une corde, des câbles d'écouteurs, un collier ou tout autre brin ?

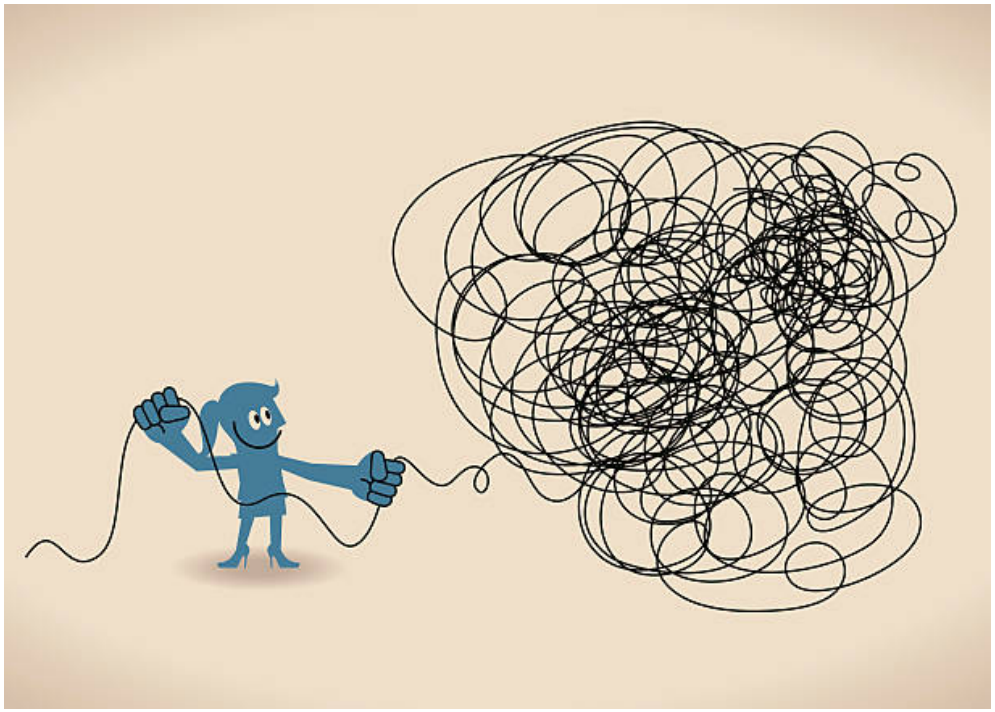
3ème  : nœud trivial

Petit défi : avez-vous déjà essayé de démêler une corde, des câbles d'écouteurs, un collier ou tout autre brin ?



3ème  : nœud trivial

Petit défi : avez-vous déjà essayé de démêler une corde, des câbles d'écouteurs, un collier ou tout autre brin ?



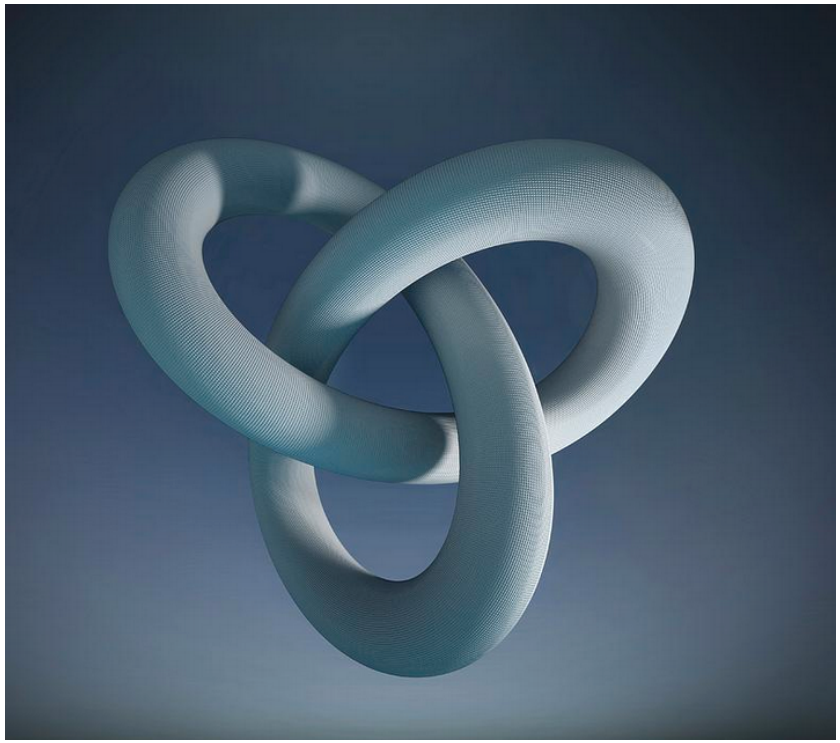
Plus un brin est long, plus il est susceptible de s'emmêler.

Théorie des noeuds

Un nœud est une courbe simple fermée, sans intersection avec elle-même, dans l'espace 3-dimensionnel.

Théorie des noeuds

Un nœud est une courbe simple fermée, sans intersection avec elle-même, dans l'espace 3-dimensionnel.

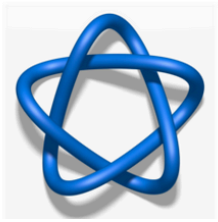


Quelques diagrammes


Trivial


Trèfle


Figure-huit

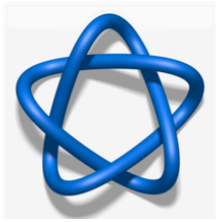


Quelques diagrammes


Trivial


Trèfle

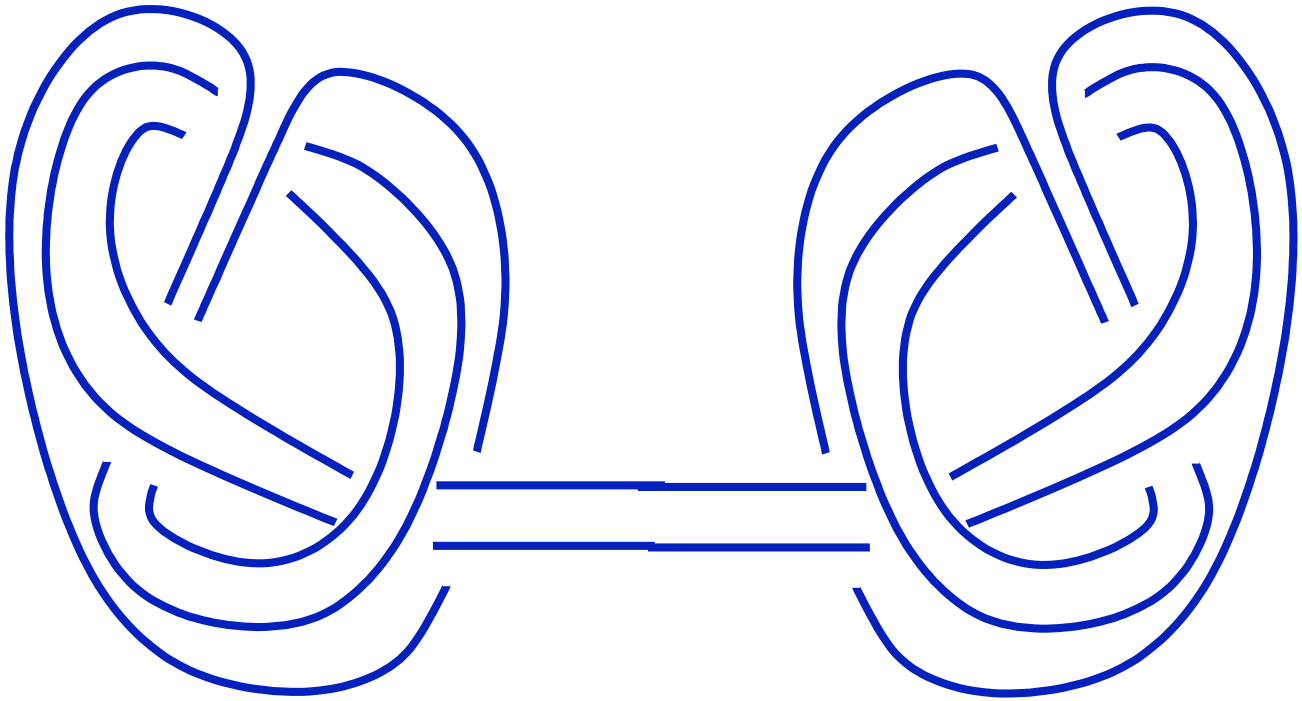

Figure-huit



Problème fondamental du domaine : classification des nœuds

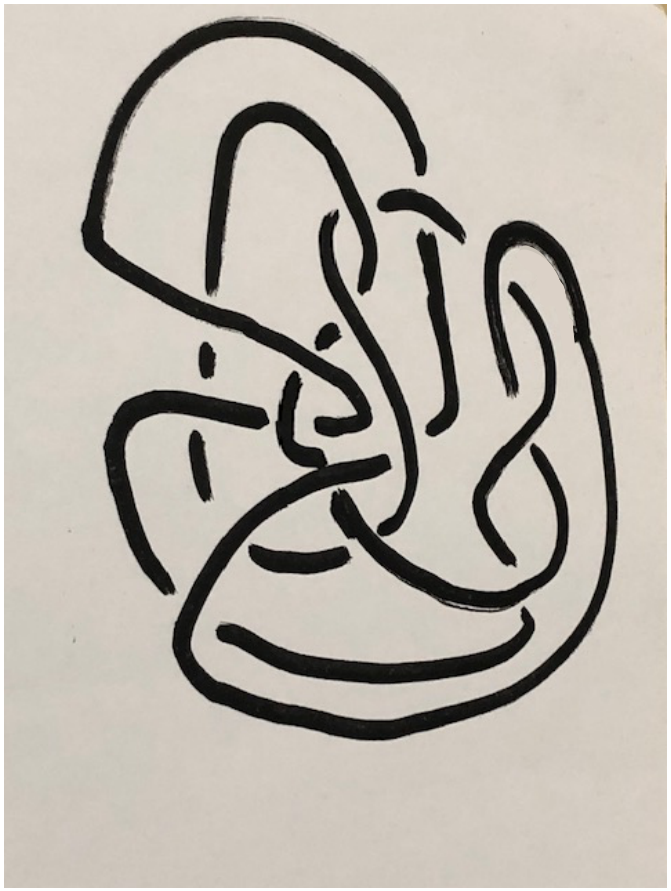
Problème du dénouage : étant donné un diagramme d'un nœud K, existe-t-il un algorithme « *efficient* » qui décide si K est trivial ?

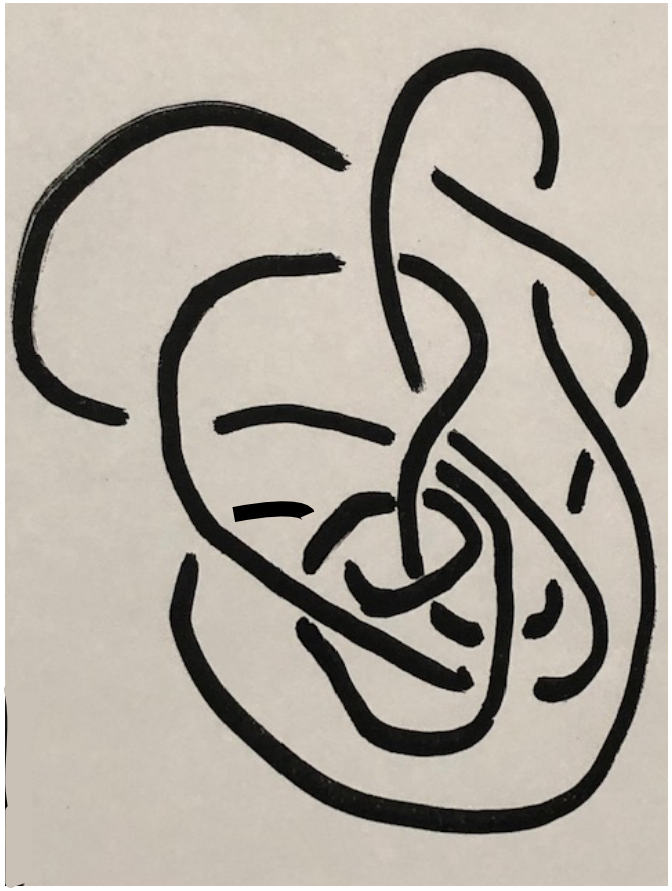
Problème du dénouage : étant donné un diagramme d'un nœud K, existe-t-il un algorithme « *efficient* » qui décide si K est trivial ?



Théorie des noeuds

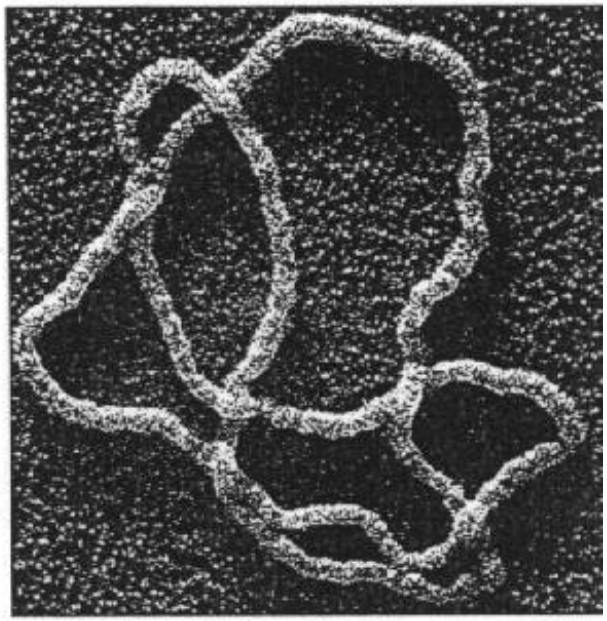
Problème du dénouage : étant donné un diagramme d'un nœud K, existe-t-il un algorithme « *efficient* » qui décide si K est trivial ?





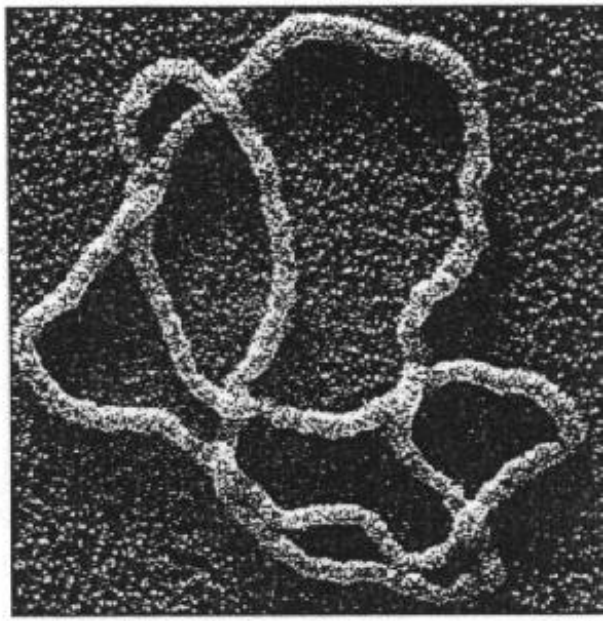
Application : ADN (acide désoxyribonucléique)

Une application fondamentale du problème du dénouage se trouve dans l'étude de l'ADN.



Application : ADN (acide désoxyribonucléique)

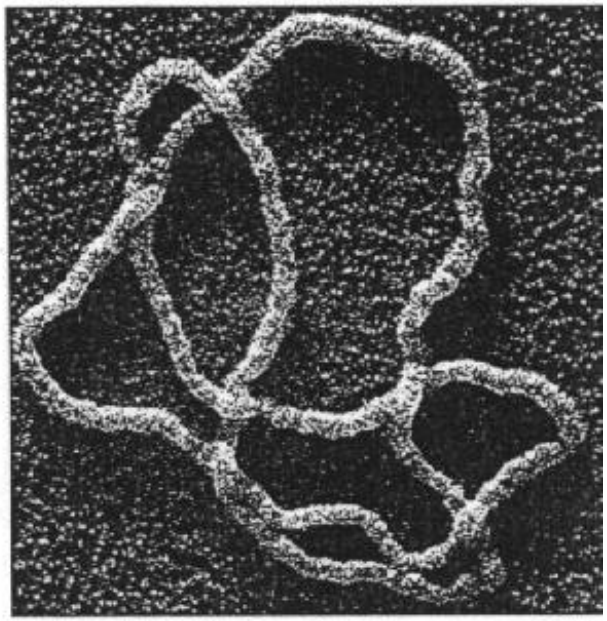
Une application fondamentale du problème du dénouage se trouve dans l'étude de l'ADN.



Suite à l'agissement des ≪ *enzymes* ≫ sur un ADN, nous souhaitons connaître si les nouvelles formes produites sont dénouées.

Application : ADN (acide désoxyribonucléique)

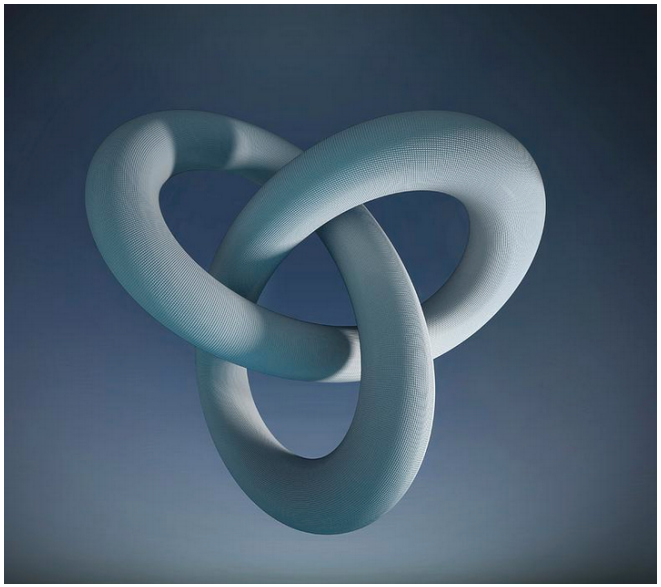
Une application fondamentale du problème du dénouage se trouve dans l'étude de l'ADN.



Suite à l'agissement des ≪ *enzymes* ≫ sur un ADN, nous souhaitons connaître si les nouvelles formes produites sont dénouées.
Difficulté : l'ADN est très emmêlé à l'intérieur de la cellule (équivalent à environ 200 km de fil de pêche à l'intérieur d'un ballon de football).

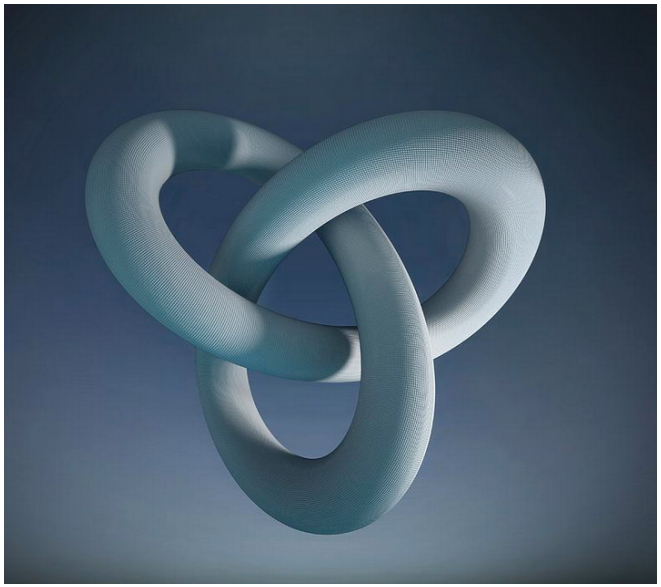
Premier pas ...

Le Trèfle, est-il trivial ?



Premier pas ...

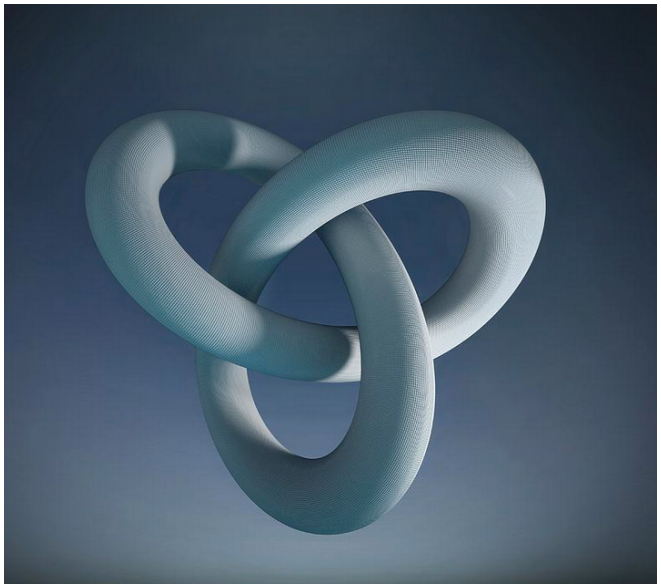
Le Trèfle, est-il trivial ?



Théorème (Papakyrikopoulos, 1957) Un nœud K est trivial si et seulement si le groupe fondamental de l'espace complémentaire de K est commutatif.

Premier pas ...

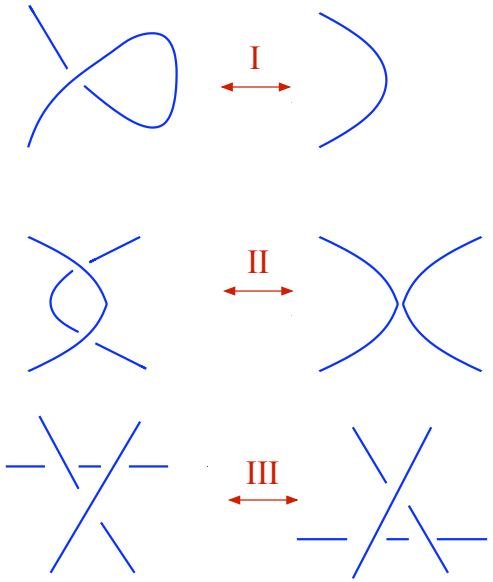
Le Trèfle, est-il trivial ?



Théorème (Papakyrikopoulos, 1957) Un nœud K est trivial si et seulement si le groupe fondamental de l'espace complémentaire de K est commutatif.

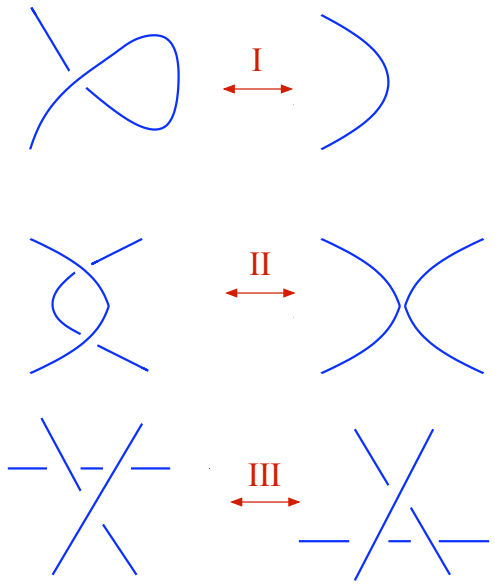
Mouvements de Reidemeister

Considérons les mouvements locaux suivants :



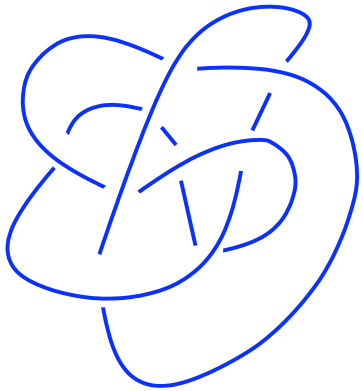
Mouvements de Reidemeister

Considérons les mouvements locaux suivants :

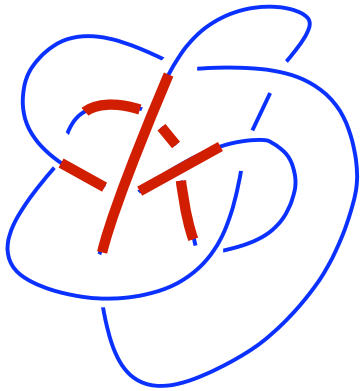


Théorème (Reidemeister, 1926) Deux nœuds sont équivalents si et seulement si les diagrammes correspondants peuvent être obtenus l'un à partir de l'autre par une suite de mouvements I, II ou III.

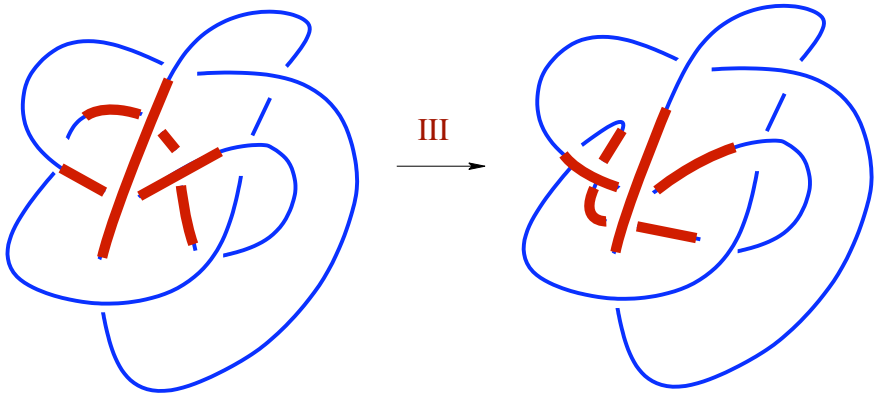
Exemple



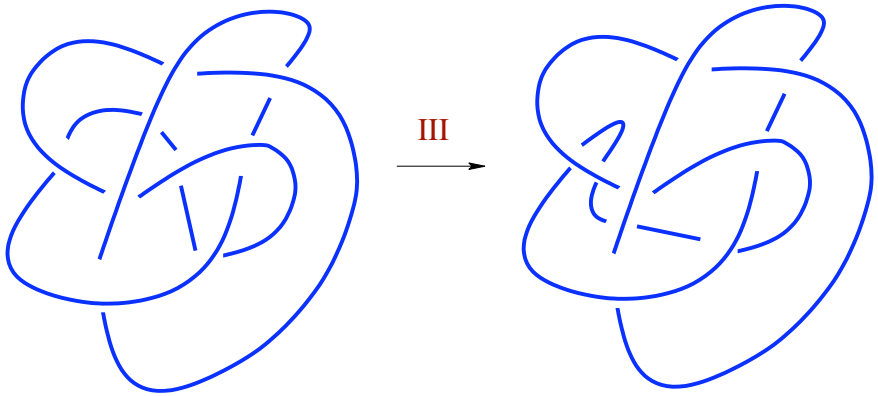
Exemple



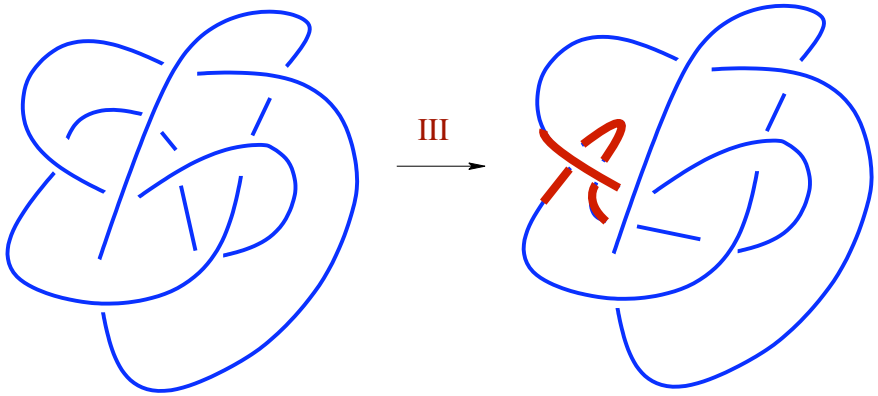
Exemple



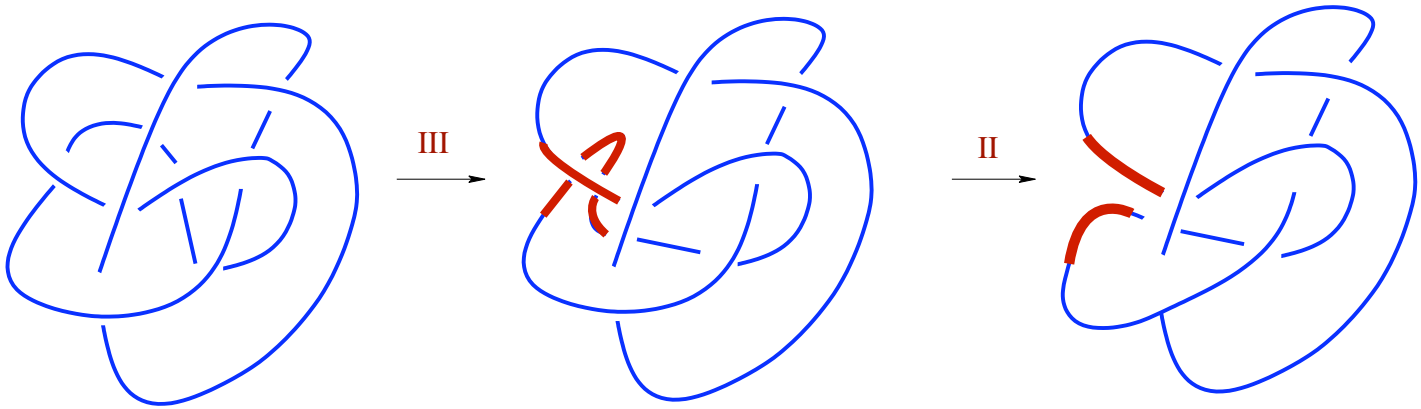
Exemple



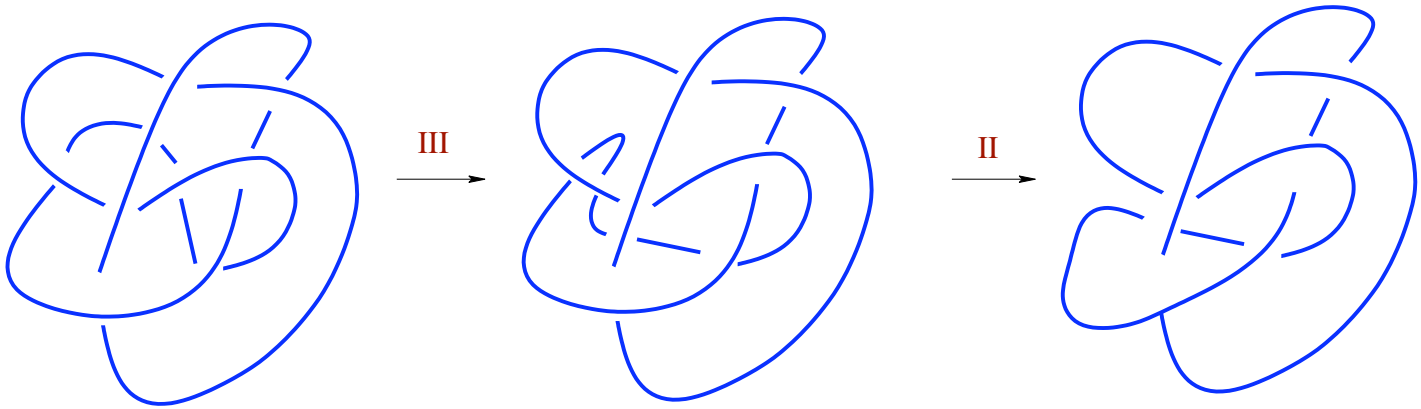
Exemple



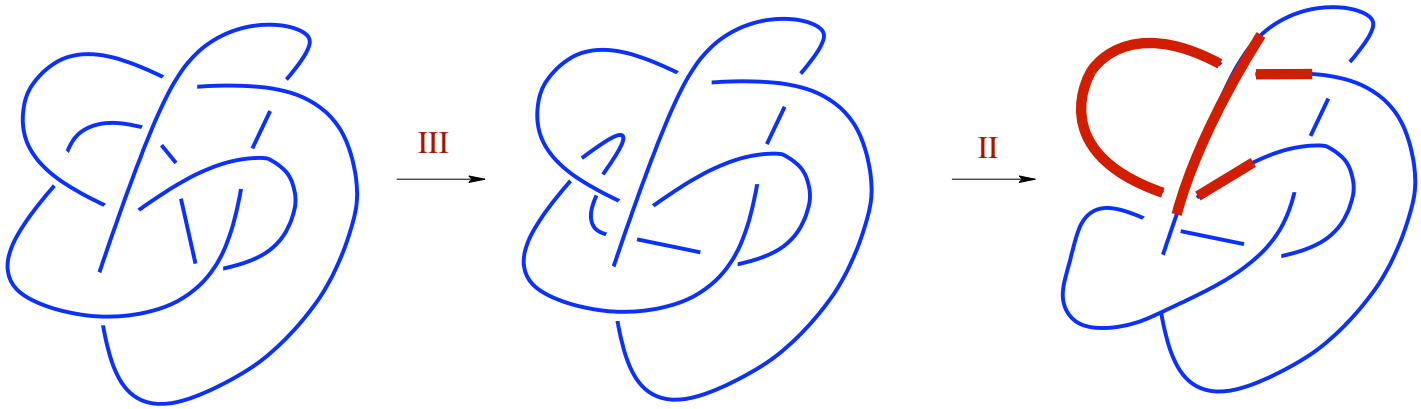
Exemple



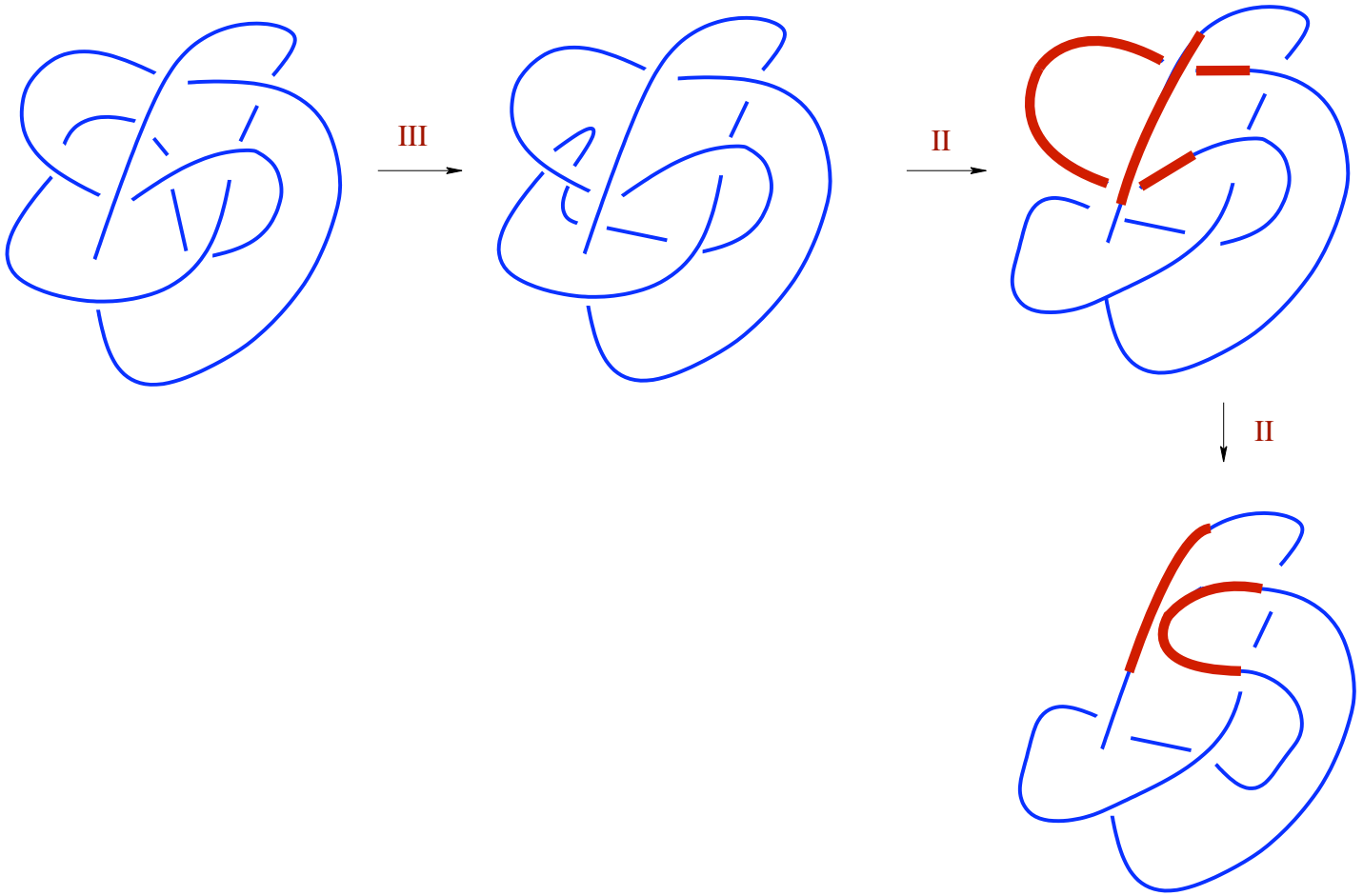
Exemple



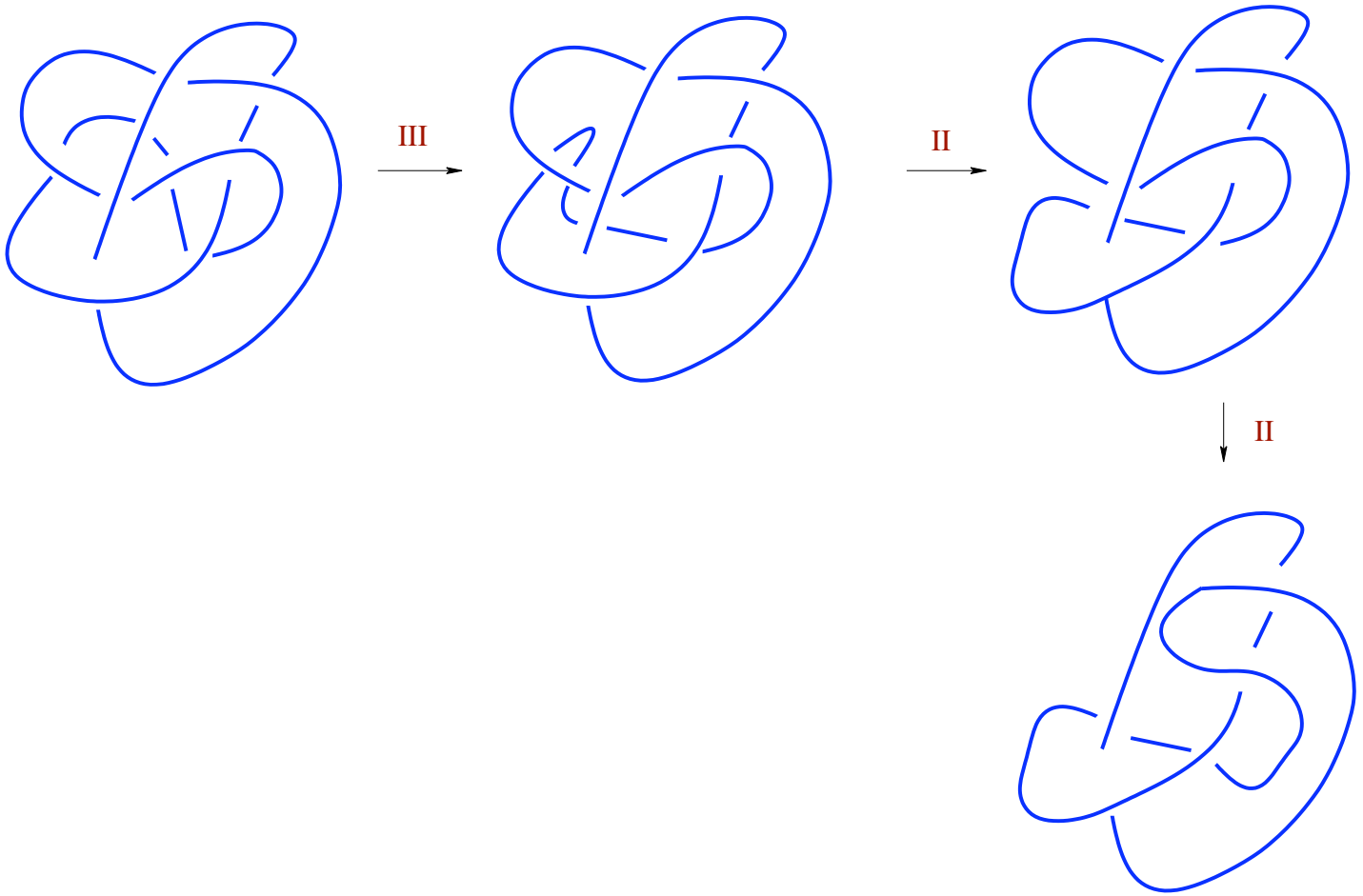
Exemple



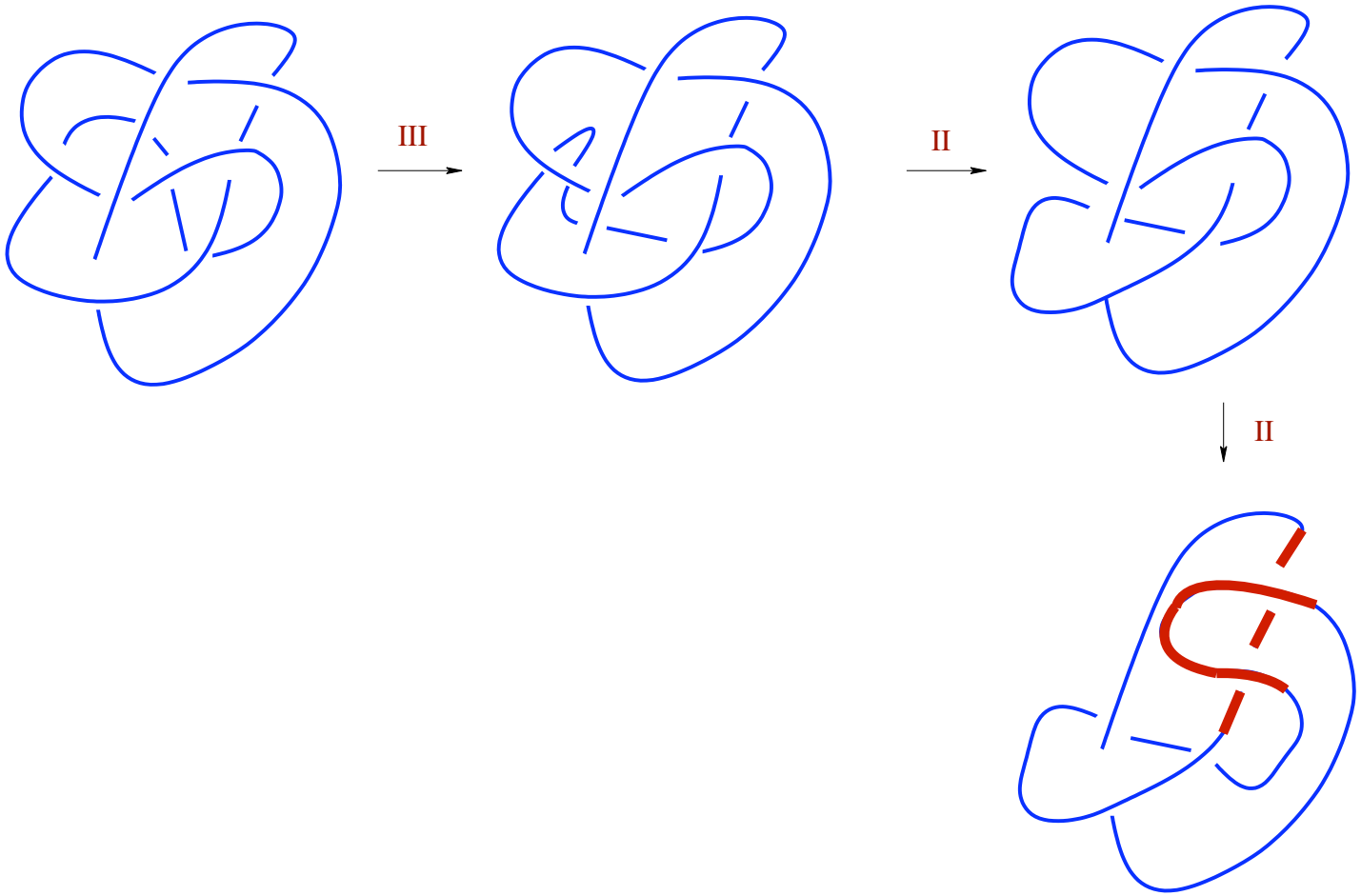
Exemple



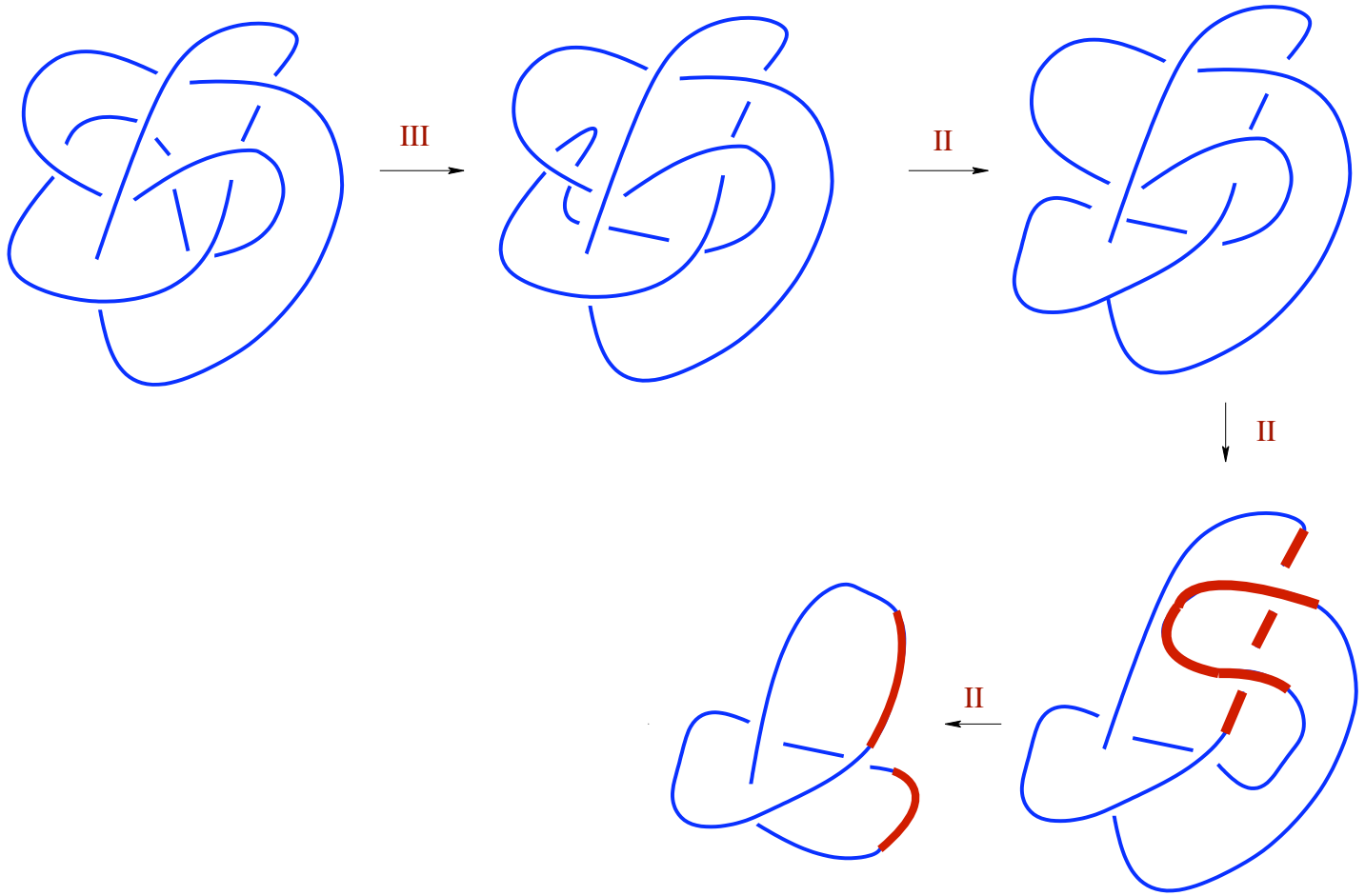
Exemple



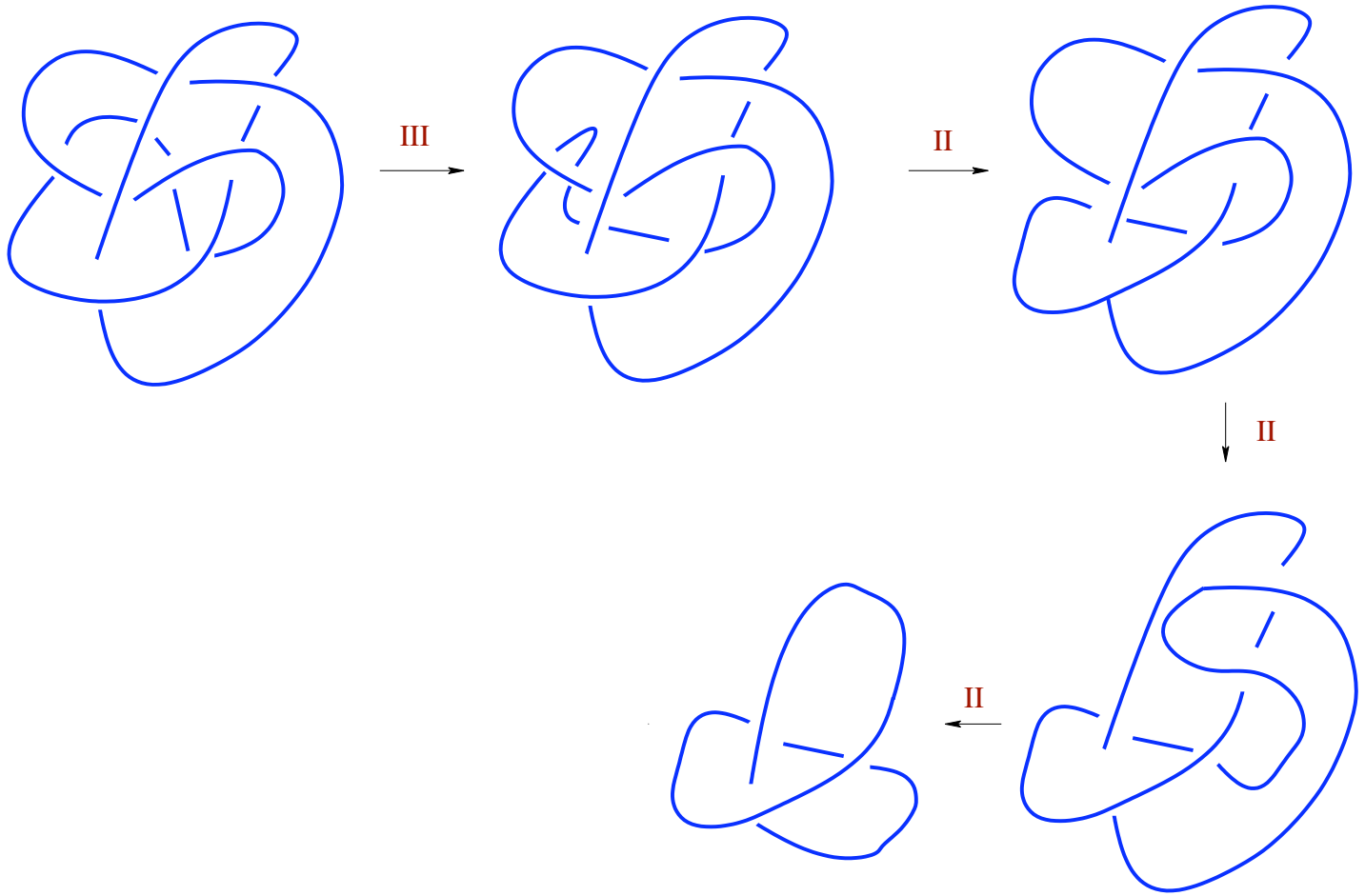
Exemple



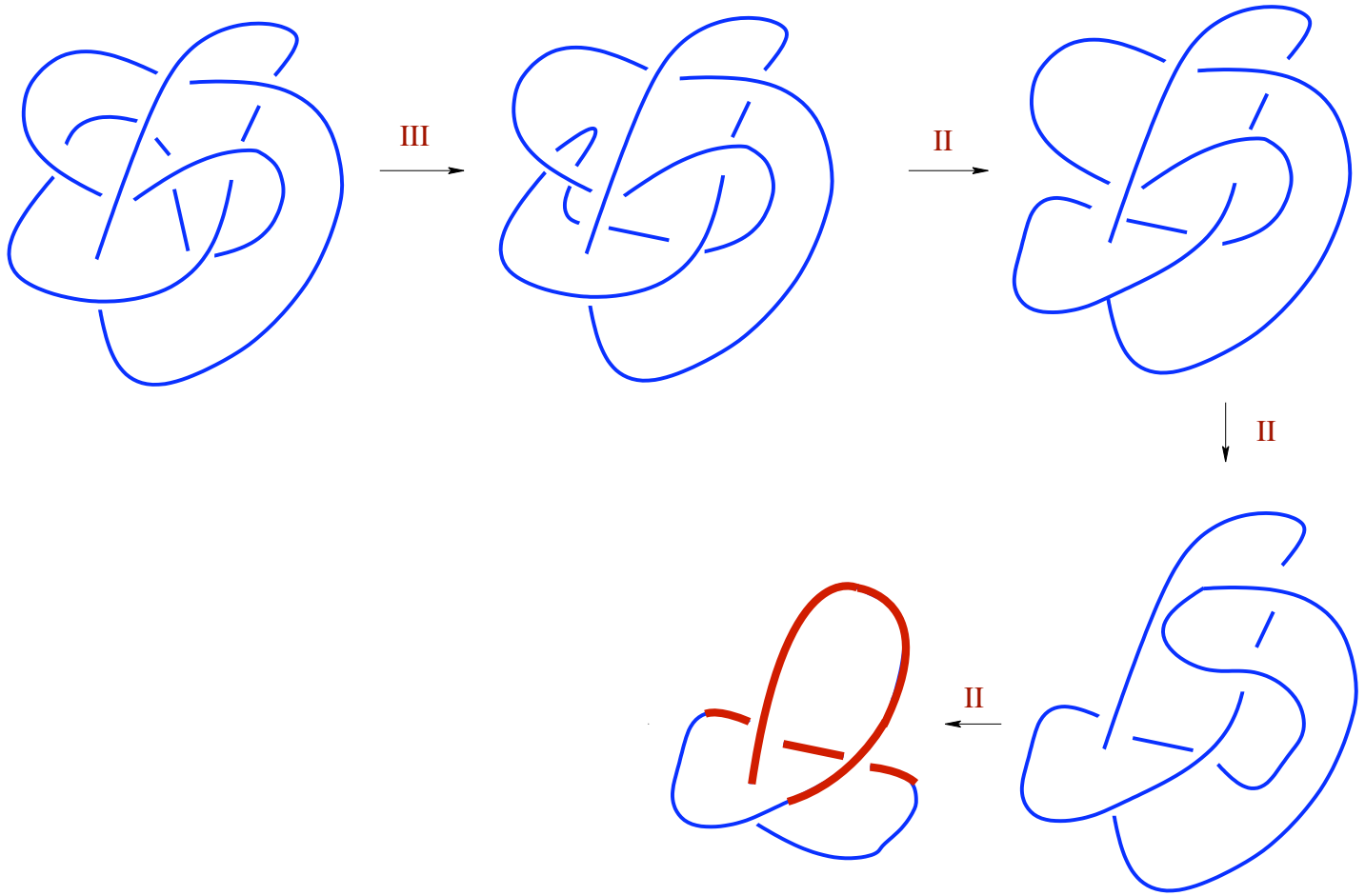
Exemple



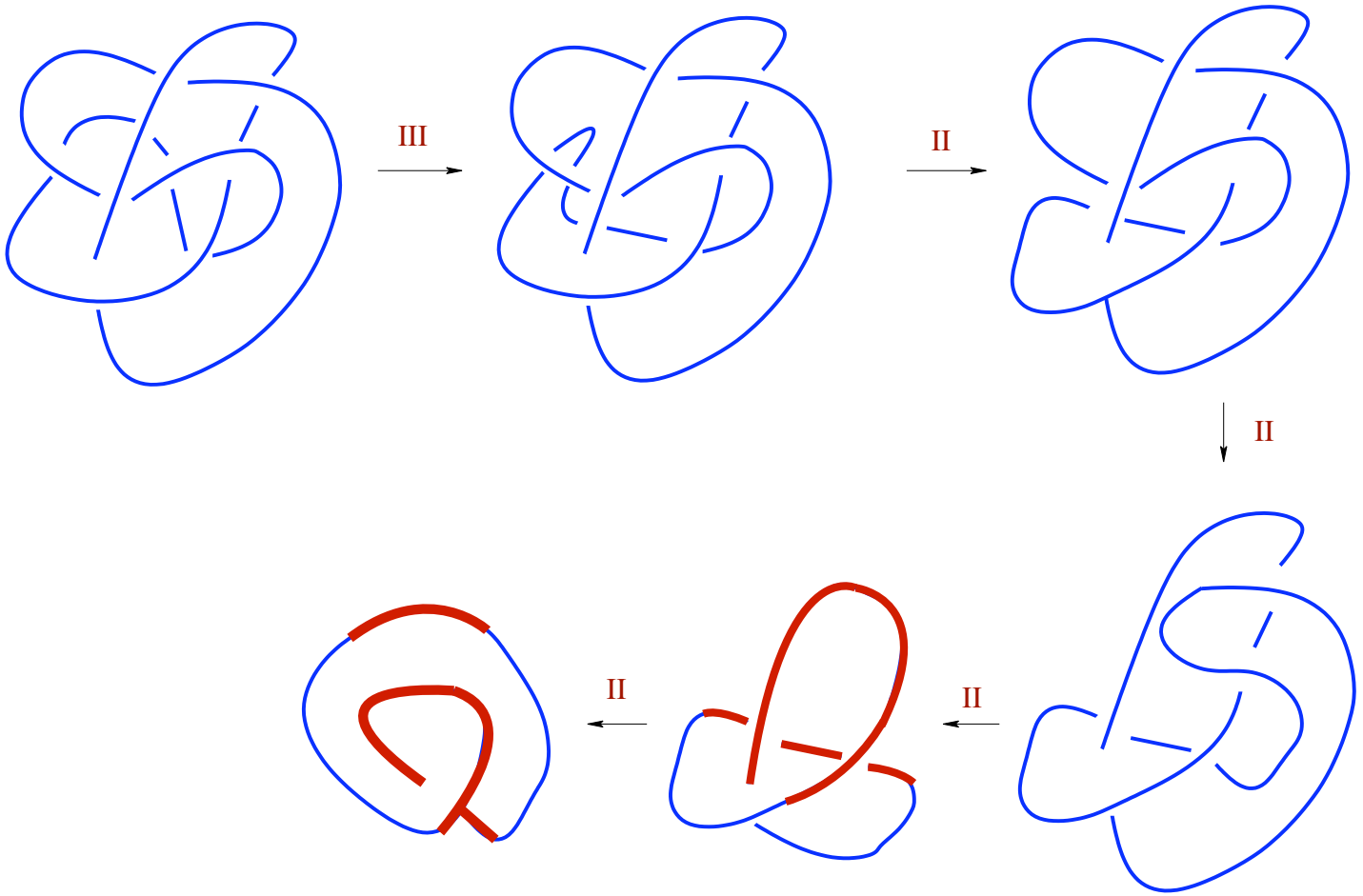
Exemple



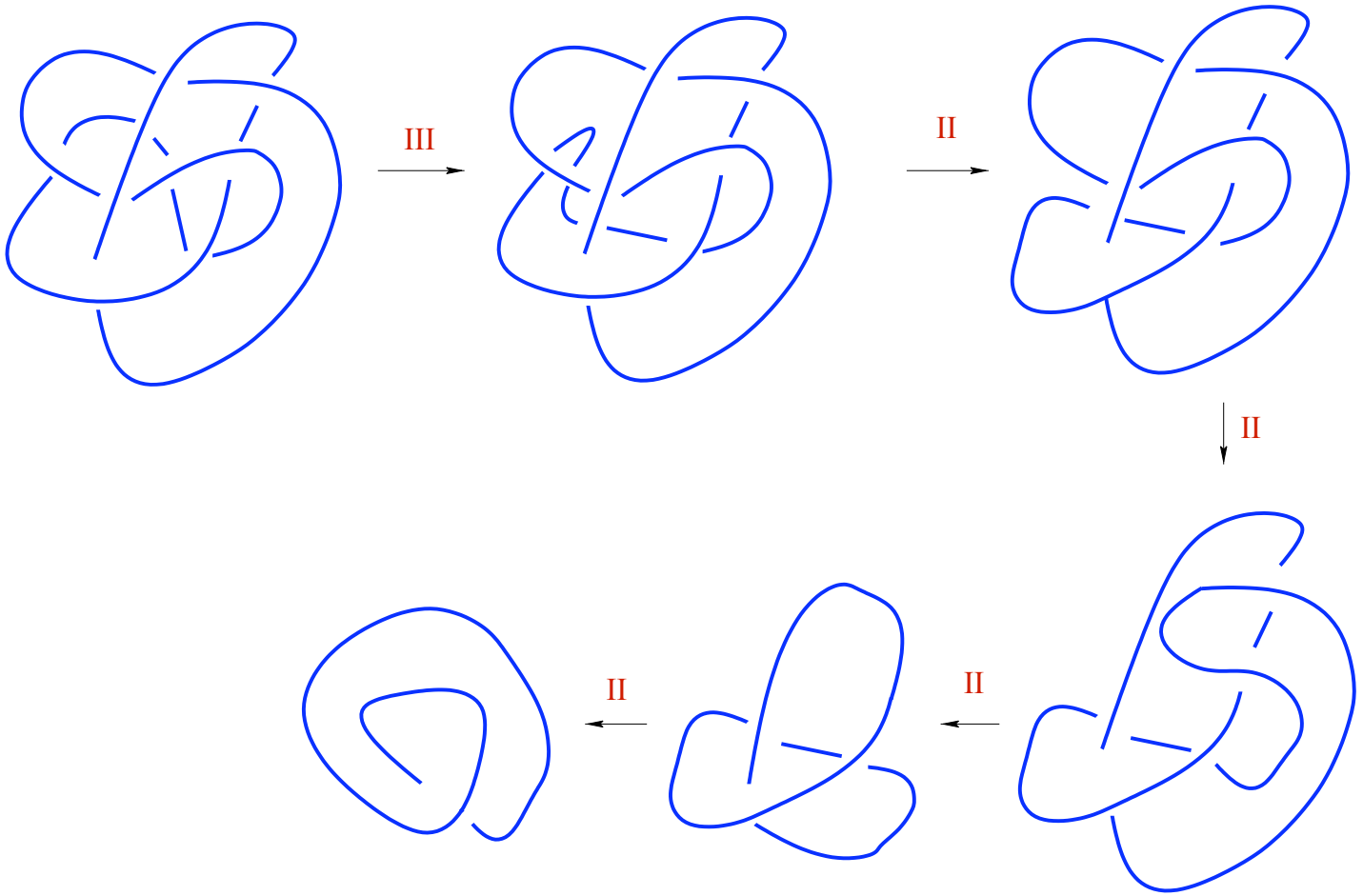
Exemple



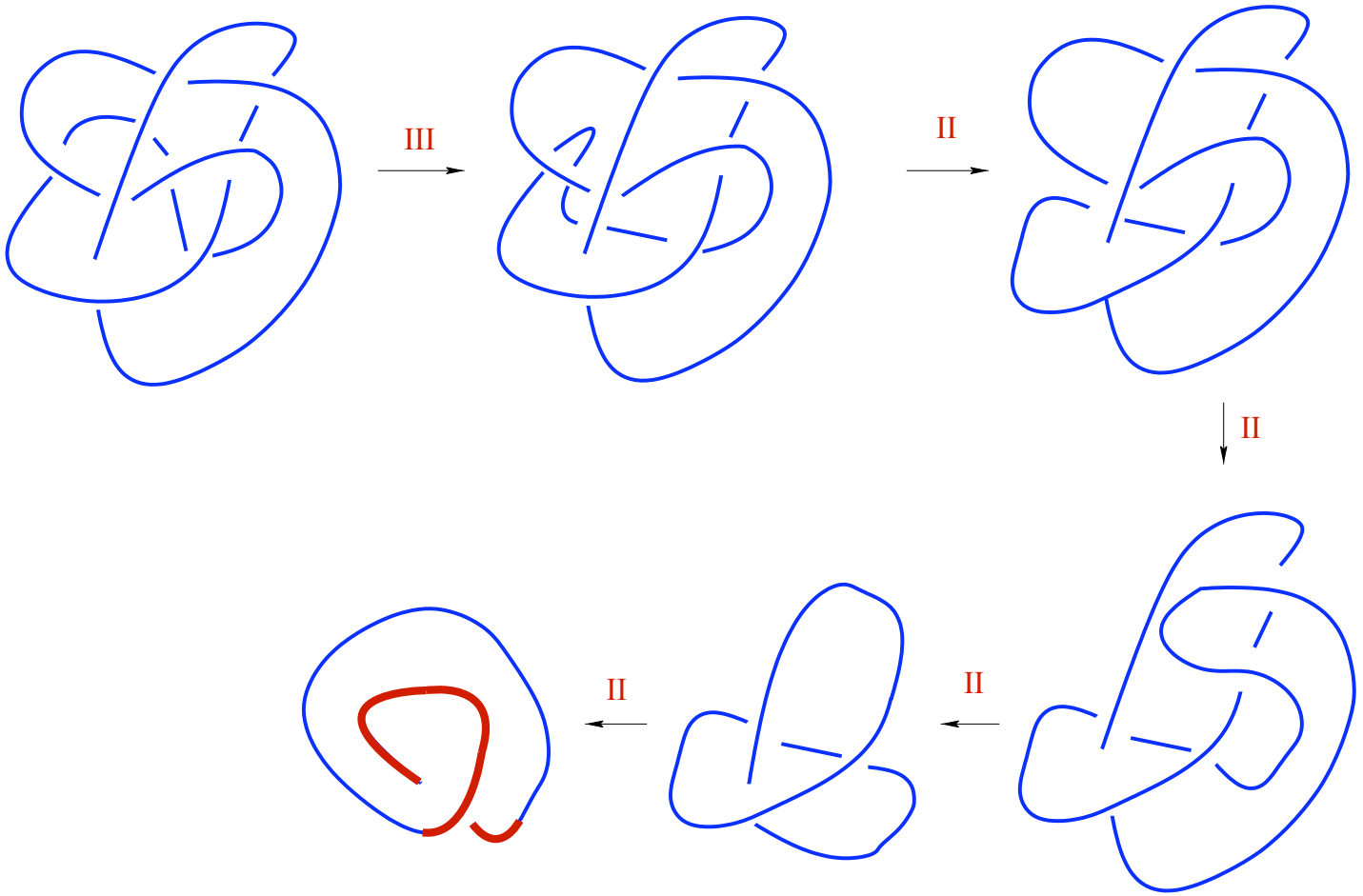
Exemple



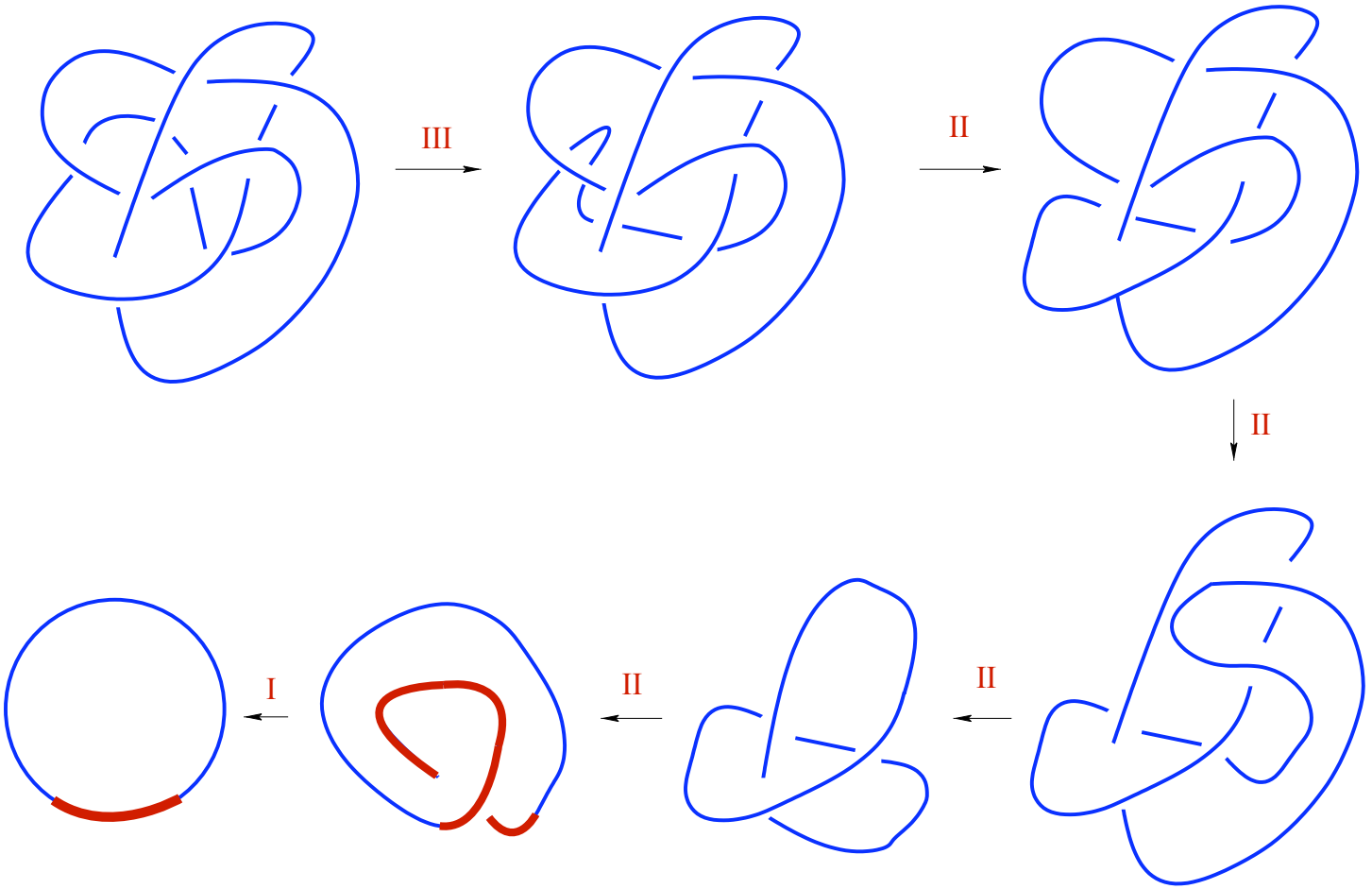
Exemple



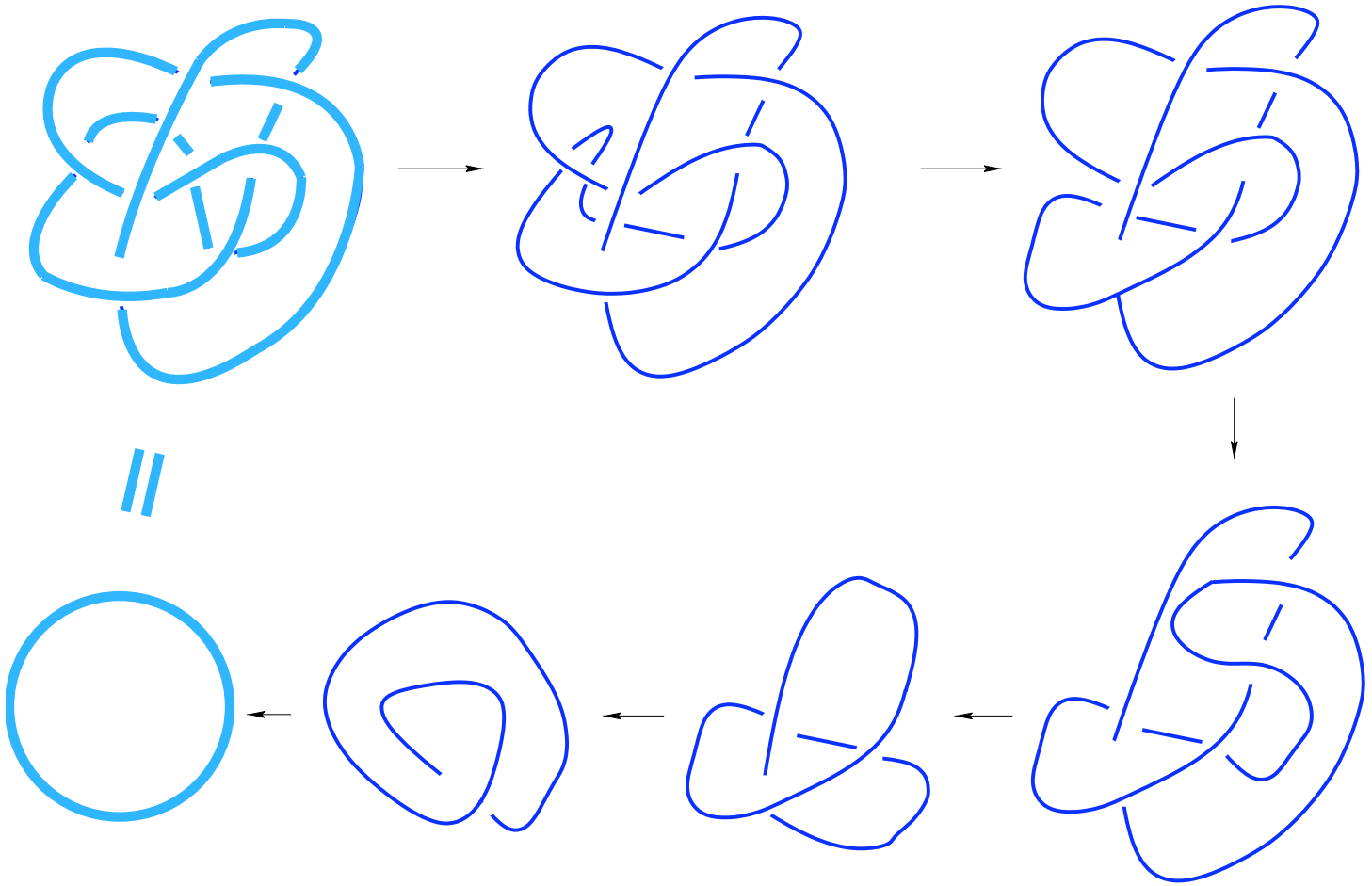
Exemple



Exemple



Exemple



3-coloriage

Le diagramme d'un nœud K est dit 3-coloriable si l'on peut colorier chaque arc du diagramme, en **rouge**, **bleu** et **vert**, tel que

- au moins 2 couleurs sont utilisées,

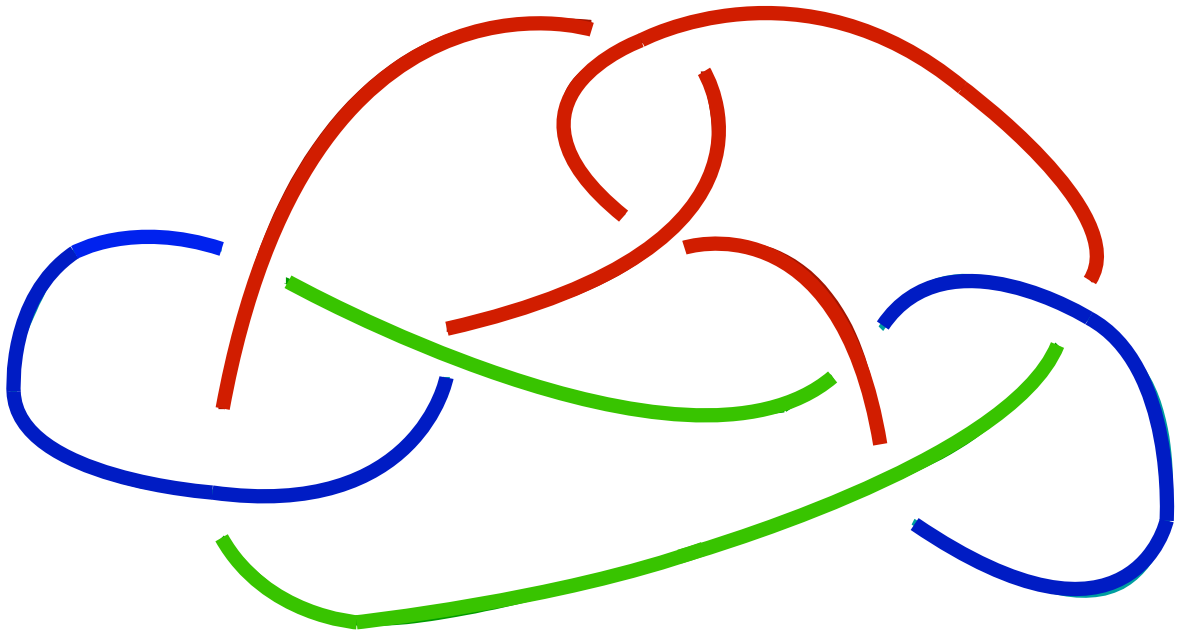
- à chaque croisement on ait soit 3 couleurs distinctes, soit une seule couleur.

3-coloriage

Le diagramme d'un nœud K est dit 3-coloriable si l'on peut colorier chaque arc du diagramme, en **rouge**, **bleu** et **vert**, tel que

- au moins 2 couleurs sont utilisées,

- à chaque croisement on ait soit 3 couleurs distinctes, soit une seule couleur.

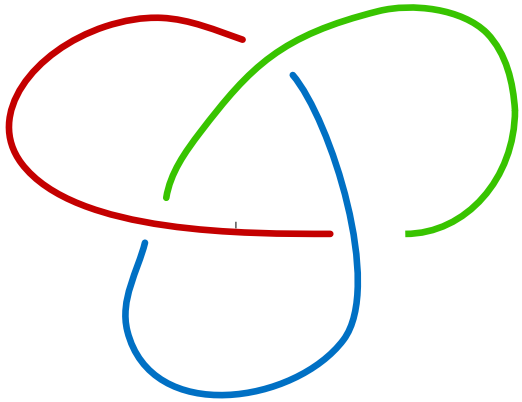


3-coloriage est un invariant

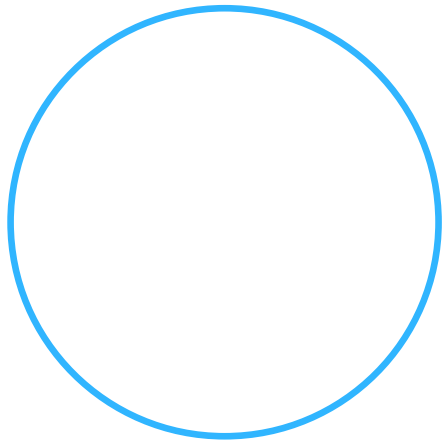
Théorème Si un diagramme d'un nœud K est 3-coloriable alors tout diagramme de K est 3-coloriable.

3-coloriage est un invariant

Théorème Si un diagramme d'un nœud K est 3-coloriable alors tout diagramme de K est 3-coloriable.



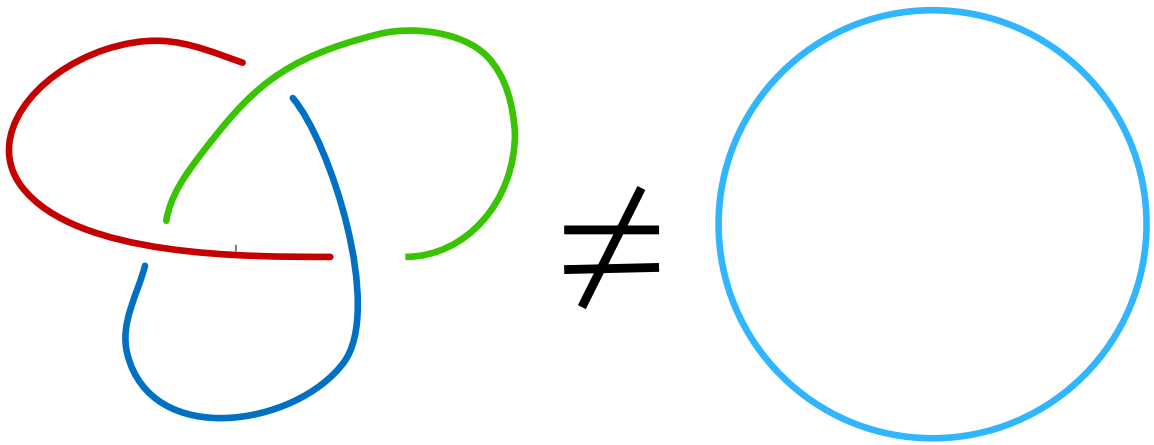
3-coloriable



n'est pas 3-coloriable

3-coloriage est un invariant

Théorème Si un diagramme d'un nœud K est 3-coloriable alors tout diagramme de K est 3-coloriable.



3-coloriable n'est pas 3-coloriable


FIN
MERCI DE VOTRE ATTENTION
À SUIVRE ...