Théorème des 4 couleurs: preuve et démonstration(s) par ordinateur

Michaël Rao

CNRS - ENS Lyon
LIP - Laboratoire de l'Informatique du Parallélisme
équipe MC2

Comment un ordinateur peut-il aider un mathématicien ?

- Systèmes de calculs formels (Maple, Mathematica, Sage...)

Comment un ordinateur peut-il aider un mathématicien ?

- Systèmes de calculs formels (Maple, Mathematica, Sage...)

  Un ordinateur peut calculer exactement avec des rationnels, des nombres algébriques, systèmes d'équations polynomiales...

- Tester une idée ou une conjecture sur beaucoup d'exemples

Comment un ordinateur peut-il aider un mathématicien ?

- Systèmes de calculs formels (Maple, Mathematica, Sage...)

  Un ordinateur peut calculer exactement avec des rationnels, des nombres algébriques, systèmes d'équations polynomiales...

- Tester une idée ou une conjecture sur beaucoup d'exemples
- Trouver un objet avec certaines propriétés

Comment un ordinateur peut-il aider un mathématicien ?

- Systèmes de calculs formels (Maple, Mathematica, Sage...)

  Un ordinateur peut calculer exactement avec des rationnels, des nombres algébriques, systèmes d'équations polynomiales...

- Tester une idée ou une conjecture sur beaucoup d'exemples
- Trouver un objet avec certaines propriétés
  - Pour prouver une existence (par construction)

Comment un ordinateur peut-il aider un mathématicien ?

- Systèmes de calculs formels (Maple, Mathematica, Sage...)

  Un ordinateur peut calculer exactement avec des rationnels, des nombres algébriques, systèmes d'équations polynomiales…

- Tester une idée ou une conjecture sur beaucoup d'exemples
- Trouver un objet avec certaines propriétés
  - Pour prouver une existence (par construction)
  - Pour "casser" une conjecture

Comment un ordinateur peut-il aider un mathématicien ?

- Systèmes de calculs formels (Maple, Mathematica, Sage...)

  Un ordinateur peut calculer exactement avec des rationnels, des nombres algébriques, systèmes d'équations polynomiales...

- Tester une idée ou une conjecture sur beaucoup d'exemples
- Trouver un objet avec certaines propriétés
  - Pour prouver une existence (par construction)
  - Pour "casser" une conjecture
- Étude de cas : prouver un ensemble long de cas similaires

Comment un ordinateur peut-il aider un mathématicien ?

- Systèmes de calculs formels (Maple, Mathematica, Sage...)

  Un ordinateur peut calculer exactement avec des rationnels, des nombres algébriques, systèmes d'équations polynomiales...

- Tester une idée ou une conjecture sur beaucoup d'exemples
- Trouver un objet avec certaines propriétés
  - Pour prouver une existence (par construction)
  - Pour "casser" une conjecture
- Étude de cas : prouver un ensemble long de cas similaires
- Assistants de preuves formelles (Coq...)

Comment un ordinateur peut-il aider un mathématicien ?

- Systèmes de calculs formels (Maple, Mathematica, Sage...)

  Un ordinateur peut calculer exactement avec des rationnels, des nombres algébriques, systèmes d'équations polynomiales...

- Tester une idée ou une conjecture sur beaucoup d'exemples
- Trouver un objet avec certaines propriétés
  - Pour prouver une existence (par construction)
  - Pour "casser" une conjecture
- Étude de cas : prouver un ensemble long de cas similaires
- Assistants de preuves formelles (Coq...)

Avantages de l'ordinateur : la rigueur, la vitesse

Comment un ordinateur peut-il aider un mathématicien ?

- Systèmes de calculs formels (Maple, Mathematica, Sage...)

  Un ordinateur peut calculer exactement avec des rationnels, des nombres algébriques, systèmes d'équations polynomiales...

- Tester une idée ou une conjecture sur beaucoup d'exemples
- Trouver un objet avec certaines propriétés
  - Pour prouver une existence (par construction)
  - Pour "casser" une conjecture
- Étude de cas : prouver un ensemble long de cas similaires
- Assistants de preuves formelles (Coq...)

Avantages de l'ordinateur : la rigueur, la vitesse

Désavantages : il faut savoir programmer, c'est (des fois) plus difficile de trouver des erreurs, et sa puissance de calcul est aussi limitée

Problèmes résolus avec l'aide de l'ordinateur

- Théorème des 4 couleurs (Appel & Haken, 1976)

Problèmes résolus avec l'aide de l'ordinateur

- Théorème des 4 couleurs (Appel & Haken, 1976)
- Conjecture de Kepler (Hales & Ferguson, 1998)
- Non existence d'un plan projectif fini d'ordre 10 (Lam, 1991)
- Des jeux : Puissance 4, Awalé, Dames 8×8...
- Des casses-têtes : Rubik's cube, Sudoku...
- ...

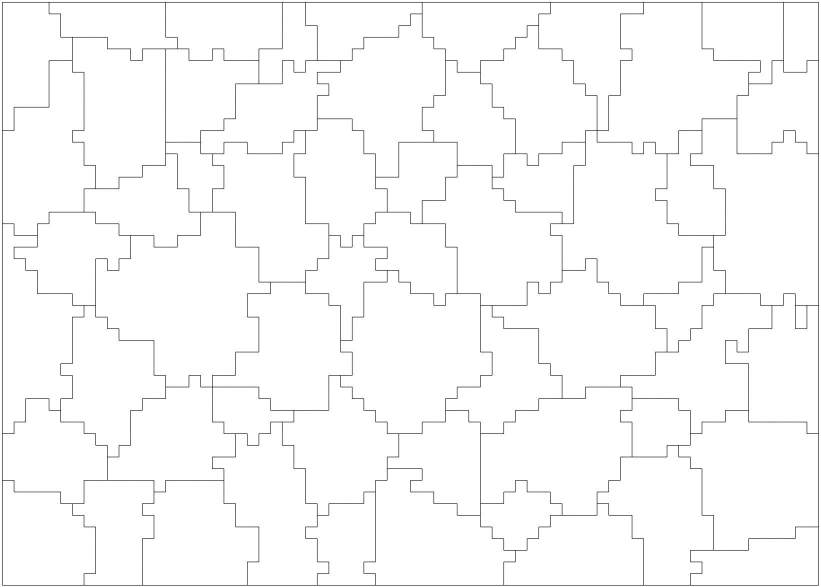
Problèmes résolus avec l'aide de l'ordinateur

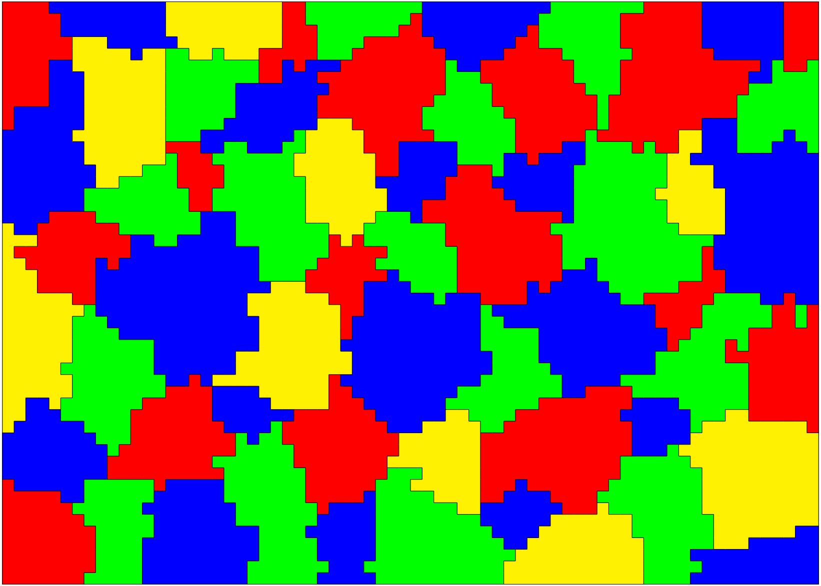
- Théorème des 4 couleurs (Appel & Haken, 1976)
- Conjecture de Kepler (Hales & Ferguson, 1998)
- Non existence d'un plan projectif fini d'ordre 10 (Lam, 1991)
- Des jeux : Puissance 4, Awalé, Dames 8×8...
- Des casses-têtes : Rubik's cube, Sudoku...
- ...

Le théorème des 4 couleurs

Théorème des 4 couleurs

Toute carte constituée de régions connexes peut être coloriée avec (au plus) 4 couleurs, de sorte que deux régions limitrophes aient des couleurs différentes





Le théorème des 4 couleurs

Théorème des 4 couleurs

Toute carte constituée de régions connexes peut être coloriée avec (au plus) 4 couleurs, de sorte que deux régions limitrophes aient des couleurs différentes

Le théorème des 4 couleurs

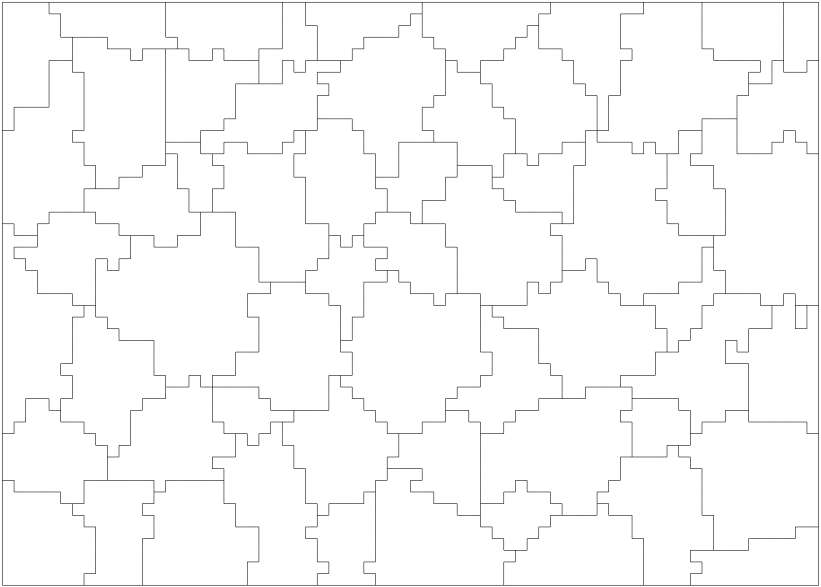
Théorème des 4 couleurs

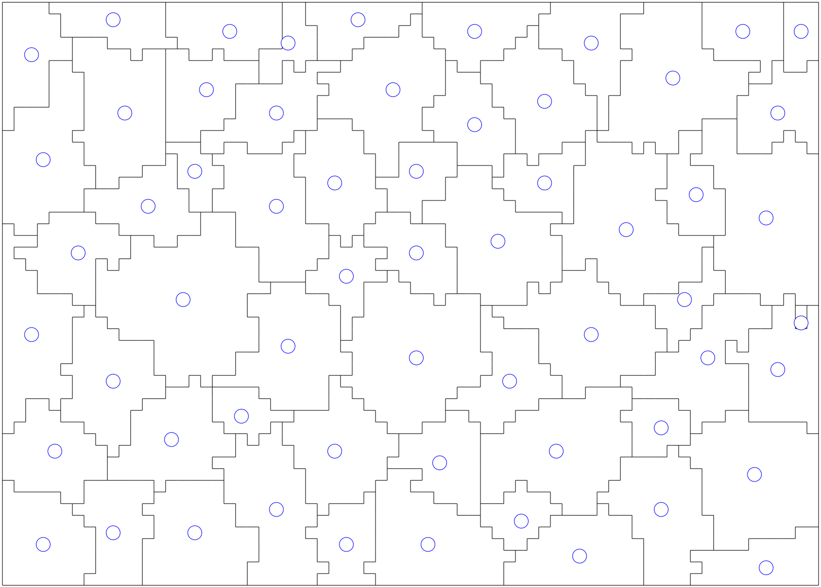
Toute carte constituée de régions connexes peut être coloriée avec (au plus) 4 couleurs, de sorte que deux régions limitrophes aient des couleurs différentes

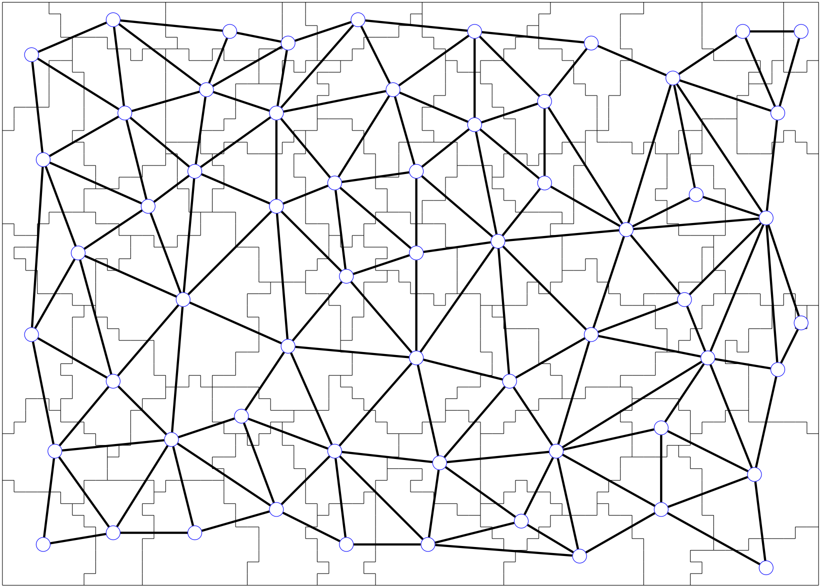
En termes de graphes :

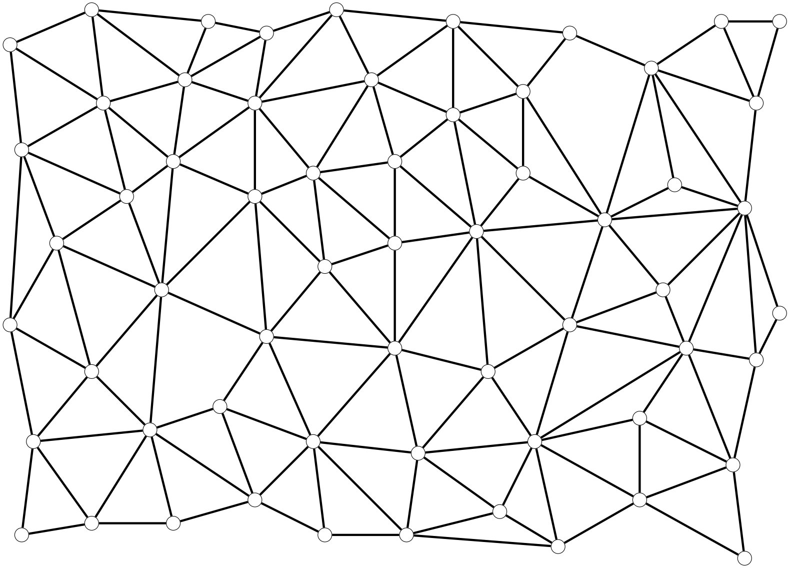
Théorème des 4 couleurs

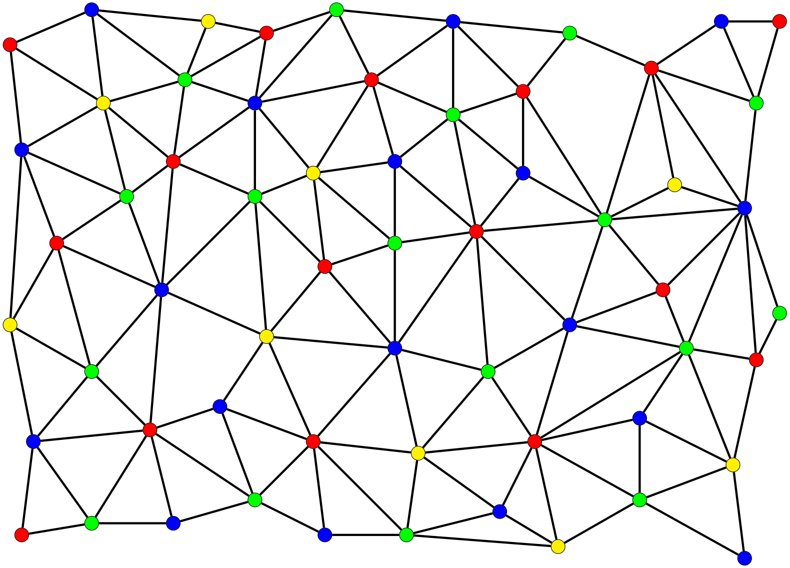
Tout graphe planaire est 4-colorable











Théorème des 4 couleurs : historique

- Conjecture énoncée par Guthrie en 1852

Théorème des 4 couleurs : historique

- Conjecture énoncée par Guthrie en 1852
- Démonstration par Kempe en 1879

Lemme

Dans tout graphe planaire, il existe un sommet de degré au plus 5

Lemme

Dans tout graphe planaire, il existe un sommet de degré au plus 5

Preuve. Utilisation de la formule d'Euler :

$$\#\text{sommets} - \#\text{arêtes} + \#\text{faces} = 2$$

Lemme

Dans tout graphe planaire, il existe un sommet de degré au plus 5

Preuve. Utilisation de la formule d'Euler :

$$\#\text{sommets} - \#\text{arêtes} + \#\text{faces} = 2$$

Une face a au moins 3 arêtes :

Lemme

Dans tout graphe planaire, il existe un sommet de degré au plus 5

Preuve. Utilisation de la formule d'Euler :

$$\#\text{sommets} - \#\text{arêtes} + \#\text{faces} = 2$$

Une face a au moins 3 arêtes : $\#\text{faces} \leq \frac{2}{3} \times \#\text{arêtes}$

Lemme

Dans tout graphe planaire, il existe un sommet de degré au plus 5

Preuve. Utilisation de la formule d'Euler :

$$\#\text{sommets} - \#\text{arêtes} + \#\text{faces} = 2$$

Une face a au moins 3 arêtes : $\#\text{faces} \leq \frac{2}{3} \times \#\text{arêtes}$
Si tous les sommets ont des degrés ≥ 6 :

Lemme

Dans tout graphe planaire, il existe un sommet de degré au plus 5

Preuve. Utilisation de la formule d'Euler :

$$\#\text{sommets} - \#\text{arêtes} + \#\text{faces} = 2$$

Une face a au moins 3 arêtes : $\#\text{faces} \leq \frac{2}{3} \times \#\text{arêtes}$
Si tous les sommets ont des degrés ≥ 6 : $\#\text{sommets} \leq \frac{2}{6} \times \#\text{arêtes}$

Formule d'Euler et 6 couleurs

Lemme

Dans tout graphe planaire, il existe un sommet de degré au plus 5

Preuve. Utilisation de la formule d'Euler :

$$\#\text{sommets} - \#\text{arêtes} + \#\text{faces} = 2$$

Une face a au moins 3 arêtes : $\#\text{faces} \leq \frac{2}{3} \times \#\text{arêtes}$
Si tous les sommets ont des degrés ≥ 6 : $\#\text{sommets} \leq \frac{2}{6} \times \#\text{arêtes}$

$$\#\text{faces} + \#\text{sommets} \leq \left(\frac{2}{6} + \frac{2}{3}\right) \times \#\text{arêtes}$$

Lemme

Dans tout graphe planaire, il existe un sommet de degré au plus 5

Preuve. Utilisation de la formule d'Euler :

$$\#\text{sommets} - \#\text{arêtes} + \#\text{faces} = 2$$

Une face a au moins 3 arêtes : $\#\text{faces} \leq \frac{2}{3} \times \#\text{arêtes}$
Si tous les sommets ont des degrés ≥ 6 : $\#\text{sommets} \leq \frac{2}{6} \times \#\text{arêtes}$

$$\#\text{faces} + \#\text{sommets} \leq \left(\frac{2}{6} + \frac{2}{3}\right) \times \#\text{arêtes}$$

Contradiction

Formule d'Euler et 6 couleurs

Tout graphe planaire est 6-colorable :

Algorithme (récursif) qui colorie avec 6 couleurs

- Soit v un sommet de G de degré au plus 5
- On colorie $G - v$ avec 6 couleurs (appel récursif)
- On colorie v avec une couleur libre.

Théorème des 6 couleurs

Algorithme (récursif) qui colorie un graphe planaire G avec 6 couleurs :

Théorème des 6 couleurs

Algorithme (récursif) qui colorie un graphe planaire G avec 6 couleurs :

- Soit v un sommet de G de degré au plus 5

Théorème des 6 couleurs

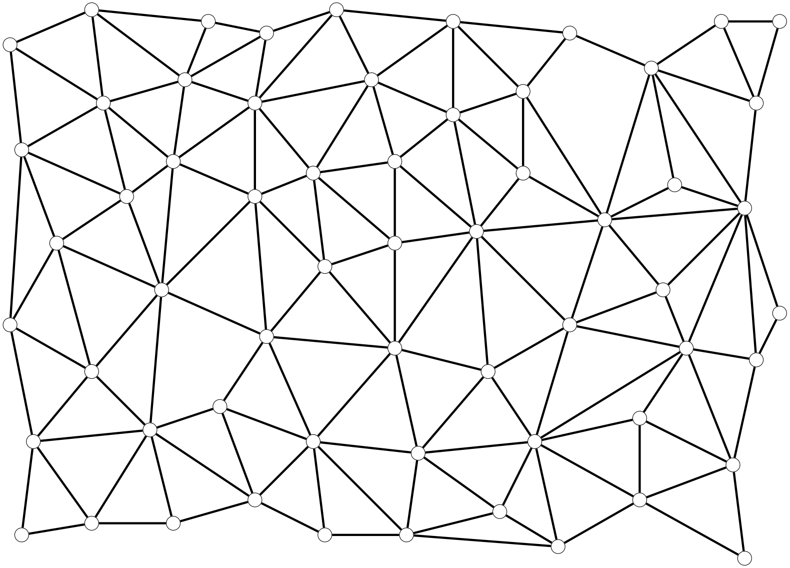
Algorithme (récursif) qui colorie un graphe planaire G avec 6 couleurs :

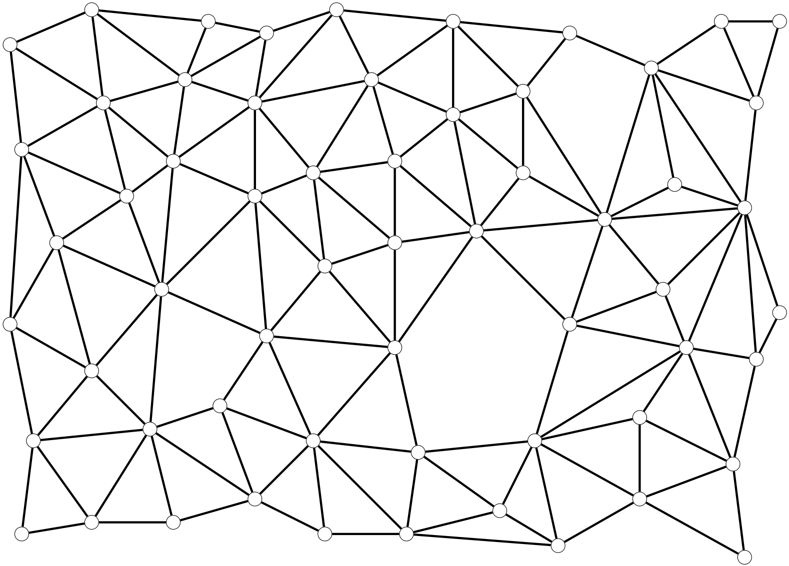
- Soit v un sommet de G de degré au plus 5
- On colorie $G - v$ avec 6 couleurs (appel récursif)

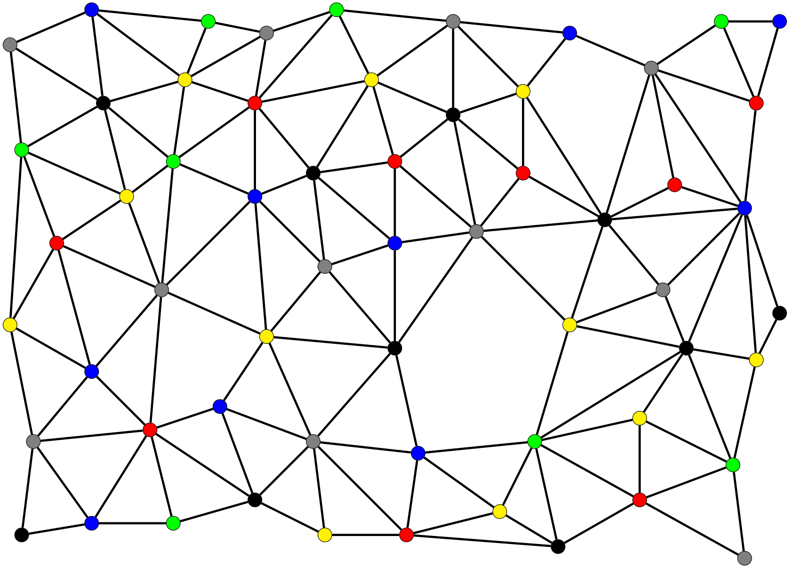
Théorème des 6 couleurs

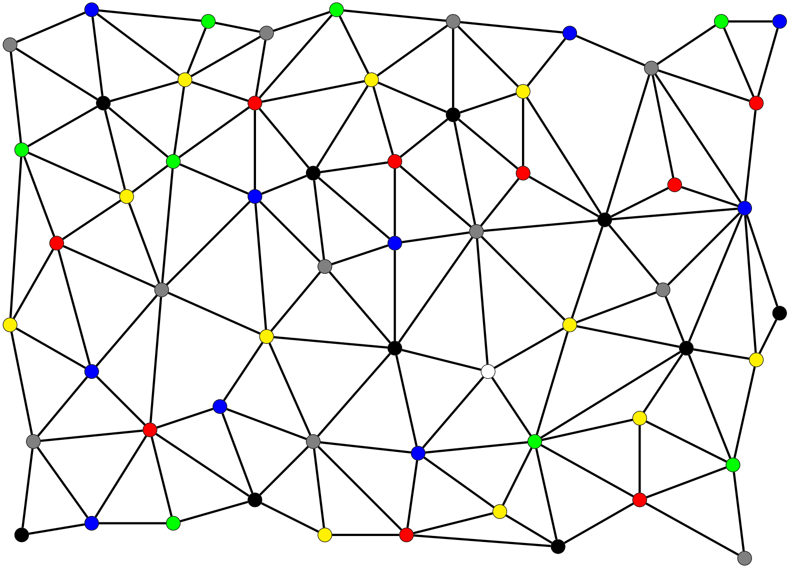
Algorithme (récursif) qui colorie un graphe planaire G avec 6 couleurs :

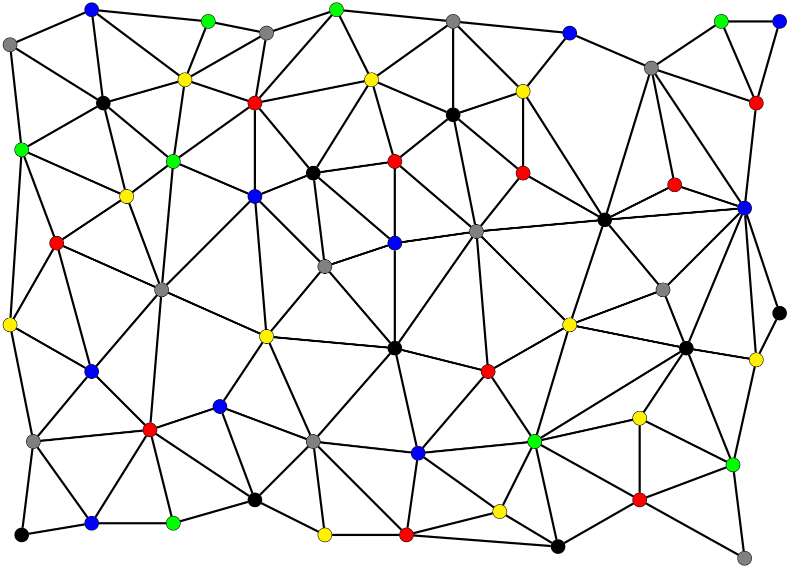
- Soit v un sommet de G de degré au plus 5
- On colorie $G - v$ avec 6 couleurs (appel récursif)
- Au moins une des 6 couleurs n'est pas utilisée parmi les voisins de v dans G. On colorie v avec une couleur libre.











Théorème des 6 couleurs

Algorithme (récursif) qui colorie un graphe planaire G avec 6 couleurs :

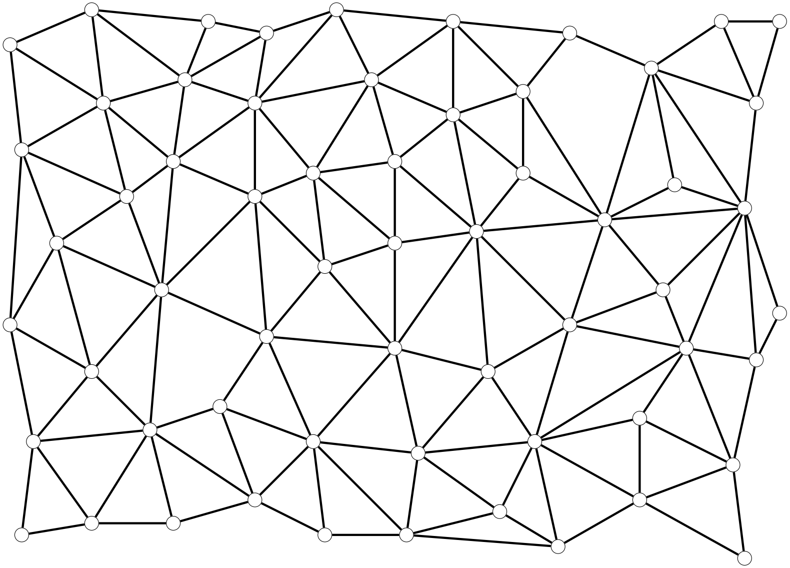
- Soit v un sommet de G de degré au plus 5
- On colorie $G - v$ avec 6 couleurs (appel récursif)
- Au moins une des 6 couleurs n'est pas utilisée parmi les voisins de v dans G. On colorie v avec une couleur libre.

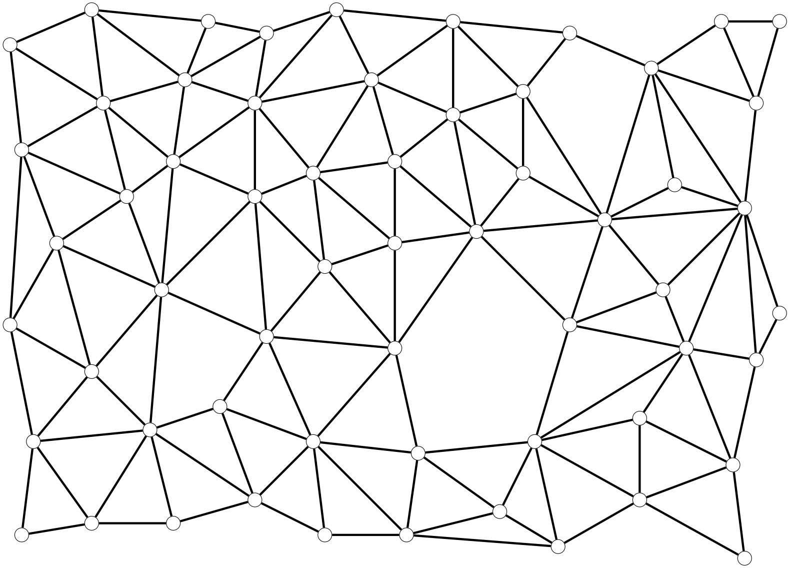
Tout graphe planaire est 6-colorable

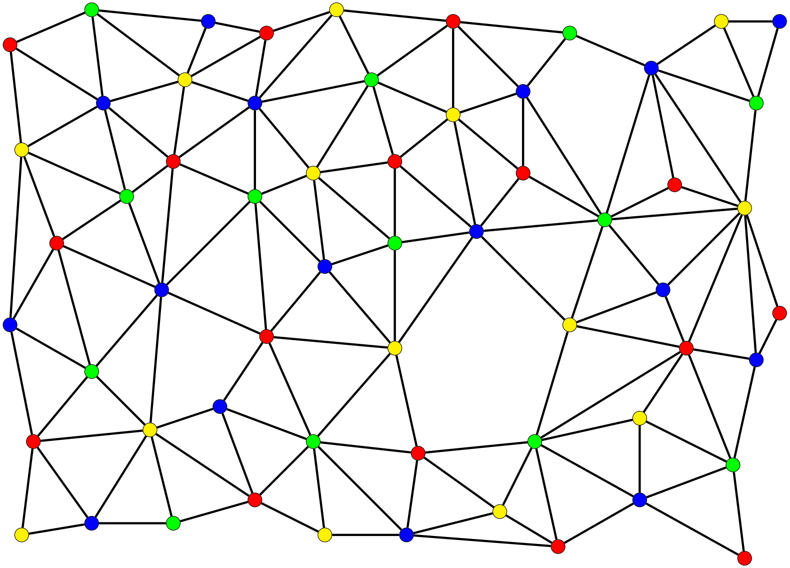
Théorème des 4 couleurs (Kempe)

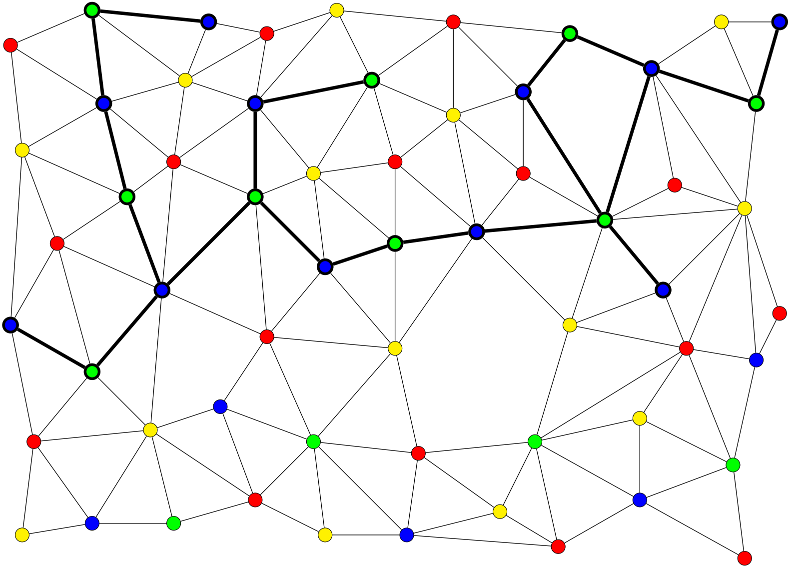
Algorithme (récursif) qui colorie un graphe planaire G avec 4 couleurs :

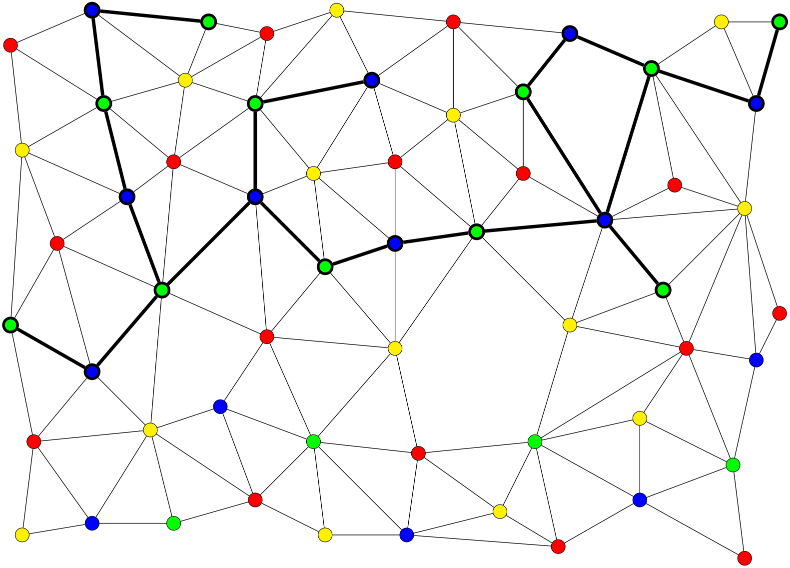
- Soit v un sommet de G de degré au plus 5
- On colorie $G - v$ avec 4 couleurs (appel récursif)
- Si une des 4 couleurs n'est pas utilisée parmi les voisins de v dans G, on l'utilise pour colorier v
- Sinon, on fait des changements locaux (via des chaînes de Kempe) pour « gagner » une couleur

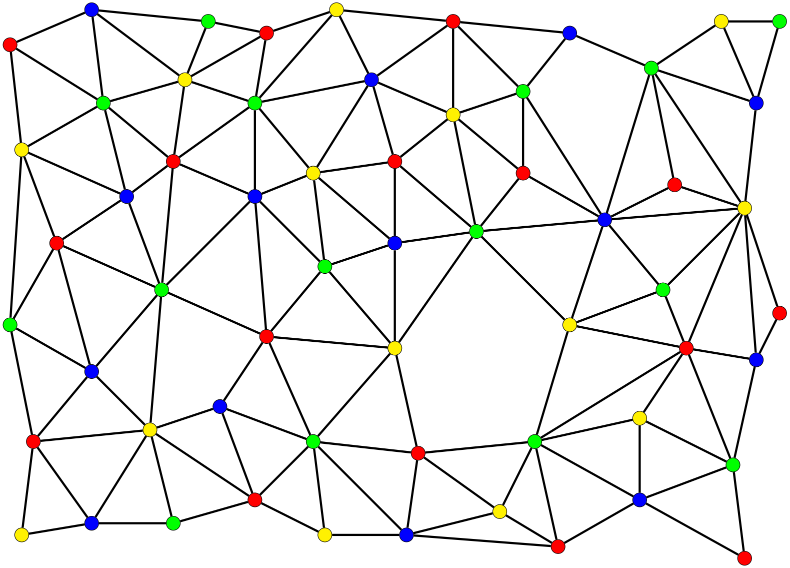


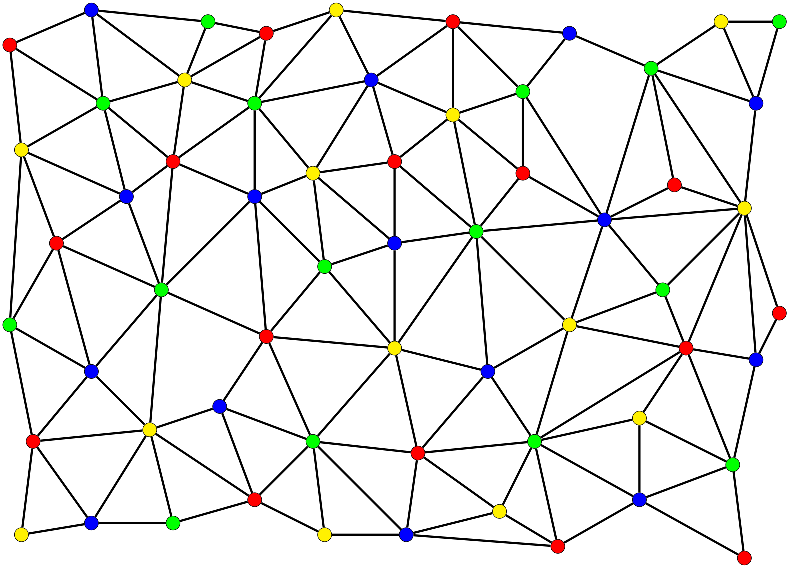


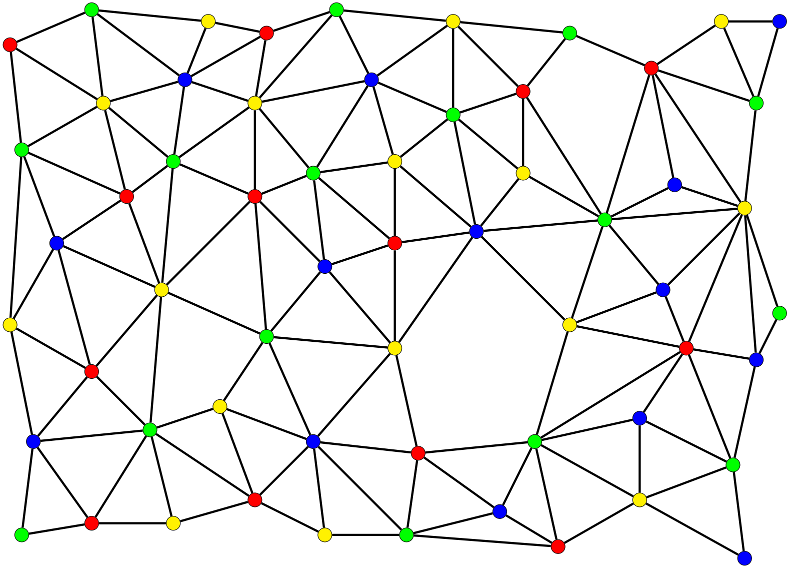


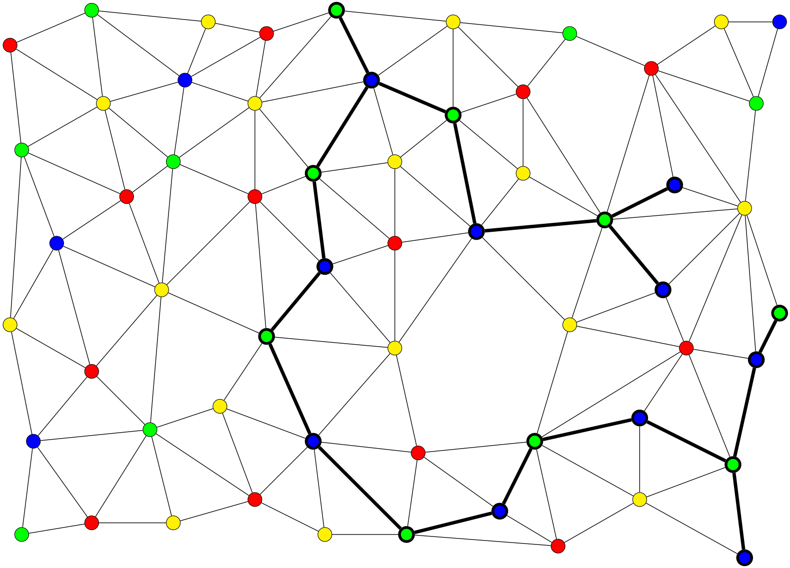


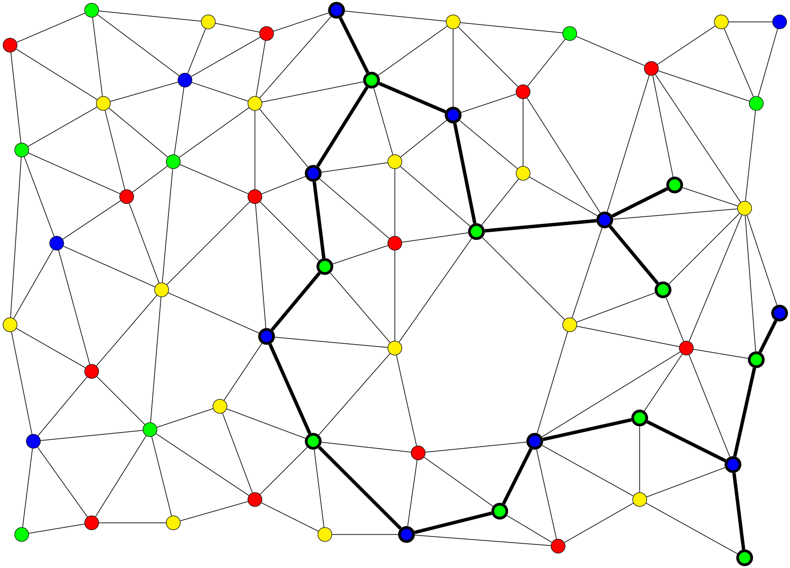


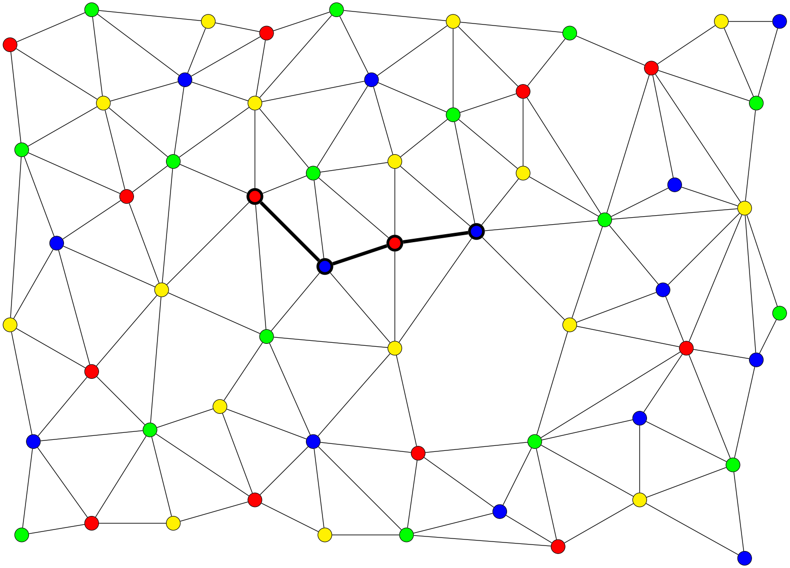


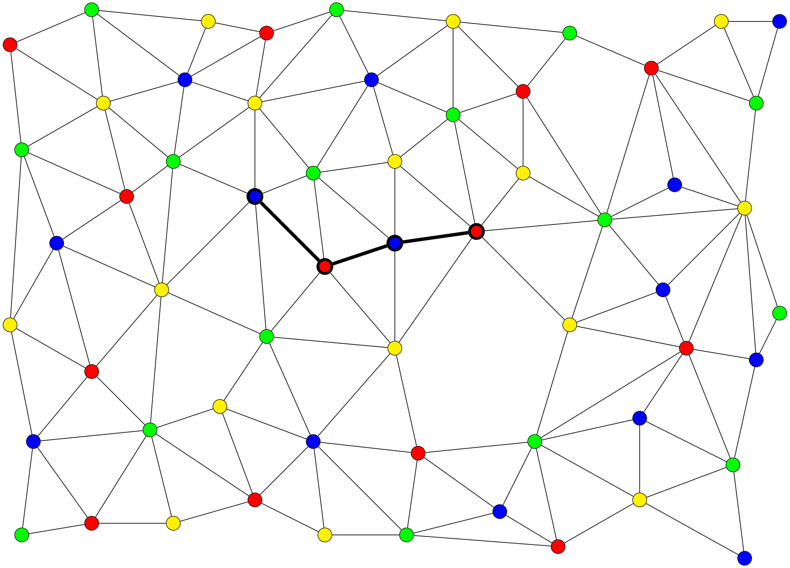


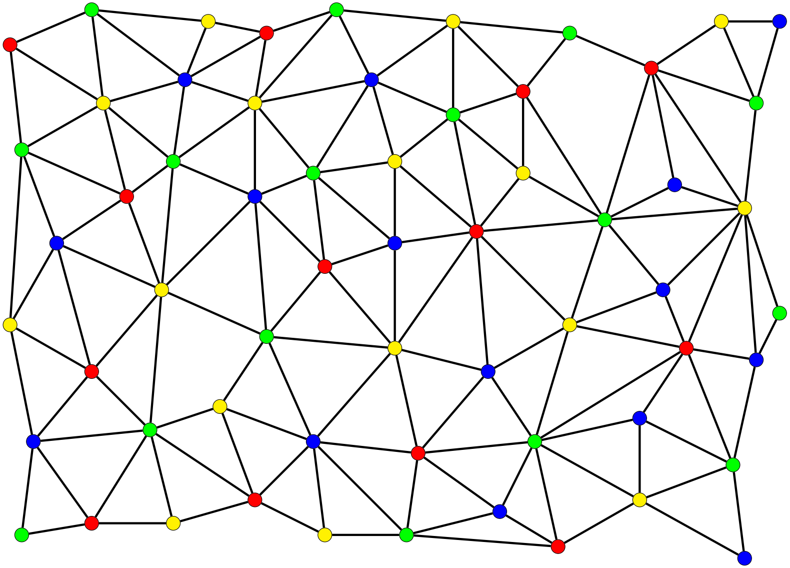












Théorème des 4 couleurs (Kempe)

Algorithme (récursif) qui colorie un graphe planaire G avec 4 couleurs :

- Soit v un sommet de G de degré au plus 5
- On colorie $G - v$ avec 4 couleurs (appel récursif)
- Si une des 4 couleurs n'est pas utilisée parmi les voisins de v dans G, on l'utilise pour colorier v
- Sinon, on fait des changements locaux (via des chaînes de Kempe) pour « gagner » une couleur

Tout graphe planaire est 4-colorable

Le théorème des 4 couleurs est démontré

Théorème des 4 couleurs (Kempe) ?

Algorithme (récursif) qui colorie un graphe planaire G avec 4 couleurs :

- Soit v un sommet de G de degré au plus 5
- On colorie $G - v$ avec 4 couleurs (appel récursif)
- Si une des 4 couleurs n'est pas utilisée parmi les voisins de v dans G, on l'utilise pour colorier v
- Sinon, on fait des changements locaux (via des chaînes de Kempe) pour « gagner » une couleur

Tout graphe planaire est 4-colorable

Le théorème des 4 couleurs est démontré (?)

Théorème des 4 couleurs : historique

- Conjecture énoncée par Guthrie en 1852
- Démonstration par Kempe en 1879

Théorème des 4 couleurs : historique

- Conjecture énoncée par Guthrie en 1852
- ~~Démonstration~~ par Kempe en 1879

- Heawood trouve une faute dans la preuve de Kempe en 1890 !

Théorème des 4 couleurs : historique

- Conjecture énoncée par Guthrie en 1852
- ~~Démonstration~~ par Kempe en 1879
- Démonstration alternative par Tait en 1880
- Heawood trouve une faute dans la preuve de Kempe en 1890 !

Théorème des 4 couleurs : historique

- Conjecture énoncée par Guthrie en 1852
- ~~Démonstration~~ par Kempe en 1879
- ~~Démonstration alternative~~ par Tait en 1880
- Heawood trouve une faute dans la preuve de Kempe en 1890 !
- Petersen trouve une faute dans la preuve de Tait en 1891 !

Théorème des 4 couleurs : historique

- Conjecture énoncée par Guthrie en 1852
- ~~Démonstration~~ par Kempe en 1879
- ~~Démonstration alternative~~ par Tait en 1880
- Heawood trouve une faute dans la preuve de Kempe en 1890 !
- Petersen trouve une faute dans la preuve de Tait en 1891 !
- Heesch en 1955 : première idée d'informatisation

Théorème des 4 couleurs : historique

- Conjecture énoncée par Guthrie en 1852
- ~~Démonstration~~ par Kempe en 1879
- ~~Démonstration alternative~~ par Tait en 1880
- Heawood trouve une faute dans la preuve de Kempe en 1890 !
- Petersen trouve une faute dans la preuve de Tait en 1891 !
- Heesch en 1955 : première idée d'informatisation
- Démonstration par Appel & Haken en 1977 (avec l'aide de l'ordinateur pour une partie)

La preuve de Kempe contenait une erreur : deux chaines de Kempe peuvent se croiser...

La preuve de Kempe contenait une erreur : deux chaines de Kempe peuvent se croiser...Mais, il y avait déjà beaucoup d'idées !

La preuve de Kempe contenait une erreur : deux chaines de Kempe peuvent se croiser...Mais, il y avait déjà beaucoup d'idées !

Idée d'une preuve :

- Si le théorème est faux, alors il existe un contre exemple minimal : un graphe planaire non 4-colorable, mais si on retire un sommet, il devient 4-colorable
- Configuration réductible : configuration qui ne peut pas apparaite dans un contre exemple minimal.

La preuve de Kempe contenait une erreur : deux chaines de Kempe peuvent se croiser...Mais, il y avait déjà beaucoup d'idées !

Idée d'une preuve :

- Si le théorème est faux, alors il existe un contre exemple minimal : un graphe planaire non 4-colorable, mais si on retire un sommet, il devient 4-colorable
- Configuration réductible : configuration qui ne peut pas apparaite dans un contre exemple minimal.
  Exemples : sommet de degré 3, sommet de degré 4 (Kempe)

La preuve de Kempe contenait une erreur : deux chaines de Kempe peuvent se croiser...Mais, il y avait déjà beaucoup d'idées !

Idée d'une preuve :

- Si le théorème est faux, alors il existe un contre exemple minimal : un graphe planaire non 4-colorable, mais si on retire un sommet, il devient 4-colorable
- Configuration réductible : configuration qui ne peut pas apparaite dans un contre exemple minimal.
  Exemples : sommet de degré 3, sommet de degré 4 (Kempe)
- Si il existe un ensemble de configurations réductibles $\mathcal{C}$ qui est inévitable dans un graphe planaire, le théorème est vrai.

La preuve de Kempe contenait une erreur : deux chaines de Kempe peuvent se croiser...Mais, il y avait déjà beaucoup d'idées !

Idée d'une preuve :

- Si le théorème est faux, alors il existe un contre exemple minimal : un graphe planaire non 4-colorable, mais si on retire un sommet, il devient 4-colorable
- Configuration réductible : configuration qui ne peut pas apparaite dans un contre exemple minimal.
  Exemples : sommet de degré 3, sommet de degré 4 (Kempe)
- Si il existe un ensemble de configurations réductibles $\mathcal{C}$ qui est inévitable dans un graphe planaire, le théorème est vrai.

Note : une preuve suivant ce schéma serait en même temps un algorithme 4-coloration !

Deux grandes parties dans cette approche de preuve :

1. Trouver des configurations réductibles
2. Montrer que $\mathcal{C}$ est inévitable.

Deux grandes parties dans cette approche de preuve :

1. Trouver des configurations réductibles
2. Montrer que $\mathcal{C}$ est inévitable.

Problèmes :

1. Heesch fait des simulations, et estime qu'il faut environ $|\mathcal{C}| \sim 8900$
   $\Rightarrow$ utilisation de l'ordinateur semble inévitable...
2. Comment faire le (2) ?

Idée de Heesch

De la formule d'Euler
$\Rightarrow$ Il existe un sommet v de degré au plus 5

Coloriage de $G - v \rightarrow$ Coloriage de G

Idée de Heesch

De la formule d'Euler

~~$\Rightarrow$ Il existe un sommet v de degré au plus 5~~

$\Rightarrow$ Il existe une configuration parmi $\mathcal{C}$, avec $\mathcal{C}$ fini

Heesch estime la taille de $\mathcal{C}$ à $\sim$8900

Coloriage de $G - v \rightarrow$ Coloriage de G

Idée de Heesch

De la formule d'Euler

~~$\Rightarrow$ Il existe un sommet v de degré au plus 5~~

$\Rightarrow$ Il existe une configuration parmi $\mathcal{C}$, avec $\mathcal{C}$ fini

Heesch estime la taille de $\mathcal{C}$ à $\sim$8900

~~Coloriage de $G - v \rightarrow$ Coloriage de G~~

Pour tout $C \in \mathcal{C}$, il existe C' plus petit t.q.
Coloriage de $G[C'] \rightarrow$ Coloriage de $G[C]$

De la formule d'Euler
~~$\Rightarrow$ Il existe un sommet v de degré au plus 5~~
$\Rightarrow$ Il existe une configuration parmi $\mathcal{C}$, avec $\mathcal{C}$ fini

Heesch estime la taille de $\mathcal{C}$ à $\sim$8900

~~Coloriage de $G - v \rightarrow$ Coloriage de G~~

Pour tout $C \in \mathcal{C}$, il existe C' plus petit t.q.
Coloriage de $G[C'] \rightarrow$ Coloriage de $G[C]$

c.a.d. C ne peut pas apparaître dans un contre exemple minimal

Idée de Heesch

« Déchargement »

De la formule d'Euler

~~$\Rightarrow$ Il existe un sommet v de degré au plus 5~~

$\Rightarrow$ Il existe une configuration parmi $\mathcal{C}$, avec $\mathcal{C}$ fini

Heesch estime la taille de $\mathcal{C}$ à $\sim$8900

« Réduction »

~~Coloriage de $G - v$ $\rightarrow$ Coloriage de G~~

Pour tout $C \in \mathcal{C}$, il existe C' plus petit t.q.
Coloriage de $G[C']$ $\rightarrow$ Coloriage de $G[C]$

c.a.d. C ne peut pas apparaître dans un contre exemple minimal

Théorème des 4 couleurs : historique

- Conjecture énoncée par Guthrie en 1852
- ~~Démonstration~~ par Kempe en 1879
- ~~Démonstration alternative~~ par Tait en 1880
- Heawood trouve une faute dans la preuve de Kempe en 1890 !
- Petersen trouve une faute dans la preuve de Tait en 1891 !
- Heesch en 1955 : première idée d'informatisation

Théorème des 4 couleurs : historique

- Conjecture énoncée par Guthrie en 1852
- ~~Démonstration~~ par Kempe en 1879
- ~~Démonstration alternative~~ par Tait en 1880
- Heawood trouve une faute dans la preuve de Kempe en 1890 !
- Petersen trouve une faute dans la preuve de Tait en 1891 !
- Heesch en 1955 : première idée d'informatisation
- Démonstration par Appel & Haken en 1977 (avec l'aide de l'ordinateur pour une partie)

Critiques

La preuve d'Appel et Haken n'a pas été acceptée par tout le monde...

Critiques

La preuve d'Appel et Haken n'a pas été acceptée par tout le monde...

Il y a le scepticisme des preuves longues :

- La première partie est faite à la main et longue
- Plusieurs petites fautes ont étés trouvées

Critiques

La preuve d'Appel et Haken n'a pas été acceptée par tout le monde...

Il y a le scepticisme des preuves longues :

- La première partie est faite à la main et longue
- Plusieurs petites fautes ont étés trouvées

À ceux-là se rajoutent les sceptiques des preuves par ordinateur...

Critiques

La preuve d'Appel et Haken n'a pas été acceptée par tout le monde...

Il y a le scepticisme des preuves longues :

- La première partie est faite à la main et longue
- Plusieurs petites fautes ont étés trouvées

À ceux-là se rajoutent les sceptiques des preuves par ordinateur...

- La deuxième partie est vérifiée par ordinateur
- Le programme est codé en assembleur sur un IBM 370/168. Comment être sûr qu'il ne contient pas de bug ?
- Comment être sûr que l'ordinateur n'a pas un bug matériel ?

```
HELLO    CSECT                The name of this program is 'HELLO'
*                             Register 15 points here on entry from OPSYS or caller.
         STM   14,12,12(13)   Save registers 14,15, and 0 thru 12 in caller's Save area
         LR    12,15          Set up base register with program's entry point address
         USING HELLO,12       Tell assembler which register we are using for pgm. base
         LA    15,SAVE        Now Point at our own save area
         ST    15,8(13)       Set forward chain
         ST    13,4(15)       Set back chain
         LR    13,15          Set R13 to address of new save area
*                             -end of housekeeping (similar for most programs) -
         WTO   'Hello World'  Write To Operator  (Operating System macro)
*
         L     13,4(13)       restore address to caller-provided save area
         XC    8(4,13),8(13)  Clear forward chain
         LM    14,12,12(13)   Restore registers as on entry
         DROP  12             The opposite of 'USING'
         SR    15,15          Set register 15 to 0 so that the return code (R15) is Zero
         BR    14             Return to caller
*
SAVE     DS    18F            Define 18 fullwords to save calling program registers
         END  HELLO           This is the end of the program
```

Théorème des 4 couleurs : historique

- Conjecture énoncée par Guthrie en 1852
- ~~Démonstration~~ par Kempe en 1879
- ~~Démonstration alternative~~ par Tait en 1880
- Heawood trouve une faute dans la preuve de Kempe en 1890 !
- Petersen trouve une faute dans la preuve de Tait en 1891 !
- Heesch en 1955 : première idée d'informatisation
- Démonstration par Appel & Haken en 1977 (avec l'aide de l'ordinateur pour une partie)

Théorème des 4 couleurs : historique

- Conjecture énoncée par Guthrie en 1852
- ~~Démonstration~~ par Kempe en 1879
- ~~Démonstration alternative~~ par Tait en 1880
- Heawood trouve une faute dans la preuve de Kempe en 1890 !
- Petersen trouve une faute dans la preuve de Tait en 1891 !
- Heesch en 1955 : première idée d'informatisation
- Démonstration par Appel & Haken en 1977 (avec l'aide de l'ordinateur pour une partie)
- Démonstration par Robertson, Sanders, Seymour & Thomas en 1997 (avec l'aide de l'ordinateur pour toutes les parties)

Théorème des 4 couleurs : historique

- Conjecture énoncée par Guthrie en 1852
- ~~Démonstration~~ par Kempe en 1879
- ~~Démonstration alternative~~ par Tait en 1880
- Heawood trouve une faute dans la preuve de Kempe en 1890 !
- Petersen trouve une faute dans la preuve de Tait en 1891 !
- Heesch en 1955 : première idée d'informatisation
- Démonstration par Appel & Haken en 1977 (avec l'aide de l'ordinateur pour une partie)
- Démonstration par Robertson, Sanders, Seymour & Thomas en 1997 (avec l'aide de l'ordinateur pour toutes les parties)
- Vérification de la démonstration par Gonthier en 2005 (avec l'aide d'un ordinateur, via un assistant de preuves)

Assistant de preuves

Comment être sûr qu'une preuve (informatique ou non) ne contient pas d'erreur ?

Assistant de preuves

Comment être sûr qu'une preuve (informatique ou non) ne contient pas d'erreur ?

$\Rightarrow$ Assistant de preuves

Assistant de preuves

Comment être sûr qu'une preuve (informatique ou non) ne contient pas d'erreur ?
$\Rightarrow$ Assistant de preuves

Un *theorème* est une proposition qui est obtenue en combinant des axiomes, via des règles d'inférence
Sa *preuve* est l'arbre des combinainaisons pour obtenir la proposition

Assistant de preuves

Comment être sûr qu'une preuve (informatique ou non) ne contient pas d'erreur ?
$\Rightarrow$ Assistant de preuves

Un *theorème* est une proposition qui est obtenue en combinant des axiomes, via des règles d'inférence
Sa *preuve* est l'arbre des combinainaisons pour obtenir la proposition

L'ordinateur peut vérifier si une preuve est correcte
C'est ce que font les « assistants de preuves », comme Coq
(Ils permettent aussi de manipuler les preuves, et de prouver automatiquement certaines étapes)

Assistant de preuves

La preuve du théorème des 4 couleurs vérifiée formellement par Gonthier (2005), en Coq

(Traduction de la preuve de 1997 dans la théorie utilisée par Coq)

Assistant de preuves

La preuve du théorème des 4 couleurs vérifiée formellement par Gonthier (2005), en Coq

(Traduction de la preuve de 1997 dans la théorie utilisée par Coq)

Travail difficile... : il faut formaliser tous les aspects dans la théorie

Assistant de preuves

La preuve du théorème des 4 couleurs vérifiée formellement par Gonthier (2005), en Coq

(Traduction de la preuve de 1997 dans la théorie utilisée par Coq)

Travail difficile... : il faut formaliser <u>tous</u> les aspects dans la théorie

La preuve de la conjecture de Kepler a également été démontrée formellement (Hales & al., 2014)

Assistant de preuves

La preuve du théorème des 4 couleurs vérifiée formellement par Gonthier (2005), en Coq

(Traduction de la preuve de 1997 dans la théorie utilisée par Coq)

Travail difficile... : il faut formaliser tous les aspects dans la théorie

La preuve de la conjecture de Kepler a également été démontrée formellement (Hales & al., 2014)

Ce n'est pas réservé qu'aux preuves par ordinateur :
Le théorème de Feit-Thompson (groupes d'ordre impair) a été vérifié formellement par Gonthier et al. (2012)