

P = NP ?

Jacques Sauloy

sauloy@math.univ-toulouse.fr
Institut de Mathématiques de Toulouse

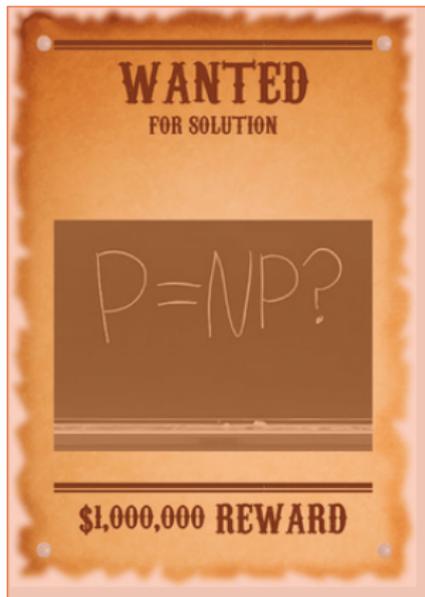
Résumé

Supposez que vous ayez demandé à votre agence de voyage de vous organiser un tour de France en train, avec la condition suivante: vous passerez dans chaque ville ayant une gare une fois et une seule. Si votre agence vous propose un trajet, vous devriez pouvoir vérifier en quelques heures si ce trajet est correct. Mais combien de temps faudra-t-il à l'agence pour trouver un tel trajet ? Même avec les ordinateurs les plus puissants du moment, probablement un temps énorme. Il est facile d'écrire un programme efficace pour vérifier une proposition de l'agence: on dit que le problème est "dans la classe NP". On ignore actuellement s'il existera un jour un programme efficace pour trouver un bon trajet, autrement dit si le problème est "dans la classe P". En l'an 2000, dernière année du précédent millénaire, la

Fondation Clay a proposé sept prix d'un million de dollars chacun pour la solution de sept problèmes importants de mathématiques. L'un d'eux a été résolu trois ans plus tard par le russe Grigori Perelman (conjecture de Poincaré). L'un des six problèmes non résolus est la question "P = NP ?", qui touche aux mathématiques, à la logique et à l'informatique.

Nous discuterons de nombreux exemples de problèmes plus ou moins "difficiles" (NP ou pires) voire impossibles à traiter par ordinateur, et plus généralement de ce que l'on sait dire du temps nécessaire à un ordinateur pour exécuter un algorithme.

Nous discuterons aussi de la question suivante: **est-il vraiment utile de concevoir de bons algorithmes dans une époque où les machines sont si puissantes ?**



P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Contents

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

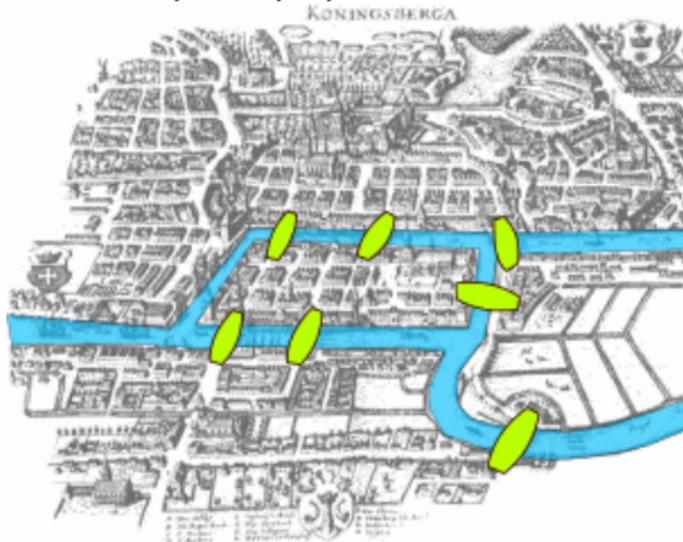
La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Les ponts de Königsberg

Dans Königsberg, devenue Kaliningrad en 1945, passe la Pregolia (en allemand "Pregel") qui y forme deux îles reliées aux rives par sept ponts.



Le dimanche, dit la légende, les bourgeois de Königsberg se promenaient en famille et essayaient de traverser chaque pont *une fois et une seule*. Mais ils n'y arrivaient jamais.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

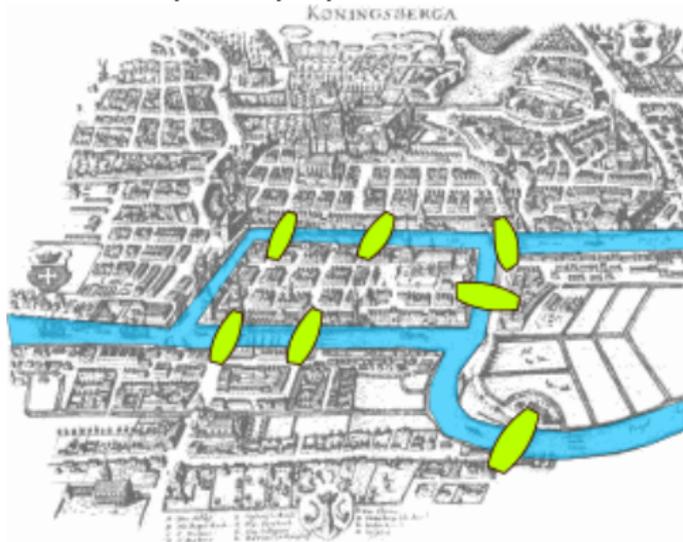
La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Les ponts de Königsberg

Dans Königsberg, devenue Kaliningrad en 1945, passe la Pregolia (en allemand "Pregel") qui y forme deux îles reliées aux rives par sept ponts.



Le dimanche, dit la légende, les bourgeois de Königsberg se promenaient en famille et essayaient de traverser chaque pont *une fois et une seule*. Mais ils n'y arrivaient jamais.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

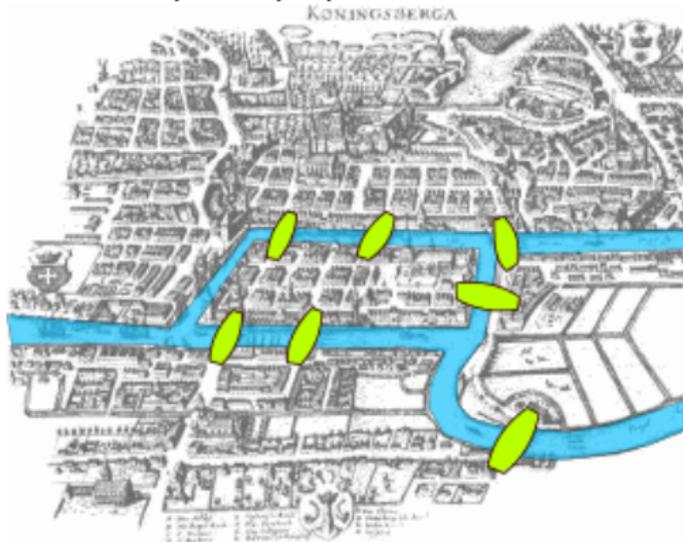
La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Les ponts de Königsberg

Dans Königsberg, devenue Kaliningrad en 1945, passe la Pregolia (en allemand "Pregel") qui y forme deux îles reliées aux rives par sept ponts.



Le dimanche, dit la légende, les bourgeois de Königsberg se promenaient en famille et essayaient de traverser chaque pont *une fois et une seule*. **Mais ils n'y arrivaient jamais.**

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

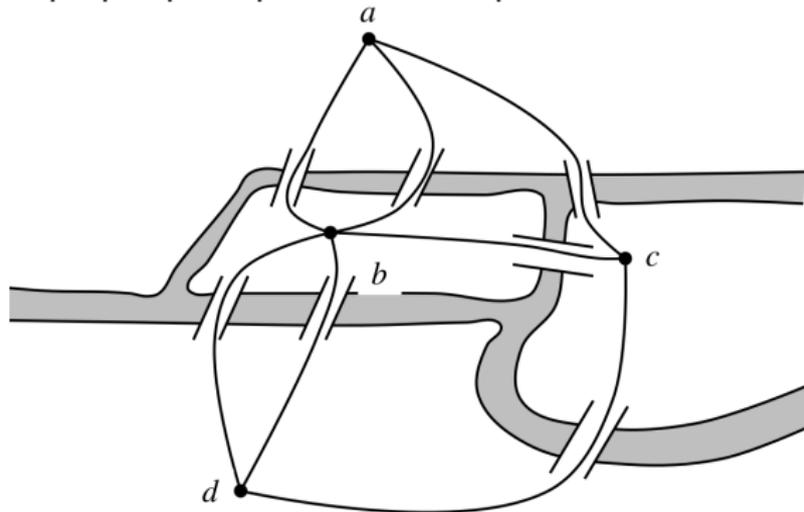
La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Les ponts de Königsberg

Leonhard Euler, mathématicien et physicien suisse, leur expliqua pourquoi c'était impossible. Prenez la rive nord.



Il en part trois ponts. À chaque aller vers le sud correspond un retour vers le nord. Mais il y a un aller sans retour, ou bien un retour sans aller. Donc la promenade doit y commencer ou y finir. Mais le même raisonnement s'applique à la rive sud et à chacune des deux îles !

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

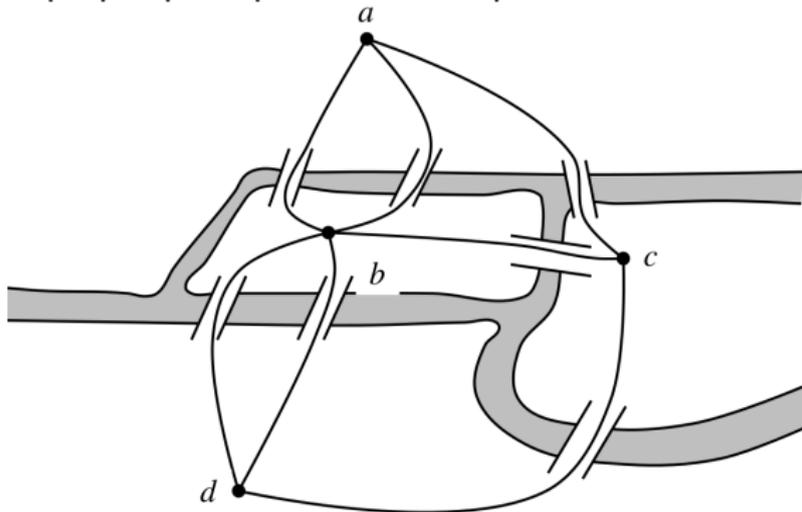
La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Les ponts de Königsberg

Leonhard Euler, mathématicien et physicien suisse, leur expliqua pourquoi c'était impossible. Prenez la rive nord.



Il en part trois ponts. À chaque aller vers le sud correspond un retour vers le nord. Mais il y a un aller sans retour, ou bien un retour sans aller. Donc la promenade doit y commencer ou y finir. Mais le même raisonnement s'applique à la rive sud et à chacune des deux îles !

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

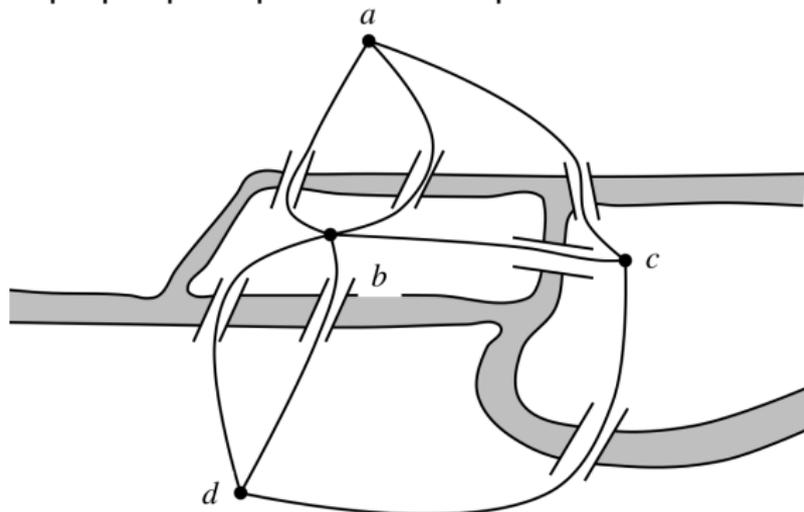
La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Les ponts de Königsberg

Leonhard Euler, mathématicien et physicien suisse, leur expliqua pourquoi c'était impossible. Prenez la rive nord.



Il en part trois ponts. À chaque aller vers le sud correspond un retour vers le nord. Mais il y a un aller sans retour, ou bien un retour sans aller. Donc la promenade doit y commencer ou y finir. Mais le même raisonnement s'applique à la rive sud et à chacune des deux îles !

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

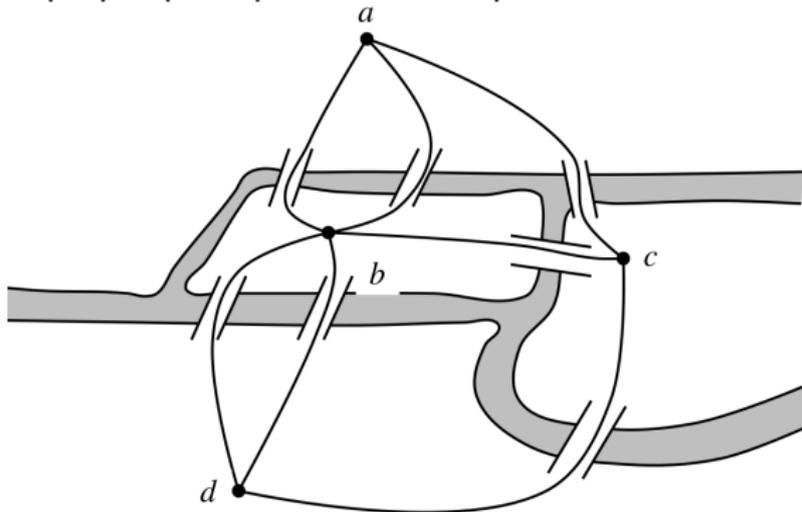
La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Les ponts de Königsberg

Leonhard Euler, mathématicien et physicien suisse, leur expliqua pourquoi c'était impossible. Prenez la rive nord.



Il en part trois ponts. À chaque aller vers le sud correspond un retour vers le nord. Mais il y a un aller sans retour, ou bien un retour sans aller. Donc la promenade doit y commencer ou y finir. Mais le même raisonnement s'applique à la rive sud et à chacune des deux îles !

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

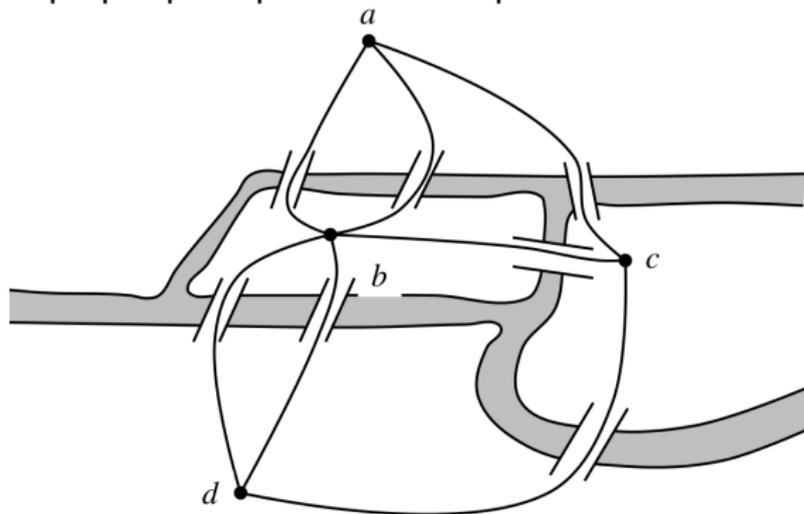
La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Les ponts de Königsberg

Leonhard Euler, mathématicien et physicien suisse, leur expliqua pourquoi c'était impossible. Prenez la rive nord.



Il en part trois ponts. À chaque aller vers le sud correspond un retour vers le nord. Mais il y a un aller sans retour, ou bien un retour sans aller. Donc la promenade doit y commencer ou y finir. **Mais le même raisonnement s'applique à la rive sud et à chacune des deux îles !**

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

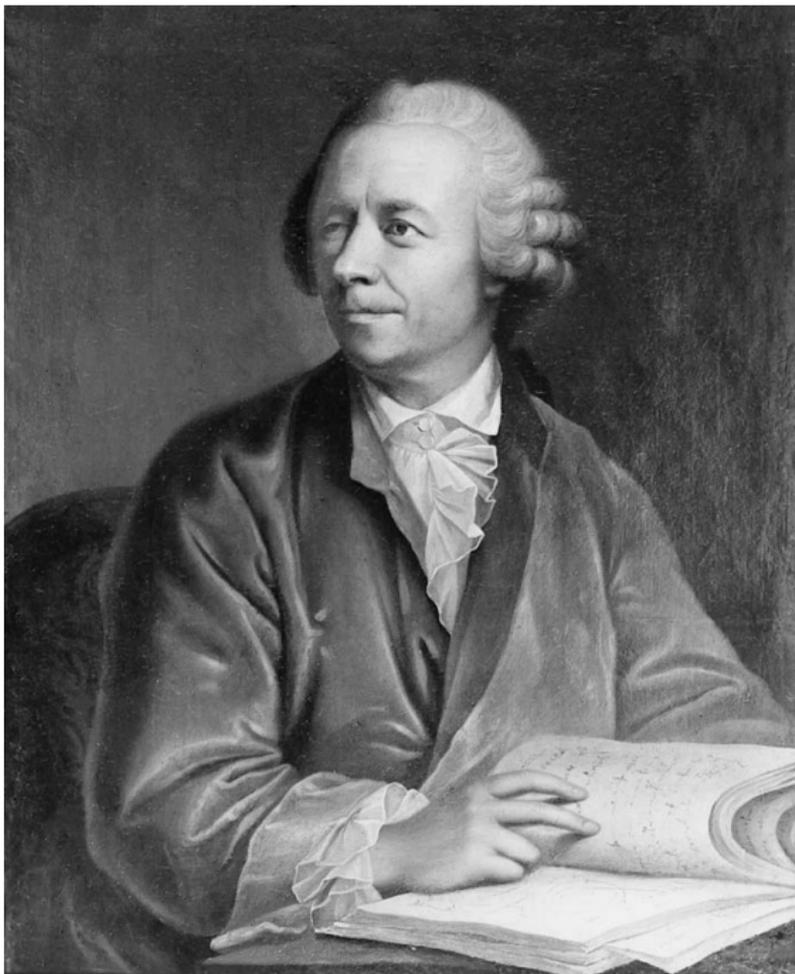
Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction



$P = NP ?$

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

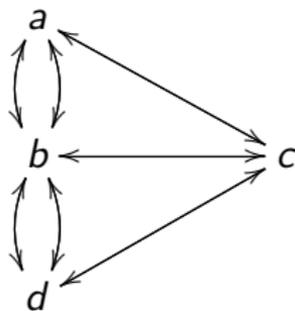
La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Les ponts de Königsberg

Euler généralisa le problème et inventa la théorie des graphes. Il y a des *nœuds* et des *arêtes*. Les nœuds d'où partent un nombre *impair* d'arêtes sont dits *impairs*. Un *chemin eulérien* doit passer par chaque arête une fois et une seule. S'il revient au point de départ, c'est un *circuit eulérien*.



Notre graphe a quatre nœuds impairs: c'est au moins deux de trop car chacun doit être le départ ou l'arrivée.

Ce n'est donc pas la peine de chercher.

Un petit exercice (facultatif): dans tout graphe, il y a un nombre pair de nœuds impairs.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

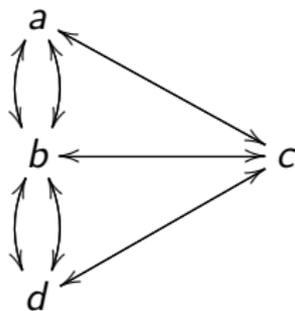
La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Les ponts de Königsberg

Euler généralisa le problème et inventa la théorie des graphes. Il y a des *nœuds* et des *arêtes*. Les nœuds d'où partent un nombre *impair* d'arêtes sont dits *impairs*. Un *chemin eulérien* doit passer par chaque arête une fois et une seule. S'il revient au point de départ, c'est un *circuit eulérien*.



Notre graphe a quatre nœuds impairs: c'est au moins deux de trop car chacun doit être le départ ou l'arrivée.

Ce n'est donc pas la peine de chercher.

Un petit exercice (facultatif): dans tout graphe, il y a un nombre pair de nœuds impairs.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

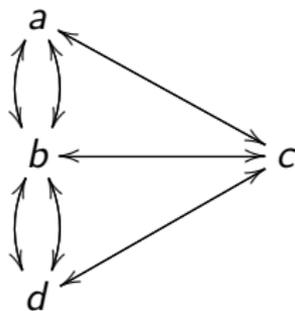
La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Les ponts de Königsberg

Euler généralisa le problème et inventa la théorie des graphes. Il y a des *nœuds* et des *arêtes*. Les nœuds d'où partent un nombre *impair* d'arêtes sont dits *impairs*. Un *chemin eulérien* doit passer par chaque arête une fois et une seule. S'il revient au point de départ, c'est un *circuit eulérien*.



Notre graphe a quatre nœuds impairs: c'est au moins deux de trop car chacun doit être le départ ou l'arrivée.

Ce n'est donc pas la peine de chercher.

Un petit exercice (facultatif): dans tout graphe, il y a un nombre pair de nœuds impairs.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

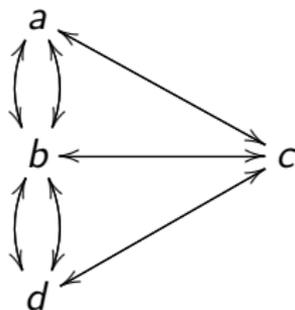
La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Les ponts de Königsberg

Euler généralisa le problème et inventa la théorie des graphes. Il y a des *nœuds* et des *arêtes*. Les nœuds d'où partent un nombre *impair* d'arêtes sont dits *impairs*. Un *chemin eulérien* doit passer par chaque arête une fois et une seule. S'il revient au point de départ, c'est un *circuit eulérien*.



Notre graphe a quatre nœuds impairs: c'est au moins deux de trop car chacun doit être le départ ou l'arrivée.

Ce n'est donc pas la peine de chercher.

Un petit exercice (facultatif): dans tout graphe, il y a un nombre pair de nœuds impairs.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

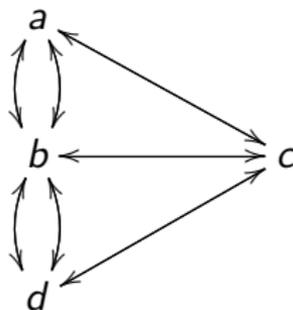
La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Les ponts de Königsberg

Euler généralisa le problème et inventa la théorie des graphes. Il y a des *nœuds* et des *arêtes*. Les nœuds d'où partent un nombre *impair* d'arêtes sont dits *impairs*. Un *chemin eulérien* doit passer par chaque arête une fois et une seule. S'il revient au point de départ, c'est un *circuit eulérien*.



Notre graphe a quatre nœuds impairs: c'est au moins deux de trop car chacun doit être le départ ou l'arrivée.

Ce n'est donc pas la peine de chercher.

Un petit exercice (facultatif): dans tout graphe, il y a un nombre pair de nœuds impairs.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

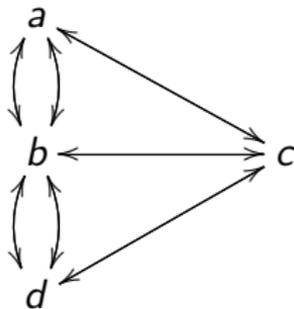
La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Les ponts de Königsberg

Euler généralisa le problème et inventa la théorie des graphes. Il y a des *nœuds* et des *arêtes*. Les nœuds d'où partent un nombre *impair* d'arêtes sont dits *impairs*. Un *chemin eulérien* doit passer par chaque arête une fois et une seule. S'il revient au point de départ, c'est un *circuit eulérien*.



Notre graphe a quatre nœuds impairs: c'est au moins deux de trop car chacun doit être le départ ou l'arrivée.

Ce n'est donc pas la peine de chercher.

Un petit exercice (facultatif): dans tout graphe, il y a un nombre pair de nœuds impairs.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

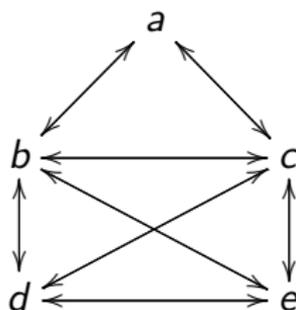
Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Une autre application

Voici par exemple comment tracer une enveloppe sans doubler les traits et sans lever le crayon: c'est un problème de "chemin eulerien" !

Les seuls sommets impairs sont d et e . Tout chemin eulerien devra donc partir de l'un et arriver à l'autre. Des chemins possibles sont: $dbacedcbe$ et $dcebcabde$ (il y en a d'autres).



Et que pensez-vous du chemin $abcdebd$? et du chemin $abcdebdce$?

Combien de chemins faut-il ainsi tester pour être certain d'en trouver un bon s'il en existe ?

P = NP ?

Jacques Sauloy

Königsberg et les chemins euleriens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

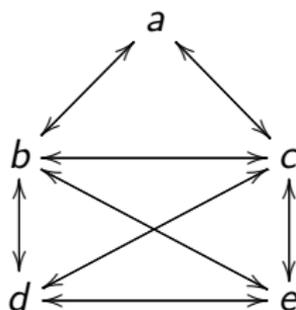
Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Une autre application

Voici par exemple comment tracer une enveloppe sans doubler les traits et sans lever le crayon: c'est un problème de "chemin eulerien" !

Les seuls sommets impairs sont d et e . Tout chemin eulerien devra donc partir de l'un et arriver à l'autre. Des chemins possibles sont: $dbacedcbe$ et $dcebcabde$ (il y en a d'autres).



Et que pensez-vous du chemin $abcdebd$? et du chemin $abcdebdce$?

Combien de chemins faut-il ainsi tester pour être certain d'en trouver un bon s'il en existe ?

P = NP ?

Jacques Sauloy

Königsberg et les chemins euleriens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

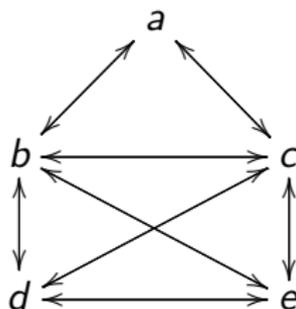
Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Une autre application

Voici par exemple comment tracer une enveloppe sans doubler les traits et sans lever le crayon: c'est un problème de "chemin eulerien" !

Les seuls sommets impairs sont d et e . Tout chemin eulerien devra donc partir de l'un et arriver à l'autre. Des chemins possibles sont: $dbacedcbe$ et $dcebcabde$ (il y en a d'autres).



Et que pensez-vous du chemin $abcdebd$? et du chemin $abcdebdce$?

Combien de chemins faut-il ainsi tester pour être certain d'en trouver un bon s'il en existe ?

P = NP ?

Jacques Sauloy

Königsberg et les chemins euleriens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Encore une autre application

Le responsable de la sécurité veut vérifier toutes les portes. Comme il n'a pas beaucoup de temps (16 étages !), il veut passer par chaque porte une fois et une seule.



C'est encore un problème de circuit eulerien.

P = NP ?

Jacques Sauloy

Königsberg et les chemins euleriens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Pour résumer ce que l'on sait

On peut tester un chemin en temps raisonnable pour voir s'il est eulerien.

On peut essayer tous les chemins possibles jusqu'à en trouver un qui soit eulerien.

Mais en fait il y a un bon *algorithme* qui évite cette exploration systématique.

“Non deterministic polynomial” : si on a de la chance (“non deterministic”), on tombe rapidement (“polynomial”) sur un chemin eulerien et on a gagné en peu de temps.

On dit que le problème est NP pour “non deterministic polynomial”.

Cette méthode de “force brutale” n'est pas viable pour de grands graphes: elle est “de coût exponentiel”.

On dit que le problème est P pour “polynomial”.

P = NP ?

Jacques Sauloy

Königsberg et les chemins euleriens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Pour résumer ce que l'on sait

On peut tester un chemin en temps raisonnable pour voir s'il est eulerien.

On peut essayer tous les chemins possibles jusqu'à en trouver un qui soit eulerien.

Mais en fait il y a un bon *algorithme* qui évite cette exploration systématique.

“Non deterministic polynomial” : si on a de la chance (“non deterministic”), on tombe rapidement (“polynomial”) sur un chemin eulerien et on a gagné en peu de temps.

On dit que le problème est NP pour “non deterministic polynomial” .

Cette méthode de “force brutale” n'est pas viable pour de grands graphes: elle est “de coût exponentiel” .

On dit que le problème est P pour “polynomial” .

P = NP ?

Jacques Sauloy

Königsberg et les chemins euleriens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Pour résumer ce que l'on sait

On peut tester un chemin en temps raisonnable pour voir s'il est eulerien.

On peut essayer tous les chemins possibles jusqu'à en trouver un qui soit eulerien.

Mais en fait il y a un bon *algorithme* qui évite cette exploration systématique.

“Non deterministic polynomial” : si on a de la chance (“non deterministic”), on tombe rapidement (“polynomial”) sur un chemin eulerien et on a gagné en peu de temps.

On dit que le problème est NP pour “non deterministic polynomial” .

Cette méthode de “force brutale” n'est pas viable pour de grands graphes: elles est “de coût exponentiel” .

On dit que le problème est P pour “polynomial” .

P = NP ?

Jacques Sauloy

Königsberg et les chemins euleriens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Pour résumer ce que l'on sait

On peut tester un chemin en temps raisonnable pour voir s'il est eulerien.

On peut essayer tous les chemins possibles jusqu'à en trouver un qui soit eulerien.

Mais en fait il y a un bon *algorithme* qui évite cette exploration systématique.

“Non deterministic polynomial” : si on a de la chance (“non deterministic”), on tombe rapidement (“polynomial”) sur un chemin eulerien et on a gagné en peu de temps.

On dit que le problème est NP pour “non deterministic polynomial” .

Cette méthode de “force brutale” n'est pas viable pour de grands graphes: elle est “de coût exponentiel” .

On dit que le problème est P pour “polynomial” .

P = NP ?

Jacques Sauloy

Königsberg et les chemins euleriens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Pour résumer ce que l'on sait

On peut tester un chemin en temps raisonnable pour voir s'il est eulerien.

On peut essayer tous les chemins possibles jusqu'à en trouver un qui soit eulerien.

Mais en fait il y a un bon *algorithme* qui évite cette exploration systématique.

On dit que le problème est NP pour "non deterministic polynomial".

Cette méthode de "force brutale" n'est pas viable pour de grands graphes: elle est "de coût exponentiel".

On dit que le problème est P pour "polynomial".

"Non deterministic polynomial": si on a de la chance ("non deterministic"), on tombe rapidement ("polynomial") sur un chemin eulerien et on a gagné en peu de temps.

P = NP ?

Jacques Sauloy

Königsberg et les chemins euleriens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Pour résumer ce que l'on sait

On peut tester un chemin en temps raisonnable pour voir s'il est eulerien.

On peut essayer tous les chemins possibles jusqu'à en trouver un qui soit eulerien.

Mais en fait il y a un bon *algorithme* qui évite cette exploration systématique.

On dit que le problème est NP pour "non deterministic polynomial".

Cette méthode de "force brutale" n'est pas viable pour de grands graphes: elle est "de coût exponentiel".

On dit que le problème est P pour "polynomial".

"Non deterministic polynomial": si on a de la chance ("non deterministic"), on tombe rapidement ("polynomial") sur un chemin eulerien et on a gagné en peu de temps.

P = NP ?

Jacques Sauloy

Königsberg et les chemins euleriens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Pour résumer ce que l'on sait

On peut tester un chemin en temps raisonnable pour voir s'il est eulerien.

On peut essayer tous les chemins possibles jusqu'à en trouver un qui soit eulerien.

Mais en fait il y a un bon *algorithme* qui évite cette exploration systématique.

On dit que le problème est NP pour "non deterministic polynomial".

Cette méthode de "force brutale" n'est pas viable pour de grands graphes: elle est "de coût exponentiel".

On dit que le problème est P pour "polynomial".

"Non deterministic polynomial": si on a de la chance ("non deterministic"), on tombe rapidement ("polynomial") sur un chemin eulerien et on a gagné en peu de temps.

P = NP ?

Jacques Sauloy

Königsberg et les chemins euleriens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Plan

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Le voyageur de commerce: ce qu'il veut

P = NP ?

Jacques Sauloy

Il voudrait passer par toutes les villes (desservies par une gare) une fois et une seule; et revenir à son point de départ.

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction



De plus, il voudrait *minimiser* la distance totale parcourue.

Le voyageur de commerce: ce qu'il veut

P = NP ?

Jacques Sauloy

Il voudrait passer par toutes les villes (desservies par une gare) une fois et une seule; et revenir à son point de départ.

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction



De plus, il voudrait *minimiser* la distance totale parcourue.

Circuit hamiltonien

P = NP ?

Jacques Sauloy

Nous allons simplifier le problème et simplement chercher un trajet qui passe par chaque ville une fois et une seule et qui revienne au point de départ.

C'est encore un problème de graphe, et l'on y cherche un *circuit hamiltonien*.

C'est encore un problème NP: la vérification d'une solution potentielle ne prend pas beaucoup de temps.

Si l'on n'exige pas le retour au point de départ, on parle de *chemin* Hamiltonien. Cela ne change rien d'essentiel à ce qui va suivre (et cela ne changeait rien d'essentiel non plus dans le cas des chemins et circuits eulériens).

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Circuit hamiltonien

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Nous allons simplifier le problème et simplement chercher un trajet qui passe par chaque ville une fois et une seule et qui revienne au point de départ.

C'est encore un problème de graphe, et l'on y cherche un *circuit hamiltonien*.

C'est encore un problème NP: la vérification d'une solution potentielle ne prend pas beaucoup de temps.

Si l'on n'exige pas le retour au point de départ, on parle de *chemin* Hamiltonien. Cela ne change rien d'essentiel à ce qui va suivre (et cela ne changeait rien d'essentiel non plus dans le cas des chemins et circuits eulériens).

Circuit hamiltonien

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Nous allons simplifier le problème et simplement chercher un trajet qui passe par chaque ville une fois et une seule et qui revienne au point de départ.

C'est encore un problème de graphe, et l'on y cherche un *circuit hamiltonien*.

C'est encore un problème NP: la vérification d'une solution potentielle ne prend pas beaucoup de temps.

Si l'on n'exige pas le retour au point de départ, on parle de *chemin* Hamiltonien. Cela ne change rien d'essentiel à ce qui va suivre (et cela ne changeait rien d'essentiel non plus dans le cas des chemins et circuits eulériens).

Circuit hamiltonien

P = NP ?

Jacques Sauloy

Nous allons simplifier le problème et simplement chercher un trajet qui passe par chaque ville une fois et une seule et qui revienne au point de départ.

C'est encore un problème de graphe, et l'on y cherche un *circuit hamiltonien*.

C'est encore un problème NP: la vérification d'une solution potentielle ne prend pas beaucoup de temps.

Si l'on n'exige pas le retour au point de départ, on parle de *chemin* Hamiltonien. Cela ne change rien d'essentiel à ce qui va suivre (et cela ne changeait rien d'essentiel non plus dans le cas des chemins et circuits eulériens).

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

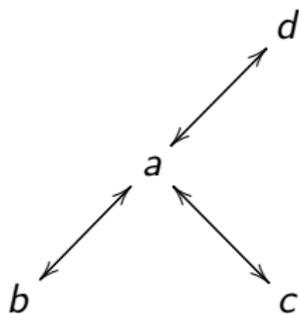
La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Un exemple facile

Voici par exemple où l'on "voit" instantanément qu'il n'y a pas de circuit hamiltonien, ni même de chemin hamiltonien d'ailleurs.



Cependant, si l'on est bête (comme une machine mal programmée par exemple), il faut essayer chacun des 24 chemins possibles: *abcd*, *abdc*, *acbd*, *acdb*, *adbc*, *adcb*, *bacd*, *badc*, *bcad*, *bcda*, *bdac*, *bdca*, *cabd*, *cadb*, *cbad*, *cbda*, *cdab*, *cdba*, *dabc*, *dacb*, *dbac*, *dbca*, *dcab*, *dcba*.

Est-on certain de n'avoir rien oublié ?

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

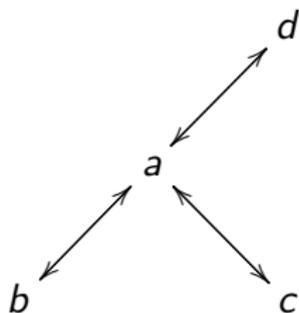
La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Un exemple facile

Voici par exemple où l'on "voit" instantanément qu'il n'y a pas de circuit hamiltonien, ni même de chemin hamiltonien d'ailleurs.



Cependant, si l'on est bête (comme une machine mal programmée par exemple), il faut essayer chacun des 24 chemins possibles: $abcd$, $abdc$, $acbd$, $acdb$, $adbc$, $adcb$, $bacd$, $badc$, $bcad$, $bcda$, $bdac$, $bdca$, $cabd$, $cadb$, $cbad$, $cbda$, $cdab$, $cdba$, $dabc$, $dacb$, $dbac$, $dbca$, $dcab$, $dcba$.

Est-on certain de n'avoir rien oublié ?

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

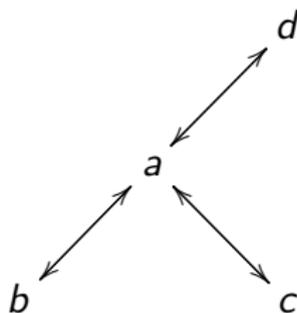
La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Un exemple facile

Voici par exemple où l'on "voit" instantanément qu'il n'y a pas de circuit hamiltonien, ni même de chemin hamiltonien d'ailleurs.



Cependant, si l'on est bête (comme une machine mal programmée par exemple), il faut essayer chacun des 24 chemins possibles: $abcd$, $abdc$, $acbd$, $acdb$, $adbc$, $adcb$, $bacd$, $badc$, $bcad$, $bcda$, $bdac$, $bdca$, $cabd$, $cadb$, $cbad$, $cbda$, $cdab$, $cdba$, $dabc$, $dacb$, $dbac$, $dbca$, $dcab$, $dcba$.

Est-on certain de n'avoir rien oublié ?

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

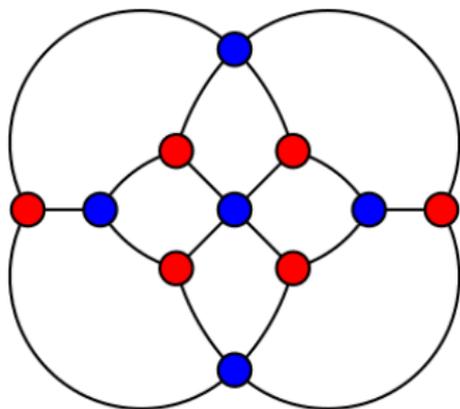
La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Un exemple moins facile: le graphe de Herschel

Voici par exemple où l'on "voit" facilement qu'il y a un chemin hamiltonien, et moins facilement qu'il n'y a pas de circuit hamiltonien.



Argument: on est obligé de visiter alternativement les nœuds rouges (chinois) et les nœuds bleus (français) ... mais il n'y en a pas le même nombre !

Mais si l'on ne trouve pas l'astuce, comment fait-on ?

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

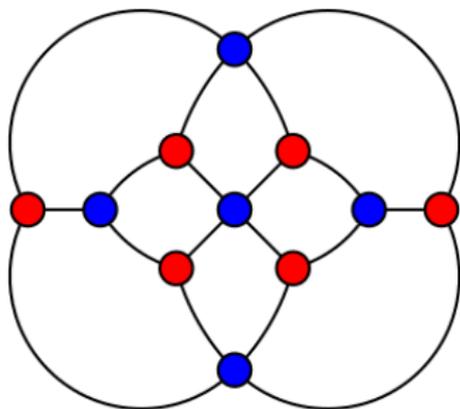
La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Un exemple moins facile: le graphe de Herschel

Voici par exemple où l'on "voit" facilement qu'il y a un chemin hamiltonien, et moins facilement qu'il n'y a pas de circuit hamiltonien.



Argument: on est obligé de visiter alternativement les nœuds rouges (chinois) et les nœuds bleus (français) ... mais il n'y en a pas le même nombre !

Mais si l'on ne trouve pas l'astuce, comment fait-on ?

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

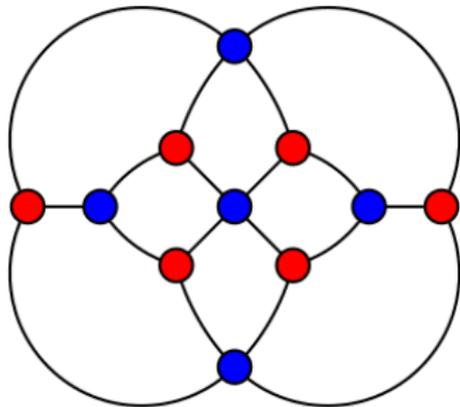
La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Un exemple moins facile: le graphe de Herschel

Voici par exemple où l'on "voit" facilement qu'il y a un chemin hamiltonien, et moins facilement qu'il n'y a pas de circuit hamiltonien.



Argument: on est obligé de visiter alternativement les nœuds rouges (chinois) et les nœuds bleus (français) ... mais il n'y en a pas le même nombre !

Mais si l'on ne trouve pas l'astuce, comment fait-on ?.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

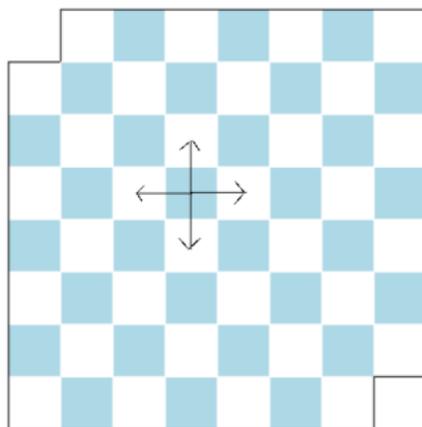
La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Un exemple: parcours de la tour sur un échiquier écorné

Déplacements possibles de la tour:



La tour peut-elle visiter toutes les cases une seule fois ?

C'est encore un problème de chemin hamiltonien.

Mais la réponse est non !

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

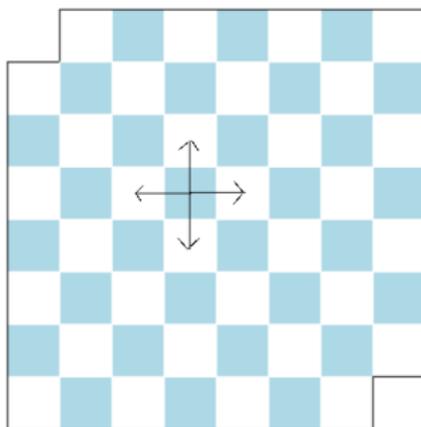
La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Un exemple: parcours de la tour sur un échiquier écorné

Déplacements possibles de la tour:



La tour peut-elle visiter toutes les cases une seule fois ?
C'est encore un problème de chemin hamiltonien.

Mais la réponse est non !

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

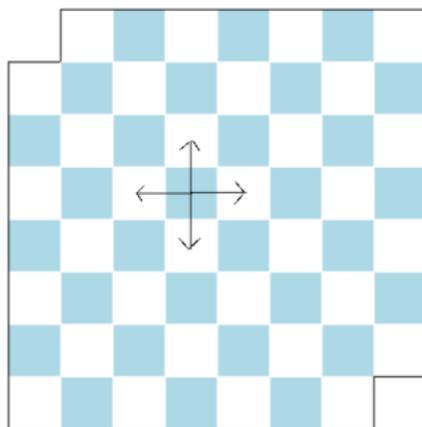
La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Un exemple: parcours de la tour sur un échiquier écorné

Déplacements possibles de la tour:



La tour peut-elle visiter toutes les cases une seule fois ?
C'est encore un problème de chemin hamiltonien.

Mais la réponse est non !

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

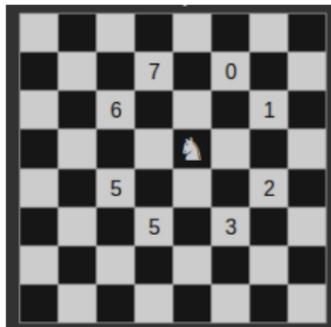
La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

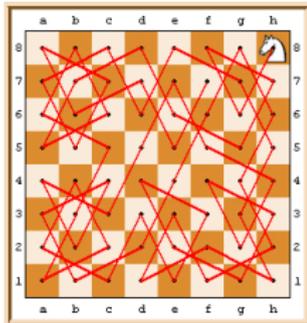
Un autre exemple: le parcours du cavalier

Déplacements possibles du cavalier:



Le cavalier peut-il visiter toutes les cases une seule fois ?
C'est encore un problème de chemin hamiltonien.

La solution de al Adli ar Rumi (840)



La solution d'Euler (1759)

37	62	43	56	35	60	41	50
44	55	36	61	42	49	34	59
63	38	53	46	57	40	51	48
54	45	64	39	52	47	58	33
1	26	15	20	7	32	13	22
16	19	8	25	14	21	6	31
27	2	17	10	29	4	23	12
18	9	28	3	24	11	30	5

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

La triste vérité

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Déclaration

On ne connaît aucune méthode intelligente pour trouver un chemin ou un circuit hamiltonien dans un graphe.

“Intelligente” signifie: essentiellement meilleure que la force brutale.

En particulier, on ne sait pas s'il existe une solution “polynomiale”.

La triste vérité

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Déclaration

On ne connaît aucune méthode intelligente pour trouver un chemin ou un circuit hamiltonien dans un graphe.

“Intelligente” signifie: essentiellement meilleure que la force brutale.

En particulier, on ne sait pas s'il existe une solution “polynomiale”.

La triste vérité

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Déclaration

On ne connaît aucune méthode intelligente pour trouver un chemin ou un circuit hamiltonien dans un graphe.

“Intelligente” signifie: essentiellement meilleure que la force brutale.

En particulier, on ne sait pas s'il existe une solution “polynomiale”.

Plan

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

À la brute

Commençons par des exemples simples.

S'il y a trois villes, Paris, Lille et Toulouse par exemple, il faudrait essayer six parcours:

Paris-Lille-Toulouse	Toulouse-Lille-Paris
Paris-Toulouse-Lille	Lille-Toulouse-Paris
Lille-Paris-Toulouse	Toulouse-Paris-Lille

Si l'on a de la chance, on trouvera un bon parcours (un chemin hamiltonien) avant d'avoir tout essayé; mais dans le pire des cas, il faudra vraiment les tester tous les six.

Bien entendu, on pourrait éviter de tester Toulouse-Lille-Paris si le parcours en sens inverse Paris-Lille-Toulouse a échoué.

Ce genre de petites optimisations ne modifie pas essentiellement le temps de recherche, et nous n'en tiendrons pas compte.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

À la brute

Commençons par des exemples simples.

S'il y a trois villes, Paris, Lille et Toulouse par exemple, il faudrait essayer six parcours:

Paris-Lille-Toulouse Toulouse-Lille-Paris
Paris-Toulouse-Lille Lille-Toulouse-Paris
Lille-Paris-Toulouse Toulouse-Paris-Lille

Si l'on a de la chance, on trouvera un bon parcours (un chemin hamiltonien) avant d'avoir tout essayé; mais dans le pire des cas, il faudra vraiment les tester tous les six.

Bien entendu, on pourrait éviter de tester Toulouse-Lille-Paris si le parcours en sens inverse Paris-Lille-Toulouse a échoué.

Ce genre de petites optimisations ne modifie pas essentiellement le temps de recherche, et nous n'en tiendrons pas compte.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

À la brute

Commençons par des exemples simples.

S'il y a trois villes, Paris, Lille et Toulouse par exemple, il faudrait essayer six parcours:

Paris-Lille-Toulouse	Toulouse-Lille-Paris
Paris-Toulouse-Lille	Lille-Toulouse-Paris
Lille-Paris-Toulouse	Toulouse-Paris-Lille

Si l'on a de la chance, on trouvera un bon parcours (un chemin hamiltonien) avant d'avoir tout essayé; mais dans le pire des cas, il faudra vraiment les tester tous les six.

Bien entendu, on pourrait éviter de tester Toulouse-Lille-Paris si le parcours en sens inverse Paris-Lille-Toulouse a échoué.

Ce genre de petites optimisations ne modifie pas essentiellement le temps de recherche, et nous n'en tiendrons pas compte.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

À la brute

Commençons par des exemples simples.

S'il y a trois villes, Paris, Lille et Toulouse par exemple, il faudrait essayer six parcours:

Paris-Lille-Toulouse	Toulouse-Lille-Paris
Paris-Toulouse-Lille	Lille-Toulouse-Paris
Lille-Paris-Toulouse	Toulouse-Paris-Lille

Si l'on a de la chance, on trouvera un bon parcours (un chemin hamiltonien) avant d'avoir tout essayé; mais dans le pire des cas, il faudra vraiment les tester tous les six.

Bien entendu, on pourrait éviter de tester Toulouse-Lille-Paris si le parcours en sens inverse Paris-Lille-Toulouse a échoué.

Ce genre de petites optimisations ne modifie pas essentiellement le temps de recherche, et nous n'en tiendrons pas compte.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

À la brute

Commençons par des exemples simples.

S'il y a trois villes, Paris, Lille et Toulouse par exemple, il faudrait essayer six parcours:

Paris-Lille-Toulouse	Toulouse-Lille-Paris
Paris-Toulouse-Lille	Lille-Toulouse-Paris
Lille-Paris-Toulouse	Toulouse-Paris-Lille

Si l'on a de la chance, on trouvera un bon parcours (un chemin hamiltonien) avant d'avoir tout essayé; mais dans le pire des cas, il faudra vraiment les tester tous les six.

Bien entendu, on pourrait éviter de tester Toulouse-Lille-Paris si le parcours en sens inverse Paris-Lille-Toulouse a échoué.

Ce genre de petites optimisations ne modifie pas essentiellement le temps de recherche, et nous n'en tiendrons pas compte.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

À la brute

Commençons par des exemples simples.

S'il y a trois villes, Paris, Lille et Toulouse par exemple, il faudrait essayer six parcours:

Paris-Lille-Toulouse	Toulouse-Lille-Paris
Paris-Toulouse-Lille	Lille-Toulouse-Paris
Lille-Paris-Toulouse	Toulouse-Paris-Lille

Si l'on a de la chance, on trouvera un bon parcours (un chemin hamiltonien) avant d'avoir tout essayé; mais dans le pire des cas, il faudra vraiment les tester tous les six.

Bien entendu, on pourrait éviter de tester Toulouse-Lille-Paris si le parcours en sens inverse Paris-Lille-Toulouse a échoué.

Ce genre de petites optimisations ne modifie pas essentiellement le temps de recherche, et nous n'en tiendrons pas compte.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

À la brute, un peu plus gros

Supposons maintenant qu'il y a quatre villes, A,B,C,D (en mathématiques et en algorithmique, les noms sont souvent un peu bêtes ...). Voici les vingt-quatre parcours possibles:

ABCD	ABDC	ACBD	ACDB	ADBC	ADCB
BACD	BADC	BCAD	BCDA	BDAC	BDCA
CABD	CADB	CBAD	CBDA	CDAB	CDBA
DABC	DACB	DBAC	DBCA	DCAB	DCBA

En réfléchissant, on trouve que, pour n villes, il y a $1 \times 2 \times 3 \times \dots \times (n-1) \times n = n!$ parcours possibles.

Par exemple:

$1! = 1$	$2! = 2$	$3! = 6$
$4! = 24$	$5! = 120$	$6! = 720$
$7! = 5040$	$8! = 40320$	$9! = 362880$
$10! = 3628800$	$11! = 39916800$	$12! = 479001600$

Quand le nombre n de villes croît, le nombre $n!$ de parcours croît *très rapidement*. C'est la raison pour laquelle la recherche par "force brutale" est si inefficace.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

À la brute, un peu plus gros

Supposons maintenant qu'il y a quatre villes, A,B,C,D (en mathématiques et en algorithmique, les noms sont souvent un peu bêtes ...). Voici les vingt-quatre parcours possibles:

ABCD	ABDC	ACBD	ACDB	ADBC	ADCB
BACD	BADC	BCAD	BCDA	BDAC	BDCA
CABD	CADB	CBAD	CBDA	CDAB	CDBA
DABC	DACB	DBAC	DBCA	DCAB	DCBA

En réfléchissant, on trouve que, pour n villes, il y a $1 \times 2 \times 3 \times \dots \times (n-1) \times n = n!$ parcours possibles.

Par exemple:

$1! = 1$	$2! = 2$	$3! = 6$
$4! = 24$	$5! = 120$	$6! = 720$
$7! = 5040$	$8! = 40320$	$9! = 362880$
$10! = 3628800$	$11! = 39916800$	$12! = 479001600$

Quand le nombre n de villes croît, le nombre $n!$ de parcours croît *très rapidement*. C'est la raison pour laquelle la recherche par "force brutale" est si inefficace.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

À la brute, un peu plus gros

Supposons maintenant qu'il y a quatre villes, A,B,C,D (en mathématiques et en algorithmique, les noms sont souvent un peu bêtes ...). Voici les vingt-quatre parcours possibles:

ABCD	ABDC	ACBD	ACDB	ADBC	ADCB
BACD	BADC	BCAD	BCDA	BDAC	BDCA
CABD	CADB	CBAD	CBDA	CDAB	CDBA
DABC	DACB	DBAC	DBCA	DCAB	DCBA

En réfléchissant, on trouve que, pour n villes, il y a $1 \times 2 \times 3 \times \dots \times (n-1) \times n = n!$ parcours possibles.

Par exemple:

$1! = 1$	$2! = 2$	$3! = 6$
$4! = 24$	$5! = 120$	$6! = 720$
$7! = 5040$	$8! = 40320$	$9! = 362880$
$10! = 3628800$	$11! = 39916800$	$12! = 479001600$

Quand le nombre n de villes croît, le nombre $n!$ de parcours croît *très rapidement*. C'est la raison pour laquelle la recherche par "force brutale" est si inefficace.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

À la brute, un peu plus gros

Supposons maintenant qu'il y a quatre villes, A,B,C,D (en mathématiques et en algorithmique, les noms sont souvent un peu bêtes ...). Voici les vingt-quatre parcours possibles:

ABCD	ABDC	ACBD	ACDB	ADBC	ADCB
BACD	BADC	BCAD	BCDA	BDAC	BDCA
CABD	CADB	CBAD	CBDA	CDAB	CDBA
DABC	DACB	DBAC	DBCA	DCAB	DCBA

En réfléchissant, on trouve que, pour n villes, il y a $1 \times 2 \times 3 \times \dots \times (n - 1) \times n = n!$ parcours possibles.

Par exemple:

$1! = 1$	$2! = 2$	$3! = 6$
$4! = 24$	$5! = 120$	$6! = 720$
$7! = 5040$	$8! = 40320$	$9! = 362880$
$10! = 3628800$	$11! = 39916800$	$12! = 479001600$

Quand le nombre n de villes croît, le nombre $n!$ de parcours croît *très rapidement*. C'est la raison pour laquelle la recherche par "force brutale" est si inefficace.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

À la brute, un peu plus gros

Supposons maintenant qu'il y a quatre villes, A,B,C,D (en mathématiques et en algorithmique, les noms sont souvent un peu bêtes ...). Voici les vingt-quatre parcours possibles:

ABCD	ABDC	ACBD	ACDB	ADBC	ADCB
BACD	BADC	BCAD	BCDA	BDAC	BDCA
CABD	CADB	CBAD	CBDA	CDAB	CDBA
DABC	DACB	DBAC	DBCA	DCAB	DCBA

En réfléchissant, on trouve que, pour n villes, il y a $1 \times 2 \times 3 \times \dots \times (n-1) \times n = n!$ parcours possibles.

Par exemple:

$1! = 1$	$2! = 2$	$3! = 6$
$4! = 24$	$5! = 120$	$6! = 720$
$7! = 5040$	$8! = 40320$	$9! = 362880$
$10! = 3628800$	$11! = 39916800$	$12! = 479001600$

Quand le nombre n de villes croît, le nombre $n!$ de parcours croît *très rapidement*. C'est la raison pour laquelle la recherche par "force brutale" est si inefficace.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

De plus en plus gros

Voici un grand nombre, l'âge de l'univers (seize milliards d'années) compté en secondes:

$$16.10^9 \times 365 \times 24 \times 3600 \simeq 5,04576 \times 10^{17}.$$

Maintenant, la même chose comptée en “nanosecondes”, c'est-à-dire en milliardièmes de secondes; nous lui donnons un nom:

$$N = 5,05 \times 10^{26}.$$

À titre de comparaison:

$$27! \simeq 1,09 \times 10^{28} \simeq 20 \times N.$$

Supposons que l'on veuille tester les trajets possibles entre vingt-sept villes. Supposons que chaque trajet soit testé en une nanoseconde (on teste donc un milliard de trajets chaque seconde). **Le temps nécessaire serait de l'ordre de vingt fois l'âge de l'univers.**

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

De plus en plus gros

Voici un grand nombre, l'âge de l'univers (seize milliards d'années) compté en secondes:

$$16.10^9 \times 365 \times 24 \times 3600 \simeq 5,04576 \times 10^{17}.$$

Maintenant, la même chose comptée en “nanosecondes”, c'est-à-dire en milliardièmes de secondes; nous lui donnons un nom:

$$N = 5,05 \times 10^{26}.$$

À titre de comparaison:

$$27! \simeq 1,09 \times 10^{28} \simeq 20 \times N.$$

Supposons que l'on veuille tester les trajets possibles entre vingt-sept villes. Supposons que chaque trajet soit testé en une nanoseconde (on teste donc un milliard de trajets chaque seconde). **Le temps nécessaire serait de l'ordre de vingt fois l'âge de l'univers.**

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

De plus en plus gros

Voici un grand nombre, l'âge de l'univers (seize milliards d'années) compté en secondes:

$$16.10^9 \times 365 \times 24 \times 3600 \simeq 5,04576 \times 10^{17}.$$

Maintenant, la même chose comptée en “nanosecondes”, c'est-à-dire en milliardièmes de secondes; nous lui donnons un nom:

$$N = 5,05 \times 10^{26}.$$

À titre de comparaison:

$$27! \simeq 1,09 \times 10^{28} \simeq 20 \times N.$$

Supposons que l'on veuille tester les trajets possibles entre vingt-sept villes. Supposons que chaque trajet soit testé en une nanoseconde (on teste donc un milliard de trajets chaque seconde). **Le temps nécessaire serait de l'ordre de vingt fois l'âge de l'univers.**

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

De plus en plus gros

Voici un grand nombre, l'âge de l'univers (seize milliards d'années) compté en secondes:

$$16.10^9 \times 365 \times 24 \times 3600 \simeq 5,04576 \times 10^{17}.$$

Maintenant, la même chose comptée en “nanosecondes”, c'est-à-dire en milliardièmes de secondes; nous lui donnons un nom:

$$N = 5,05 \times 10^{26}.$$

À titre de comparaison:

$$27! \simeq 1,09 \times 10^{28} \simeq 20 \times N.$$

Supposons que l'on veuille tester les trajets possibles entre vingt-sept villes. Supposons que chaque trajet soit testé en une nanoseconde (on teste donc un milliard de trajets chaque seconde). **Le temps nécessaire serait de l'ordre de vingt fois l'âge de l'univers.**

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

De plus en plus gros

Voici un grand nombre, l'âge de l'univers (seize milliards d'années) compté en secondes:

$$16.10^9 \times 365 \times 24 \times 3600 \simeq 5,04576 \times 10^{17}.$$

Maintenant, la même chose comptée en “nanosecondes”, c'est-à-dire en milliardièmes de secondes; nous lui donnons un nom:

$$N = 5,05 \times 10^{26}.$$

À titre de comparaison:

$$27! \simeq 1,09 \times 10^{28} \simeq 20 \times N.$$

Supposons que l'on veuille tester les trajets possibles entre vingt-sept villes. Supposons que chaque trajet soit testé en une nanoseconde (on teste donc un milliard de trajets chaque seconde). **Le temps nécessaire serait de l'ordre de vingt fois l'âge de l'univers.**

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Les machines entrent en scène

Les chiffres n'ont pas été choisis au hasard. Un “microprocesseur” moderne peut effectuer environ dix opérations numériques en une nanoseconde (on parle de “dix gigaflops”).

On peut admettre qu'un programme d'ordinateur bien conçu arrive à tester un trajet de vingt-sept villes dans le même temps.

Comme on l'a vu, pour tester *tous* les trajets, il lui faudra vingt fois l'âge de l'univers.

Mais la technique progresse ! Les ordinateurs vont de plus en plus vite ! Notre problème sera bientôt résolu par la puissance des machines !

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Les machines entrent en scène

Les chiffres n'ont pas été choisis au hasard. Un “microprocesseur” moderne peut effectuer environ dix opérations numériques en une nanoseconde (on parle de “dix gigaflops”).

On peut admettre qu'un programme d'ordinateur bien conçu arrive à tester un trajet de vingt-sept villes dans le même temps.

Comme on l'a vu, pour tester *tous* les trajets, il lui faudra vingt fois l'âge de l'univers.

Mais la technique progresse ! Les ordinateurs vont de plus en plus vite ! Notre problème sera bientôt résolu par la puissance des machines !

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Les machines entrent en scène

Les chiffres n'ont pas été choisis au hasard. Un “microprocesseur” moderne peut effectuer environ dix opérations numériques en une nanoseconde (on parle de “dix gigaflops”).

On peut admettre qu'un programme d'ordinateur bien conçu arrive à tester un trajet de vingt-sept villes dans le même temps.

Comme on l'a vu, pour tester *tous* les trajets, il lui faudra vingt fois l'âge de l'univers.

Mais la technique progresse ! Les ordinateurs vont de plus en plus vite ! Notre problème sera bientôt résolu par la puissance des machines !

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Les machines entrent en scène

Les chiffres n'ont pas été choisis au hasard. Un “microprocesseur” moderne peut effectuer environ dix opérations numériques en une nanoseconde (on parle de “dix gigaflops”).

On peut admettre qu'un programme d'ordinateur bien conçu arrive à tester un trajet de vingt-sept villes dans le même temps.

Comme on l'a vu, pour tester *tous* les trajets, il lui faudra vingt fois l'âge de l'univers.

Mais la technique progresse ! Les ordinateurs vont de plus en plus vite ! Notre problème sera bientôt résolu par la puissance des machines !

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

De plus en plus vite

Une loi de sociologie industrielle, la “loi de Moore”, dit que la puissance des machines double tous les dix-huit mois. C'est une loi empirique, mais elle semble proche de la réalité des trente dernières années.

Sur cette base, en un siècle les ordinateurs iraient 10^{20} fois plus vite.

Dans un siècle, le problème des vingt-sept villes pourra être résolu en un dixième de seconde.

Mais il faudra plusieurs fois l'âge de l'univers pour traiter quarante villes.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

De plus en plus vite

Une loi de sociologie industrielle, la “loi de Moore”, dit que la puissance des machines double tous les dix-huit mois. C’est une loi empirique, mais elle semble proche de la réalité des trente dernières années.

Sur cette base, en un siècle les ordinateurs iraient 10^{20} fois plus vite.

Dans un siècle, le problème des vingt-sept villes pourra être résolu en un dixième de seconde.

Mais il faudra plusieurs fois l’âge de l’univers pour traiter quarante villes.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

De plus en plus vite

Une loi de sociologie industrielle, la “loi de Moore”, dit que la puissance des machines double tous les dix-huit mois. C’est une loi empirique, mais elle semble proche de la réalité des trente dernières années.

Sur cette base, en un siècle les ordinateurs iraient 10^{20} fois plus vite.

Dans un siècle, le problème des vingt-sept villes pourra être résolu en un dixième de seconde.

Mais il faudra plusieurs fois l’âge de l’univers pour traiter quarante villes.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

De plus en plus vite

Une loi de sociologie industrielle, la “loi de Moore”, dit que la puissance des machines double tous les dix-huit mois. C'est une loi empirique, mais elle semble proche de la réalité des trente dernières années.

Sur cette base, en un siècle les ordinateurs iraient 10^{20} fois plus vite.

Dans un siècle, le problème des vingt-sept villes pourra être résolu en un dixième de seconde.

Mais il faudra plusieurs fois l'âge de l'univers pour traiter quarante villes.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

À propos de la soi-disant “loi de Moore”

Celle qui est énoncée ci-dessus (“deux fois plus vite tous les dix-huit mois”) n’a pas réellement été formulée telle quelle par Gordon E. Moore (l’un des fondateurs de Intel). Pour les détails, voir Wikipedia.

La pseudo-loi de Moore a plutôt bien décrit la réalité pendant quelques décennies, mais elle est maintenant à bout de souffle en ce qui concerne les performances. (Elle aurait tendance à se reporter sur les *prix* !)

Elle pourrait être relancée par le passage de l’ère de la micro-électronique (10^{-6} m) à celle des nano-technologies (10^{-9} m).

Mais la vraie révolution espérée (redoutée ?) viendrait de l’informatique quantique.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

À propos de la soi-disant “loi de Moore”

Celle qui est énoncée ci-dessus (“deux fois plus vite tous les dix-huit mois”) n’a pas réellement été formulée telle quelle par Gordon E. Moore (l’un des fondateurs de Intel). Pour les détails, voir Wikipedia.

La pseudo-loi de Moore a plutôt bien décrit la réalité pendant quelques décennies, mais elle est maintenant à bout de souffle en ce qui concerne les performances. (Elle aurait tendance à se reporter sur les *prix* !)

Elle pourrait être relancée par le passage de l’ère de la micro-électronique (10^{-6} m) à celle des nano-technologies (10^{-9} m).

Mais la vraie révolution espérée (redoutée ?) viendrait de l’informatique quantique.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

À propos de la soi-disant “loi de Moore”

Celle qui est énoncée ci-dessus (“deux fois plus vite tous les dix-huit mois”) n’a pas réellement été formulée telle quelle par Gordon E. Moore (l’un des fondateurs de Intel). Pour les détails, voir Wikipedia.

La pseudo-loi de Moore a plutôt bien décrit la réalité pendant quelques décennies, mais elle est maintenant à bout de souffle en ce qui concerne les performances. (Elle aurait tendance à se reporter sur les *prix* !)

Elle pourrait être relancée par le passage de l’ère de la micro-électronique (10^{-6} m) à celle des nano-technologies (10^{-9} m).

Mais la vraie révolution espérée (redoutée ?) viendrait de l’informatique quantique.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

À propos de la soi-disant “loi de Moore”

Celle qui est énoncée ci-dessus (“deux fois plus vite tous les dix-huit mois”) n’a pas réellement été formulée telle quelle par Gordon E. Moore (l’un des fondateurs de Intel). Pour les détails, voir Wikipedia.

La pseudo-loi de Moore a plutôt bien décrit la réalité pendant quelques décennies, mais elle est maintenant à bout de souffle en ce qui concerne les performances. (Elle aurait tendance à se reporter sur les *prix* !)

Elle pourrait être relancée par le passage de l’ère de la micro-électronique (10^{-6} m) à celle des nano-technologies (10^{-9} m).

Mais la vraie révolution espérée (redoutée ?) viendrait de l’informatique quantique.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction



P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction



Avec le temps, rien ne s'arrange

Pour de plus grands nombres, c'est pire. Quand on en sera à être capable de traiter cent villes en un temps raisonnable, le progrès technique d'un siècle permettra de passer de cent à cent-dix.

Les mauvais algorithmes ne profitent pas du progrès technique.

ATTENTION ! On parle ici du progrès technique "normal". Une véritable révolution, instaurant des principes totalement nouveaux (comme l'advenue de l'ordinateur "quantique") changerait la donne.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Avec le temps, rien ne s'arrange

Pour de plus grands nombres, c'est pire. Quand on en sera à être capable de traiter cent villes en un temps raisonnable, le progrès technique d'un siècle permettra de passer de cent à cent-dix.

Les mauvais algorithmes ne profitent pas du progrès technique.

ATTENTION ! On parle ici du progrès technique "normal". Une véritable révolution, instaurant des principes totalement nouveaux (comme l'advenue de l'ordinateur "quantique") changerait la donne.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Avec le temps, rien ne s'arrange

Pour de plus grands nombres, c'est pire. Quand on en sera à être capable de traiter cent villes en un temps raisonnable, le progrès technique d'un siècle permettra de passer de cent à cent-dix.

Les mauvais algorithmes ne profitent pas du progrès technique.

ATTENTION ! On parle ici du progrès technique "normal". Une véritable révolution, instaurant des principes totalement nouveaux (comme l'advenue de l'ordinateur "quantique") changerait la donne.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Un exercice

Démontrer la formule suivante:

$$\log_{10} n! \simeq n \log_{10} n.$$

Indication pour la preuve:

$$\ln n! = \ln 1 + \dots + \ln n \simeq \int_0^n \ln t \, dt \simeq n \ln n.$$

Interprétation de la formule: si $n \simeq 10^N$, alors $n!$ s'écrit avec à peu près $N10^N$ chiffres décimaux. Par exemple:
100! s'écrit avec à peu près deux cents chiffres décimaux.
1000! s'écrit avec à peu près trois mille chiffres décimaux.
1000000! s'écrit avec à peu près six millions de chiffres décimaux. Etc ...

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Un exercice

Démontrer la formule suivante:

$$\log_{10} n! \simeq n \log_{10} n.$$

Indication pour la preuve:

$$\ln n! = \ln 1 + \dots + \ln n \simeq \int_0^n \ln t \, dt \simeq n \ln n.$$

Interprétation de la formule: si $n \simeq 10^N$, alors $n!$ s'écrit avec à peu près $N10^N$ chiffres décimaux. Par exemple:
100! s'écrit avec à peu près deux cents chiffres décimaux.
1000! s'écrit avec à peu près trois mille chiffres décimaux.
1000000! s'écrit avec à peu près six millions de chiffres décimaux. Etc ...

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Un exercice

Démontrer la formule suivante:

$$\log_{10} n! \simeq n \log_{10} n.$$

Indication pour la preuve:

$$\ln n! = \ln 1 + \dots + \ln n \simeq \int_0^n \ln t \, dt \simeq n \ln n.$$

Interprétation de la formule: si $n \simeq 10^N$, alors $n!$ s'écrit avec à peu près $N10^N$ chiffres décimaux. Par exemple:

100! s'écrit avec à peu près deux cents chiffres décimaux.

1000! s'écrit avec à peu près trois mille chiffres décimaux.

1000000! s'écrit avec à peu près six millions de chiffres décimaux. Etc ...

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Un exercice

Démontrer la formule suivante:

$$\log_{10} n! \simeq n \log_{10} n.$$

Indication pour la preuve:

$$\ln n! = \ln 1 + \dots + \ln n \simeq \int_0^n \ln t \, dt \simeq n \ln n.$$

Interprétation de la formule: si $n \simeq 10^N$, alors $n!$ s'écrit avec à peu près $N10^N$ chiffres décimaux. Par exemple:

100! s'écrit avec à peu près deux cents chiffres décimaux.

1000! s'écrit avec à peu près trois mille chiffres décimaux.

1000000! s'écrit avec à peu près six millions de chiffres décimaux. Etc ...

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Un exercice

P = NP ?

Jacques Sauloy

Démontrer la formule suivante:

$$\log_{10} n! \simeq n \log_{10} n.$$

Indication pour la preuve:

$$\ln n! = \ln 1 + \dots + \ln n \simeq \int_0^n \ln t \, dt \simeq n \ln n.$$

Interprétation de la formule: si $n \simeq 10^N$, alors $n!$ s'écrit avec à peu près $N10^N$ chiffres décimaux. Par exemple:

100! s'écrit avec à peu près deux cents chiffres décimaux.

1000! s'écrit avec à peu près trois mille chiffres décimaux.

1000000! s'écrit avec à peu près six millions de chiffres décimaux. Etc ...

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Un exercice

Démontrer la formule suivante:

$$\log_{10} n! \simeq n \log_{10} n.$$

Indication pour la preuve:

$$\ln n! = \ln 1 + \dots + \ln n \simeq \int_0^n \ln t \, dt \simeq n \ln n.$$

Interprétation de la formule: si $n \simeq 10^N$, alors $n!$ s'écrit avec à peu près $N10^N$ chiffres décimaux. Par exemple:

100! s'écrit avec à peu près deux cents chiffres décimaux.

1000! s'écrit avec à peu près trois mille chiffres décimaux.

1000000! s'écrit avec à peu près six millions de chiffres décimaux. Etc ...

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Un exercice

Démontrer la formule suivante:

$$\log_{10} n! \simeq n \log_{10} n.$$

Indication pour la preuve:

$$\ln n! = \ln 1 + \dots + \ln n \simeq \int_0^n \ln t \, dt \simeq n \ln n.$$

Interprétation de la formule: si $n \simeq 10^N$, alors $n!$ s'écrit avec à peu près $N10^N$ chiffres décimaux. Par exemple:

100! s'écrit avec à peu près deux cents chiffres décimaux.

1000! s'écrit avec à peu près trois mille chiffres décimaux.

1000000! s'écrit avec à peu près six millions de chiffres décimaux. Etc ...

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Un exercice

P = NP ?

Jacques Sauloy

Démontrer la formule suivante:

$$\log_{10} n! \simeq n \log_{10} n.$$

Indication pour la preuve:

$$\ln n! = \ln 1 + \dots + \ln n \simeq \int_0^n \ln t \, dt \simeq n \ln n.$$

Interprétation de la formule: si $n \simeq 10^N$, alors $n!$ s'écrit avec à peu près $N10^N$ chiffres décimaux. Par exemple:

100! s'écrit avec à peu près deux cents chiffres décimaux.

1000! s'écrit avec à peu près trois mille chiffres décimaux.

1000000! s'écrit avec à peu près six millions de chiffres décimaux. Etc ...

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Plan

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Cramer et Gauß

En météorologie, dans les centrales nucléaires, dans l'étude de l'écoulement de l'air autour des avions, dans l'extraction et le stockage de gaz naturel . . . , on résout de très gros "systèmes d'équations".

Ces problèmes ont certains points communs avec le problème du circuit hamiltonien:

- ▶ Si l'on a une solution candidate, il est facile de vérifier si elle est correcte ou non.
- ▶ Il existe une méthode de résolution "à la brute" qui est très coûteuse (méthode de Cramer). En fait son coût est du même ordre que celui de la recherche de circuit hamiltonien: pour résoudre n équations à n inconnues, il faut environ $n!$ opérations.

La différence essentielle est qu'il existe aussi un bon algorithme, qui demande environ $n^3 = n \times n \times n$ opérations (algorithme du pivot de Gauß).

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Cramer et Gauß

En météorologie, dans les centrales nucléaires, dans l'étude de l'écoulement de l'air autour des avions, dans l'extraction et le stockage de gaz naturel . . . , on résout de très gros "systèmes d'équations".

Ces problèmes ont certains points communs avec le problème du circuit hamiltonien:

- ▶ Si l'on a une solution candidate, il est facile de vérifier si elle est correcte ou non.
- ▶ Il existe une méthode de résolution "à la brute" qui est très coûteuse (méthode de Cramer). En fait son coût est du même ordre que celui de la recherche de circuit hamiltonien: pour résoudre n équations à n inconnues, il faut environ $n!$ opérations.

La différence essentielle est qu'il existe aussi un bon algorithme, qui demande environ $n^3 = n \times n \times n$ opérations (algorithme du pivot de Gauß).

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Cramer et Gauß

En météorologie, dans les centrales nucléaires, dans l'étude de l'écoulement de l'air autour des avions, dans l'extraction et le stockage de gaz naturel . . . , on résout de très gros "systèmes d'équations".

Ces problèmes ont certains points communs avec le problème du circuit hamiltonien:

- ▶ Si l'on a une solution candidate, il est facile de vérifier si elle est correcte ou non.
- ▶ Il existe une méthode de résolution "à la brute" qui est très coûteuse (méthode de Cramer). En fait son coût est du même ordre que celui de la recherche de circuit hamiltonien: pour résoudre n équations à n inconnues, il faut environ $n!$ opérations.

La différence essentielle est qu'il existe aussi un bon algorithme, qui demande environ $n^3 = n \times n \times n$ opérations (algorithme du pivot de Gauß).

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Cramer et Gauß

En météorologie, dans les centrales nucléaires, dans l'étude de l'écoulement de l'air autour des avions, dans l'extraction et le stockage de gaz naturel . . . , on résout de très gros "systèmes d'équations".

Ces problèmes ont certains points communs avec le problème du circuit hamiltonien:

- ▶ Si l'on a une solution candidate, il est facile de vérifier si elle est correcte ou non.
- ▶ Il existe une méthode de résolution "à la brute" qui est très coûteuse (méthode de Cramer). En fait son coût est du même ordre que celui de la recherche de circuit hamiltonien: pour résoudre n équations à n inconnues, il faut environ $n!$ opérations.

La différence essentielle est qu'il existe aussi un bon algorithme, qui demande environ $n^3 = n \times n \times n$ opérations (algorithme du pivot de Gauß).

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Cramer et Gauß

En météorologie, dans les centrales nucléaires, dans l'étude de l'écoulement de l'air autour des avions, dans l'extraction et le stockage de gaz naturel . . . , on résout de très gros "systèmes d'équations".

Ces problèmes ont certains points communs avec le problème du circuit hamiltonien:

- ▶ Si l'on a une solution candidate, il est facile de vérifier si elle est correcte ou non.
- ▶ Il existe une méthode de résolution "à la brute" qui est très coûteuse (méthode de Cramer). En fait son coût est du même ordre que celui de la recherche de circuit hamiltonien: pour résoudre n équations à n inconnues, il faut environ $n!$ opérations.

La différence essentielle est qu'il existe aussi un bon algorithme, qui demande environ $n^3 = n \times n \times n$ opérations (algorithme du pivot de Gauß).

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction



Et c'est bien un bon algorithme ?

Selon la loi de Moore, avec la méthode à la brute, en un siècle on peut passer de cent à cent-dix équations tout en conservant un temps de calcul raisonnable.

Avec la méthode de Gauß, il faut huit mois pour passer de cent à cent-dix.

En un siècle on passe de cent à quatre-cents cinquante millions.

Les bons algorithmes profitent mieux du progrès technique.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Et c'est bien un bon algorithme ?

Selon la loi de Moore, avec la méthode à la brute, en un siècle on peut passer de cent à cent-dix équations tout en conservant un temps de calcul raisonnable.

Avec la méthode de Gauß, il faut huit mois pour passer de cent à cent-dix.

En un siècle on passe de cent à quatre-cents cinquante millions.

Les bons algorithmes profitent mieux du progrès technique.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Et c'est bien un bon algorithme ?

Selon la loi de Moore, avec la méthode à la brute, en un siècle on peut passer de cent à cent-dix équations tout en conservant un temps de calcul raisonnable.

Avec la méthode de Gauß, il faut huit mois pour passer de cent à cent-dix.

En un siècle on passe de cent à quatre-cents cinquante millions.

Les bons algorithmes profitent mieux du progrès technique.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Et c'est bien un bon algorithme ?

Selon la loi de Moore, avec la méthode à la brute, en un siècle on peut passer de cent à cent-dix équations tout en conservant un temps de calcul raisonnable.

Avec la méthode de Gauß, il faut huit mois pour passer de cent à cent-dix.

En un siècle on passe de cent à quatre-cents cinquante millions.

Les bons algorithmes profitent mieux du progrès technique.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Plan

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Peut-on bien vivre ?

Dans un certain nombre d'endroits de ce monde bureaucratique, les décisions dépendent de systèmes de règles compliquées. Mais il y a aussi d'autres genres d'endroits où c'est le cas: gestion des crises dans une centrale nucléaire, ou des situations exceptionnelles dans un avion ou une fusée par exemple.

Quand on écrit un système de règles, une question qui se pose (ou qui devrait se poser !) est la suivante: est-il possible de satisfaire toutes ces règles ?

Mon gourou m'a dit: pour bien vivre, il faut que tu satisfasses à *toutes* les conditions suivantes:

1. Tu dois avoir du travail ou pas d'enfants.
2. Tu dois avoir des enfants ou des amis.
3. Tu dois avoir pas d'enfants ou une maison.
4. Tu dois avoir pas d'amis ou des enfants.

Attention ! En mathématiques, le "ou" est *inclusif*. La deuxième règle autorise à avoir des amis *et* des enfants.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Peut-on bien vivre ?

Dans un certain nombre d'endroits de ce monde bureaucratique, les décisions dépendent de systèmes de règles compliquées. Mais il y a aussi d'autres genres d'endroits où c'est le cas: gestion des crises dans une centrale nucléaire, ou des situations exceptionnelles dans un avion ou une fusée par exemple.

Quand on écrit un système de règles, une question qui se pose (ou qui devrait se poser !) est la suivante: est-il possible de satisfaire toutes ces règles ?

Mon gourou m'a dit: pour bien vivre, il faut que tu satisfasses à *toutes* les conditions suivantes:

1. Tu dois avoir du travail ou pas d'enfants.
2. Tu dois avoir des enfants ou des amis.
3. Tu dois avoir pas d'enfants ou une maison.
4. Tu dois avoir pas d'amis ou des enfants.

Attention ! En mathématiques, le "ou" est *inclusif*. La deuxième règle autorise à avoir des amis *et* des enfants.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Peut-on bien vivre ?

Dans un certain nombre d'endroits de ce monde bureaucratique, les décisions dépendent de systèmes de règles compliquées. Mais il y a aussi d'autres genres d'endroits où c'est le cas: gestion des crises dans une centrale nucléaire, ou des situations exceptionnelles dans un avion ou une fusée par exemple.

Quand on écrit un système de règles, une question qui se pose (ou qui devrait se poser !) est la suivante: est-il possible de satisfaire toutes ces règles ?

Mon gourou m'a dit: pour bien vivre, il faut que tu satisfasses à *toutes* les conditions suivantes:

1. Tu dois avoir du travail ou pas d'enfants.
2. Tu dois avoir des enfants ou des amis.
3. Tu dois avoir pas d'enfants ou une maison.
4. Tu dois avoir pas d'amis ou des enfants.

Attention ! En mathématiques, le "ou" est *inclusif*. La deuxième règle autorise à avoir des amis *et* des enfants.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Peut-on bien vivre ?

Dans un certain nombre d'endroits de ce monde bureaucratique, les décisions dépendent de systèmes de règles compliquées. Mais il y aussi d'autres genres d'endroits où c'est le cas: gestion des crises dans une centrale nucléaire, ou des situations exceptionnelles dans un avion ou une fusée par exemple.

Quand on écrit un système de règles, une question qui se pose (ou qui devrait se poser !) est la suivante: est-il possible de satisfaire toutes ces règles ?

Mon gourou m'a dit: pour bien vivre, il faut que tu satisfasses à *toutes* les conditions suivantes:

1. Tu dois avoir du travail ou pas d'enfants.
2. Tu dois avoir des enfants ou des amis.
3. Tu dois avoir pas d'enfants ou une maison.
4. Tu dois avoir pas d'amis ou des enfants.

Attention ! En mathématiques, le "ou" est *inclusif*. La deuxième règle autorise à avoir des amis *et* des enfants.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Peut-on bien vivre ?

Dans un certain nombre d'endroits de ce monde bureaucratique, les décisions dépendent de systèmes de règles compliquées. Mais il y a aussi d'autres genres d'endroits où c'est le cas: gestion des crises dans une centrale nucléaire, ou des situations exceptionnelles dans un avion ou une fusée par exemple.

Quand on écrit un système de règles, une question qui se pose (ou qui devrait se poser !) est la suivante: est-il possible de satisfaire toutes ces règles ?

Mon gourou m'a dit: pour bien vivre, il faut que tu satisfasses à *toutes* les conditions suivantes:

1. Tu dois avoir du travail ou pas d'enfants.
2. Tu dois avoir des enfants ou des amis.
3. Tu dois avoir pas d'enfants ou une maison.
4. Tu dois avoir pas d'amis ou des enfants.

Attention ! En mathématiques, le "ou" est *inclusif*. La deuxième règle autorise à avoir des amis *et* des enfants.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Peut-on bien vivre ?

Dans un certain nombre d'endroits de ce monde bureaucratique, les décisions dépendent de systèmes de règles compliquées. Mais il y aussi d'autres genres d'endroits où c'est le cas: gestion des crises dans une centrale nucléaire, ou des situations exceptionnelles dans un avion ou une fusée par exemple.

Quand on écrit un système de règles, une question qui se pose (ou qui devrait se poser !) est la suivante: est-il possible de satisfaire toutes ces règles ?

Mon gourou m'a dit: pour bien vivre, il faut que tu satisfasses à *toutes* les conditions suivantes:

1. Tu dois avoir du travail ou pas d'enfants.
2. Tu dois avoir des enfants ou des amis.
3. Tu dois avoir pas d'enfants ou une maison.
4. Tu dois avoir pas d'amis ou des enfants.

Attention ! En mathématiques, le "ou" est *inclusif*. La deuxième règle autorise à avoir des amis *et* des enfants.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Peut-on bien vivre ?

Dans un certain nombre d'endroits de ce monde bureaucratique, les décisions dépendent de systèmes de règles compliquées. Mais il y a aussi d'autres genres d'endroits où c'est le cas: gestion des crises dans une centrale nucléaire, ou des situations exceptionnelles dans un avion ou une fusée par exemple.

Quand on écrit un système de règles, une question qui se pose (ou qui devrait se poser !) est la suivante: est-il possible de satisfaire toutes ces règles ?

Mon gourou m'a dit: pour bien vivre, il faut que tu satisfasses à *toutes* les conditions suivantes:

1. Tu dois avoir du travail ou pas d'enfants.
2. Tu dois avoir des enfants ou des amis.
3. Tu dois avoir pas d'enfants ou une maison.
4. Tu dois avoir pas d'amis ou des enfants.

Attention ! En mathématiques, le "ou" est *inclusif*. La deuxième règle autorise à avoir des amis *et* des enfants.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Peut-on bien vivre ?

Dans un certain nombre d'endroits de ce monde bureaucratique, les décisions dépendent de systèmes de règles compliquées. Mais il y a aussi d'autres genres d'endroits où c'est le cas: gestion des crises dans une centrale nucléaire, ou des situations exceptionnelles dans un avion ou une fusée par exemple.

Quand on écrit un système de règles, une question qui se pose (ou qui devrait se poser !) est la suivante: est-il possible de satisfaire toutes ces règles ?

Mon gourou m'a dit: pour bien vivre, il faut que tu satisfasses à *toutes* les conditions suivantes:

1. Tu dois avoir du travail ou pas d'enfants.
2. Tu dois avoir des enfants ou des amis.
3. Tu dois avoir pas d'enfants ou une maison.
4. Tu dois avoir pas d'amis ou des enfants.

Attention ! En mathématiques, le "ou" est *inclusif*. La deuxième règle autorise à avoir des amis *et* des enfants.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Peut-on bien vivre ?

P = NP ?

Jacques Sauloy

Mon gourou m'a dit: pour bien vivre, il faut que tu satisfasses à *toutes* les conditions suivantes:

1. Tu dois avoir du travail ou pas d'enfants.
2. Tu dois avoir des enfants ou des amis.
3. Tu dois avoir pas d'enfants ou une maison.
4. Tu dois avoir pas d'amis ou des enfants.

Est-ce possible ???

Trop facile ! Il me suffit d'avoir des enfants et une maison et des amis et du travail.

Ou alors: des enfants et une maison et du travail et pas d'amis (c'est moins gai, mais ça marche aussi).

En fait, il n'y a aucune autre solution.

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Peut-on bien vivre ?

P = NP ?

Jacques Sauloy

Mon gourou m'a dit: pour bien vivre, il faut que tu satisfasses à *toutes* les conditions suivantes:

1. Tu dois avoir du travail ou pas d'enfants.
2. Tu dois avoir des enfants ou des amis.
3. Tu dois avoir pas d'enfants ou une maison.
4. Tu dois avoir pas d'amis ou des enfants.

Est-ce possible ???

Trop facile ! Il me suffit d'avoir des enfants et une maison et des amis et du travail.

Ou alors: des enfants et une maison et du travail et pas d'amis (c'est moins gai, mais ça marche aussi).

En fait, il n'y a aucune autre solution.

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Peut-on bien vivre ?

P = NP ?

Jacques Sauloy

Mon gourou m'a dit: pour bien vivre, il faut que tu satisfasses à *toutes* les conditions suivantes:

1. Tu dois avoir du travail ou pas d'enfants.
2. Tu dois avoir des enfants ou des amis.
3. Tu dois avoir pas d'enfants ou une maison.
4. Tu dois avoir pas d'amis ou des enfants.

Est-ce possible ???

Trop facile ! Il me suffit d'avoir des enfants et une maison et des amis et du travail.

Ou alors: des enfants et une maison et du travail et pas d'amis (c'est moins gai, mais ça marche aussi).

En fait, il n'y a aucune autre solution.

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Peut-on bien vivre ?

P = NP ?

Jacques Sauloy

Mon gourou m'a dit: pour bien vivre, il faut que tu satisfasses à *toutes* les conditions suivantes:

1. Tu dois avoir du travail ou pas d'enfants.
2. Tu dois avoir des enfants ou des amis.
3. Tu dois avoir pas d'enfants ou une maison.
4. Tu dois avoir pas d'amis ou des enfants.

Est-ce possible ???

Trop facile ! Il me suffit d'avoir des enfants et une maison et des amis et du travail.

Ou alors: des enfants et une maison et du travail et pas d'amis (c'est moins gai, mais ça marche aussi).

En fait, il n'y a aucune autre solution.

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Peut-on bien vivre ?

P = NP ?

Jacques Sauloy

Mon gourou m'a dit: pour bien vivre, il faut que tu satisfasses à *toutes* les conditions suivantes:

1. Tu dois avoir du travail ou pas d'enfants.
2. Tu dois avoir des enfants ou des amis.
3. Tu dois avoir pas d'enfants ou une maison.
4. Tu dois avoir pas d'amis ou des enfants.

Est-ce possible ???

Trop facile ! Il me suffit d'avoir des enfants et une maison et des amis et du travail.

Ou alors: des enfants et une maison et du travail et pas d'amis (c'est moins gai, mais ça marche aussi).

En fait, il n'y a aucune autre solution.

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Peut-on bien vivre ?

Mon gourou m'a dit: tu as triché, c'était trop facile.
Dorénavant, pour bien vivre, il faut que tu satisfasses à *toutes* les conditions suivantes:

1. Tu dois avoir du travail ou pas d'enfants.
2. Tu dois avoir des enfants ou des amis.
3. Tu dois avoir pas d'enfants ou une maison.
4. Tu dois avoir pas d'amis ou des enfants.
5. Tu dois avoir pas de maison ou pas de travail.

Possible ? Pas possible ?

Il y a une méthode avec des lettres et des petits dessins:

E = avoir des enfants A = avoir des amis

M = avoir une maison T = avoir du travail

Première règle: $E \rightarrow T$ et $\bar{T} \rightarrow \bar{E}$.

Deuxième règle: $\bar{A} \rightarrow E$ et $\bar{E} \rightarrow A$.

etc

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Peut-on bien vivre ?

Mon gourou m'a dit: tu as triché, c'était trop facile.
Dorénavant, pour bien vivre, il faut que tu satisfasses à *toutes* les conditions suivantes:

1. Tu dois avoir du travail ou pas d'enfants.
2. Tu dois avoir des enfants ou des amis.
3. Tu dois avoir pas d'enfants ou une maison.
4. Tu dois avoir pas d'amis ou des enfants.
5. Tu dois avoir pas de maison ou pas de travail.

Possible ? Pas possible ?

Il y a une méthode avec des lettres et des petits dessins:

E = avoir des enfants A = avoir des amis

M = avoir une maison T = avoir du travail

Première règle: $E \rightarrow T$ et $\bar{T} \rightarrow \bar{E}$.

Deuxième règle: $\bar{A} \rightarrow E$ et $\bar{E} \rightarrow A$.

etc

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Peut-on bien vivre ?

Mon gourou m'a dit: tu as triché, c'était trop facile.
Dorénavant, pour bien vivre, il faut que tu satisfasses à *toutes* les conditions suivantes:

1. Tu dois avoir du travail ou pas d'enfants.
2. Tu dois avoir des enfants ou des amis.
3. Tu dois avoir pas d'enfants ou une maison.
4. Tu dois avoir pas d'amis ou des enfants.
5. Tu dois avoir pas de maison ou pas de travail.

Possible ? Pas possible ?

Il y a une méthode avec des lettres et des petits dessins:

E = avoir des enfants A = avoir des amis

M = avoir une maison T = avoir du travail

Première règle: $E \rightarrow T$ et $\bar{T} \rightarrow \bar{E}$.

Deuxième règle: $\bar{A} \rightarrow E$ et $\bar{E} \rightarrow A$.

etc

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Peut-on bien vivre ?

Mon gourou m'a dit: tu as triché, c'était trop facile.
Dorénavant, pour bien vivre, il faut que tu satisfasses à *toutes* les conditions suivantes:

1. Tu dois avoir du travail ou pas d'enfants.
2. Tu dois avoir des enfants ou des amis.
3. Tu dois avoir pas d'enfants ou une maison.
4. Tu dois avoir pas d'amis ou des enfants.
5. Tu dois avoir pas de maison ou pas de travail.

Possible ? Pas possible ?

Il y a une méthode avec des lettres et des petits dessins:

E = avoir des enfants A = avoir des amis

M = avoir une maison T = avoir du travail

Première règle: $E \rightarrow T$ et $\bar{T} \rightarrow \bar{E}$.

Deuxième règle: $\bar{A} \rightarrow E$ et $\bar{E} \rightarrow A$.

etc

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Peut-on bien vivre ?

Mon gourou m'a dit: tu as triché, c'était trop facile.
Dorénavant, pour bien vivre, il faut que tu satisfasses à *toutes* les conditions suivantes:

1. Tu dois avoir du travail ou pas d'enfants.
2. Tu dois avoir des enfants ou des amis.
3. Tu dois avoir pas d'enfants ou une maison.
4. Tu dois avoir pas d'amis ou des enfants.
5. Tu dois avoir pas de maison ou pas de travail.

Possible ? Pas possible ?

Il y a une méthode avec des lettres et des petits dessins:

E = avoir des enfants A = avoir des amis

M = avoir une maison T = avoir du travail

Première règle: $E \rightarrow T$ et $\bar{T} \rightarrow \bar{E}$.

Deuxième règle: $\bar{A} \rightarrow E$ et $\bar{E} \rightarrow A$.

etc

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Peut-on bien vivre ?

Mon gourou m'a dit: tu as triché, c'était trop facile.
Dorénavant, pour bien vivre, il faut que tu satisfasses à *toutes* les conditions suivantes:

1. Tu dois avoir du travail ou pas d'enfants.
2. Tu dois avoir des enfants ou des amis.
3. Tu dois avoir pas d'enfants ou une maison.
4. Tu dois avoir pas d'amis ou des enfants.
5. Tu dois avoir pas de maison ou pas de travail.

Possible ? Pas possible ?

Il y a une méthode avec des lettres et des petits dessins:

E = avoir des enfants A = avoir des amis

M = avoir une maison T = avoir du travail

Première règle: $E \rightarrow T$ et $\overline{T} \rightarrow \overline{E}$.

Deuxième règle: $\overline{A} \rightarrow E$ et $\overline{E} \rightarrow A$.

etc

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Peut-on bien vivre ?

Mon gourou m'a dit: tu as triché, c'était trop facile.
Dorénavant, pour bien vivre, il faut que tu satisfasses à *toutes* les conditions suivantes:

1. Tu dois avoir du travail ou pas d'enfants.
2. Tu dois avoir des enfants ou des amis.
3. Tu dois avoir pas d'enfants ou une maison.
4. Tu dois avoir pas d'amis ou des enfants.
5. Tu dois avoir pas de maison ou pas de travail.

Possible ? Pas possible ?

Il y a une méthode avec des lettres et des petits dessins:

E = avoir des enfants A = avoir des amis

M = avoir une maison T = avoir du travail

Première règle: $E \rightarrow T$ et $\overline{T} \rightarrow \overline{E}$.

Deuxième règle: $\overline{A} \rightarrow E$ et $\overline{E} \rightarrow A$.

etc

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

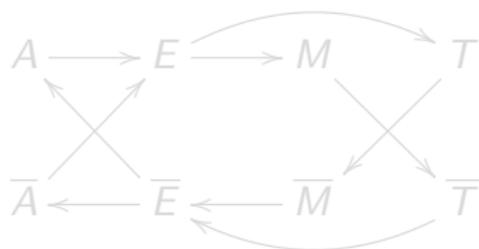
Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Satisfait ? Pas satisfait ?

1. Tu dois avoir du travail ou pas d'enfants.
2. Tu dois avoir des enfants ou des amis.
3. Tu dois avoir pas d'enfants ou une maison.
4. Tu dois avoir pas d'amis ou des enfants.
5. Tu dois avoir pas de maison ou pas de travail.

E = avoir des enfants A = avoir des amis
 M = avoir une maison T = avoir du travail



Mauvais cycle: de E à \bar{E} ;

puis de \bar{E} à E . **Impossible !**

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

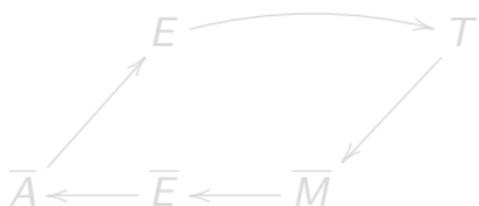
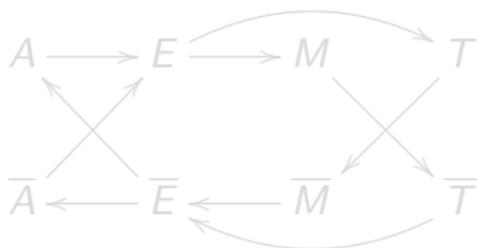
Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Satisfait ? Pas satisfait ?

1. Tu dois avoir du travail ou pas d'enfants.
2. Tu dois avoir des enfants ou des amis.
3. Tu dois avoir pas d'enfants ou une maison.
4. Tu dois avoir pas d'amis ou des enfants.
5. Tu dois avoir pas de maison ou pas de travail.

E = avoir des enfants A = avoir des amis
M = avoir une maison T = avoir du travail



Mauvais cycle: de E à \bar{E} ;

puis de \bar{E} à E. **Impossible !**

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

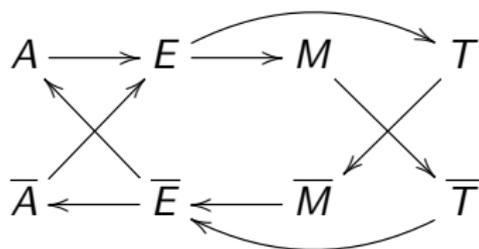
Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Satisfait ? Pas satisfait ?

1. Tu dois avoir du travail ou pas d'enfants.
2. Tu dois avoir des enfants ou des amis.
3. Tu dois avoir pas d'enfants ou une maison.
4. Tu dois avoir pas d'amis ou des enfants.
5. Tu dois avoir pas de maison ou pas de travail.

E = avoir des enfants A = avoir des amis
 M = avoir une maison T = avoir du travail



Mauvais cycle: de E à \bar{E} ;

puis de \bar{E} à E . **Impossible !**

$P = NP ?$

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

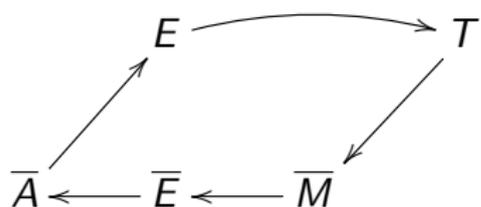
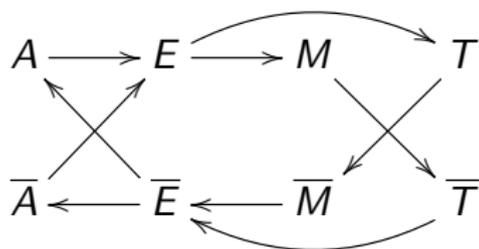
Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Satisfait ? Pas satisfait ?

1. Tu dois avoir du travail ou pas d'enfants.
2. Tu dois avoir des enfants ou des amis.
3. Tu dois avoir pas d'enfants ou une maison.
4. Tu dois avoir pas d'amis ou des enfants.
5. Tu dois avoir pas de maison ou pas de travail.

E = avoir des enfants A = avoir des amis
 M = avoir une maison T = avoir du travail



Mauvais cycle: de E à \bar{E} ;

puis de \bar{E} à E . **Impossible !**

$P = NP ?$

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

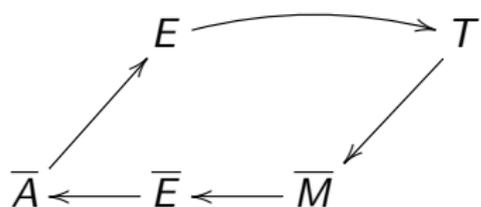
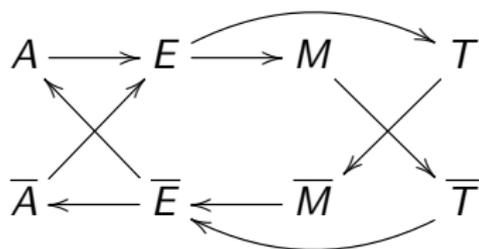
Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Satisfait ? Pas satisfait ?

1. Tu dois avoir du travail ou pas d'enfants.
2. Tu dois avoir des enfants ou des amis.
3. Tu dois avoir pas d'enfants ou une maison.
4. Tu dois avoir pas d'amis ou des enfants.
5. Tu dois avoir pas de maison ou pas de travail.

E = avoir des enfants A = avoir des amis
 M = avoir une maison T = avoir du travail



Mauvais cycle: de E à \bar{E} ;

puis de \bar{E} à E . **Impossible !**

$P = NP ?$

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

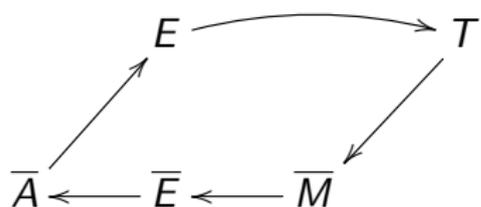
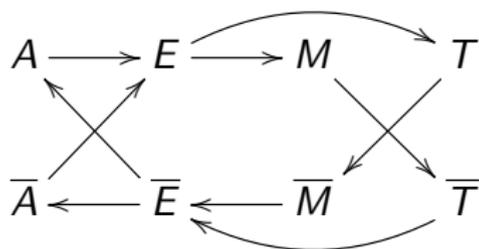
Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Satisfait ? Pas satisfait ?

1. Tu dois avoir du travail ou pas d'enfants.
2. Tu dois avoir des enfants ou des amis.
3. Tu dois avoir pas d'enfants ou une maison.
4. Tu dois avoir pas d'amis ou des enfants.
5. Tu dois avoir pas de maison ou pas de travail.

E = avoir des enfants A = avoir des amis
 M = avoir une maison T = avoir du travail



Mauvais cycle: de E à \bar{E} ;

puis de \bar{E} à E . **Impossible !**

$P = NP ?$

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

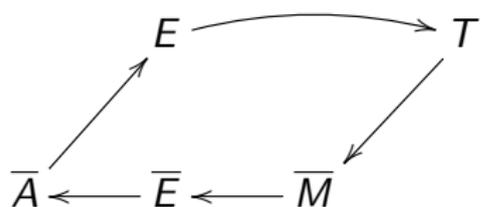
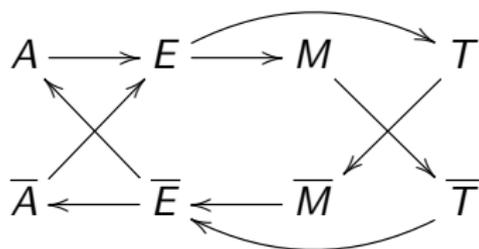
Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Satisfait ? Pas satisfait ?

1. Tu dois avoir du travail ou pas d'enfants.
2. Tu dois avoir des enfants ou des amis.
3. Tu dois avoir pas d'enfants ou une maison.
4. Tu dois avoir pas d'amis ou des enfants.
5. Tu dois avoir pas de maison ou pas de travail.

E = avoir des enfants A = avoir des amis
 M = avoir une maison T = avoir du travail



Mauvais cycle: de E à \bar{E} ;

puis de \bar{E} à E . **Impossible !**

$P = NP ?$

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

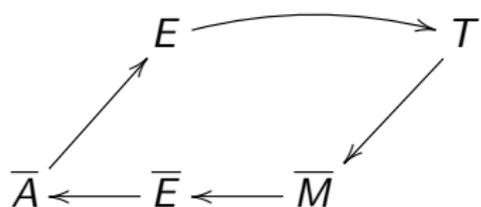
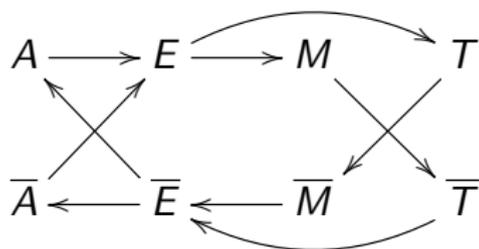
Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Satisfait ? Pas satisfait ?

1. Tu dois avoir du travail ou pas d'enfants.
2. Tu dois avoir des enfants ou des amis.
3. Tu dois avoir pas d'enfants ou une maison.
4. Tu dois avoir pas d'amis ou des enfants.
5. Tu dois avoir pas de maison ou pas de travail.

E = avoir des enfants A = avoir des amis
 M = avoir une maison T = avoir du travail



Mauvais cycle: de E à \bar{E} ;

puis de \bar{E} à E . **Impossible !**

$P = NP ?$

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Satisfait ? Pas satisfait ?

Le gourou a dit: tu triches encore, tu as un algorithme P.

Dorénavant, pour bien vivre, il faut que tu satisfasses à *toutes* les conditions suivantes; tu dois avoir:

1. du travail ou pas d'enfants ou une bonne santé.
2. des enfants ou des amis ou pas de télévision.
3. pas d'enfants ou une maison ou pas de dettes.
4. pas d'amis ou des enfants ou pas de dettes.
5. des dettes ou une bonne santé ou pas de maison.
6. pas de télévision ou pas de dettes.

Possible ? Impossible ?

On ne connaît *aucun* bon algorithme (meilleur que de chercher "à la brute") pour résoudre ce problème. Et la recherche "à la brute" est *vraiment* impraticable.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Satisfait ? Pas satisfait ?

Le gourou a dit: tu triches encore, tu as un algorithme P.
Dorénavant, pour bien vivre, il faut que tu satisfasses à *toutes* les conditions suivantes; tu dois avoir:

1. du travail ou pas d'enfants ou une bonne santé.
2. des enfants ou des amis ou pas de télévision.
3. pas d'enfants ou une maison ou pas de dettes.
4. pas d'amis ou des enfants ou pas de dettes.
5. des dettes ou une bonne santé ou pas de maison.
6. pas de télévision ou pas de dettes.

Possible ? Impossible ?

On ne connaît *aucun* bon algorithme (meilleur que de chercher "à la brute") pour résoudre ce problème. Et la recherche "à la brute" est *vraiment* impraticable.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Satisfait ? Pas satisfait ?

Le gourou a dit: tu triches encore, tu as un algorithme P.
Dorénavant, pour bien vivre, il faut que tu satisfasses à *toutes* les conditions suivantes; tu dois avoir:

1. du travail ou pas d'enfants ou une bonne santé.
2. des enfants ou des amis ou pas de télévision.
3. pas d'enfants ou une maison ou pas de dettes.
4. pas d'amis ou des enfants ou pas de dettes.
5. des dettes ou une bonne santé ou pas de maison.
6. pas de télévision ou pas de dettes.

Possible ? Impossible ?

On ne connaît *aucun* bon algorithme (meilleur que de chercher "à la brute") pour résoudre ce problème. Et la recherche "à la brute" est *vraiment* impraticable.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Satisfait ? Pas satisfait ?

Le gourou a dit: tu triches encore, tu as un algorithme P.
Dorénavant, pour bien vivre, il faut que tu satisfasses à *toutes* les conditions suivantes; tu dois avoir:

1. du travail ou pas d'enfants ou une bonne santé.
2. des enfants ou des amis ou pas de télévision.
3. pas d'enfants ou une maison ou pas de dettes.
4. pas d'amis ou des enfants ou pas de dettes.
5. des dettes ou une bonne santé ou pas de maison.
6. pas de télévision ou pas de dettes.

Possible ? Impossible ?

On ne connaît *aucun* bon algorithme (meilleur que de chercher "à la brute") pour résoudre ce problème. Et la recherche "à la brute" est *vraiment* impraticable.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Satisfait ? Pas satisfait ?

Le gourou a dit: tu triches encore, tu as un algorithme P.
Dorénavant, pour bien vivre, il faut que tu satisfasses à *toutes* les conditions suivantes; tu dois avoir:

1. du travail ou pas d'enfants ou une bonne santé.
2. des enfants ou des amis ou pas de télévision.
3. pas d'enfants ou une maison ou pas de dettes.
4. pas d'amis ou des enfants ou pas de dettes.
5. des dettes ou une bonne santé ou pas de maison.
6. pas de télévision ou pas de dettes.

Possible ? Impossible ?

On ne connaît *aucun* bon algorithme (meilleur que de chercher "à la brute") pour résoudre ce problème. Et la recherche "à la brute" est *vraiment* impraticable.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Satisfait ? Pas satisfait ?

Le gourou a dit: tu triches encore, tu as un algorithme P.
Dorénavant, pour bien vivre, il faut que tu satisfasses à *toutes* les conditions suivantes; tu dois avoir:

1. du travail ou pas d'enfants ou une bonne santé.
2. des enfants ou des amis ou pas de télévision.
3. pas d'enfants ou une maison ou pas de dettes.
4. pas d'amis ou des enfants ou pas de dettes.
5. des dettes ou une bonne santé ou pas de maison.
6. pas de télévision ou pas de dettes.

Possible ? Impossible ?

On ne connaît *aucun* bon algorithme (meilleur que de chercher "à la brute") pour résoudre ce problème. Et la recherche "à la brute" est *vraiment* impraticable.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Satisfait ? Pas satisfait ?

Le gourou a dit: tu triches encore, tu as un algorithme P.
Dorénavant, pour bien vivre, il faut que tu satisfasses à *toutes* les conditions suivantes; tu dois avoir:

1. du travail ou pas d'enfants ou une bonne santé.
2. des enfants ou des amis ou pas de télévision.
3. pas d'enfants ou une maison ou pas de dettes.
4. pas d'amis ou des enfants ou pas de dettes.
5. des dettes ou une bonne santé ou pas de maison.
6. pas de télévision ou pas de dettes.

Possible ? Impossible ?

On ne connaît *aucun* bon algorithme (meilleur que de chercher "à la brute") pour résoudre ce problème. Et la recherche "à la brute" est *vraiment* impraticable.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Satisfait ? Pas satisfait ?

Le gourou a dit: tu triches encore, tu as un algorithme P.
Dorénavant, pour bien vivre, il faut que tu satisfasses à *toutes* les conditions suivantes; tu dois avoir:

1. du travail ou pas d'enfants ou une bonne santé.
2. des enfants ou des amis ou pas de télévision.
3. pas d'enfants ou une maison ou pas de dettes.
4. pas d'amis ou des enfants ou pas de dettes.
5. des dettes ou une bonne santé ou pas de maison.
6. pas de télévision ou pas de dettes.

Possible ? Impossible ?

On ne connaît *aucun* bon algorithme (meilleur que de chercher "à la brute") pour résoudre ce problème. Et la recherche "à la brute" est *vraiment* impraticable.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Satisfait ? Pas satisfait ?

Le gourou a dit: tu triches encore, tu as un algorithme P.
Dorénavant, pour bien vivre, il faut que tu satisfasses à *toutes* les conditions suivantes; tu dois avoir:

1. du travail ou pas d'enfants ou une bonne santé.
2. des enfants ou des amis ou pas de télévision.
3. pas d'enfants ou une maison ou pas de dettes.
4. pas d'amis ou des enfants ou pas de dettes.
5. des dettes ou une bonne santé ou pas de maison.
6. pas de télévision ou pas de dettes.

Possible ? Impossible ?

On ne connaît *aucun* bon algorithme (meilleur que de chercher "à la brute") pour résoudre ce problème. Et la recherche "à la brute" est *vraiment* impraticable.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Satisfait ? Pas satisfait ?

Le gourou a dit: tu triches encore, tu as un algorithme P.
Dorénavant, pour bien vivre, il faut que tu satisfasses à *toutes* les conditions suivantes; tu dois avoir:

1. du travail ou pas d'enfants ou une bonne santé.
2. des enfants ou des amis ou pas de télévision.
3. pas d'enfants ou une maison ou pas de dettes.
4. pas d'amis ou des enfants ou pas de dettes.
5. des dettes ou une bonne santé ou pas de maison.
6. pas de télévision ou pas de dettes.

Possible ? Impossible ?

On ne connaît *aucun* bon algorithme (meilleur que de chercher "à la brute") pour résoudre ce problème. Et la recherche "à la brute" est *vraiment* impraticable.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Pour s'amuser un peu.

Le problème suivant est dû à Lewis Carroll (Logique sans peine, collection L'esprit et la main, Hermann, 1966).

1. Les seuls animaux de cette maison sont des chats.
2. Tout animal qui aime à contempler la lune est apte à devenir un animal familier.
3. Quand je déteste un animal, je l'évite soigneusement.
4. Aucun animal n'est carnivore, à moins qu'il n'aille rôder dehors la nuit.
5. Aucun chat ne manque jamais de tuer les souris.
6. Aucun animal ne s'attache jamais à moi, excepté ceux qui sont dans la maison.
7. Les kangourous ne sont pas aptes à devenir des animaux familiers.
8. Aucun animal non carnivore ne tue de souris.
9. Je déteste les animaux qui ne s'attachent pas à moi.
10. Les animaux qui vont rôder dehors la nuit aiment toujours contempler la lune.

À vous de jouer ...

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Pour s'amuser un peu.

Le problème suivant est dû à Lewis Carroll (Logique sans peine, collection L'esprit et la main, Hermann, 1966).

1. Les seuls animaux de cette maison sont des chats.
2. Tout animal qui aime à contempler la lune est apte à devenir un animal familier.
3. Quand je déteste un animal, je l'évite soigneusement.
4. Aucun animal n'est carnivore, à moins qu'il n'aille rôder dehors la nuit.
5. Aucun chat ne manque jamais de tuer les souris.
6. Aucun animal ne s'attache jamais à moi, excepté ceux qui sont dans la maison.
7. Les kangourous ne sont pas aptes à devenir des animaux familiers.
8. Aucun animal non carnivore ne tue de souris.
9. Je déteste les animaux qui ne s'attachent pas à moi.
10. Les animaux qui vont rôder dehors la nuit aiment toujours contempler la lune.

À vous de jouer ...

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Pour s'amuser un peu.

Le problème suivant est dû à Lewis Carroll (Logique sans peine, collection L'esprit et la main, Hermann, 1966).

1. Les seuls animaux de cette maison sont des chats.
2. Tout animal qui aime à contempler la lune est apte à devenir un animal familier.
3. Quand je déteste un animal, je l'évite soigneusement.
4. Aucun animal n'est carnivore, à moins qu'il n'aille rôder dehors la nuit.
5. Aucun chat ne manque jamais de tuer les souris.
6. Aucun animal ne s'attache jamais à moi, excepté ceux qui sont dans la maison.
7. Les kangourous ne sont pas aptes à devenir des animaux familiers.
8. Aucun animal non carnivore ne tue de souris.
9. Je déteste les animaux qui ne s'attachent pas à moi.
10. Les animaux qui vont rôder dehors la nuit aiment toujours contempler la lune.

À vous de jouer ...

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Pour s'amuser un peu.

Le problème suivant est dû à Lewis Carroll (Logique sans peine, collection L'esprit et la main, Hermann, 1966).

1. Les seuls animaux de cette maison sont des chats.
2. Tout animal qui aime à contempler la lune est apte à devenir un animal familier.
3. Quand je déteste un animal, je l'évite soigneusement.
4. Aucun animal n'est carnivore, à moins qu'il n'aille rôder dehors la nuit.
5. Aucun chat ne manque jamais de tuer les souris.
6. Aucun animal ne s'attache jamais à moi, excepté ceux qui sont dans la maison.
7. Les kangourous ne sont pas aptes à devenir des animaux familiers.
8. Aucun animal non carnivore ne tue de souris.
9. Je déteste les animaux qui ne s'attachent pas à moi.
10. Les animaux qui vont rôder dehors la nuit aiment toujours contempler la lune.

À vous de jouer ...

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Pour s'amuser un peu.

Le problème suivant est dû à Lewis Carroll (Logique sans peine, collection L'esprit et la main, Hermann, 1966).

1. Les seuls animaux de cette maison sont des chats.
2. Tout animal qui aime à contempler la lune est apte à devenir un animal familier.
3. Quand je déteste un animal, je l'évite soigneusement.
4. Aucun animal n'est carnivore, à moins qu'il n'aille rôder dehors la nuit.
5. Aucun chat ne manque jamais de tuer les souris.
6. Aucun animal ne s'attache jamais à moi, excepté ceux qui sont dans la maison.
7. Les kangourous ne sont pas aptes à devenir des animaux familiers.
8. Aucun animal non carnivore ne tue de souris.
9. Je déteste les animaux qui ne s'attachent pas à moi.
10. Les animaux qui vont rôder dehors la nuit aiment toujours contempler la lune.

À vous de jouer ...

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Pour s'amuser un peu.

Le problème suivant est dû à Lewis Carroll (Logique sans peine, collection L'esprit et la main, Hermann, 1966).

1. Les seuls animaux de cette maison sont des chats.
2. Tout animal qui aime à contempler la lune est apte à devenir un animal familier.
3. Quand je déteste un animal, je l'évite soigneusement.
4. Aucun animal n'est carnivore, à moins qu'il n'aille rôder dehors la nuit.
5. Aucun chat ne manque jamais de tuer les souris.
6. Aucun animal ne s'attache jamais à moi, excepté ceux qui sont dans la maison.
7. Les kangourous ne sont pas aptes à devenir des animaux familiers.
8. Aucun animal non carnivore ne tue de souris.
9. Je déteste les animaux qui ne s'attachent pas à moi.
10. Les animaux qui vont rôder dehors la nuit aiment toujours contempler la lune.

À vous de jouer ...

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Pour s'amuser un peu.

Le problème suivant est dû à Lewis Carroll (Logique sans peine, collection L'esprit et la main, Hermann, 1966).

1. Les seuls animaux de cette maison sont des chats.
2. Tout animal qui aime à contempler la lune est apte à devenir un animal familier.
3. Quand je déteste un animal, je l'évite soigneusement.
4. Aucun animal n'est carnivore, à moins qu'il n'aille rôder dehors la nuit.
5. Aucun chat ne manque jamais de tuer les souris.
6. Aucun animal ne s'attache jamais à moi, excepté ceux qui sont dans la maison.
7. Les kangourous ne sont pas aptes à devenir des animaux familiers.
8. Aucun animal non carnivore ne tue de souris.
9. Je déteste les animaux qui ne s'attachent pas à moi.
10. Les animaux qui vont rôder dehors la nuit aiment toujours contempler la lune.

À vous de jouer ...

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Pour s'amuser un peu.

Le problème suivant est dû à Lewis Carroll (Logique sans peine, collection L'esprit et la main, Hermann, 1966).

1. Les seuls animaux de cette maison sont des chats.
2. Tout animal qui aime à contempler la lune est apte à devenir un animal familier.
3. Quand je déteste un animal, je l'évite soigneusement.
4. Aucun animal n'est carnivore, à moins qu'il n'aille rôder dehors la nuit.
5. Aucun chat ne manque jamais de tuer les souris.
6. Aucun animal ne s'attache jamais à moi, excepté ceux qui sont dans la maison.
7. Les kangourous ne sont pas aptes à devenir des animaux familiers.
8. Aucun animal non carnivore ne tue de souris.
9. Je déteste les animaux qui ne s'attachent pas à moi.
10. Les animaux qui vont rôder dehors la nuit aiment toujours contempler la lune.

À vous de jouer ...

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Pour s'amuser un peu.

Le problème suivant est dû à Lewis Carroll (Logique sans peine, collection L'esprit et la main, Hermann, 1966).

1. Les seuls animaux de cette maison sont des chats.
2. Tout animal qui aime à contempler la lune est apte à devenir un animal familier.
3. Quand je déteste un animal, je l'évite soigneusement.
4. Aucun animal n'est carnivore, à moins qu'il n'aille rôder dehors la nuit.
5. Aucun chat ne manque jamais de tuer les souris.
6. Aucun animal ne s'attache jamais à moi, excepté ceux qui sont dans la maison.
7. Les kangourous ne sont pas aptes à devenir des animaux familiers.
8. Aucun animal non carnivore ne tue de souris.
9. Je déteste les animaux qui ne s'attachent pas à moi.
10. Les animaux qui vont rôder dehors la nuit aiment toujours contempler la lune.

À vous de jouer ...

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Pour s'amuser un peu.

Le problème suivant est dû à Lewis Carroll (Logique sans peine, collection L'esprit et la main, Hermann, 1966).

1. Les seuls animaux de cette maison sont des chats.
2. Tout animal qui aime à contempler la lune est apte à devenir un animal familier.
3. Quand je déteste un animal, je l'évite soigneusement.
4. Aucun animal n'est carnivore, à moins qu'il n'aille rôder dehors la nuit.
5. Aucun chat ne manque jamais de tuer les souris.
6. Aucun animal ne s'attache jamais à moi, excepté ceux qui sont dans la maison.
7. Les kangourous ne sont pas aptes à devenir des animaux familiers.
8. Aucun animal non carnivore ne tue de souris.
9. Je déteste les animaux qui ne s'attachent pas à moi.
10. Les animaux qui vont rôder dehors la nuit aiment toujours contempler la lune.

À vous de jouer ...

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Pour s'amuser un peu.

Le problème suivant est dû à Lewis Carroll (Logique sans peine, collection L'esprit et la main, Hermann, 1966).

1. Les seuls animaux de cette maison sont des chats.
2. Tout animal qui aime à contempler la lune est apte à devenir un animal familier.
3. Quand je déteste un animal, je l'évite soigneusement.
4. Aucun animal n'est carnivore, à moins qu'il n'aille rôder dehors la nuit.
5. Aucun chat ne manque jamais de tuer les souris.
6. Aucun animal ne s'attache jamais à moi, excepté ceux qui sont dans la maison.
7. Les kangourous ne sont pas aptes à devenir des animaux familiers.
8. Aucun animal non carnivore ne tue de souris.
9. Je déteste les animaux qui ne s'attachent pas à moi.
10. Les animaux qui vont rôder dehors la nuit aiment toujours contempler la lune.

À vous de jouer ...

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Pour s'amuser un peu.

Le problème suivant est dû à Lewis Carroll (Logique sans peine, collection L'esprit et la main, Hermann, 1966).

1. Les seuls animaux de cette maison sont des chats.
2. Tout animal qui aime à contempler la lune est apte à devenir un animal familier.
3. Quand je déteste un animal, je l'évite soigneusement.
4. Aucun animal n'est carnivore, à moins qu'il n'aille rôder dehors la nuit.
5. Aucun chat ne manque jamais de tuer les souris.
6. Aucun animal ne s'attache jamais à moi, excepté ceux qui sont dans la maison.
7. Les kangourous ne sont pas aptes à devenir des animaux familiers.
8. Aucun animal non carnivore ne tue de souris.
9. Je déteste les animaux qui ne s'attachent pas à moi.
10. Les animaux qui vont rôder dehors la nuit aiment toujours contempler la lune.

À vous de jouer ...

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction



P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Qu'est-ce qui marche, qu'est-ce qui ne marche pas ?

Les deux premiers ensembles de règles donnés par mon gourou "du travail ou pas d'enfants", etc, sont des "2-clauses".

Le problème s'appelle "2-SAT" (satisfiabilité pour les formules 2-clausales). Il admet une solution efficace. Il est dans la classe P.

Le troisième ensemble de règles donné par mon gourou "du travail ou pas d'enfants ou une bonne santé", etc, comprend des "3-clauses".

Le problème s'appelle "3-SAT" (satisfiabilité pour les formules 3-clausales).

On sait tester facilement les solutions. Il est dans la classe NP.

On ne sait pas les trouver efficacement. On ne sait pas s'il est dans la classe P.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Qu'est-ce qui marche, qu'est-ce qui ne marche pas ?

Les deux premiers ensembles de règles donnés par mon gourou “du travail ou pas d'enfants”, etc, sont des “2-clauses” .

Le problème s'appelle “2-SAT” (satisfiabilité pour les formules 2-clausales). Il admet une solution efficace. Il est dans la classe P.

Le troisième ensemble de règles donné par mon gourou “du travail ou pas d'enfants ou une bonne santé”, etc, comprend des “3-clauses” .

Le problème s'appelle “3-SAT” (satisfiabilité pour les formules 3-clausales).

On sait tester facilement les solutions. Il est dans la classe NP.

On ne sait pas les trouver efficacement. On ne sait pas s'il est dans la classe P.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Qu'est-ce qui marche, qu'est-ce qui ne marche pas ?

Les deux premiers ensembles de règles donnés par mon gourou “du travail ou pas d'enfants”, etc, sont des “2-clauses” .

Le problème s'appelle “2-SAT” (satisfiabilité pour les formules 2-clausales). Il admet une solution efficace. Il est dans la classe P.

Le troisième ensemble de règles donné par mon gourou “du travail ou pas d'enfants ou une bonne santé”, etc, comprend des “3-clauses” .

Le problème s'appelle “3-SAT” (satisfiabilité pour les formules 3-clausales).

On sait tester facilement les solutions. Il est dans la classe NP.

On ne sait pas les trouver efficacement. On ne sait pas s'il est dans la classe P.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Qu'est-ce qui marche, qu'est-ce qui ne marche pas ?

Les deux premiers ensembles de règles donnés par mon gourou “du travail ou pas d'enfants”, etc, sont des “2-clauses” .

Le problème s'appelle “2-SAT” (satisfiabilité pour les formules 2-clausales). Il admet une solution efficace. Il est dans la classe P.

Le troisième ensemble de règles donné par mon gourou “du travail ou pas d'enfants ou une bonne santé”, etc, comprend des “3-clauses” .

Le problème s'appelle “3-SAT” (satisfiabilité pour les formules 3-clausales).

On sait tester facilement les solutions. Il est dans la classe NP.

On ne sait pas les trouver efficacement. On ne sait pas s'il est dans la classe P.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Qu'est-ce qui marche, qu'est-ce qui ne marche pas ?

Les deux premiers ensembles de règles donnés par mon gourou “du travail ou pas d'enfants”, etc, sont des “2-clauses” .

Le problème s'appelle “2-SAT” (satisfiabilité pour les formules 2-clausales). Il admet une solution efficace. Il est dans la classe P.

Le troisième ensemble de règles donné par mon gourou “du travail ou pas d'enfants ou une bonne santé”, etc, comprend des “3-clauses” .

Le problème s'appelle “3-SAT” (satisfiabilité pour les formules 3-clausales).

On sait tester facilement les solutions. Il est dans la classe NP.

On ne sait pas les trouver efficacement. On ne sait pas s'il est dans la classe P.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Qu'est-ce qui marche, qu'est-ce qui ne marche pas ?

Les deux premiers ensembles de règles donnés par mon gourou “du travail ou pas d'enfants”, etc, sont des “2-clauses” .

Le problème s'appelle “2-SAT” (satisfiabilité pour les formules 2-clausales). Il admet une solution efficace. Il est dans la classe P.

Le troisième ensemble de règles donné par mon gourou “du travail ou pas d'enfants ou une bonne santé”, etc, comprend des “3-clauses” .

Le problème s'appelle “3-SAT” (satisfiabilité pour les formules 3-clausales).

On sait tester facilement les solutions. Il est dans la classe NP.

On ne sait pas les trouver efficacement. On ne sait pas s'il est dans la classe P.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Plan

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Ce que l'on sait

Nous avons rencontré cinq problèmes:

Les problèmes:

- Chemin eulerien (Königsberg)
- Chemin hamiltonien (gares et trains)
- Systèmes d'équations
- 2-SAT (kangourous)
- 3-SAT (règles à 3 clauses)

Ce que l'on en sait:

- P
- NP
- P
- P
- NP

Rappelons que:

P signifie que l'on sait *trouver* une solution en temps raisonnable.

NP signifie que l'on sait *tester* une solution en temps raisonnable.

Ce que l'on ne sait pas:

Le problème du chemin hamiltonien et le problème 3-SAT sont-ils dans P ?

Peut-on leur *trouver* une solution en temps raisonnable ?

P = NP ?

Jacques Sauloy

Königsberg et les chemins euleriens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Ce que l'on sait

Nous avons rencontré cinq problèmes:

Les problèmes:

Chemin eulerien (Königsberg)	P
Chemin hamiltonien (gares et trains)	NP
Systèmes d'équations	P
2-SAT (kangourous)	P
3-SAT (règles à 3 clauses)	NP

Ce que l'on en sait:

P
NP
P
P
NP

Rappelons que:

P signifie que l'on sait *trouver* une solution en temps raisonnable.

NP signifie que l'on sait *tester* une solution en temps raisonnable.

Ce que l'on ne sait pas:

Le problème du chemin hamiltonien et le problème 3-SAT sont-ils dans P ?

Peut-on leur *trouver* une solution en temps raisonnable ?

P = NP ?

Jacques Sauloy

Königsberg et les chemins euleriens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Ce que l'on sait

Nous avons rencontré cinq problèmes:

Les problèmes:

Chemin eulerien (Königsberg)

Chemin hamiltonien (gares et trains)

Systèmes d'équations

2-SAT (kangourous)

3-SAT (règles à 3 clauses)

Ce que l'on en sait:

P

NP

P

P

NP

Rappelons que:

P signifie que l'on sait *trouver* une solution en temps raisonnable.

NP signifie que l'on sait *tester* une solution en temps raisonnable.

Ce que l'on ne sait pas:

Le problème du chemin hamiltonien et le problème 3-SAT sont-ils dans P ?

Peut-on leur *trouver* une solution en temps raisonnable ?

P = NP ?

Jacques Sauloy

Königsberg et les chemins euleriens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Ce que l'on sait

Nous avons rencontré cinq problèmes:

Les problèmes:

Chemin eulerien (Königsberg)

Chemin hamiltonien (gares et trains)

Systèmes d'équations

2-SAT (kangourous)

3-SAT (règles à 3 clauses)

Ce que l'on en sait:

P

NP

P

P

NP

Rappelons que:

P signifie que l'on sait *trouver* une solution en temps raisonnable.

NP signifie que l'on sait *tester* une solution en temps raisonnable.

Ce que l'on ne sait pas:

Le problème du chemin hamiltonien et le problème 3-SAT sont-ils dans P ?

Peut-on leur *trouver* une solution en temps raisonnable ?

P = NP ?

Jacques Sauloy

Königsberg et les chemins euleriens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Ce que l'on sait

Nous avons rencontré cinq problèmes:

Les problèmes:

Chemin eulerien (Königsberg)

Chemin hamiltonien (gares et trains)

Systèmes d'équations

2-SAT (kangourous)

3-SAT (règles à 3 clauses)

Ce que l'on en sait:

P

NP

P

P

NP

Rappelons que:

P signifie que l'on sait *trouver* une solution en temps raisonnable.

NP signifie que l'on sait *tester* une solution en temps raisonnable.

Ce que l'on ne sait pas:

Le problème du chemin hamiltonien et le problème 3-SAT sont-ils dans P ?

Peut-on leur *trouver* une solution en temps raisonnable ?

P = NP ?

Jacques Sauloy

Königsberg et les chemins euleriens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Ce que l'on sait

Nous avons rencontré cinq problèmes:

Les problèmes:

Chemin eulerien (Königsberg)

Chemin hamiltonien (gares et trains)

Systèmes d'équations

2-SAT (kangourous)

3-SAT (règles à 3 clauses)

Ce que l'on en sait:

P

NP

P

P

NP

Rappelons que:

P signifie que l'on sait *trouver* une solution en temps raisonnable.

NP signifie que l'on sait *tester* une solution en temps raisonnable.

Ce que l'on ne sait pas:

Le problème du chemin hamiltonien et le problème 3-SAT sont-ils dans P ?

Peut-on leur *trouver* une solution en temps raisonnable ?

P = NP ?

Jacques Sauloy

Königsberg et les chemins euleriens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Ce que l'on sait

Nous avons rencontré cinq problèmes:

Les problèmes:

Chemin eulerien (Königsberg)

Chemin hamiltonien (gares et trains)

Systèmes d'équations

2-SAT (kangourous)

3-SAT (règles à 3 clauses)

Ce que l'on en sait:

P

NP

P

P

NP

Rappelons que:

P signifie que l'on sait *trouver* une solution en temps raisonnable.

NP signifie que l'on sait *tester* une solution en temps raisonnable.

Ce que l'on ne sait pas:

Le problème du chemin hamiltonien et le problème 3-SAT sont-ils dans P ?

Peut-on leur *trouver* une solution en temps raisonnable ?

P = NP ?

Jacques Sauloy

Königsberg et les chemins euleriens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Ce que l'on sait

Nous avons rencontré cinq problèmes:

Les problèmes:

Chemin eulerien (Königsberg)

Chemin hamiltonien (gares et trains)

Systèmes d'équations

2-SAT (kangourous)

3-SAT (règles à 3 clauses)

Ce que l'on en sait:

P

NP

P

P

NP

Rappelons que:

P signifie que l'on sait *trouver* une solution en temps raisonnable.

NP signifie que l'on sait *tester* une solution en temps raisonnable.

Ce que l'on ne sait pas:

Le problème du chemin hamiltonien et le problème 3-SAT sont-ils dans P ?

Peut-on leur *trouver* une solution en temps raisonnable ?

P = NP ?

Jacques Sauloy

Königsberg et les chemins euleriens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Ce que l'on sait

Nous avons rencontré cinq problèmes:

Les problèmes:

Chemin eulerien (Königsberg)

Chemin hamiltonien (gares et trains)

Systèmes d'équations

2-SAT (kangourous)

3-SAT (règles à 3 clauses)

Ce que l'on en sait:

P

NP

P

P

NP

Rappelons que:

P signifie que l'on sait *trouver* une solution en temps raisonnable.

NP signifie que l'on sait *tester* une solution en temps raisonnable.

Ce que l'on ne sait pas:

Le problème du chemin hamiltonien et le problème 3-SAT sont-ils dans P ?

Peut-on leur *trouver* une solution en temps raisonnable ?

P = NP ?

Jacques Sauloy

Königsberg et les chemins euleriens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Ce que l'on sait

Nous avons rencontré cinq problèmes:

Les problèmes:

Chemin eulerien (Königsberg)

Chemin hamiltonien (gares et trains)

Systèmes d'équations

2-SAT (kangourous)

3-SAT (règles à 3 clauses)

Ce que l'on en sait:

P

NP

P

P

NP

Rappelons que:

P signifie que l'on sait *trouver* une solution en temps raisonnable.

NP signifie que l'on sait *tester* une solution en temps raisonnable.

Ce que l'on ne sait pas:

Le problème du chemin hamiltonien et le problème 3-SAT sont-ils dans P ?

Peut-on leur *trouver* une solution en temps raisonnable ?

P = NP ?

Jacques Sauloy

Königsberg et les chemins euleriens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Ce que l'on sait

Nous avons rencontré cinq problèmes:

Les problèmes:

Chemin eulerien (Königsberg)

Chemin hamiltonien (gares et trains)

Systèmes d'équations

2-SAT (kangourous)

3-SAT (règles à 3 clauses)

Ce que l'on en sait:

P

NP

P

P

NP

Rappelons que:

P signifie que l'on sait *trouver* une solution en temps raisonnable.

NP signifie que l'on sait *tester* une solution en temps raisonnable.

Ce que l'on ne sait pas:

Le problème du chemin hamiltonien et le problème 3-SAT sont-ils dans P ?

Peut-on leur *trouver* une solution en temps raisonnable ?

P = NP ?

Jacques Sauloy

Königsberg et les chemins euleriens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Ce que l'on sait

Nous avons rencontré cinq problèmes:

Les problèmes:

Chemin eulerien (Königsberg)

Chemin hamiltonien (gares et trains)

Systèmes d'équations

2-SAT (kangourous)

3-SAT (règles à 3 clauses)

Ce que l'on en sait:

P

NP

P

P

NP

Rappelons que:

P signifie que l'on sait *trouver* une solution en temps raisonnable.

NP signifie que l'on sait *tester* une solution en temps raisonnable.

Ce que l'on ne sait pas:

Le problème du chemin hamiltonien et le problème 3-SAT sont-ils dans P ?

Peut-on leur *trouver* une solution en temps raisonnable ?

P = NP ?

Jacques Sauloy

Königsberg et les chemins euleriens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Ce que l'on sait

Nous avons rencontré cinq problèmes:

Les problèmes:

Chemin eulerien (Königsberg)

Chemin hamiltonien (gares et trains)

Systèmes d'équations

2-SAT (kangourous)

3-SAT (règles à 3 clauses)

Ce que l'on en sait:

P

NP

P

P

NP

Rappelons que:

P signifie que l'on sait *trouver* une solution en temps raisonnable.

NP signifie que l'on sait *tester* une solution en temps raisonnable.

Ce que l'on ne sait pas:

Le problème du chemin hamiltonien et le problème 3-SAT sont-ils dans P ?

Peut-on leur *trouver* une solution en temps raisonnable ?

P = NP ?

Jacques Sauloy

Königsberg et les chemins euleriens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Ce que l'on sait

Nous avons rencontré cinq problèmes:

Les problèmes:

Chemin eulerien (Königsberg)

Chemin hamiltonien (gares et trains)

Systèmes d'équations

2-SAT (kangourous)

3-SAT (règles à 3 clauses)

Ce que l'on en sait:

P

NP

P

P

NP

Rappelons que:

P signifie que l'on sait *trouver* une solution en temps raisonnable.

NP signifie que l'on sait *tester* une solution en temps raisonnable.

Ce que l'on ne sait pas:

Le problème du chemin hamiltonien et le problème 3-SAT sont-ils dans P ?

Peut-on leur *trouver* une solution en temps raisonnable ?

P = NP ?

Jacques Sauloy

Königsberg et les chemins euleriens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Ce que l'on sait

Nous avons rencontré cinq problèmes:

Les problèmes:

Chemin eulerien (Königsberg)

Chemin hamiltonien (gares et trains)

Systèmes d'équations

2-SAT (kangourous)

3-SAT (règles à 3 clauses)

Ce que l'on en sait:

P

NP

P

P

NP

Rappelons que:

P signifie que l'on sait *trouver* une solution en temps raisonnable.

NP signifie que l'on sait *tester* une solution en temps raisonnable.

Ce que l'on ne sait pas:

Le problème du chemin hamiltonien et le problème 3-SAT sont-ils dans P ?

Peut-on leur *trouver* une solution en temps raisonnable ?

Königsberg et les chemins euleriens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Ce que l'on sait

Nous avons rencontré cinq problèmes:

Les problèmes:

Chemin eulerien (Königsberg)

Chemin hamiltonien (gares et trains)

Systèmes d'équations

2-SAT (kangourous)

3-SAT (règles à 3 clauses)

Ce que l'on en sait:

P

NP

P

P

NP

Rappelons que:

P signifie que l'on sait *trouver* une solution en temps raisonnable.

NP signifie que l'on sait *tester* une solution en temps raisonnable.

Ce que l'on ne sait pas:

Le problème du chemin hamiltonien et le problème 3-SAT sont-ils dans P ?

Peut-on leur *trouver* une solution en temps raisonnable ?

P = NP ?

Jacques Sauloy

Königsberg et les chemins euleriens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Ce que l'on sait

Nous avons rencontré cinq problèmes:

Les problèmes:

Chemin eulerien (Königsberg)

Chemin hamiltonien (gares et trains)

Systèmes d'équations

2-SAT (kangourous)

3-SAT (règles à 3 clauses)

Ce que l'on en sait:

P

NP

P

P

NP

Rappelons que:

P signifie que l'on sait *trouver* une solution en temps raisonnable.

NP signifie que l'on sait *tester* une solution en temps raisonnable.

Ce que l'on ne sait pas:

Le problème du chemin hamiltonien et le problème 3-SAT sont-ils dans P ?

Peut-on leur *trouver* une solution en temps raisonnable ?

P = NP ?

Jacques Sauloy

Königsberg et les chemins euleriens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Ce que l'on sait

Nous avons rencontré cinq problèmes:

Les problèmes:

Chemin eulerien (Königsberg)

Chemin hamiltonien (gares et trains)

Systèmes d'équations

2-SAT (kangourous)

3-SAT (règles à 3 clauses)

Ce que l'on en sait:

P

NP

P

P

NP

Rappelons que:

P signifie que l'on sait *trouver* une solution en temps raisonnable.

NP signifie que l'on sait *tester* une solution en temps raisonnable.

Ce que l'on ne sait pas:

Le problème du chemin hamiltonien et le problème 3-SAT sont-ils dans P ?

Peut-on leur *trouver* une solution en temps raisonnable ?

P = NP ?

Jacques Sauloy

Königsberg et les chemins euleriens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Ce que l'on sait

Nous avons rencontré cinq problèmes:

Les problèmes:

Chemin eulerien (Königsberg)

Chemin hamiltonien (gares et trains)

Systèmes d'équations

2-SAT (kangourous)

3-SAT (règles à 3 clauses)

Ce que l'on en sait:

P

NP

P

P

NP

Rappelons que:

P signifie que l'on sait *trouver* une solution en temps raisonnable.

NP signifie que l'on sait *tester* une solution en temps raisonnable.

Ce que l'on ne sait pas:

Le problème du chemin hamiltonien et le problème 3-SAT sont-ils dans P ?

Peut-on leur *trouver* une solution en temps raisonnable ?

P = NP ?

Jacques Sauloy

Königsberg et les chemins euleriens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Le million de dollars

En l'an 2000, dernière année du précédent millénaire, la fondation Clay a proposé sept prix d'un million de dollars chacun pour la solution des sept problèmes suivants:

1. Poincaré conjecture
2. P versus NP Maths + Info
3. Hodge conjecture
4. Riemann hypothesis
5. YangMills existence and mass gap Maths + Phy
6. NavierStokes existence and smoothness Maths + Phy
7. Birch and Swinnerton-Dyer conjecture

Les problèmes 1,3,4 et 7 sont au cœur des "mathématiques pures".

Le problème 2 est de plus relié à l'informatique.

Les problèmes 5 et 6 sont reliés à la physique.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Le million de dollars

En l'an 2000, dernière année du précédent millénaire, la fondation Clay a proposé sept prix d'un million de dollars chacun pour la solution des sept problèmes suivants:

1. Poincaré conjecture

2. P versus NP

Maths + Info

3. Hodge conjecture

4. Riemann hypothesis

5. YangMills existence and mass gap

Maths + Phy

6. NavierStokes existence and smoothness

Maths + Phy

7. Birch and Swinnerton-Dyer conjecture

Les problèmes 1,3,4 et 7 sont au cœur des "mathématiques pures".

Le problème 2 est de plus relié à l'informatique.

Les problèmes 5 et 6 sont reliés à la physique.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Le million de dollars

En l'an 2000, dernière année du précédent millénaire, la fondation Clay a proposé sept prix d'un million de dollars chacun pour la solution des sept problèmes suivants:

1. Poincaré conjecture
2. P versus NP Maths + Info
3. Hodge conjecture
4. Riemann hypothesis
5. YangMills existence and mass gap Maths + Phy
6. NavierStokes existence and smoothness Maths + Phy
7. Birch and Swinnerton-Dyer conjecture

Les problèmes 1,3,4 et 7 sont au cœur des “mathématiques pures”.

Le problème 2 est de plus relié à l'informatique.

Les problèmes 5 et 6 sont reliés à la physique.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Le million de dollars

En l'an 2000, dernière année du précédent millénaire, la fondation Clay a proposé sept prix d'un million de dollars chacun pour la solution des sept problèmes suivants:

1. Poincaré conjecture
2. P versus NP Maths + Info
3. Hodge conjecture
4. Riemann hypothesis
5. YangMills existence and mass gap Maths + Phy
6. NavierStokes existence and smoothness Maths + Phy
7. Birch and Swinnerton-Dyer conjecture

Les problèmes 1,3,4 et 7 sont au cœur des "mathématiques pures".

Le problème 2 est de plus relié à l'informatique.

Les problèmes 5 et 6 sont reliés à la physique.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Le million de dollars

En l'an 2000, dernière année du précédent millénaire, la fondation Clay a proposé sept prix d'un million de dollars chacun pour la solution des sept problèmes suivants:

1. Poincaré conjecture
2. P versus NP Maths + Info
3. Hodge conjecture
4. Riemann hypothesis
5. YangMills existence and mass gap Maths + Phy
6. NavierStokes existence and smoothness Maths + Phy
7. Birch and Swinnerton-Dyer conjecture

Les problèmes 1,3,4 et 7 sont au cœur des "mathématiques pures".

Le problème 2 est de plus relié à l'informatique.

Les problèmes 5 et 6 sont reliés à la physique.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Le million de dollars

En l'an 2000, dernière année du précédent millénaire, la fondation Clay a proposé sept prix d'un million de dollars chacun pour la solution des sept problèmes suivants:

1. Poincaré conjecture
2. P versus NP Maths + Info
3. Hodge conjecture
4. Riemann hypothesis
5. YangMills existence and mass gap Maths + Phy
6. NavierStokes existence and smoothness Maths + Phy
7. Birch and Swinnerton-Dyer conjecture

Les problèmes 1,3,4 et 7 sont au cœur des "mathématiques pures".

Le problème 2 est de plus relié à l'informatique.

Les problèmes 5 et 6 sont reliés à la physique.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Le million de dollars

En l'an 2000, dernière année du précédent millénaire, la fondation Clay a proposé sept prix d'un million de dollars chacun pour la solution des sept problèmes suivants:

1. Poincaré conjecture
2. P versus NP Maths + Info
3. Hodge conjecture
4. Riemann hypothesis
5. YangMills existence and mass gap Maths + Phy
6. NavierStokes existence and smoothness Maths + Phy
7. Birch and Swinnerton-Dyer conjecture

Les problèmes 1,3,4 et 7 sont au cœur des "mathématiques pures".

Le problème 2 est de plus relié à l'informatique.

Les problèmes 5 et 6 sont reliés à la physique.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Le million de dollars

En l'an 2000, dernière année du précédent millénaire, la fondation Clay a proposé sept prix d'un million de dollars chacun pour la solution des sept problèmes suivants:

1. Poincaré conjecture
2. P versus NP Maths + Info
3. Hodge conjecture
4. Riemann hypothesis
5. YangMills existence and mass gap Maths + Phy
6. NavierStokes existence and smoothness Maths + Phy
7. Birch and Swinnerton-Dyer conjecture

Les problèmes 1,3,4 et 7 sont au cœur des "mathématiques pures".

Le problème 2 est de plus relié à l'informatique.

Les problèmes 5 et 6 sont reliés à la physique.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Le million de dollars

En l'an 2000, dernière année du précédent millénaire, la fondation Clay a proposé sept prix d'un million de dollars chacun pour la solution des sept problèmes suivants:

1. Poincaré conjecture
2. P versus NP Maths + Info
3. Hodge conjecture
4. Riemann hypothesis
5. YangMills existence and mass gap Maths + Phy
6. NavierStokes existence and smoothness Maths + Phy
7. Birch and Swinnerton-Dyer conjecture

Les problèmes 1,3,4 et 7 sont au cœur des “mathématiques pures” .

Le problème 2 est de plus relié à l'informatique.

Les problèmes 5 et 6 sont reliés à la physique.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Le million de dollars

En l'an 2000, dernière année du précédent millénaire, la fondation Clay a proposé sept prix d'un million de dollars chacun pour la solution des sept problèmes suivants:

1. Poincaré conjecture
2. P versus NP Maths + Info
3. Hodge conjecture
4. Riemann hypothesis
5. YangMills existence and mass gap Maths + Phy
6. NavierStokes existence and smoothness Maths + Phy
7. Birch and Swinnerton-Dyer conjecture

Les problèmes 1,3,4 et 7 sont au cœur des “mathématiques pures”.

Le problème 2 est de plus relié à l'informatique.

Les problèmes 5 et 6 sont reliés à la physique.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Le million de dollars

En l'an 2000, dernière année du précédent millénaire, la fondation Clay a proposé sept prix d'un million de dollars chacun pour la solution des sept problèmes suivants:

1. Poincaré conjecture
2. P versus NP **Maths + Info**
3. Hodge conjecture
4. Riemann hypothesis
5. YangMills existence and mass gap **Maths + Phy**
6. NavierStokes existence and smoothness **Maths + Phy**
7. Birch and Swinnerton-Dyer conjecture

Les problèmes 1,3,4 et 7 sont au cœur des “mathématiques pures”.

Le problème 2 est de plus relié à l'informatique.

Les problèmes 5 et 6 sont reliés à la physique.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Qui aura le million de dollars ?

- | | |
|--|--------|
| 1. Poincaré conjecture | Résolu |
| 2. P versus NP | Ouvert |
| 3. Hodge conjecture | Ouvert |
| 4. Riemann hypothesis | Ouvert |
| 5. YangMills existence and mass gap | Ouvert |
| 6. NavierStokes existence and smoothness | Ouvert |
| 7. Birch and Swinnerton-Dyer conjecture | Ouvert |

Voici où l'on en est de ces problèmes:

Le premier problème a été résolu en 2003 par le russe Grigori Perelman. Le prix Clay et la médaille Fields (équivalent du prix Nobel en mathématiques) lui ont été décernés, mais il les a refusés.

Les six autres problèmes ne sont pas résolus. Au travail !

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Qui aura le million de dollars ?

- | | |
|--|--------|
| 1. Poincaré conjecture | Résolu |
| 2. P versus NP | Ouvert |
| 3. Hodge conjecture | Ouvert |
| 4. Riemann hypothesis | Ouvert |
| 5. YangMills existence and mass gap | Ouvert |
| 6. NavierStokes existence and smoothness | Ouvert |
| 7. Birch and Swinnerton-Dyer conjecture | Ouvert |

Voici où l'on en est de ces problèmes:

Le premier problème a été résolu en 2003 par le russe Grigori Perelman. Le prix Clay et la médaille Fields (équivalent du prix Nobel en mathématiques) lui ont été décernés, mais il les a refusés.

Les six autres problèmes ne sont pas résolus. Au travail !

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Qui aura le million de dollars ?

- | | |
|--|--------|
| 1. Poincaré conjecture | Résolu |
| 2. P versus NP | Ouvert |
| 3. Hodge conjecture | Ouvert |
| 4. Riemann hypothesis | Ouvert |
| 5. YangMills existence and mass gap | Ouvert |
| 6. NavierStokes existence and smoothness | Ouvert |
| 7. Birch and Swinnerton-Dyer conjecture | Ouvert |

Voici où l'on en est de ces problèmes:

Le premier problème a été résolu en 2003 par le russe Grigori Perelman. Le prix Clay et la médaille Fields (équivalent du prix Nobel en mathématiques) lui ont été décernés, mais il les a refusés.

Les six autres problèmes ne sont pas résolus. Au travail !

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Qui aura le million de dollars ?

- | | |
|--|--------|
| 1. Poincaré conjecture | Résolu |
| 2. P versus NP | Ouvert |
| 3. Hodge conjecture | Ouvert |
| 4. Riemann hypothesis | Ouvert |
| 5. YangMills existence and mass gap | Ouvert |
| 6. NavierStokes existence and smoothness | Ouvert |
| 7. Birch and Swinnerton-Dyer conjecture | Ouvert |

Voici où l'on en est de ces problèmes:

Le premier problème a été résolu en 2003 par le russe Grigori Perelman. Le prix Clay et la médaille Fields (équivalent du prix Nobel en mathématiques) lui ont été décernés, mais il les a refusés.

Les six autres problèmes ne sont pas résolus. Au travail !

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Qui aura le million de dollars ?

- | | |
|--|--------|
| 1. Poincaré conjecture | Résolu |
| 2. P versus NP | Ouvert |
| 3. Hodge conjecture | Ouvert |
| 4. Riemann hypothesis | Ouvert |
| 5. YangMills existence and mass gap | Ouvert |
| 6. NavierStokes existence and smoothness | Ouvert |
| 7. Birch and Swinnerton-Dyer conjecture | Ouvert |

Voici où l'on en est de ces problèmes:

Le premier problème a été résolu en 2003 par le russe Grigori Perelman. Le prix Clay et la médaille Fields (équivalent du prix Nobel en mathématiques) lui ont été décernés, mais il les a refusés.

Les six autres problèmes ne sont pas résolus. Au travail !

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Pourquoi le problème “ $P = NP$?” est-il intéressant ?

D'abord, ce n'est pas un problème concernant des cas isolés. on a découvert depuis cinquante ans de *nombreux* problèmes de “calcul” (au sens large) dont on sait qu'ils sont NP et dont on ne sait pas s'ils sont P.

Ces problèmes sont reliés entre eux par une relation logique étonnante:

Si l'on prouve que l'un d'entre eux est P, alors tous sont P.

Ces problèmes sont caractérisés par une propriété logique encore plus étonnante (“NP-complétude”):

Si l'on prouve que l'un d'entre eux est P, alors tout problème NP est P. (Théorèmes de Cook, Rabin, Karp.)

$P = NP$?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Pourquoi le problème “ $P = NP$?” est-il intéressant ?

D’abord, ce n’est pas un problème concernant des cas isolés. on a découvert depuis cinquante ans de *nombreux* problèmes de “calcul” (au sens large) dont on sait qu’ils sont NP et dont on ne sait pas s’ils sont P.

Ces problèmes sont reliés entre eux par une relation logique étonnante:

Si l’on prouve que l’un d’entre eux est P, alors tous sont P.

Ces problèmes sont caractérisés par une propriété logique encore plus étonnante (“NP-complétude”):

Si l’on prouve que l’un d’entre eux est P, alors tout problème NP est P. (Théorèmes de Cook, Rabin, Karp.)

$P = NP$?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c’est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Pourquoi le problème “P = NP ?” est-il intéressant ?

D’abord, ce n’est pas un problème concernant des cas isolés. on a découvert depuis cinquante ans de *nombreux* problèmes de “calcul” (au sens large) dont on sait qu’ils sont NP et dont on ne sait pas s’ils sont P.

Ces problèmes sont reliés entre eux par une relation logique étonnante:

Si l’on prouve que l’un d’entre eux est P, alors tous sont P.

Ces problèmes sont caractérisés par une propriété logique encore plus étonnante (“NP-complétude”):

Si l’on prouve que l’un d’entre eux est P, alors tout problème NP est P. (Théorèmes de Cook, Rabin, Karp.)

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c’est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Pourquoi le problème “P = NP ?” est-il intéressant ?

D'abord, ce n'est pas un problème concernant des cas isolés. on a découvert depuis cinquante ans de *nombreux* problèmes de “calcul” (au sens large) dont on sait qu'ils sont NP et dont on ne sait pas s'ils sont P.

Ces problèmes sont reliés entre eux par une relation logique étonnante:

Si l'on prouve que l'un d'entre eux est P, alors tous sont P.

Ces problèmes sont caractérisés par une propriété logique encore plus étonnante (“NP-complétude”):

Si l'on prouve que l'un d'entre eux est P, alors tout problème NP est P. (Théorèmes de Cook, Rabin, Karp.)

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Pourquoi le problème “P = NP ?” est-il intéressant ?

D'abord, ce n'est pas un problème concernant des cas isolés. on a découvert depuis cinquante ans de *nombreux* problèmes de “calcul” (au sens large) dont on sait qu'ils sont NP et dont on ne sait pas s'ils sont P.

Ces problèmes sont reliés entre eux par une relation logique étonnante:

Si l'on prouve que l'un d'entre eux est P, alors tous sont P.

Ces problèmes sont caractérisés par une propriété logique encore plus étonnante (“NP-complétude”):

Si l'on prouve que l'un d'entre eux est P, alors tout problème NP est P. (Théorèmes de Cook, Rabin, Karp.)

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Pourquoi le problème “ $P = NP$?” est-il intéressant ?

D’abord, ce n’est pas un problème concernant des cas isolés. on a découvert depuis cinquante ans de *nombreux* problèmes de “calcul” (au sens large) dont on sait qu’ils sont NP et dont on ne sait pas s’ils sont P.

Ces problèmes sont reliés entre eux par une relation logique étonnante:

Si l’on prouve que l’un d’entre eux est P, alors tous sont P.

Ces problèmes sont caractérisés par une propriété logique encore plus étonnante (“NP-complétude”):

Si l’on prouve que l’un d’entre eux est P, alors tout problème NP est P. (Théorèmes de Cook, Rabin, Karp.)

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c’est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

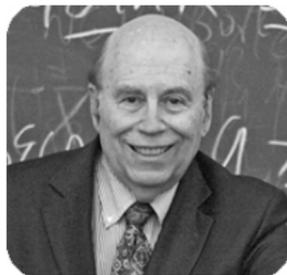
Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction



Pourquoi le problème “ $P = NP$?” est-il important ?

La majorité des experts pense que $P \neq NP$, autrement dit qu'il n'y aura jamais de solution facile à ces problèmes.

Beaucoup en sont contents, ils pensent que le monde est plus intéressant comme cela.

Essentiellement cela signifie qu'il faut un point de vue radicalement nouveau pour les aborder.

Dire que les ordinateurs, les programmeurs, le calcul ont des limites *insurmontables* à leur efficacité est un encouragement à regarder ailleurs.

$P = NP$?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Pourquoi le problème “ $P = NP$?” est-il important ?

La majorité des experts pense que $P \neq NP$, autrement dit qu'il n'y aura jamais de solution facile à ces problèmes.

Beaucoup en sont contents, ils pensent que le monde est plus intéressant comme cela.

Essentiellement cela signifie qu'il faut un point de vue radicalement nouveau pour les aborder.

Dire que les ordinateurs, les programmeurs, le calcul ont des limites *insurmontables* à leur efficacité est un encouragement à regarder ailleurs.

$P = NP$?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Pourquoi le problème “ $P = NP$?” est-il important ?

La majorité des experts pense que $P \neq NP$, autrement dit qu'il n'y aura jamais de solution facile à ces problèmes.

Beaucoup en sont contents, ils pensent que le monde est plus intéressant comme cela.

Essentiellement cela signifie qu'il faut un point de vue radicalement nouveau pour les aborder.

Dire que les ordinateurs, les programmeurs, le calcul ont des limites *insurmontables* à leur efficacité est un encouragement à regarder ailleurs.

$P = NP$?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Pourquoi le problème “ $P = NP$?” est-il important ?

La majorité des experts pense que $P \neq NP$, autrement dit qu'il n'y aura jamais de solution facile à ces problèmes.

Beaucoup en sont contents, ils pensent que le monde est plus intéressant comme cela.

Essentiellement cela signifie qu'il faut un point de vue radicalement nouveau pour les aborder.

Dire que les ordinateurs, les programmeurs, le calcul ont des limites *insurmontables* à leur efficacité est un encouragement à regarder ailleurs.

$P = NP$?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Le problème “ $P = NP$?” a-t’il des conséquences pratiques ?

Si $P = NP$:

De nombreux problèmes de logistique (optimisation des transports, gestion des tâches sur un grand chantier ...) pourront être traités par des programmes efficaces.

On pourra résoudre plus rapidement les situations de crises dans les systèmes critiques (avions, centrales nucléaires ...).

Plus aucune des méthodes de cryptage connues ne sera sûre: disparition du secret financier, militaire ...

$P = NP$?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Le problème “ $P = NP$?” a-t’il des conséquences pratiques ?

Si $P = NP$:

De nombreux problèmes de logistique (optimisation des transports, gestion des tâches sur un grand chantier ...) pourront être traités par des programmes efficaces.

On pourra résoudre plus rapidement les situations de crises dans les systèmes critiques (avions, centrales nucléaires ...).

Plus aucune des méthodes de cryptage connues ne sera sûre: disparition du secret financier, militaire ...

$P = NP$?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Le problème “ $P = NP$?” a-t’il des conséquences pratiques ?

Si $P = NP$:

De nombreux problèmes de logistique (optimisation des transports, gestion des tâches sur un grand chantier ...) pourront être traités par des programmes efficaces.

On pourra résoudre plus rapidement les situations de crises dans les systèmes critiques (avions, centrales nucléaires ...).

Plus aucune des méthodes de cryptage connues ne sera sûre: disparition du secret financier, militaire ...

$P = NP$?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Le problème “ $P = NP$?” a-t’il des conséquences pratiques ?

Si $P = NP$:

De nombreux problèmes de logistique (optimisation des transports, gestion des tâches sur un grand chantier ...) pourront être traités par des programmes efficaces.

On pourra résoudre plus rapidement les situations de crises dans les systèmes critiques (avions, centrales nucléaires ...).

Plus aucune des méthodes de cryptage connues ne sera sûre: disparition du secret financier, militaire ...

$P = NP$?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Un exemple de problème de logistique NP-complet

Il s'agit du *problème de l'ordonnancement*:

Il y a n tâches à exécuter sur machine, ou bien sur un chantier ...

Chaque tâche a un temps d'exécution p_i une date de disponibilité r_i et une date d'échéance d_i .

L'objectif est de trouver un ordonnancement qui minimise $L_{max} := \max(C_i - d_i, 0)$, où C_i dénote le temps de fin de la tâche i .

Le nombre y étant donné, existe t-il un ordonnancement tel que $L_{max} \leq y$?

C'est un problème NP-complet.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Un exemple de problème de logistique NP-complet

Il s'agit du *problème de l'ordonnancement*:

Il y a n tâches à exécuter sur machine, ou bien sur un chantier ...

Chaque tâche a un temps d'exécution p_i une date de disponibilité r_i et une date d'échéance d_i .

L'objectif est de trouver un ordonnancement qui minimise $L_{max} := \max(C_i - d_i, 0)$, où C_i dénote le temps de fin de la tâche i .

Le nombre y étant donné, existe t-il un ordonnancement tel que $L_{max} \leq y$?

C'est un problème NP-complet.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Un exemple de problème de logistique NP-complet

Il s'agit du *problème de l'ordonnancement*:

Il y a n tâches à exécuter sur machine, ou bien sur un chantier ...

Chaque tâche a un temps d'exécution p_i une date de disponibilité r_i et une date d'échéance d_i .

L'objectif est de trouver un ordonnancement qui minimise $L_{max} := \max(C_i - d_i, 0)$, où C_i dénote le temps de fin de la tâche i .

Le nombre y étant donné, existe-t-il un ordonnancement tel que $L_{max} \leq y$?

C'est un problème NP-complet.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Un exemple de problème de logistique NP-complet

Il s'agit du *problème de l'ordonnancement*:

Il y a n tâches à exécuter sur machine, ou bien sur un chantier ...

Chaque tâche a un temps d'exécution p_i une date de disponibilité r_i et une date d'échéance d_i .

L'objectif est de trouver un ordonnancement qui minimise $L_{max} := \max(C_i - d_i, 0)$, où C_i dénote le temps de fin de la tâche i .

Le nombre y étant donné, existe t-il un ordonnancement tel que $L_{max} \leq y$?

C'est un problème NP-complet.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Un exemple de problème de logistique NP-complet

Il s'agit du *problème de l'ordonnancement*:

Il y a n tâches à exécuter sur machine, ou bien sur un chantier ...

Chaque tâche a un temps d'exécution p_i une date de disponibilité r_i et une date d'échéance d_i .

L'objectif est de trouver un ordonnancement qui minimise $L_{max} := \max(C_i - d_i, 0)$, où C_i dénote le temps de fin de la tâche i .

Le nombre y étant donné, existe t-il un ordonnancement tel que $L_{max} \leq y$?

C'est un problème NP-complet.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Plan

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Il y a pire qu'infaisable

Il y a de nombreux problèmes dont on peut *prouver* qu'ils n'admettent *aucune* solution programmable (et n'en admettront jamais).

1. Problème de l'arrêt
2. Problème des mots
3. Dixième problème de Hilbert
4. Prouvabilité d'un théorème
5. Non contradiction d'une théorie

Ce n'est pas une limite de nos connaissances.

Ce n'est peut-être même pas une limite de l'esprit humain.

C'est une limite d'une manière d'aborder les choses.

Bon, on arrête là la philosophie de salle de café.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Il y a pire qu'infaisable

Il y a de nombreux problèmes dont on peut *prouver* qu'ils n'admettent *aucune* solution programmable (et n'en admettront jamais).

1. Problème de l'arrêt
2. Problème des mots
3. Dixième problème de Hilbert
4. Prouvabilité d'un théorème
5. Non contradiction d'une théorie

Ce n'est pas une limite de nos connaissances.

Ce n'est peut-être même pas une limite de l'esprit humain.

C'est une limite d'une manière d'aborder les choses.

Bon, on arrête là la philosophie de salle de café.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Il y a pire qu'infaisable

Il y a de nombreux problèmes dont on peut *prouver* qu'ils n'admettent *aucune* solution programmable (et n'en admettront jamais).

1. Problème de l'arrêt
2. Problème des mots
3. Dixième problème de Hilbert
4. Prouvabilité d'un théorème
5. Non contradiction d'une théorie

Ce n'est pas une limite de nos connaissances.

Ce n'est peut-être même pas une limite de l'esprit humain.

C'est une limite d'une manière d'aborder les choses.

Bon, on arrête là la philosophie de salle de café.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Il y a pire qu'infaisable

Il y a de nombreux problèmes dont on peut *prouver* qu'ils n'admettent *aucune* solution programmable (et n'en admettront jamais).

1. Problème de l'arrêt
2. Problème des mots
3. Dixième problème de Hilbert
4. Prouvabilité d'un théorème
5. Non contradiction d'une théorie

Ce n'est pas une limite de nos connaissances.

Ce n'est peut-être même pas une limite de l'esprit humain.

C'est une limite d'une manière d'aborder les choses.

Bon, on arrête là la philosophie de salle de café.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Il y a pire qu'infaisable

Il y a de nombreux problèmes dont on peut *prouver* qu'ils n'admettent *aucune* solution programmable (et n'en admettront jamais).

1. Problème de l'arrêt
2. Problème des mots
3. Dixième problème de Hilbert
4. Prouvabilité d'un théorème
5. Non contradiction d'une théorie

Ce n'est pas une limite de nos connaissances.

Ce n'est peut-être même pas une limite de l'esprit humain.

C'est une limite d'une manière d'aborder les choses.

Bon, on arrête là la philosophie de salle de café.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Il y a pire qu'infaisable

Il y a de nombreux problèmes dont on peut *prouver* qu'ils n'admettent *aucune* solution programmable (et n'en admettront jamais).

1. Problème de l'arrêt
2. Problème des mots
3. Dixième problème de Hilbert
4. Prouvabilité d'un théorème
5. Non contradiction d'une théorie

Ce n'est pas une limite de nos connaissances.

Ce n'est peut-être même pas une limite de l'esprit humain.

C'est une limite d'une manière d'aborder les choses.

Bon, on arrête là la philosophie de salle de café.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Il y a pire qu'infaisable

Il y a de nombreux problèmes dont on peut *prouver* qu'ils n'admettent *aucune* solution programmable (et n'en admettront jamais).

1. Problème de l'arrêt
2. Problème des mots
3. Dixième problème de Hilbert
4. Prouvabilité d'un théorème
5. Non contradiction d'une théorie

Ce n'est pas une limite de nos connaissances.

Ce n'est peut-être même pas une limite de l'esprit humain.

C'est une limite d'une manière d'aborder les choses.

Bon, on arrête là la philosophie de salle de café.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Il y a pire qu'infaisable

Il y a de nombreux problèmes dont on peut *prouver* qu'ils n'admettent *aucune* solution programmable (et n'en admettront jamais).

1. Problème de l'arrêt
2. Problème des mots
3. Dixième problème de Hilbert
4. Prouvabilité d'un théorème
5. Non contradiction d'une théorie

Ce n'est pas une limite de nos connaissances.

Ce n'est peut-être même pas une limite de l'esprit humain.

C'est une limite d'une manière d'aborder les choses.

Bon, on arrête là la philosophie de salle de café.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Il y a pire qu'infaisable

Il y a de nombreux problèmes dont on peut *prouver* qu'ils n'admettent *aucune* solution programmable (et n'en admettront jamais).

1. Problème de l'arrêt
2. Problème des mots
3. Dixième problème de Hilbert
4. Prouvabilité d'un théorème
5. Non contradiction d'une théorie

Ce n'est pas une limite de nos connaissances.

Ce n'est peut-être même pas une limite de l'esprit humain.

C'est une limite d'une manière d'aborder les choses.

Bon, on arrête là la philosophie de salle de café.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Il y a pire qu'infaisable

Il y a de nombreux problèmes dont on peut *prouver* qu'ils n'admettent *aucune* solution programmable (et n'en admettront jamais).

1. Problème de l'arrêt
2. Problème des mots
3. Dixième problème de Hilbert
4. Prouvabilité d'un théorème
5. Non contradiction d'une théorie

Ce n'est pas une limite de nos connaissances.

Ce n'est peut-être même pas une limite de l'esprit humain.

C'est une limite d'une manière d'aborder les choses.

Bon, on arrête là la philosophie de salle de café.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Le problème de l'arrêt

Soit le programme de division euclidienne $a = qb + r$:

```
diveucl(a,b):  
q := 0; r := a;  
while r > 0 do (r := r - b; q := q + 1);  
return(q,r);;
```

Un compilateur malin avertira que, si $a > 0$ et $b < 0$ (par exemple), le programme "boucle".

Aucun compilateur, aucun programme, ne peut déclarer *en toute généralité* si un programme donné va boucler ou non.

C'est un théorème, il est dû à Alan Turing.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Le problème de l'arrêt

Soit le programme de division euclidienne $a = qb + r$:

```
diveucl(a,b):  
q := 0; r := a;  
while r > 0 do (r := r - b; q := q + 1);  
return(q,r);;
```

Un compilateur malin avertira que, si $a > 0$ et $b < 0$ (par exemple), le programme “boucle”.

Aucun compilateur, aucun programme, ne peut déclarer *en toute généralité* si un programme donné va boucler ou non.

C'est un théorème, il est dû à Alan Turing.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Le problème de l'arrêt

Soit le programme de division euclidienne $a = qb + r$:

```
diveucl(a,b):  
q := 0; r := a;  
while r > 0 do (r := r - b; q := q + 1);  
return(q,r);;
```

Un compilateur malin avertira que, si $a > 0$ et $b < 0$ (par exemple), le programme "boucle".

Aucun compilateur, aucun programme, ne peut déclarer *en toute généralité* si un programme donné va boucler ou non.

C'est un théorème, il est dû à Alan Turing.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Le problème de l'arrêt

Soit le programme de division euclidienne $a = qb + r$:

```
diveucl(a,b):  
q := 0; r := a;  
while r > 0 do (r := r - b; q := q + 1);  
return(q,r);;
```

Un compilateur malin avertira que, si $a > 0$ et $b < 0$ (par exemple), le programme “boucle”.

Aucun compilateur, aucun programme, ne peut déclarer *en toute généralité* si un programme donné va boucler ou non.

C'est un théorème, il est dû à Alan Turing.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction



Une "preuve" de l'indécidabilité de l'arrêt

Supposons un programme magique A tel que, si f est un programme quelconque et x une donnée quelconque pour ce programme, l'appel de $A(f, x)$

1. termine à coup sûr
2. rend 1 si l'appel de $f(x)$ termine
3. rend 0 sinon

On définit un nouveau programme *récuratif*:

$g(x)$
si $A(g, x) = 1$
 alors $g(x)$
 sinon 0

On voit immédiatement que, si $A(g, x) = 1$ alors $g(x)$ boucle, si $A(g, x) = 0$ il termine. Contradiction !

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Une "preuve" de l'indécidabilité de l'arrêt

Supposons un programme magique A tel que, si f est un programme quelconque et x une donnée quelconque pour ce programme, l'appel de $A(f, x)$

1. termine à coup sûr
2. rend 1 si l'appel de $f(x)$ termine
3. rend 0 sinon

On définit un nouveau programme *récuratif*:

$g(x)$
si $A(g, x) = 1$
alors $g(x)$
sinon 0

On voit immédiatement que, si $A(g, x) = 1$ alors $g(x)$ boucle, si $A(g, x) = 0$ il termine. Contradiction !

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Une "preuve" de l'indécidabilité de l'arrêt

Supposons un programme magique A tel que, si f est un programme quelconque et x une donnée quelconque pour ce programme, l'appel de $A(f, x)$

1. termine à coup sûr
2. rend 1 si l'appel de $f(x)$ termine
3. rend 0 sinon

On définit un nouveau programme *récuratif*:

$g(x)$
si $A(g, x) = 1$
 alors $g(x)$
 sinon 0

On voit immédiatement que, si $A(g, x) = 1$ alors $g(x)$ boucle, si $A(g, x) = 0$ il termine. Contradiction !

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Une “preuve” de l’indécidabilité de l’arrêt

Supposons un programme magique A tel que, si f est un programme quelconque et x une donnée quelconque pour ce programme, l’appel de $A(f, x)$

1. termine à coup sûr
2. rend 1 si l’appel de $f(x)$ termine
3. rend 0 sinon

On définit un nouveau programme *récuratif*:

```
g(x)
si A(g,x) = 1
  alors g(x)
sinon 0
```

On voit immédiatement que, si $A(g, x) = 1$ alors $g(x)$ boucle, si $A(g, x) = 0$ il termine. Contradiction !

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Une "preuve" de l'indécidabilité de l'arrêt

Supposons un programme magique A tel que, si f est un programme quelconque et x une donnée quelconque pour ce programme, l'appel de $A(f, x)$

1. termine à coup sûr
2. rend 1 si l'appel de $f(x)$ termine
3. rend 0 sinon

On définit un nouveau programme *récuratif*:

$g(x)$
si $A(g, x) = 1$
 alors $g(x)$
 sinon 0

On voit immédiatement que, si $A(g, x) = 1$ alors $g(x)$ boucle, si $A(g, x) = 0$ il termine. Contradiction !

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Une "preuve" de l'indécidabilité de l'arrêt

Supposons un programme magique A tel que, si f est un programme quelconque et x une donnée quelconque pour ce programme, l'appel de $A(f, x)$

1. termine à coup sûr
2. rend 1 si l'appel de $f(x)$ termine
3. rend 0 sinon

On définit un nouveau programme *récuratif*:

$g(x)$
si $A(g, x) = 1$
 alors $g(x)$
 sinon 0

On voit immédiatement que, si $A(g, x) = 1$ alors $g(x)$ boucle, si $A(g, x) = 0$ il termine. Contradiction !

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Le problème des mots

On fixe “deux générateurs” a, b et des règles (“trois relations”) portant sur ces générateurs:

$$a^2 = 1, \quad b^2 = 1, \quad ab = ba.$$

Est-ce que $abababab = 1$? On voit facilement que oui.

Est-ce que $ababababab = 1$? On voit facilement que non.

Plus généralement, si l'on forme un “mot” w avec des a et des b , il est facile de décider si, selon les règles ci-dessus, $w = 1$. (C'est un exercice pour vous !)

Étant donnés n générateurs g_1, \dots, g_n et p relations r_1, \dots, r_p , il n'existe aucun programme général qui permette de décider si un mot w formé avec g_1, \dots, g_n vérifie $w = 1$.

Ce théorème est dû à Dehn, Post, Novikov, Boone, Britton.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Le problème des mots

On fixe “deux générateurs” a, b et des règles (“trois relations”) portant sur ces générateurs:

$$a^2 = 1, \quad b^2 = 1, \quad ab = ba.$$

Est-ce que $abababab = 1$? On voit facilement que oui.

Est-ce que $ababababab = 1$? On voit facilement que non.

Plus généralement, si l'on forme un “mot” w avec des a et des b , il est facile de décider si, selon les règles ci-dessus, $w = 1$. (C'est un exercice pour vous !)

Étant donnés n générateurs g_1, \dots, g_n et p relations r_1, \dots, r_p , il n'existe aucun programme général qui permette de décider si un mot w formé avec g_1, \dots, g_n vérifie $w = 1$.

Ce théorème est dû à Dehn, Post, Novikov, Boone, Britton.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Le problème des mots

On fixe “deux générateurs” a, b et des règles (“trois relations”) portant sur ces générateurs:

$$a^2 = 1, \quad b^2 = 1, \quad ab = ba.$$

Est-ce que $abababab = 1$? On voit facilement que oui.

Est-ce que $ababababab = 1$? On voit facilement que non.

Plus généralement, si l'on forme un “mot” w avec des a et des b , il est facile de décider si, selon les règles ci-dessus, $w = 1$. (C'est un exercice pour vous !)

Étant donnés n générateurs g_1, \dots, g_n et p relations r_1, \dots, r_p , il n'existe aucun programme général qui permette de décider si un mot w formé avec g_1, \dots, g_n vérifie $w = 1$.

Ce théorème est dû à Dehn, Post, Novikov, Boone, Britton.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Le problème des mots

On fixe “deux générateurs” a, b et des règles (“trois relations”) portant sur ces générateurs:

$$a^2 = 1, \quad b^2 = 1, \quad ab = ba.$$

Est-ce que $abababab = 1$? On voit facilement que oui.

Est-ce que $ababababab = 1$? On voit facilement que non.

Plus généralement, si l'on forme un “mot” w avec des a et des b , il est facile de décider si, selon les règles ci-dessus, $w = 1$. (C'est un exercice pour vous !)

Étant donnés n générateurs g_1, \dots, g_n et p relations r_1, \dots, r_p , il n'existe aucun programme général qui permette de décider si un mot w formé avec g_1, \dots, g_n vérifie $w = 1$.

Ce théorème est dû à Dehn, Post, Novikov, Boone, Britton.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Le problème des mots

On fixe “deux générateurs” a, b et des règles (“trois relations”) portant sur ces générateurs:

$$a^2 = 1, \quad b^2 = 1, \quad ab = ba.$$

Est-ce que $abababab = 1$? On voit facilement que oui.

Est-ce que $ababababab = 1$? On voit facilement que non.

Plus généralement, si l'on forme un “mot” w avec des a et des b , il est facile de décider si, selon les règles ci-dessus, $w = 1$. (C'est un exercice pour vous !)

Étant donnés n générateurs g_1, \dots, g_n et p relations r_1, \dots, r_p , il n'existe aucun programme général qui permette de décider si un mot w formé avec g_1, \dots, g_n vérifie $w = 1$.

Ce théorème est dû à Dehn, Post, Novikov, Boone, Britton.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Le dixième problème de Hilbert

Existe-t'il $a, b, c \in \mathbf{N}^*$ tels que $a^2 + b^2 = c^2$? (Oui, facile: il y a une infinité de "triplets pythagoriciens".) Existe-t'il

$a, b, c \in \mathbf{N}^*$ tels que $a^4 + b^4 = c^4$? (Non, pas très facile, prouvé par Fermat.) Existe-t'il $a, b, c \in \mathbf{N}^*$ tels que $a^3 + b^3 = c^3$? (Non, encore plus difficile, prouvé par Euler.)

Pour quels n existe-t'il $a, b, c \in \mathbf{N}^*$ tels que $a^n + b^n = c^n$? (Seulement pour $n = 1, 2$, très difficile, conjecturé par Fermat et prouvé par Wiles.)

Pour une "équation diophantienne" (autrement dit, on veut des solutions entières) complètement générale, il n'existe aucun algorithme permettant de décider si elle admet des solutions.

Ce théorème est dû à Martin Davis, Yuri Matiyasevich, Hilary Putnam et Julia Robinson.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Le dixième problème de Hilbert

Existe-t'il $a, b, c \in \mathbf{N}^*$ tels que $a^2 + b^2 = c^2$? (Oui, facile: il y a une infinité de "triplets pythagoriciens".) Existe-t'il $a, b, c \in \mathbf{N}^*$ tels que $a^4 + b^4 = c^4$? (Non, pas très facile, prouvé par Fermat.) Existe-t'il $a, b, c \in \mathbf{N}^*$ tels que $a^3 + b^3 = c^3$? (Non, encore plus difficile, prouvé par Euler.)

Pour quels n existe-t'il $a, b, c \in \mathbf{N}^*$ tels que $a^n + b^n = c^n$? (Seulement pour $n = 1, 2$, très difficile, conjecturé par Fermat et prouvé par Wiles.)

Pour une "équation diophantienne" (autrement dit, on veut des solutions entières) complètement générale, il n'existe aucun algorithme permettant de décider si elle admet des solutions.

Ce théorème est dû à Martin Davis, Yuri Matiyasevich, Hilary Putnam et Julia Robinson.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Le dixième problème de Hilbert

Existe-t'il $a, b, c \in \mathbf{N}^*$ tels que $a^2 + b^2 = c^2$? (Oui, facile: il y a une infinité de "triplets pythagoriciens".) Existe-t'il $a, b, c \in \mathbf{N}^*$ tels que $a^4 + b^4 = c^4$? (Non, pas très facile, prouvé par Fermat.) Existe-t'il $a, b, c \in \mathbf{N}^*$ tels que $a^3 + b^3 = c^3$? (Non, encore plus difficile, prouvé par Euler.)

Pour quels n existe-t'il $a, b, c \in \mathbf{N}^*$ tels que $a^n + b^n = c^n$? (Seulement pour $n = 1, 2$, très difficile, conjecturé par Fermat et prouvé par Wiles.)

Pour une "équation diophantienne" (autrement dit, on veut des solutions entières) complètement générale, il n'existe aucun algorithme permettant de décider si elle admet des solutions.

Ce théorème est dû à Martin Davis, Yuri Matiyasevich, Hilary Putnam et Julia Robinson.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Le dixième problème de Hilbert

Existe-t'il $a, b, c \in \mathbf{N}^*$ tels que $a^2 + b^2 = c^2$? (Oui, facile: il y a une infinité de "triplets pythagoriciens".) Existe-t'il $a, b, c \in \mathbf{N}^*$ tels que $a^4 + b^4 = c^4$? (Non, pas très facile, prouvé par Fermat.) Existe-t'il $a, b, c \in \mathbf{N}^*$ tels que $a^3 + b^3 = c^3$? (Non, encore plus difficile, prouvé par Euler.)

Pour quels n existe-t'il $a, b, c \in \mathbf{N}^*$ tels que $a^n + b^n = c^n$? (Seulement pour $n = 1, 2$, très difficile, conjecturé par Fermat et prouvé par Wiles.)

Pour une "équation diophantienne" (autrement dit, on veut des solutions entières) complètement générale, il n'existe aucun algorithme permettant de décider si elle admet des solutions.

Ce théorème est dû à Martin Davis, Yuri Matiyasevich, Hilary Putnam et Julia Robinson.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Le dixième problème de Hilbert

Existe-t'il $a, b, c \in \mathbf{N}^*$ tels que $a^2 + b^2 = c^2$? (Oui, facile: il y a une infinité de "triplets pythagoriciens".) Existe-t'il $a, b, c \in \mathbf{N}^*$ tels que $a^4 + b^4 = c^4$? (Non, pas très facile, prouvé par Fermat.) Existe-t'il $a, b, c \in \mathbf{N}^*$ tels que $a^3 + b^3 = c^3$? (Non, encore plus difficile, prouvé par Euler.)

Pour quels n existe-t'il $a, b, c \in \mathbf{N}^*$ tels que $a^n + b^n = c^n$? (Seulement pour $n = 1, 2$, très difficile, conjecturé par Fermat et prouvé par Wiles.)

Pour une "équation diophantienne" (autrement dit, on veut des solutions entières) complètement générale, il n'existe aucun algorithme permettant de décider si elle admet des solutions.

Ce théorème est dû à Martin Davis, Yuri Matiyasevich, Hilary Putnam et Julia Robinson.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Le dixième problème de Hilbert

Existe-t'il $a, b, c \in \mathbf{N}^*$ tels que $a^2 + b^2 = c^2$? (Oui, facile: il y a une infinité de "triplets pythagoriciens".) Existe-t'il $a, b, c \in \mathbf{N}^*$ tels que $a^4 + b^4 = c^4$? (Non, pas très facile, prouvé par Fermat.) Existe-t'il $a, b, c \in \mathbf{N}^*$ tels que $a^3 + b^3 = c^3$? (Non, encore plus difficile, prouvé par Euler.)

Pour quels n existe-t'il $a, b, c \in \mathbf{N}^*$ tels que $a^n + b^n = c^n$? (Seulement pour $n = 1, 2$, très difficile, conjecturé par Fermat et prouvé par Wiles.)

Pour une "équation diophantienne" (autrement dit, on veut des solutions entières) complètement générale, il n'existe aucun algorithme permettant de décider si elle admet des solutions.

Ce théorème est dû à Martin Davis, Yuri Matiyasevich, Hilary Putnam et Julia Robinson.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Prouvabilité d'un théorème.

Non contradiction d'une théorie

Il est possible de "coder" une théorie mathématique de telle manière qu'un programme d'ordinateur puisse produire, les unes après les autres, toutes les démonstrations correctes en commençant par les plus courtes.

Ainsi, si un énoncé est correct, un programme peut en produire une démonstration: on énumère (comme ci-dessus) toutes les démonstrations jusqu'à trouver celle que l'on cherche.

Mais si l'énoncé est faux, le programme bouclera indéfiniment: il produira toutes les démonstrations correctes, il y en a une infinité; et l'on ne verra jamais arriver celle que l'on attend.

Voici une ruse: on cherche une preuve de l'énoncé *ou de sa négation*. La première arrivée a gagné !

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Prouvabilité d'un théorème.

Non contradiction d'une théorie

Il est possible de "coder" une théorie mathématique de telle manière qu'un programme d'ordinateur puisse produire, les unes après les autres, toutes les démonstrations correctes en commençant par les plus courtes.

Ainsi, si un énoncé est correct, un programme peut en produire une démonstration: on énumère (comme ci-dessus) toutes les démonstrations jusqu'à trouver celle que l'on cherche.

Mais si l'énoncé est faux, le programme bouclera indéfiniment: il produira toutes les démonstrations correctes, il y en a une infinité; et l'on ne verra jamais arriver celle que l'on attend.

Voici une ruse: on cherche une preuve de l'énoncé *ou de sa négation*. La première arrivée a gagné !

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Prouvabilité d'un théorème.

Non contradiction d'une théorie

Il est possible de "coder" une théorie mathématique de telle manière qu'un programme d'ordinateur puisse produire, les unes après les autres, toutes les démonstrations correctes en commençant par les plus courtes.

Ainsi, si un énoncé est correct, un programme peut en produire une démonstration: on énumère (comme ci-dessus) toutes les démonstrations jusqu'à trouver celle que l'on cherche.

Mais si l'énoncé est faux, le programme bouclera indéfiniment: il produira toutes les démonstrations correctes, il y en a une infinité; et l'on ne verra jamais arriver celle que l'on attend.

Voici une ruse: on cherche une preuve de l'énoncé *ou de sa négation*. La première arrivée a gagné !

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Prouvabilité d'un théorème.

Non contradiction d'une théorie

Il est possible de "coder" une théorie mathématique de telle manière qu'un programme d'ordinateur puisse produire, les unes après les autres, toutes les démonstrations correctes en commençant par les plus courtes.

Ainsi, si un énoncé est correct, un programme peut en produire une démonstration: on énumère (comme ci-dessus) toutes les démonstrations jusqu'à trouver celle que l'on cherche.

Mais si l'énoncé est faux, le programme bouclera indéfiniment: il produira toutes les démonstrations correctes, il y en a une infinité; et l'on ne verra jamais arriver celle que l'on attend.

Voici une ruse: on cherche une preuve de l'énoncé *ou de sa négation*. La première arrivée a gagné !

Prouvabilité d'un théorème.

Non contradiction d'une théorie

Voici une ruse: on cherche une preuve de l'énoncé *ou de sa négation*. La première arrivée a gagné !

Malheureusement, cela ne marche pas: il y a des énoncés A tels que ni A ni sa négation n'admettent de démonstration !
Exemple: il existe un ensemble "strictement plus grand" que \mathbf{N} et "strictement plus petit" que \mathbf{R} . (*Hypothèse du continu*, son indécidabilité a été prouvée par Gödel et Paul Cohen.)

Il n'existe aucun programme permettant de décider si un énoncé est démontrable ou non (Gödel et Turing). De même, il n'existe aucun programme permettant de décider si une théorie est contradictoire ou non (Gödel et Turing).

Attention: ceci n'est pas exact pour les théories "très simples": par exemple la logique propositionnelle. Mais cela s'applique à *toutes* les théories mathématiques usuelles.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Prouvabilité d'un théorème.

Non contradiction d'une théorie

Voici une ruse: on cherche une preuve de l'énoncé *ou de sa négation*. La première arrivée a gagné !

Malheureusement, cela ne marche pas: il y a des énoncés A tels que ni A ni sa négation n'admettent de démonstration !

Exemple: il existe un ensemble "strictement plus grand" que \mathbf{N} et "strictement plus petit" que \mathbf{R} . (*Hypothèse du continu*, son indécidabilité a été prouvée par Gödel et Paul Cohen.)

Il n'existe aucun programme permettant de décider si un énoncé est démontrable ou non (Gödel et Turing). De même, il n'existe aucun programme permettant de décider si une théorie est contradictoire ou non (Gödel et Turing).

Attention: ceci n'est pas exact pour les théories "très simples": par exemple la logique propositionnelle. Mais cela s'applique à *toutes* les théories mathématiques usuelles.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Prouvabilité d'un théorème.

Non contradiction d'une théorie

Voici une ruse: on cherche une preuve de l'énoncé *ou de sa négation*. La première arrivée a gagné !

Malheureusement, cela ne marche pas: il y a des énoncés A tels que ni A ni sa négation n'admettent de démonstration !
Exemple: il existe un ensemble "strictement plus grand" que \mathbf{N} et "strictement plus petit" que \mathbf{R} . (*Hypothèse du continu*, son indécidabilité a été prouvée par Gödel et Paul Cohen.)

Il n'existe aucun programme permettant de décider si un énoncé est démontrable ou non (Gödel et Turing). De même, il n'existe aucun programme permettant de décider si une théorie est contradictoire ou non (Gödel et Turing).

Attention: ceci n'est pas exact pour les théories "très simples": par exemple la logique propositionnelle. Mais cela s'applique à *toutes* les théories mathématiques usuelles.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Prouvabilité d'un théorème.

Non contradiction d'une théorie

Voici une ruse: on cherche une preuve de l'énoncé *ou de sa négation*. La première arrivée a gagné !

Malheureusement, cela ne marche pas: il y a des énoncés A tels que ni A ni sa négation n'admettent de démonstration !
Exemple: il existe un ensemble "strictement plus grand" que \mathbf{N} et "strictement plus petit" que \mathbf{R} . (*Hypothèse du continu*, son indécidabilité a été prouvée par Gödel et Paul Cohen.)

Il n'existe aucun programme permettant de décider si un énoncé est démontrable ou non (Gödel et Turing). De même, il n'existe aucun programme permettant de décider si une théorie est contradictoire ou non (Gödel et Turing).

Attention: ceci n'est pas exact pour les théories "très simples": par exemple la logique propositionnelle. Mais cela s'applique à *toutes* les théories mathématiques usuelles.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Prouvabilité d'un théorème.

Non contradiction d'une théorie

Voici une ruse: on cherche une preuve de l'énoncé *ou de sa négation*. La première arrivée a gagné !

Malheureusement, cela ne marche pas: il y a des énoncés A tels que ni A ni sa négation n'admettent de démonstration !
Exemple: il existe un ensemble "strictement plus grand" que \mathbf{N} et "strictement plus petit" que \mathbf{R} . (*Hypothèse du continu*, son indécidabilité a été prouvée par Gödel et Paul Cohen.)

Il n'existe aucun programme permettant de décider si un énoncé est démontrable ou non (Gödel et Turing). De même, il n'existe aucun programme permettant de décider si une théorie est contradictoire ou non (Gödel et Turing).

Attention: ceci n'est pas exact pour les théories "très simples": par exemple la logique propositionnelle. Mais cela s'applique à *toutes* les théories mathématiques usuelles.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Prouvabilité d'un théorème.

Non contradiction d'une théorie

Voici une ruse: on cherche une preuve de l'énoncé *ou de sa négation*. La première arrivée a gagné !

Malheureusement, cela ne marche pas: il y a des énoncés A tels que ni A ni sa négation n'admettent de démonstration !
Exemple: il existe un ensemble "strictement plus grand" que \mathbf{N} et "strictement plus petit" que \mathbf{R} . (*Hypothèse du continu*, son indécidabilité a été prouvée par Gödel et Paul Cohen.)

Il n'existe aucun programme permettant de décider si un énoncé est démontrable ou non (Gödel et Turing). De même, il n'existe aucun programme permettant de décider si une théorie est contradictoire ou non (Gödel et Turing).

Attention: ceci n'est pas exact pour les théories "très simples": par exemple la logique propositionnelle. Mais cela s'applique à *toutes* les théories mathématiques usuelles.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction



P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Plan

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Il y a mieux que faisable

Parlons maintenant de choses qui marchent !

On a déjà vu un exemple de problème qui avait l'air "infaisable" mais qui ne l'était pas: résoudre un système de n équations à n inconnues.

À la chacal: environ $n! \simeq (n/e)^n \sqrt{2\pi n}$ opérations (donc coût bien pire qu'exponentiel, à cause du n^n).

Via le pivot de Gauß: environ n^3 opérations (donc coût polynomial).

Il y a beaucoup de cas où l'on sait améliorer l'approche brutale et remplacer un *algorithme* infaisable par un algorithme raisonnable.

Il faut donc distinguer *problème* infaisable de *méthode* infaisable pour un problème donné.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Il y a mieux que faisable

Parlons maintenant de choses qui marchent !

On a déjà vu un exemple de problème qui avait l'air "infaisable" mais qui ne l'était pas: résoudre un système de n équations à n inconnues.

À la chacal: environ $n! \simeq (n/e)^n \sqrt{2\pi n}$ opérations (donc coût bien pire qu'exponentiel, à cause du n^n).

Via le pivot de Gauß: environ n^3 opérations (donc coût polynomial).

Il y a beaucoup de cas où l'on sait améliorer l'approche brutale et remplacer un *algorithme* infaisable par un algorithme raisonnable.

Il faut donc distinguer *problème* infaisable de *méthode* infaisable pour un problème donné.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Il y a mieux que faisable

Parlons maintenant de choses qui marchent !

On a déjà vu un exemple de problème qui avait l'air "infaisable" mais qui ne l'était pas: résoudre un système de n équations à n inconnues.

À la chacal: environ $n! \simeq (n/e)^n \sqrt{2\pi n}$ opérations (donc coût bien pire qu'exponentiel, à cause du n^n).

Via le pivot de Gauß: environ n^3 opérations (donc coût polynomial).

Il y a beaucoup de cas où l'on sait améliorer l'approche brutale et remplacer un *algorithme* infaisable par un algorithme raisonnable.

Il faut donc distinguer *problème* infaisable de *méthode* infaisable pour un problème donné.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Il y a mieux que faisable

Parlons maintenant de choses qui marchent !

On a déjà vu un exemple de problème qui avait l'air "infaisable" mais qui ne l'était pas: résoudre un système de n équations à n inconnues.

À la chacal: environ $n! \simeq (n/e)^n \sqrt{2\pi n}$ opérations (donc coût bien pire qu'exponentiel, à cause du n^n).

Via le pivot de Gauß: environ n^3 opérations (donc coût polynomial).

Il y a beaucoup de cas où l'on sait améliorer l'approche brutale et remplacer un *algorithme* infaisable par un algorithme raisonnable.

Il faut donc distinguer *problème* infaisable de *méthode* infaisable pour un problème donné.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Il y a mieux que faisable

Parlons maintenant de choses qui marchent !

On a déjà vu un exemple de problème qui avait l'air "infaisable" mais qui ne l'était pas: résoudre un système de n équations à n inconnues.

À la chacal: environ $n! \simeq (n/e)^n \sqrt{2\pi n}$ opérations (donc coût bien pire qu'exponentiel, à cause du n^n).

Via le pivot de Gauß: environ n^3 opérations (donc coût polynomial).

Il y a beaucoup de cas où l'on sait améliorer l'approche brutale et remplacer un *algorithme* infaisable par un *algorithme* raisonnable.

Il faut donc distinguer *problème* infaisable de *méthode* infaisable pour un problème donné.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Il y a mieux que faisable

Parlons maintenant de choses qui marchent !

On a déjà vu un exemple de problème qui avait l'air "infaisable" mais qui ne l'était pas: résoudre un système de n équations à n inconnues.

À la chacal: environ $n! \simeq (n/e)^n \sqrt{2\pi n}$ opérations (donc coût bien pire qu'exponentiel, à cause du n^n).

Via le pivot de Gauß: environ n^3 opérations (donc coût polynomial).

Il y a beaucoup de cas où l'on sait améliorer l'approche brutale et remplacer un *algorithme* infaisable par un algorithme raisonnable.

Il faut donc distinguer *problème* infaisable de *méthode* infaisable pour un problème donné.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Multiplication dichotomique

Lorsque l'on veut tester la primalité d'un nombre n (par exemple en vue d'un cryptage RSA), on est amené à calculer des puissances a^m avec m proche de n . En principe, n est grand, il s'écrit sur N bits où $N \simeq$ quelques centaines.

Calculer $a^m = a \times \dots \times a$ demande $(m - 1)$ multiplications. Si le nombre de bits de n est $N = 100$ par exemple, et que m en est proche, cela représente environ $2^{100} \simeq 10^{30}$ soit mille milliards de milliards de milliards de multiplications.

L'idée de la multiplication dichotomique est (sur un exemple) la suivante: $a^{50} = a^{25} \times a^{25}$, $a^{25} = a^{12} \times a^{12} \times a$, $a^{12} = a^6 \times a^6$, $a^6 = a^3 \times a^3$, $a^3 = a \times a \times a$. Donc ici 7 multiplications au lieu de 49.

Pour $N = 100$, il faudra entre 100 et 200 multiplications au lieu de mille milliards de milliards de milliards.

En général, il faut entre N et $2N$ multiplications et non 2^N : le coût est passé de exponentiel à linéaire en la taille N de n .

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Multiplication dichotomique

Lorsque l'on veut tester la primalité d'un nombre n (par exemple en vue d'un cryptage RSA), on est amené à calculer des puissances a^m avec m proche de n . En principe, n est grand, il s'écrit sur N bits où $N \simeq$ quelques centaines.

Calculer $a^m = a \times \dots \times a$ demande $(m - 1)$ multiplications. Si le nombre de bits de n est $N = 100$ par exemple, et que m en est proche, cela représente environ $2^{100} \simeq 10^{30}$ soit mille milliards de milliards de milliards de multiplications.

L'idée de la multiplication dichotomique est (sur un exemple) la suivante: $a^{50} = a^{25} \times a^{25}$, $a^{25} = a^{12} \times a^{12} \times a$, $a^{12} = a^6 \times a^6$, $a^6 = a^3 \times a^3$, $a^3 = a \times a \times a$. Donc ici 7 multiplications au lieu de 49.

Pour $N = 100$, il faudra entre 100 et 200 multiplications au lieu de mille milliards de milliards de milliards.

En général, il faut entre N et $2N$ multiplications et non 2^N : le coût est passé de exponentiel à linéaire en la taille N de n .

Multiplication dichotomique

Lorsque l'on veut tester la primalité d'un nombre n (par exemple en vue d'un cryptage RSA), on est amené à calculer des puissances a^m avec m proche de n . En principe, n est grand, il s'écrit sur N bits où $N \simeq$ quelques centaines.

Calculer $a^m = a \times \dots \times a$ demande $(m - 1)$ multiplications. Si le nombre de bits de n est $N = 100$ par exemple, et que m en est proche, cela représente environ $2^{100} \simeq 10^{30}$ soit mille milliards de milliards de milliards de multiplications.

L'idée de la multiplication dichotomique est (sur un exemple) la suivante: $a^{50} = a^{25} \times a^{25}$, $a^{25} = a^{12} \times a^{12} \times a$, $a^{12} = a^6 \times a^6$, $a^6 = a^3 \times a^3$, $a^3 = a \times a \times a$. Donc ici 7 multiplications au lieu de 49.

Pour $N = 100$, il faudra entre 100 et 200 multiplications au lieu de mille milliards de milliards de milliards.

En général, il faut entre N et $2N$ multiplications et non 2^N : le coût est passé de exponentiel à linéaire en la taille N de n .

Multiplication dichotomique

Lorsque l'on veut tester la primalité d'un nombre n (par exemple en vue d'un cryptage RSA), on est amené à calculer des puissances a^m avec m proche de n . En principe, n est grand, il s'écrit sur N bits où $N \simeq$ quelques centaines.

Calculer $a^m = a \times \dots \times a$ demande $(m - 1)$ multiplications. Si le nombre de bits de n est $N = 100$ par exemple, et que m en est proche, cela représente environ $2^{100} \simeq 10^{30}$ soit mille milliards de milliards de milliards de multiplications.

L'idée de la multiplication dichotomique est (sur un exemple) la suivante: $a^{50} = a^{25} \times a^{25}$, $a^{25} = a^{12} \times a^{12} \times a$, $a^{12} = a^6 \times a^6$, $a^6 = a^3 \times a^3$, $a^3 = a \times a \times a$. Donc ici 7 multiplications au lieu de 49.

Pour $N = 100$, il faudra entre 100 et 200 multiplications au lieu de mille milliards de milliards de milliards.

En général, il faut entre N et $2N$ multiplications et non 2^N : le coût est passé de exponentiel à linéaire en la taille N de n .

Multiplication dichotomique

Lorsque l'on veut tester la primalité d'un nombre n (par exemple en vue d'un cryptage RSA), on est amené à calculer des puissances a^m avec m proche de n . En principe, n est grand, il s'écrit sur N bits où $N \simeq$ quelques centaines.

Calculer $a^m = a \times \dots \times a$ demande $(m - 1)$ multiplications. Si le nombre de bits de n est $N = 100$ par exemple, et que m en est proche, cela représente environ $2^{100} \simeq 10^{30}$ soit mille milliards de milliards de milliards de multiplications.

L'idée de la multiplication dichotomique est (sur un exemple) la suivante: $a^{50} = a^{25} \times a^{25}$, $a^{25} = a^{12} \times a^{12} \times a$, $a^{12} = a^6 \times a^6$, $a^6 = a^3 \times a^3$, $a^3 = a \times a \times a$. Donc ici 7 multiplications au lieu de 49.

Pour $N = 100$, il faudra entre 100 et 200 multiplications au lieu de mille milliards de milliards de milliards.

En général, il faut entre N et $2N$ multiplications et non 2^N : le coût est passé de exponentiel à linéaire en la taille N de n .

Primalité quasi-polynomiale

Il y a aussi de faux coûts exponentiels.

Pendant longtemps, le meilleur test de primalité connu a été celui de Adleman, Pomerance et Rumely (Adleman est le A de RSA). Pour un entier n de taille environ $N = \ln n$, son coût est de l'ordre de $N^{c \ln \ln \ln n}$ où c est une constante strictement positive. L'exposant $c \ln \ln \ln n$ tend vers l'infini, ce n'est donc pas un coût polynomial.

Mais la fonction $\ln \ln \ln n$ croît *très* lentement.

Si l'on prend par exemple $n := 5 \cdot 10^{24}$ (âge de l'univers compté en nanosecondes), on trouve que $\ln \ln \ln n \simeq 1,4$.

Si l'on prend $n := 10^{500}$ (ce qui est bien plus grand que les clés de cryptage de RSA), on trouve que $\ln \ln \ln n \simeq 1,95$.

On peut donc raisonnablement parler de coût quasi-polynomial.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Primalité quasi-polynomiale

Il y a aussi de faux coûts exponentiels.

Pendant longtemps, le meilleur test de primalité connu a été celui de Adleman, Pomerance et Rumely (Adleman est le A de RSA). Pour un entier n de taille environ $N = \ln n$, son coût est de l'ordre de $N^{c \ln \ln \ln n}$ où c est une constante strictement positive. L'exposant $c \ln \ln \ln n$ tend vers l'infini, ce n'est donc pas un coût polynomial.

Mais la fonction $\ln \ln \ln n$ croît *très* lentement.

Si l'on prend par exemple $n := 5 \cdot 10^{24}$ (âge de l'univers compté en nanosecondes), on trouve que $\ln \ln \ln n \simeq 1,4$.

Si l'on prend $n := 10^{500}$ (ce qui est bien plus grand que les clés de cryptage de RSA), on trouve que $\ln \ln \ln n \simeq 1,95$.

On peut donc raisonnablement parler de coût quasi-polynomial.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Primalité quasi-polynomiale

Il y a aussi de faux coûts exponentiels.

Pendant longtemps, le meilleur test de primalité connu a été celui de Adleman, Pomerance et Rumely (Adleman est le A de RSA). Pour un entier n de taille environ $N = \ln n$, son coût est de l'ordre de $N^{c \ln \ln \ln n}$ où c est une constante strictement positive. L'exposant $c \ln \ln \ln n$ tend vers l'infini, ce n'est donc pas un coût polynomial.

Mais la fonction $\ln \ln \ln n$ croît *très* lentement.

Si l'on prend par exemple $n := 5 \cdot 10^{24}$ (âge de l'univers compté en nanosecondes), on trouve que $\ln \ln \ln n \simeq 1,4$.

Si l'on prend $n := 10^{500}$ (ce qui est bien plus grand que les clés de cryptage de RSA), on trouve que $\ln \ln \ln n \simeq 1,95$.

On peut donc raisonnablement parler de coût quasi-polynomial.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Primalité quasi-polynomiale

Il y a aussi de faux coûts exponentiels.

Pendant longtemps, le meilleur test de primalité connu a été celui de Adleman, Pomerance et Rumely (Adleman est le A de RSA). Pour un entier n de taille environ $N = \ln n$, son coût est de l'ordre de $N^{c \ln \ln \ln n}$ où c est une constante strictement positive. L'exposant $c \ln \ln \ln n$ tend vers l'infini, ce n'est donc pas un coût polynomial.

Mais la fonction $\ln \ln \ln n$ croît *très* lentement.

Si l'on prend par exemple $n := 5 \cdot 10^{24}$ (âge de l'univers compté en nanosecondes), on trouve que $\ln \ln \ln n \simeq 1,4$.

Si l'on prend $n := 10^{500}$ (ce qui est bien plus grand que les clés de cryptage de RSA), on trouve que $\ln \ln \ln n \simeq 1,95$.

On peut donc raisonnablement parler de coût quasi-polynomial.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Primalité quasi-polynomiale

Il y a aussi de faux coûts exponentiels.

Pendant longtemps, le meilleur test de primalité connu a été celui de Adleman, Pomerance et Rumely (Adleman est le A de RSA). Pour un entier n de taille environ $N = \ln n$, son coût est de l'ordre de $N^{c \ln \ln \ln n}$ où c est une constante strictement positive. L'exposant $c \ln \ln \ln n$ tend vers l'infini, ce n'est donc pas un coût polynomial.

Mais la fonction $\ln \ln \ln n$ croît *très* lentement.

Si l'on prend par exemple $n := 5 \cdot 10^{24}$ (âge de l'univers compté en nanosecondes), on trouve que $\ln \ln \ln n \simeq 1,4$.

Si l'on prend $n := 10^{500}$ (ce qui est bien plus grand que les clés de cryptage de RSA), on trouve que $\ln \ln \ln n \simeq 1,95$.

On peut donc raisonnablement parler de coût quasi-polynomial.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Primalité quasi-polynomiale

Il y a aussi de faux coûts exponentiels.

Pendant longtemps, le meilleur test de primalité connu a été celui de Adleman, Pomerance et Rumely (Adleman est le A de RSA). Pour un entier n de taille environ $N = \ln n$, son coût est de l'ordre de $N^{c \ln \ln \ln n}$ où c est une constante strictement positive. L'exposant $c \ln \ln \ln n$ tend vers l'infini, ce n'est donc pas un coût polynomial.

Mais la fonction $\ln \ln \ln n$ croît *très* lentement.

Si l'on prend par exemple $n := 5 \cdot 10^{24}$ (âge de l'univers compté en nanosecondes), on trouve que $\ln \ln \ln n \simeq 1,4$.

Si l'on prend $n := 10^{500}$ (ce qui est bien plus grand que les clés de cryptage de RSA), on trouve que $\ln \ln \ln n \simeq 1,95$.

On peut donc raisonnablement parler de coût quasi-polynomial.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Primalité quasi-polynomiale

Il y a aussi de faux coûts exponentiels.

Pendant longtemps, le meilleur test de primalité connu a été celui de Adleman, Pomerance et Rumely (Adleman est le A de RSA). Pour un entier n de taille environ $N = \ln n$, son coût est de l'ordre de $N^{c \ln \ln \ln n}$ où c est une constante strictement positive. L'exposant $c \ln \ln \ln n$ tend vers l'infini, ce n'est donc pas un coût polynomial.

Mais la fonction $\ln \ln \ln n$ croît *très* lentement.

Si l'on prend par exemple $n := 5 \cdot 10^{24}$ (âge de l'univers compté en nanosecondes), on trouve que $\ln \ln \ln n \simeq 1,4$.

Si l'on prend $n := 10^{500}$ (ce qui est bien plus grand que les clés de cryptage de RSA), on trouve que $\ln \ln \ln n \simeq 1,95$.

On peut donc raisonnablement parler de coût quasi-polynomial.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Plan

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Cryptographie

La principale méthode de cryptage en usage dans le monde actuel est RSA.

Sa force repose sur la difficulté de factoriser de grands nombres.

Par exemple, on peut utiliser la “clé publique de chiffrement” 15487469. Si quelqu’un trouve deux entiers dont le produit est ce nombre, cette clé n’est plus sûre, elle est “cassée”.

On ne connaît actuellement aucune méthode efficace pour factoriser de grands nombres. C’est un problème NP, on ne sait pas s’il est P.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Cryptographie

P = NP ?

Jacques Sauloy

La principale méthode de cryptage en usage dans le monde actuel est RSA.

Sa force repose sur la difficulté de factoriser de grands nombres.

Par exemple, on peut utiliser la “clé publique de chiffrement” 15487469. Si quelqu’un trouve deux entiers dont le produit est ce nombre, cette clé n’est plus sûre, elle est “cassée”.

On ne connaît actuellement aucune méthode efficace pour factoriser de grands nombres. C’est un problème NP, on ne sait pas s’il est P.

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c’est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Cryptographie

P = NP ?

Jacques Sauloy

La principale méthode de cryptage en usage dans le monde actuel est RSA.

Sa force repose sur la difficulté de factoriser de grands nombres.

Par exemple, on peut utiliser la “clé publique de chiffrement” 15487469. Si quelqu’un trouve deux entiers dont le produit est ce nombre, cette clé n’est plus sûre, elle est “cassée” .

On ne connaît actuellement aucune méthode efficace pour factoriser de grands nombres. C’est un problème NP, on ne sait pas s’il est P.

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Cryptographie

P = NP ?

Jacques Sauloy

La principale méthode de cryptage en usage dans le monde actuel est RSA.

Sa force repose sur la difficulté de factoriser de grands nombres.

Par exemple, on peut utiliser la “clé publique de chiffrement” 15487469. Si quelqu’un trouve deux entiers dont le produit est ce nombre, cette clé n’est plus sûre, elle est “cassée”.

On ne connaît actuellement aucune méthode efficace pour factoriser de grands nombres. C’est un problème NP, on ne sait pas s’il est P.

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c’est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Cryptographie

P = NP ?

Jacques Sauloy

La principale méthode de cryptage en usage dans le monde actuel est RSA.

Sa force repose sur la difficulté de factoriser de grands nombres.

Par exemple, on peut utiliser la “clé publique de chiffrement” 15487469. Si quelqu’un trouve deux entiers dont le produit est ce nombre, cette clé n’est plus sûre, elle est “cassée”.

On ne connaît actuellement aucune méthode efficace pour factoriser de grands nombres. C’est un problème NP, on ne sait pas s’il est P.

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c’est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Difficile, mais jouable

La méthode RSA de chiffrement “à clé publique” a été inventée en 1977 par Ron Rivest, Adi Shamir et Leonard Adleman. Voici comment ils estimaient alors la capacité de résistance de leur méthode:

Table 1

<i>Digits</i>	<i>Number of operations</i>	<i>Time</i>
50	1.4×10^{10}	3.9 hours
75	9.0×10^{12}	104 days
100	2.3×10^{15}	74 years
200	1.2×10^{23}	3.8×10^9 years
300	1.5×10^{29}	4.9×10^{15} years
500	1.3×10^{39}	4.2×10^{25} years

Noter qu'il ne va pas de soi de prendre de grandes clés de chiffrement, ce n'est pas “gratuit”. En effet:

1. Il faut les produire (ce sont des produits de deux grands nombres premiers et non des nombres quelconques).
2. Plus elles sont grandes, plus leur usage coûte du temps de calcul.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Difficile, mais jouable

La méthode RSA de chiffrement “à clé publique” a été inventée en 1977 par Ron Rivest, Adi Shamir et Leonard Adleman. Voici comment ils estimaient alors la capacité de résistance de leur méthode:

Table 1

<i>Digits</i>	<i>Number of operations</i>	<i>Time</i>
50	1.4×10^{10}	3.9 hours
75	9.0×10^{12}	104 days
100	2.3×10^{15}	74 years
200	1.2×10^{23}	3.8×10^9 years
300	1.5×10^{29}	4.9×10^{15} years
500	1.3×10^{39}	4.2×10^{25} years

Noter qu'il ne va pas de soi de prendre de grandes clés de chiffrement, ce n'est pas “gratuit”. En effet:

1. Il faut les produire (ce sont des produits de deux grands nombres premiers et non des nombres quelconques).
2. Plus elles sont grandes, plus leur usage coûte du temps de calcul.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Difficile, mais jouable

La méthode RSA de chiffrement “à clé publique” a été inventée en 1977 par Ron Rivest, Adi Shamir et Leonard Adleman. Voici comment ils estimaient alors la capacité de résistance de leur méthode:

Table 1

<i>Digits</i>	<i>Number of operations</i>	<i>Time</i>
50	1.4×10^{10}	3.9 hours
75	9.0×10^{12}	104 days
100	2.3×10^{15}	74 years
200	1.2×10^{23}	3.8×10^9 years
300	1.5×10^{29}	4.9×10^{15} years
500	1.3×10^{39}	4.2×10^{25} years

Noter qu'il ne va pas de soi de prendre de grandes clés de chiffrement, ce n'est pas “gratuit”. En effet:

1. Il faut les produire (ce sont des produits de deux grands nombres premiers et non des nombres quelconques).
2. Plus elles sont grandes, plus leur usage coûte du temps de calcul.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Difficile, mais jouable

La méthode RSA de chiffrement “à clé publique” a été inventée en 1977 par Ron Rivest, Adi Shamir et Leonard Adleman. Voici comment ils estimaient alors la capacité de résistance de leur méthode:

Table 1

<i>Digits</i>	<i>Number of operations</i>	<i>Time</i>
50	1.4×10^{10}	3.9 hours
75	9.0×10^{12}	104 days
100	2.3×10^{15}	74 years
200	1.2×10^{23}	3.8×10^9 years
300	1.5×10^{29}	4.9×10^{15} years
500	1.3×10^{39}	4.2×10^{25} years

Noter qu'il ne va pas de soi de prendre de grandes clés de chiffrement, ce n'est pas “gratuit”. En effet:

1. Il faut les produire (ce sont des produits de deux grands nombres premiers et non des nombres quelconques).
2. Plus elles sont grandes, plus leur usage coûte du temps de calcul.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Et en progrès

Selon Rivest, Shamir et Adleman, il fallait alors environ quatre milliards d'années pour casser une clé de deux-cents chiffres.

D'après la loi de Moore, il aurait donc fallu en 2005, soit vingt-huit ans plus tard, deux mille ans pour casser une telle clé.

Des clés de deux-cents chiffres ont été cassées en 2005.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Et en progrès

Selon Rivest, Shamir et Adleman, il fallait alors environ quatre milliards d'années pour casser une clé de deux-cents chiffres.

D'après la loi de Moore, il aurait donc fallu en 2005, soit vingt-huit ans plus tard, deux mille ans pour casser une telle clé.

Des clés de deux-cents chiffres ont été cassées en 2005.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Selon Rivest, Shamir et Adleman, il fallait alors environ quatre milliards d'années pour casser une clé de deux-cents chiffres.

D'après la loi de Moore, il aurait donc fallu en 2005, soit vingt-huit ans plus tard, deux mille ans pour casser une telle clé.

Des clés de deux-cents chiffres ont été cassées en 2005.

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

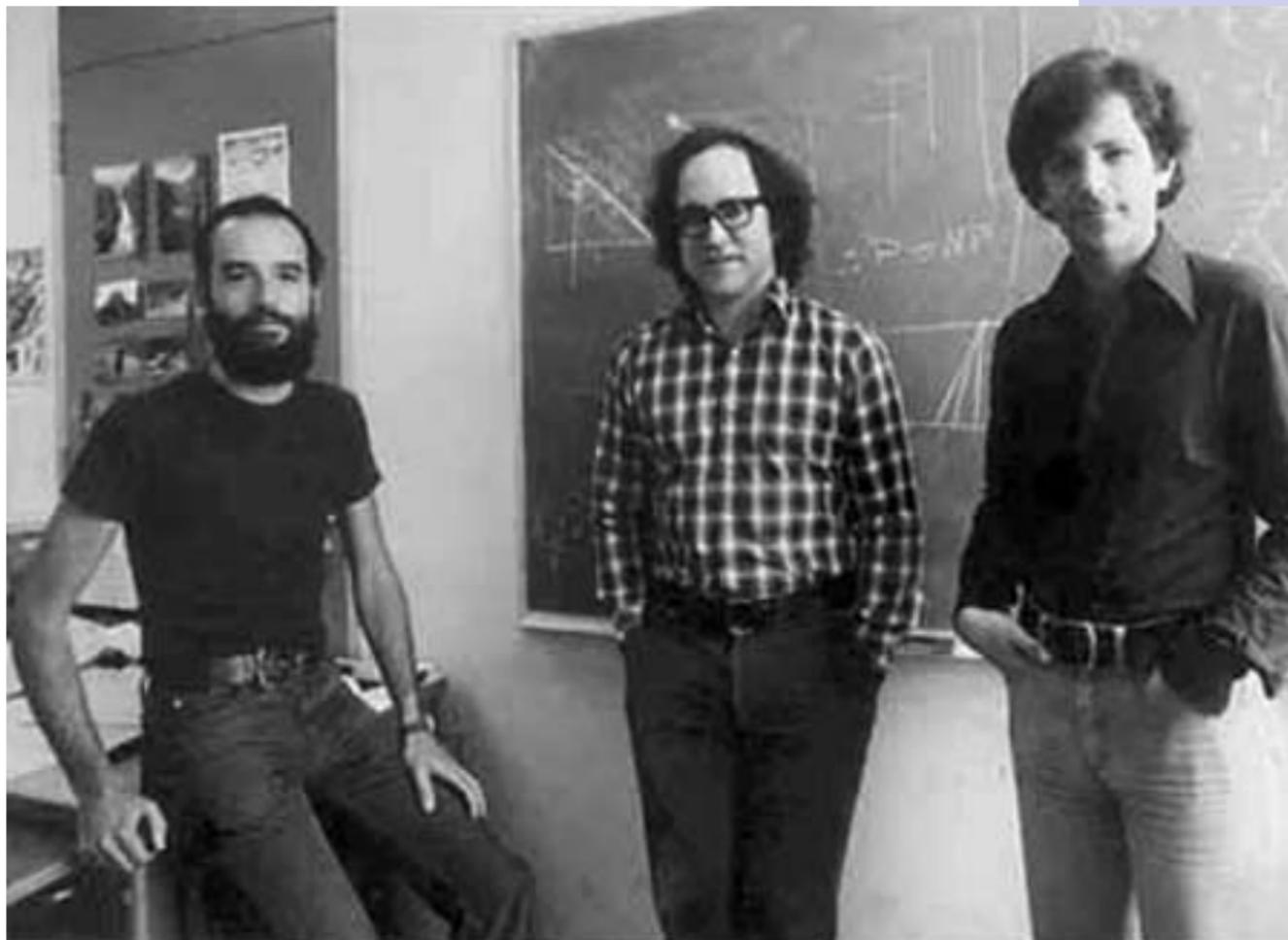
Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction



Où en est-on ?

Voici un relevé récent de l'état de l'art:

RSA Number	Decimal digits	Binary digits	Cash prize offered	Factored on	Factored by
RSA-100	100	330	US\$1,000 ^[4]	April 1, 1991 ^[5]	Arjen K. Lenstra
RSA-110	110	364	US\$4,429 ^[4]	April 14, 1992 ^[5]	Arjen K. Lenstra and M.S. Manasse
RSA-120	120	397	\$5,898 ^[4]	July 9, 1993 ^[6]	T. Denny et al.
RSA-129 ^[**]	129	426	\$100 USD	April 26, 1994 ^[5]	Arjen K. Lenstra et al.
RSA-130	130	430	US\$14,527 ^[4]	April 10, 1996	Arjen K. Lenstra et al.
RSA-140	140	463	US\$17,226	February 2, 1999	Herman te Riele et al.
RSA-150 ^{[*] ?}	150	496		April 16, 2004	Kazumaro Aoki et al.
RSA-155	155	512	\$9,383 ^[4]	August 22, 1999	Herman te Riele et al.
RSA-160	160	530		April 1, 2003	Jens Franke et al., University of Bonn
RSA-170 ^[*]	170	563		December 29, 2009	D. Bonenberger and M. Krone ^[***]
RSA-576	174	576	\$10,000 USD	December 3, 2003	Jens Franke et al., University of Bonn
RSA-180 ^[*]	180	596		May 8, 2010	S. A. Danilov and I. A. Popovyan, Moscow State University ^[7]
RSA-190 ^[*]	190	629		November 8, 2010	A. Timofeev and I. A. Popovyan
RSA-640	193	640	\$20,000 USD	November 2, 2005	Jens Franke et al., University of Bonn
RSA-200 ^{[*] ?}	200	663		May 9, 2005	Jens Franke et al., University of Bonn
RSA-210 ^[*]	210	696		September 26, 2013 ^[8]	Ryan Propper
RSA-704 ^[*]	212	704	\$30,000 USD	July 2, 2012	Shi Bai, Emmanuel Thomé and Paul Zimmermann

Ce n'est pas seulement le progrès technique qui a permis cette évolution.

C'est aussi l'avancée de la théorie mathématique (théorie des nombres, géométrie algébrique).

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Où en est-on ?

Voici un relevé récent de l'état de l'art:

RSA Number	Decimal digits	Binary digits	Cash prize offered	Factored on	Factored by
RSA-100	100	330	US\$1,000 ^[4]	April 1, 1991 ^[5]	Arjen K. Lenstra
RSA-110	110	364	US\$4,429 ^[4]	April 14, 1992 ^[5]	Arjen K. Lenstra and M.S. Manasse
RSA-120	120	397	\$5,898 ^[4]	July 9, 1993 ^[6]	T. Denny et al.
RSA-129 ^[**]	129	426	\$100 USD	April 26, 1994 ^[5]	Arjen K. Lenstra et al.
RSA-130	130	430	US\$14,527 ^[4]	April 10, 1996	Arjen K. Lenstra et al.
RSA-140	140	463	US\$17,226	February 2, 1999	Herman te Riele et al.
RSA-150 ^{[*] ?}	150	496		April 16, 2004	Kazumaro Aoki et al.
RSA-155	155	512	\$9,383 ^[4]	August 22, 1999	Herman te Riele et al.
RSA-160	160	530		April 1, 2003	Jens Franke et al., University of Bonn
RSA-170 ^[*]	170	563		December 29, 2009	D. Bonenberger and M. Krone ^[***]
RSA-576	174	576	\$10,000 USD	December 3, 2003	Jens Franke et al., University of Bonn
RSA-180 ^[*]	180	596		May 8, 2010	S. A. Danilov and I. A. Popovyan, Moscow State University ^[7]
RSA-190 ^[*]	190	629		November 8, 2010	A. Timofeev and I. A. Popovyan
RSA-640	193	640	\$20,000 USD	November 2, 2005	Jens Franke et al., University of Bonn
RSA-200 ^{[*] ?}	200	663		May 9, 2005	Jens Franke et al., University of Bonn
RSA-210 ^[*]	210	696		September 26, 2013 ^[8]	Ryan Propper
RSA-704 ^[*]	212	704	\$30,000 USD	July 2, 2012	Shi Bai, Emmanuel Thomé and Paul Zimmermann

Ce n'est pas seulement le progrès technique qui a permis cette évolution.

C'est aussi l'avancée de la théorie mathématique (théorie des nombres, géométrie algébrique).

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Où en est-on ?

Voici un relevé récent de l'état de l'art:

RSA Number	Decimal digits	Binary digits	Cash prize offered	Factored on	Factored by
RSA-100	100	330	US\$1,000 ^[4]	April 1, 1991 ^[5]	Arjen K. Lenstra
RSA-110	110	364	US\$4,429 ^[4]	April 14, 1992 ^[5]	Arjen K. Lenstra and M.S. Manasse
RSA-120	120	397	\$5,898 ^[4]	July 9, 1993 ^[6]	T. Denny et al.
RSA-129 ^[**]	129	426	\$100 USD	April 26, 1994 ^[5]	Arjen K. Lenstra et al.
RSA-130	130	430	US\$14,527 ^[4]	April 10, 1996	Arjen K. Lenstra et al.
RSA-140	140	463	US\$17,226	February 2, 1999	Herman te Riele et al.
RSA-150 ^{[*] ?}	150	496		April 16, 2004	Kazumaro Aoki et al.
RSA-155	155	512	\$9,383 ^[4]	August 22, 1999	Herman te Riele et al.
RSA-160	160	530		April 1, 2003	Jens Franke et al., University of Bonn
RSA-170 ^[*]	170	563		December 29, 2009	D. Bonenberger and M. Krone ^[***]
RSA-576	174	576	\$10,000 USD	December 3, 2003	Jens Franke et al., University of Bonn
RSA-180 ^[*]	180	596		May 8, 2010	S. A. Danilov and I. A. Popovyan, Moscow State University ^[7]
RSA-190 ^[*]	190	629		November 8, 2010	A. Timofeev and I. A. Popovyan
RSA-640	193	640	\$20,000 USD	November 2, 2005	Jens Franke et al., University of Bonn
RSA-200 ^{[*] ?}	200	663		May 9, 2005	Jens Franke et al., University of Bonn
RSA-210 ^[*]	210	696		September 26, 2013 ^[8]	Ryan Propper
RSA-704 ^[*]	212	704	\$30,000 USD	July 2, 2012	Shi Bai, Emmanuel Thomé and Paul Zimmermann

Ce n'est pas seulement le progrès technique qui a permis cette évolution.

C'est aussi l'avancée de la théorie mathématique (théorie des nombres, géométrie algébrique).

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Plan

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Comment faire quand c'est trop dur mais nécessaire ?

Quand on a prouvé qu'un problème était "infaisable", il peut tout de même arriver qu'on soit obligé de le résoudre.

Plusieurs approches pragmatiques ont été élaborées.

Approche probabiliste: un algorithme efficace donne une réponse *probablement* bonne; mais parfois (rarement) mauvaise.

Autre approche probabiliste: un algorithme efficace donne *probablement* une bonne réponse; mais parfois (rarement) pas de réponse du tout.

Approche approximative: un algorithme efficace donne une réponse raisonnablement proche de la bonne réponse.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Comment faire quand c'est trop dur mais nécessaire ?

Quand on a prouvé qu'un problème était "infaisable", il peut tout de même arriver qu'on soit obligé de le résoudre. Plusieurs approches pragmatiques ont été élaborées.

Approche probabiliste: un algorithme efficace donne une réponse *probablement* bonne; mais parfois (rarement) mauvaise.

Autre approche probabiliste: un algorithme efficace donne *probablement* une bonne réponse; mais parfois (rarement) pas de réponse du tout.

Approche approximative: un algorithme efficace donne une réponse raisonnablement proche de la bonne réponse.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Comment faire quand c'est trop dur mais nécessaire ?

Quand on a prouvé qu'un problème était "infaisable", il peut tout de même arriver qu'on soit obligé de le résoudre. Plusieurs approches pragmatiques ont été élaborées.

Approche probabiliste: un algorithme efficace donne une réponse *probablement* bonne; mais parfois (rarement) mauvaise.

Autre approche probabiliste: un algorithme efficace donne *probablement* une bonne réponse; mais parfois (rarement) pas de réponse du tout.

Approche approximative: un algorithme efficace donne une réponse raisonnablement proche de la bonne réponse.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Comment faire quand c'est trop dur mais nécessaire ?

Quand on a prouvé qu'un problème était "infaisable", il peut tout de même arriver qu'on soit obligé de le résoudre. Plusieurs approches pragmatiques ont été élaborées.

Approche probabiliste: un algorithme efficace donne une réponse *probablement* bonne; mais parfois (rarement) mauvaise.

Autre approche probabiliste: un algorithme efficace donne *probablement* une bonne réponse; mais parfois (rarement) pas de réponse du tout.

Approche approximative: un algorithme efficace donne une réponse raisonnablement proche de la bonne réponse.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Comment faire quand c'est trop dur mais nécessaire ?

Quand on a prouvé qu'un problème était "infaisable", il peut tout de même arriver qu'on soit obligé de le résoudre. Plusieurs approches pragmatiques ont été élaborées.

Approche probabiliste: un algorithme efficace donne une réponse *probablement* bonne; mais parfois (rarement) mauvaise.

Autre approche probabiliste: un algorithme efficace donne *probablement* une bonne réponse; mais parfois (rarement) pas de réponse du tout.

Approche approximative: un algorithme efficace donne une réponse raisonnablement proche de la bonne réponse.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Primalité probabiliste

Miller-Rabin-Solovay-Strassen

On veut savoir si (grand) entier n est premier.

Pour cela, on tire au sort un entier b dans $\{1, \dots, n-1\}$.
(Voir le chapitre "Générateurs aléatoires" du cours "Outils maths discrètes".)

Puis on exécute un certain programme $MRSS(b, n)$ dû aux gens mentionnés ci-dessus.

(En réalité, il y a plusieurs algorithmes apparentés, je simplifie.)

Si n est composé (non premier), le test le dira avec probabilité au moins $1/2$.

Mais il risque de le déclarer premier à tort: faux positif.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Primalité probabiliste

Miller-Rabin-Solovay-Strassen

On veut savoir si (grand) entier n est premier.

Pour cela, on tire au sort un entier b dans $\{1, \dots, n-1\}$.
(Voir le chapitre “Générateurs aléatoires” du cours “Outils maths discrètes”.)

Puis on exécute un certain programme $MRSS(b, n)$ dû aux gens mentionnés ci-dessus.

(En réalité, il y a plusieurs algorithmes apparentés, je simplifie.)

Si n est composé (non premier), le test le dira avec probabilité au moins $1/2$.

Mais il risque de le déclarer premier à tort: faux positif.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Primalité probabiliste

Miller-Rabin-Solovay-Strassen

On veut savoir si (grand) entier n est premier.

Pour cela, on tire au sort un entier b dans $\{1, \dots, n-1\}$.
(Voir le chapitre “Générateurs aléatoires” du cours “Outils maths discrètes”.)

Puis on exécute un certain programme $MRSS(b, n)$ dû aux gens mentionnés ci-dessus.

(En réalité, il y a plusieurs algorithmes apparentés, je simplifie.)

Si n est composé (non premier), le test le dira avec probabilité au moins $1/2$.

Mais il risque de le déclarer premier à tort: faux positif.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Primalité probabiliste

Miller-Rabin-Solovay-Strassen

On veut savoir si (grand) entier n est premier.

Pour cela, on tire au sort un entier b dans $\{1, \dots, n-1\}$.
(Voir le chapitre "Générateurs aléatoires" du cours "Outils maths discrètes".)

Puis on exécute un certain programme $MRSS(b, n)$ dû aux gens mentionnés ci-dessus.

(En réalité, il y a plusieurs algorithmes apparentés, je simplifie.)

Si n est composé (non premier), le test le dira avec probabilité au moins $1/2$.

Mais il risque de le déclarer premier à tort: faux positif.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Primalité probabiliste

Miller-Rabin-Solovay-Strassen

On veut savoir si (grand) entier n est premier.

Pour cela, on tire au sort un entier b dans $\{1, \dots, n-1\}$.
(Voir le chapitre “Générateurs aléatoires” du cours “Outils maths discrètes”.)

Puis on exécute un certain programme $MRSS(b, n)$ dû aux gens mentionnés ci-dessus.

(En réalité, il y a plusieurs algorithmes apparentés, je simplifie.)

Si n est composé (non premier), le test le dira avec probabilité au moins $1/2$.

Mais il risque de le déclarer premier à tort: faux positif.

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Solutions approchées

Le problème du “Bin Packing”.

On dispose d'un certain nombre de boîtes de même taille 1 et de k objets de tailles $a_1, \dots, a_k < 1$.

Si le nombre p de boîtes est fixé: problème de *décision* “peut-on ranger ces k objets dans ces p boîtes ?” Il est NP-complet.

Si l'on veut le nombre minimal de boîtes: problème d'*optimisation*. Encore plus difficile !

Mais il existe un algorithme très simple dans la classe P qui fournit une “2-approximation” (autrement dit, pas plus de 2 fois le minimum).

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Solutions approchées

Le problème du “Bin Packing”.

On dispose d'un certain nombre de boîtes de même taille 1 et de k objets de tailles $a_1, \dots, a_k < 1$.

Si le nombre p de boîtes est fixé: problème de *décision* “peut-on ranger ces k objets dans ces p boîtes ?” Il est NP-complet.

Si l'on veut le nombre minimal de boîtes: problème d'*optimisation*. Encore plus difficile !

Mais il existe un algorithme très simple dans la classe P qui fournit une “2-approximation” (autrement dit, pas plus de 2 fois le minimum).

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Solutions approchées

Le problème du “Bin Packing”.

On dispose d'un certain nombre de boîtes de même taille 1 et de k objets de tailles $a_1, \dots, a_k < 1$.

Si le nombre p de boîtes est fixé: problème de *décision* “peut-on ranger ces k objets dans ces p boîtes ?” Il est NP-complet.

Si l'on veut le nombre minimal de boîtes: problème d'*optimisation*. Encore plus difficile !

Mais il existe un algorithme très simple dans la classe P qui fournit une “2-approximation” (autrement dit, pas plus de 2 fois le minimum).

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Solutions approchées

Le problème du “Bin Packing”.

On dispose d'un certain nombre de boîtes de même taille 1 et de k objets de tailles $a_1, \dots, a_k < 1$.

Si le nombre p de boîtes est fixé: problème de *décision* “peut-on ranger ces k objets dans ces p boîtes ?” Il est NP-complet.

Si l'on veut le nombre minimal de boîtes: problème d'*optimisation*. Encore plus difficile !

Mais il existe un algorithme très simple dans la classe P qui fournit une “2-approximation” (autrement dit, pas plus de 2 fois le minimum).

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Solutions approchées

Le problème du “Bin Packing”.

On dispose d'un certain nombre de boîtes de même taille 1 et de k objets de tailles $a_1, \dots, a_k < 1$.

Si le nombre p de boîtes est fixé: problème de *décision* “peut-on ranger ces k objets dans ces p boîtes ?” Il est NP-complet.

Si l'on veut le nombre minimal de boîtes: problème d'*optimisation*. Encore plus difficile !

Mais il existe un algorithme très simple dans la classe P qui fournit une “2-approximation” (autrement dit, pas plus de 2 fois le minimum).

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Solutions ϵ -approchées

P = NP ?

Jacques Sauloy

Le problème de la “2-partition”.

On dispose de ressources a_1, \dots, a_n que l'on veut partager équitablement en deux paquets de même somme; est-ce possible ?

C'est un problème de décision NP complet.

Pour tout $\epsilon > 0$ on peut obtenir une $(1 + \epsilon)$ -approximation de la solution en temps P.

Et même, le temps de calcul ne s'aggrave pas trop quand $\epsilon \rightarrow 0$ (polynomial en $1/\epsilon$).

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Solutions ϵ -approchées

Le problème de la “2-partition”.

On dispose de ressources a_1, \dots, a_n que l'on veut partager équitablement en deux paquets de même somme; est-ce possible ?

C'est un problème de décision NP complet.

Pour tout $\epsilon > 0$ on peut obtenir une $(1 + \epsilon)$ -approximation de la solution en temps P.

Et même, le temps de calcul ne s'aggrave pas trop quand $\epsilon \rightarrow 0$ (polynomial en $1/\epsilon$).

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Solutions ϵ -approchées

P = NP ?

Jacques Sauloy

Le problème de la “2-partition”.

On dispose de ressources a_1, \dots, a_n que l'on veut partager équitablement en deux paquets de même somme; est-ce possible ?

C'est un problème de décision NP complet.

Pour tout $\epsilon > 0$ on peut obtenir une $(1 + \epsilon)$ -approximation de la solution en temps P.

Et même, le temps de calcul ne s'aggrave pas trop quand $\epsilon \rightarrow 0$ (polynomial en $1/\epsilon$).

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Solutions ϵ -approchées

P = NP ?

Jacques Sauloy

Le problème de la “2-partition”.

On dispose de ressources a_1, \dots, a_n que l'on veut partager équitablement en deux paquets de même somme; est-ce possible ?

C'est un problème de décision NP complet.

Pour tout $\epsilon > 0$ on peut obtenir une $(1 + \epsilon)$ -approximation de la solution en temps P.

Et même, le temps de calcul ne s'aggrave pas trop quand $\epsilon \rightarrow 0$ (polynomial en $1/\epsilon$).

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Solutions ϵ -approchées

P = NP ?

Jacques Sauloy

Le problème de la “2-partition”.

On dispose de ressources a_1, \dots, a_n que l'on veut partager équitablement en deux paquets de même somme; est-ce possible ?

C'est un problème de décision NP complet.

Pour tout $\epsilon > 0$ on peut obtenir une $(1 + \epsilon)$ -approximation de la solution en temps P.

Et même, le temps de calcul ne s'aggrave pas trop quand $\epsilon \rightarrow 0$ (polynomial en $1/\epsilon$).

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Hamilton presque à coup sûr

P = NP ?

Jacques Sauloy

On rappelle que la recherche de circuit hamiltonien est un problème NP-complet.

Un algorithme de classe P dû à Angluin et Valiant fait la chose suivante:

S'il y a un circuit hamiltonien, l'algorithme le dit presque à coup sûr (la probabilité de succès tend vers 1 quand la taille du graphe tend vers l'infini)

Mais il peut ne pas le trouver alors qu'il existe.

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Hamilton presque à coup sûr

P = NP ?

Jacques Sauloy

On rappelle que la recherche de circuit hamiltonien est un problème NP-complet.

Un algorithme de classe P dû à Angluin et Valiant fait la chose suivante:

S'il y a un circuit hamiltonien, l'algorithme le dit presque à coup sûr (la probabilité de succès tend vers 1 quand la taille du graphe tend vers l'infini)

Mais il peut ne pas le trouver alors qu'il existe.

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Hamilton presque à coup sûr

P = NP ?

Jacques Sauloy

On rappelle que la recherche de circuit hamiltonien est un problème NP-complet.

Un algorithme de classe P dû à Angluin et Valiant fait la chose suivante:

S'il y a un circuit hamiltonien, l'algorithme le dit presque à coup sûr (la probabilité de succès tend vers 1 quand la taille du graphe tend vers l'infini)

Mais il peut ne pas le trouver alors qu'il existe.

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Hamilton presque à coup sûr

P = NP ?

Jacques Sauloy

On rappelle que la recherche de circuit hamiltonien est un problème NP-complet.

Un algorithme de classe P dû à Angluin et Valiant fait la chose suivante:

S'il y a un circuit hamiltonien, l'algorithme le dit presque à coup sûr (la probabilité de succès tend vers 1 quand la taille du graphe tend vers l'infini)

Mais il peut ne pas le trouver alors qu'il existe.

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Plan

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Cyber-punk: le calcul analogique

P = NP ?

Jacques Sauloy



Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

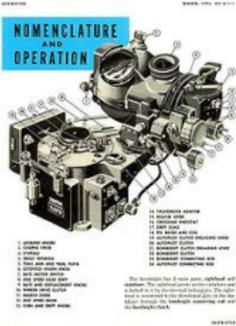
Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Tri



Détection optique de cible, calcul optique de trajectoire

Ordinateur à ADN et circuits hamiltoniens

P = NP ?

Jacques Sauloy

On rappelle à nouveau que la recherche de circuit hamiltonien est un problème NP-complet.

En 1994, Adleman (toujours le même) eut l'idée que les opérations d'insertion, de délétion, etc de l'ADN s'apparentent à un calcul non déterministe.

Il fabriqua un "ordinateur à ADN" spécialisé dans la recherche de circuits hamiltoniens.

Il réussit en une semaine de travaux de laboratoire à trouver un circuit hamiltonien dans un graphe de 7 villes.

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Ordinateur à ADN et circuits hamiltoniens

P = NP ?

Jacques Sauloy

On rappelle à nouveau que la recherche de circuit hamiltonien est un problème NP-complet.

En 1994, Adleman (toujours le même) eut l'idée que les opérations d'insertion, de délétion, etc de l'ADN s'apparentent à un calcul non déterministe.

Il fabriqua un "ordinateur à ADN" spécialisé dans la recherche de circuits hamiltoniens.

Il réussit en une semaine de travaux de laboratoire à trouver un circuit hamiltonien dans un graphe de 7 villes.

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Ordinateur à ADN et circuits hamiltoniens

P = NP ?

Jacques Sauloy

On rappelle à nouveau que la recherche de circuit hamiltonien est un problème NP-complet.

En 1994, Adleman (toujours le même) eut l'idée que les opérations d'insertion, de délétion, etc de l'ADN s'apparentent à un calcul non déterministe.

Il fabriqua un "ordinateur à ADN" spécialisé dans la recherche de circuits hamiltoniens.

Il réussit en une semaine de travaux de laboratoire à trouver un circuit hamiltonien dans un graphe de 7 villes.

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Ordinateur à ADN et circuits hamiltoniens

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

On rappelle à nouveau que la recherche de circuit hamiltonien est un problème NP-complet.

En 1994, Adleman (toujours le même) eut l'idée que les opérations d'insertion, de délétion, etc de l'ADN s'apparentent à un calcul non déterministe.

Il fabriqua un "ordinateur à ADN" spécialisé dans la recherche de circuits hamiltoniens.

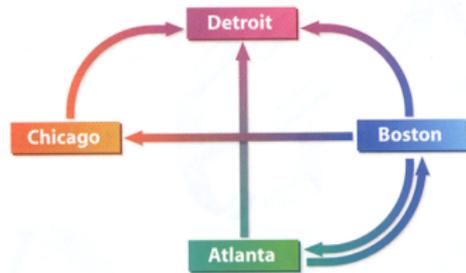
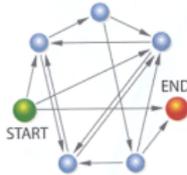
Il réussit en une semaine de travaux de laboratoire à trouver un circuit hamiltonien dans un graphe de 7 villes.

Hamiltonian Path Problem

Consider a map of cities connected by certain nonstop flights (top right). For instance, in the example shown here, it is possible to travel directly from Boston to Detroit but not vice versa. The goal is to determine whether a path exists that will commence at the start city (Atlanta), finish at the end city (Detroit) and pass through each of the remaining cities exactly once. In DNA computation, each city is assigned a DNA sequence (ACTTGCAG for Atlanta) that can be thought of as a first name (ACTT) followed by a last name (GCAG). DNA flight numbers can then be defined by concatenating the last name of the city of origin with the first name of the city of destination (bottom right).

The complementary DNA city names are the Watson-Crick complements of the DNA city names in which every C is replaced by a G, every G by a C, every A by a T, and every T by an A. (To simplify the discussion here, details of the 3' versus 5' ends of the DNA molecules have been omitted.) For this particular problem,

only one Hamiltonian path exists, and it passes through Atlanta, Boston, Chicago and Detroit in that order. In the computation, this path is represented by GCAGTCG-GACTGGGCTATGTCGGA, a DNA sequence of length 24. Shown at the left is the map with seven cities and 14 nonstop flights used in the actual experiment. —L.M.A.



CITY	DNA NAME	COMPLEMENT
ATLANTA	ACTTGCAG	TGAACGTC
BOSTON	TCGGACTG	AGCCTGAC
CHICAGO	GGCTATGT	CCGATACA
DETROIT	CCGAGCAA	GGCTCGTT
FLIGHT	DNA FLIGHT NUMBER	
ATLANTA - BOSTON	GCAGTCGG	
ATLANTA - DETROIT	GCAGCCGA	
BOSTON - CHICAGO	ACTGGGCT	
BOSTON - DETROIT	ACTGCCGA	
BOSTON - ATLANTA	ACTGACTT	
CHICAGO - DETROIT	ATGTCGGA	



P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Ordinateur quantique et factorisation

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Rappel: la factorisation est NP, on ne sait pas si elle est P.

Meilleurs algorithmes déterministes connus pour factoriser un nombre n de taille $b \simeq \log_2 n$ (nombre de bits):

$$O \left(\exp \left(\sqrt[3]{\frac{64}{9} b (\log b)^2} \right) \right)$$

Record actuel: $b = 768$ (232 chiffres décimaux).

Ordinateur quantique et factorisation

P = NP ?

Jacques Sauloy

Rappel: la factorisation est NP, on ne sait pas si elle est P.

Meilleurs algorithmes déterministes connus pour factoriser un nombre n de taille $b \simeq \log_2 n$ (nombre de bits):

$$O \left(\exp \left(\sqrt[3]{\frac{64}{9} b (\log b)^2} \right) \right)$$

Record actuel: $b = 768$ (232 chiffres décimaux).

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Ordinateur quantique et factorisation

P = NP ?

Jacques Sauloy

Rappel: la factorisation est NP, on ne sait pas si elle est P.

Meilleurs algorithmes déterministes connus pour factoriser un nombre n de taille $b \simeq \log_2 n$ (nombre de bits):

$$O \left(\exp \left(\sqrt[3]{\frac{64}{9} b (\log b)^2} \right) \right)$$

Record actuel: $b = 768$ (232 chiffres décimaux).

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Ordinateur quantique et factorisation

P = NP ?

Jacques Sauloy

Rappel: la factorisation est NP, on ne sait pas si elle est P.

Meilleurs algorithmes déterministes connus pour factoriser un nombre n de taille $b \simeq \log_2 n$ (nombre de bits):

$$O \left(\exp \left(\sqrt[3]{\frac{64}{9} b (\log b)^2} \right) \right)$$

Record actuel: $b = 768$ (232 chiffres décimaux).

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Ordinateur quantique et factorisation

P = NP ?

Jacques Sauloy

Une étape critique est la suivante: pour chaque $r = 1, \dots, n - 1$ tel que $r \wedge n = 1$, calculer son *ordre*:

$$p := \inf\{k \geq 1 \mid r^k \equiv 1 \pmod{n}\}$$

(Voir le cours “Outils maths discrètes”).

Peter Shor a l'idée de coder r et k en “bits quantiques” (qubits) qui sont chacun en des états *superposés* 0, 1. On peut alors calculer tous les r^k simultanément.

Sur un ordinateur quantique, le coût de l'algorithme de factorisation de Shor est $O(b^3)$.

Le record actuel est la factorisation de 21 en 2012.

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Ordinateur quantique et factorisation

P = NP ?

Jacques Sauloy

Une étape critique est la suivante: pour chaque $r = 1, \dots, n - 1$ tel que $r \wedge n = 1$, calculer son *ordre*:

$$p := \inf\{k \geq 1 \mid r^k \equiv 1 \pmod{n}\}$$

(Voir le cours “Outils maths discrètes”.)

Peter Shor a l'idée de coder r et k en “bits quantiques” (qubits) qui sont chacun en des états *superposés* 0, 1. On peut alors calculer tous les r^k simultanément.

Sur un ordinateur quantique, le coût de l'algorithme de factorisation de Shor est $O(b^3)$.

Le record actuel est la factorisation de 21 en 2012.

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Ordinateur quantique et factorisation

P = NP ?

Jacques Sauloy

Une étape critique est la suivante: pour chaque $r = 1, \dots, n - 1$ tel que $r \wedge n = 1$, calculer son *ordre*:

$$p := \inf\{k \geq 1 \mid r^k \equiv 1 \pmod{n}\}$$

(Voir le cours “Outils maths discrètes”.)

Peter Shor a l'idée de coder r et k en “bits quantiques” (qubits) qui sont chacun en des états *superposés* 0, 1. On peut alors calculer tous les r^k simultanément.

Sur un ordinateur quantique, le coût de l'algorithme de factorisation de Shor est $O(b^3)$.

Le record actuel est la factorisation de 21 en 2012.

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Ordinateur quantique et factorisation

P = NP ?

Jacques Sauloy

Une étape critique est la suivante: pour chaque $r = 1, \dots, n - 1$ tel que $r \wedge n = 1$, calculer son *ordre*:

$$p := \inf\{k \geq 1 \mid r^k \equiv 1 \pmod{n}\}$$

(Voir le cours “Outils maths discrètes”.)

Peter Shor a l'idée de coder r et k en “bits quantiques” (qubits) qui sont chacun en des états *superposés* 0, 1. On peut alors calculer tous les r^k simultanément.

Sur un ordinateur quantique, le coût de l'algorithme de factorisation de Shor est $O(b^3)$.

Le record actuel est la factorisation de 21 en 2012.

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Ordinateur quantique et factorisation

P = NP ?

Jacques Sauloy

Une étape critique est la suivante: pour chaque $r = 1, \dots, n - 1$ tel que $r \wedge n = 1$, calculer son *ordre*:

$$p := \inf\{k \geq 1 \mid r^k \equiv 1 \pmod{n}\}$$

(Voir le cours “Outils maths discrètes”.)

Peter Shor a l'idée de coder r et k en “bits quantiques” (qubits) qui sont chacun en des états *superposés* 0, 1. On peut alors calculer tous les r^k simultanément.

Sur un ordinateur quantique, le coût de l'algorithme de factorisation de Shor est $O(b^3)$.

Le record actuel est la factorisation de 21 en 2012.

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction



$P = NP ?$

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Réseaux neuronaux et apprentissage

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Je n'ai pas réussi à comprendre si cette approche apportait quelque chose !

Réseaux neuronaux et apprentissage

P = NP ?

Jacques Sauloy

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction

Je n'ai pas réussi à comprendre si cette approche apportait quelque chose !

Réseaux hiérarchiques et autorité

P = NP ?

Jacques Sauloy



- J'ai un problème, Daphné : trouvez immédiatement une solution et apportez-la-moi dans mon bureau.

Königsberg et les chemins eulériens

Le voyageur de commerce et les chemins hamiltoniens

Est-ce que c'est grave ?

Un exemple plus technique

Un exemple plutôt amusant

P et NP

Le côté obscur de la force

Le côté lumineux de la force

La guerre entre les deux côtés de la force

Crépuscule (entre ombre et lumière)

Un peu de science-fiction