Preuves sur ordinateur, preuves avec ordinateur et le théorème des quatre couleurs

Benjamin Werner

INRIA et Ecole Polytechnique
Projet TypiCal

Séminaire du LAL, Orsay
7 avril 2009

C'est quoi les maths ?

Tous les hommes sont mortels, Socrate est un homme, donc Socrate est mortel.

C'est quoi les maths ?

Tous les hommes sont mortels, Socrate est un homme, donc Socrate est mortel.

C'est quoi les maths ?

Tous les hommes sont mortels, Socrate est un homme, donc Socrate est mortel.

correction : critère *syntaxique*

C'est quoi les maths ?

Tous les hommes sont mortels, Socrate est un homme, donc Socrate est mortel.

correction : critère *syntaxique*

$$\frac{\vdash A \Rightarrow B \qquad \vdash A}{\vdash B}$$

Les briques du raisonnement mathématique

C'est quoi les maths ?

Tous les hommes sont mortels, Socrate est un homme, donc Socrate est mortel.

correction : critère *syntaxique*

$$\frac{\vdash A \Rightarrow B \qquad \vdash A}{\vdash B}$$

Les briques du raisonnement mathématique

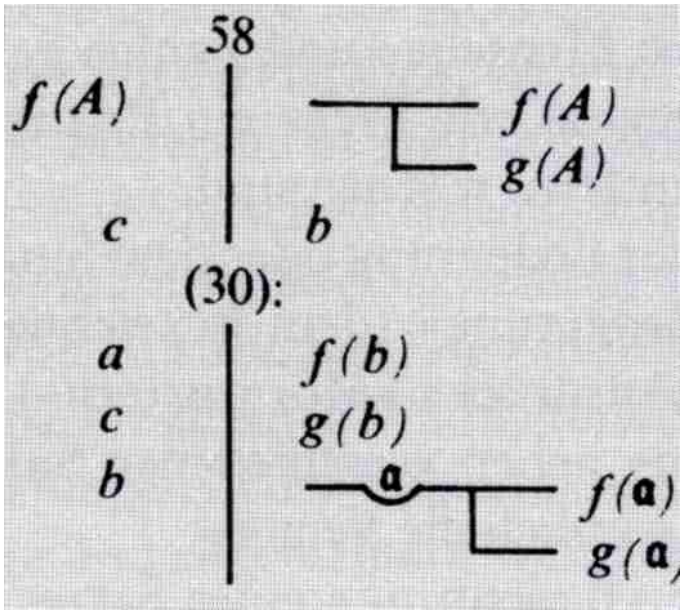
$$\frac{\dfrac{\vdash \forall x.H(x) \Rightarrow M(x)}{\vdash H(s) \Rightarrow M(S)} \qquad \vdash H(S)}{\vdash M(S)}$$

Une démonstration mathématique est une *construction*

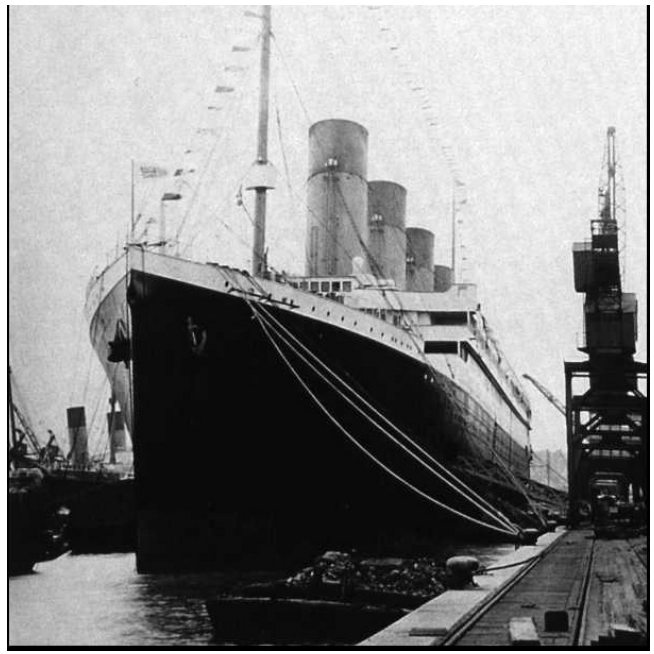
Naissance de la logique mathématique moderne

L'idée de la vérité mathématique définie de manière totalement *objective* grâce à des règles *syntaxiques*.

1872 : la *Begriffsschrift* de Frege



preuve= structure de donnée arborescente



vérification mécanique

Un siècle plus tard

La vérification mécanique du raisonnement devient réalité.

Premier système de preuves : Automath (1968)

N. G. de Bruijn

Les preuves formelles sont construites *en fait*

Un siècle plus tard

La vérification mécanique du raisonnement devient réalité.

Premier système de preuves : Automath (1968)

N. G. de Bruijn

Les preuves formelles sont construites *en fait*

Aujourd'hui

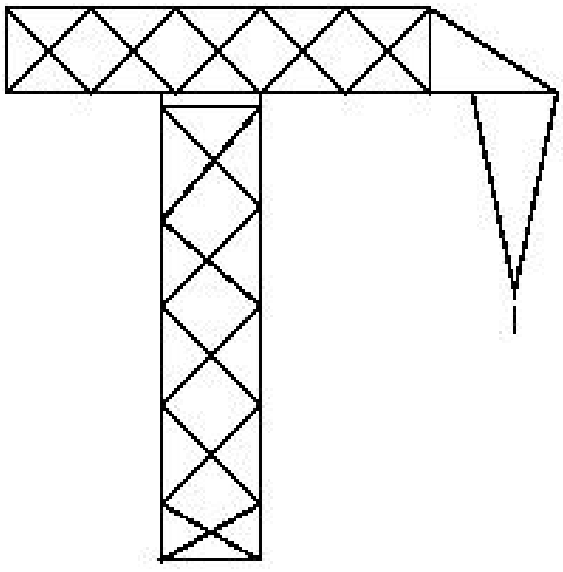
Un système de preuves moderne : Coq

- Même principe
- Formalisme un peu plus moderne

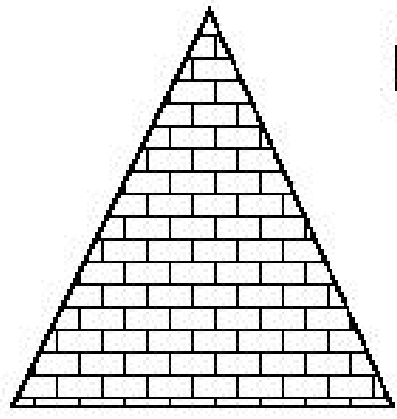
Mini-démo

Good cop, bad cop

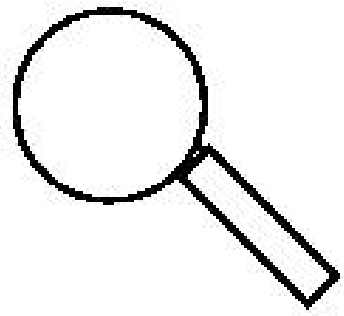
Architecture du système de preuves :



Aide à la preuve



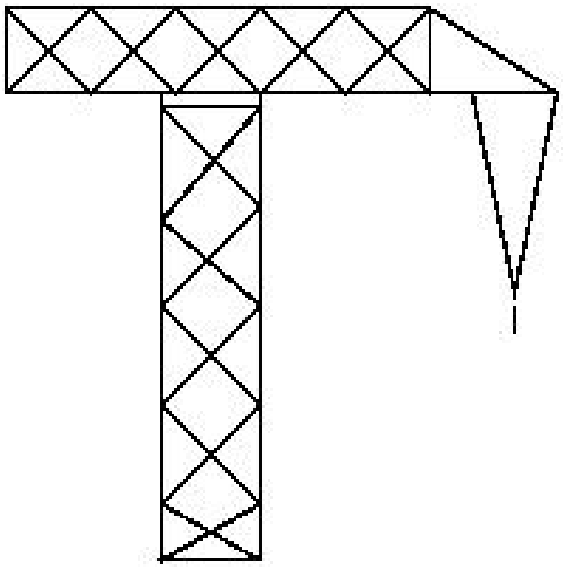
Preuve



Vérificateur
(noyau)

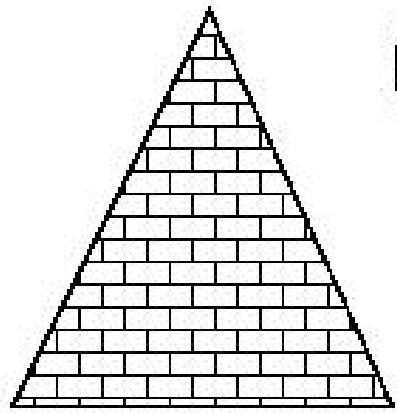
Good cop, bad cop

Architecture du système de preuves :

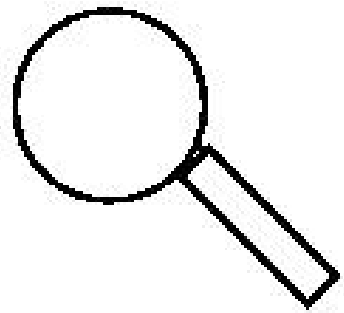


Aide à la preuve

compliqué si nécessaire



Preuve

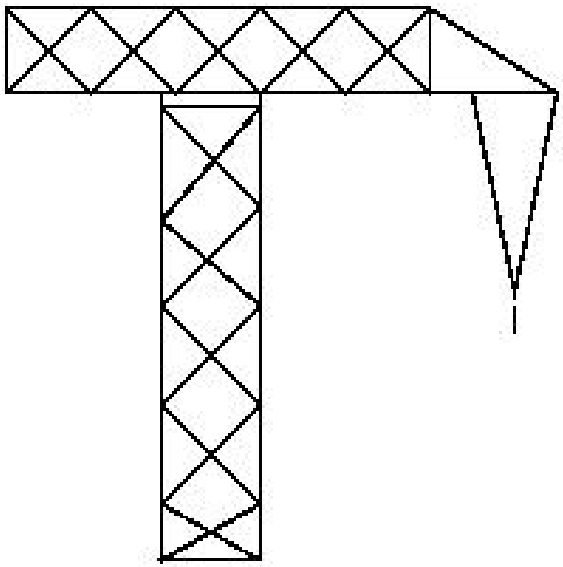


Vérificateur
(noyau)

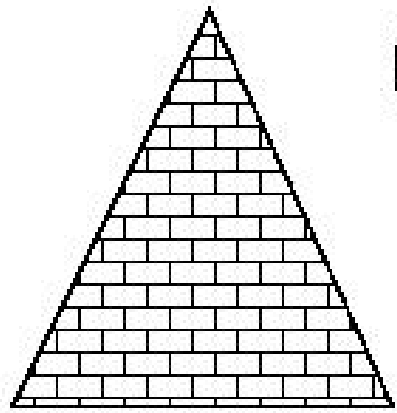
aussi simple que possible

Good cop, bad cop

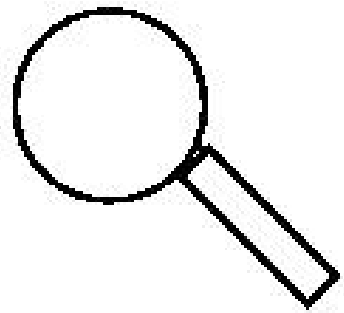
Architecture du système de preuves :



Aide à la preuve



Preuve



Vérificateur
(noyau)

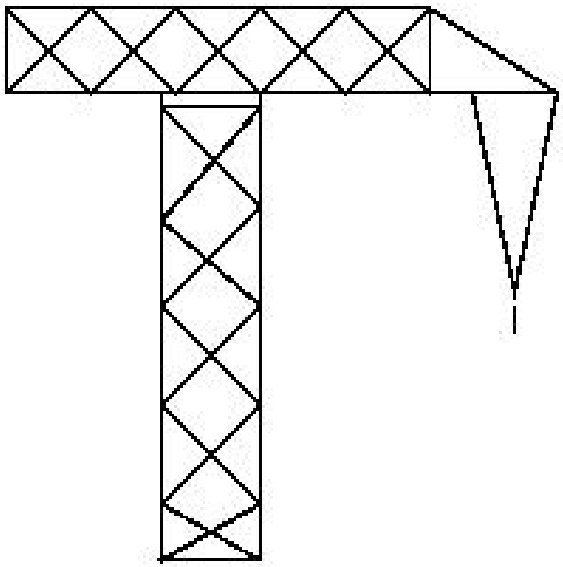
compliqué si nécessaire

aussi simple que possible

La vérité mathématique est validée expérimentalement !

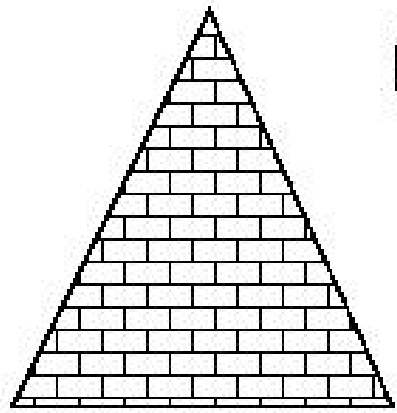
Good cop, bad cop

Architecture du système de preuves :

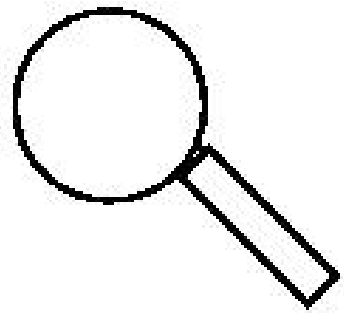


Aide à la preuve

compliqué si nécessaire



Preuve



Vérificateur
(noyau)

aussi simple que possible

La vérité mathématique est validée expérimentalement !

Mapple, Mathlab, Mathematica ne sont pas des systèmes de preuves

Peut-on faire confiance à la machine ?

Des règles logiques bien définies

- Cohérence : question de logique
- Théorème de Gödel : toujours une part d'incertitude de principe

Peut-on faire confiance à la machine ?

Des règles logiques bien définies

- Cohérence : question de logique
- Théorème de Gödel : toujours une part d'incertitude de principe

Le programme doit implémenter les règles

- On peut prouver formellement la correction du noyau
- D'abord une question d'architecture logicielle

On peut rejouer la vérification sur une autre machine, un autre OS, avec un autre noyau : varier les conditions expérimentales
Les Mathématiques deviennent une science comme les autres !

A quoi ça sert ?

Ca sert à être sûr.

A quoi ça sert ?

Ca sert à être sûr.

- En maths

A quoi ça sert ?

Ca sert à être sûr.

- En maths
- En informatique : preuves de correction de logiciels critiques

A quoi ça sert ?

Ca sert à être sûr.

- En maths
- En informatique : preuves de correction de logiciels critiques
  - Logiciels embarqués (ABS, ligne 14...)
  - Robots médicaux
  - Argent en jeu : protocoles de cartes bancaires...

A quoi ça sert ?

Ca sert à être sûr.

- En maths
- En informatique : preuves de correction de logiciels critiques
  - Logiciels embarqués (ABS, ligne 14...)
  - Robots médicaux
  - Argent en jeu : protocoles de cartes bancaires...

On sait prouver des propriétés de programmes !

More good cop

Nouvelles utilisations de l'ordinateur dans la recherche scientifique :

- Physique : simulations, calcul numériques, Monte-Carlo...
- Biologie : génomique, simulations du cycle cellulaire...
- Économie : modèles d'interactions entre agents vérifiés par simulation
- Chimie
- Mathématiques (!)
- Informatique

On peut établir des vérités jusque là inaccessibles

Le télescope du mathématicien

plus grand nombre premier connu en 1951 :

$$(2^{148} + 1)/17 \quad \text{(44 chiffres)}$$

aujourd'hui : $2^{25964951} - 1$ (7.816.230 chiffres)
cause du progrès : évidente
Mais aussi de nouvelles mathématiques intéressantes

Le télescope du mathématicien

plus grand nombre premier connu en 1951 :

$$(2^{148}+1)/17 \quad \text{(44 chiffres)}$$

aujourd'hui : $2^{25964951}-1$ (7.816.230 chiffres)
cause du progrès : évidente
Mais aussi de nouvelles mathématiques intéressantes

Quel est le statut des ces "preuves" du point de vue formel ?

Le télescope du mathématicien

plus grand nombre premier connu en 1951 :

$$(2^{148}+1)/17 \quad (44 \text{ chiffres})$$

aujourd'hui : $2^{25964951}-1$ (7.816.230 chiffres)
cause du progrès : évidente
Mais aussi de nouvelles mathématiques intéressantes

Quel est le statut des ces "preuves" du point de vue formel ?

Dans quel *langage* sont-elles écrites ?

Formalismes calculatoires

Les objets du formalismes sont des programmes : l'addition est définie par un algorithme.
Qui dit programme dit calcul ; les objets sont identifiés modulo évaluation.

$$2 + 2 \rhd 4$$

par congruence :

$$2 + 2 = 4 \text{ est identifiée à } 4 = 4$$

$\Rightarrow$ preuve par réflexivité.
On n'a pas plus de théorèmes, mais les preuves sont plus courtes.

l'intégration du calcul donne plus de preuves *en pratique*

28554254222827961390156356610216400832616423864470288919924745660228440039060065387595457150553984323975451391589615029787839937056071435169747221107988791198200988477531339214282772016059009904586686254989084815735422480409022344297588352526004383890632616124076317387416881148592486188361873904175783145696016919574390765598280188599035784485910776836771755204340742877265780062667596159707595213278285556627816783856915818444364448125115624281367424904593632128101802760960881140100337757036354572512092407364692157679714619938761929656030268026179011813292501232304644443862230887792460937377301248168167242449367447448853777015578300688085264816151306714481479028836666406225727466527578712737464923109637500117090189078626332461957879573142569380507305611967758033808433338198750090296883193591309526982131114132239335649017848872898228815628260081383129614366384594543114404375382154287127774560644785856415921332844358020642271469491309176271644704168967807009677359042980890961675045292725800084350034483162829708990272864998199438764723457427626372969484830475091717418618113068851879274862261229334136892805663438446664632657247616727566083910565052897571389320211121495795311427946254553305387067821067601768750977866100460014602138408448021225053689054793742003095722096732954750721718115531871310231057902608580607est premier

2855425422282796139015635661021640083261642386447028891992474566022844
0039060065387595457150553984 615029787839937705607143516
9747221107988791198200988477 016059009904586686254989084
8157354224804090223442975883 326161240763173874168811485
9248618836187390417578314569 559828018859903557844859107
7683677175520434074287726578 759521327828555662781678385
6915818444364448125115624281 128101802760960881114010033
7757036354572512092407364692 761929656030268026179011813
2925012323046444438622308877 481681672424493674474488537
770155783006880852648161 062257274665275787 1273
74649231096375001170901 25693805073056119677 58
0338084333381987500902 1322393356490178488728

Proved in Coq

9822881562826008138312961436638459454311440437538215428712777456064478
5856415921332844358020642271469491309176271644704168967807009677359042
9808909616750452927258000843500344831628297089902728649981994387647234
5742762637296948483047509171741861811306885187927486226122933413689280
5663438446664632657247616727566083910565052897571389932021112149579531
1427946254553305387067821067601768750977866100460014602138408448021225
0536890547937420030957220967329547507217181155318713102310579026085806 07
est premier

Le calcul est partout

It is not just about the numbers

Certains théorèmes ne semblent pas être de nature calculatoire. Pourtant leurs seules preuves connues demandent des calculs importants.

- Le théorème des quatre couleurs (1976)
- La conjecture de Kepler (Thomas Hales, 1998)

Intéressant car les arguments utilisées mélangent de la déduction mathématique au sens usuel et des gros calculs mécaniques ; les deux parties sont sophistiquées.

Un problème de standards de vérification

Le calcul est partout

It is not just about the numbers

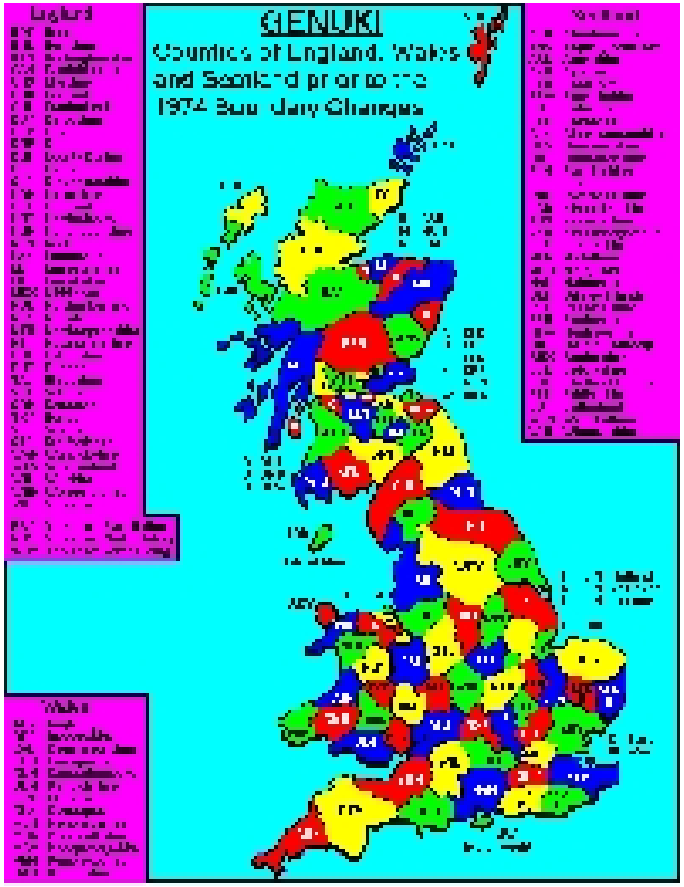
Certains théorèmes ne semblent pas être de nature calculatoire. Pourtant leurs seules preuves connues demandent des calculs importants.

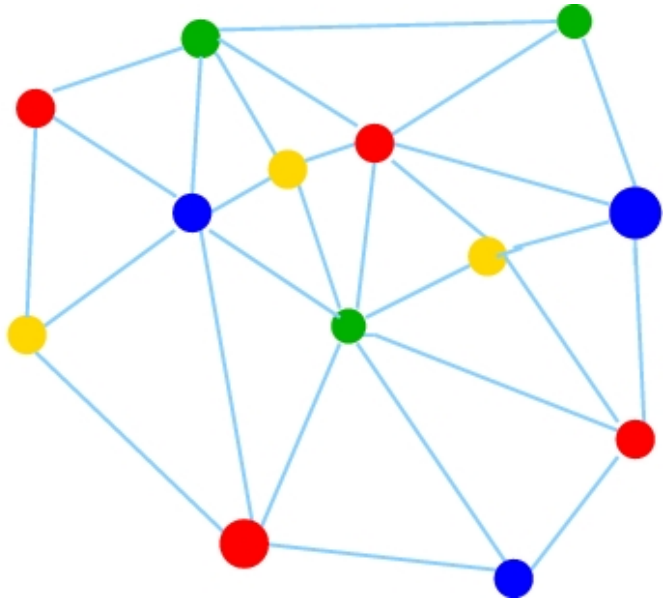
- Le théorème des quatre couleurs (1976) prouvé in Coq
- La conjecture de Kepler (Thomas Hales, 1998)

Intéressant car les arguments utilisées mélangent de la déduction mathématique au sens usuel et des gros calculs mécaniques ; les deux parties sont sophistiquées.

Un problème de standards de vérification

Les quatre couleurs





Historique

1852 conjecture par Francis Guthrie

1878 conjecture publiée par Cayley

1879 Preuve par Alfred Kempe

1880 Preuve par Tait

1890 Heawood découvre une erreur dans la preuve ; on n'obtient que le théorème des cinq couleurs.

1913 Birkhoff introduit les *configurations réductibles* et réduit le problème aux graphes internement 6-connexes. Contre-exemple a au moins 26 sommets.

1926 au moins 28 sommets (puis 32 en 1937, 36 en 1970)

1969 Heesch conçoit un programme pour obtenir le résultat

1976 Appel et Haken réalisent le programme de Hesch et prouvent le théorème. La preuve détaille 1476 configurations. La vérification de leur réductibilité demande 1200 heures de calcul.

1995 Robertson, Sanders, Seymour et Thomas proposent une preuve simplifiée : 633 configurations seulement. La vérification de la réductibilité prend 10mn sur un PC moderne.

La formalisation en Coq

Effort de longue durée : commencée à Rocquencourt (1999 ?), finie en 2004.
Georges Gonthier (INRIA puis MSR) moi-même.

- 20.000 lignes code (de preuve)
- suit les étapes de la preuve de 1995 (633 configurations),
- idées intéressantes sur la formalisation des graphes planaires,
- Pas mal de publicité (Science, Economist, Süddeutsche, Science& Vie, La Recherche...)

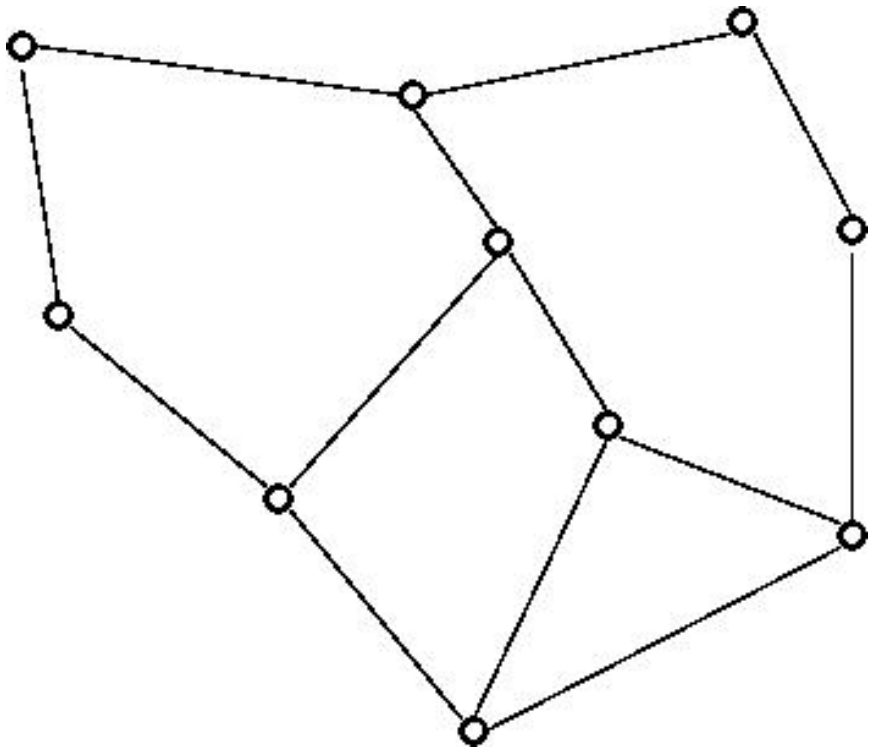
Au départ : un sujet excitant pour essayer les capacités de calcul de Coq

Où intervient le calcul ?

Revenons en 1879. . .

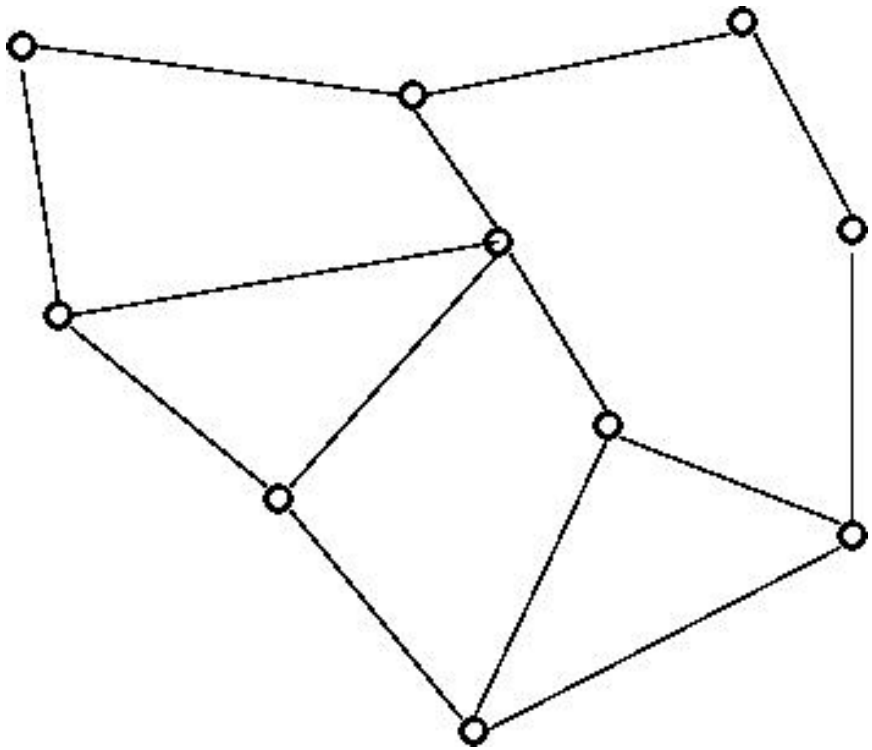
Qui peut le plus peut le moins

Première remarque : il suffit de savoir traiter les graphes triangulés



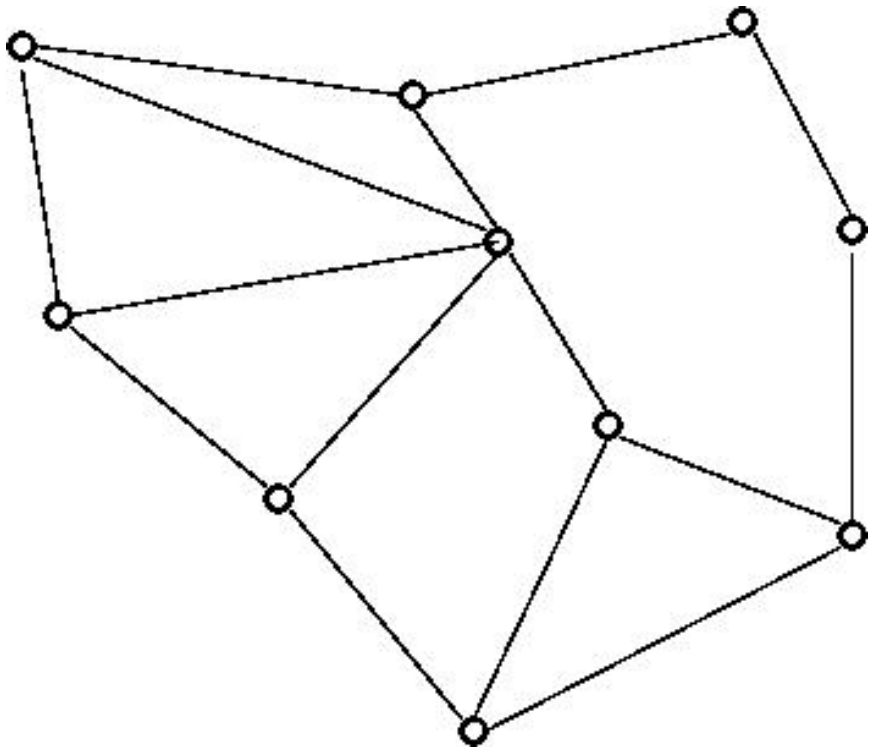
Qui peut le plus peut le moins

Première remarque : il suffit de savoir traiter les graphes triangulés



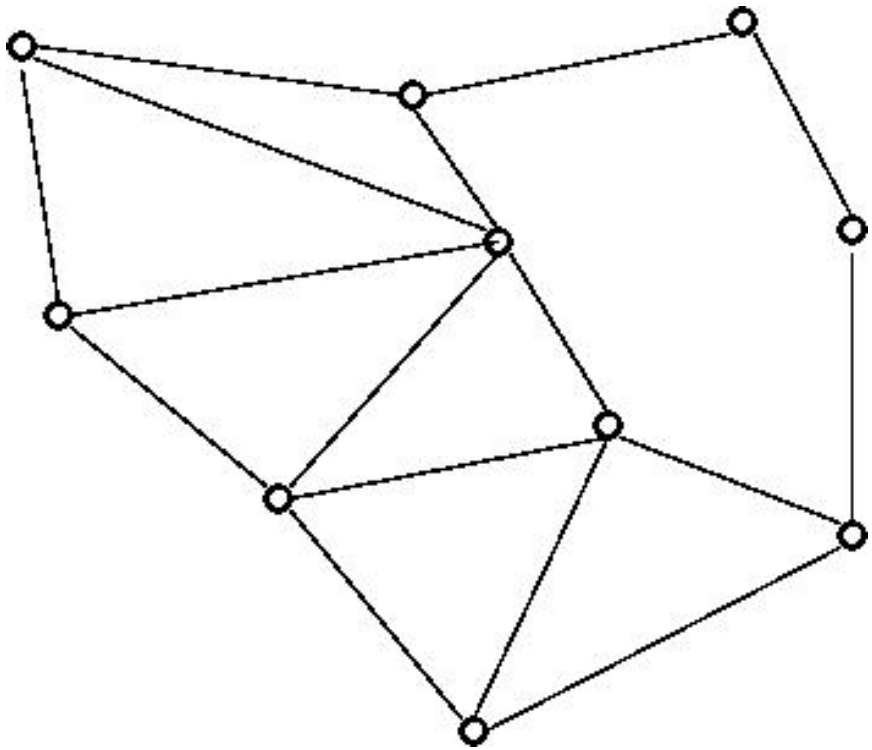
Qui peut le plus peut le moins

Première remarque : il suffit de savoir traiter les graphes triangulés



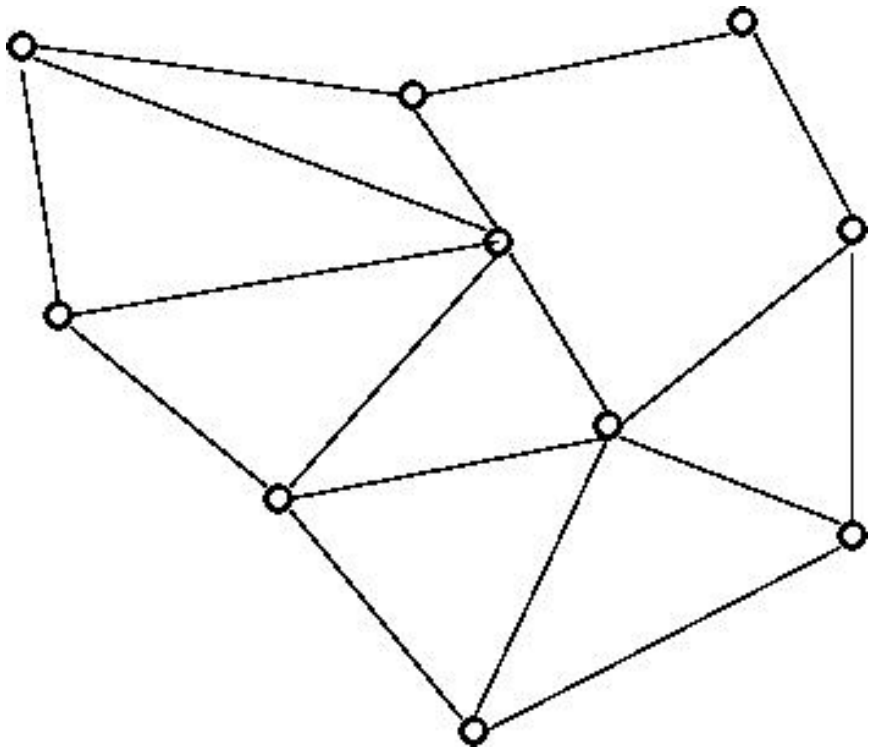
Qui peut le plus peut le moins

Première remarque : il suffit de savoir traiter les graphes triangulés



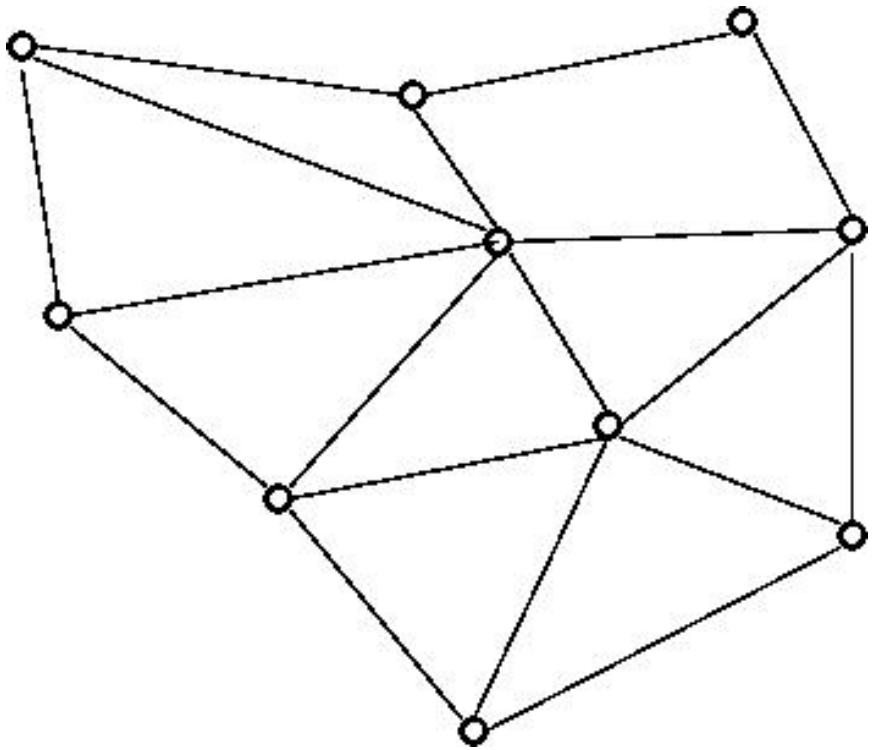
Qui peut le plus peut le moins

Première remarque : il suffit de savoir traiter les graphes triangulés



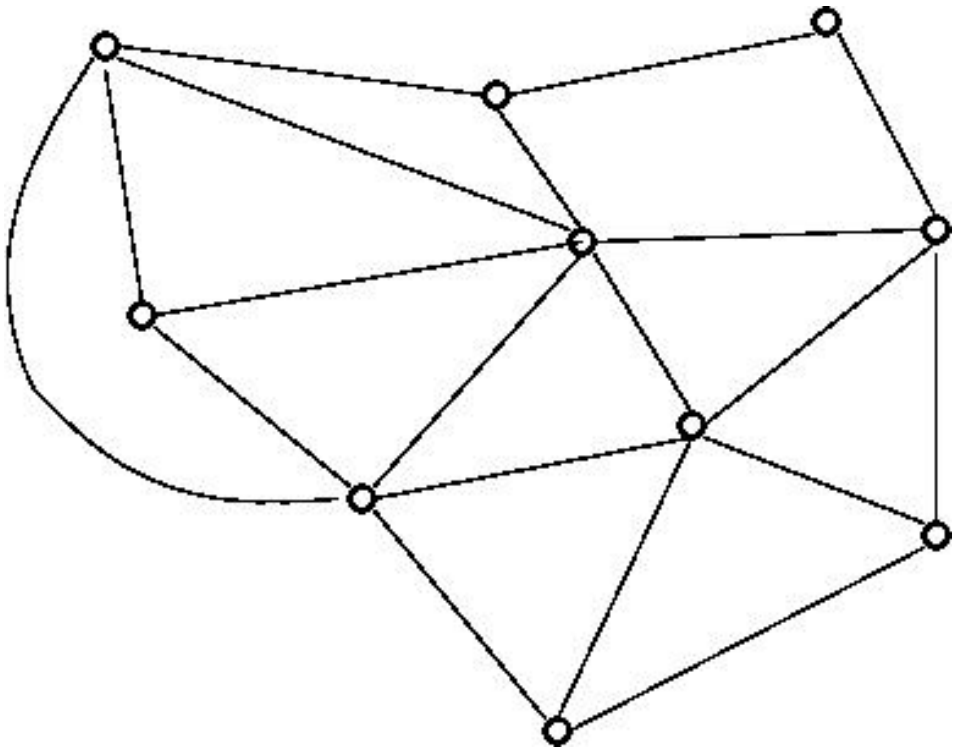
Qui peut le plus peut le moins

Première remarque : il suffit de savoir traiter les graphes triangulés



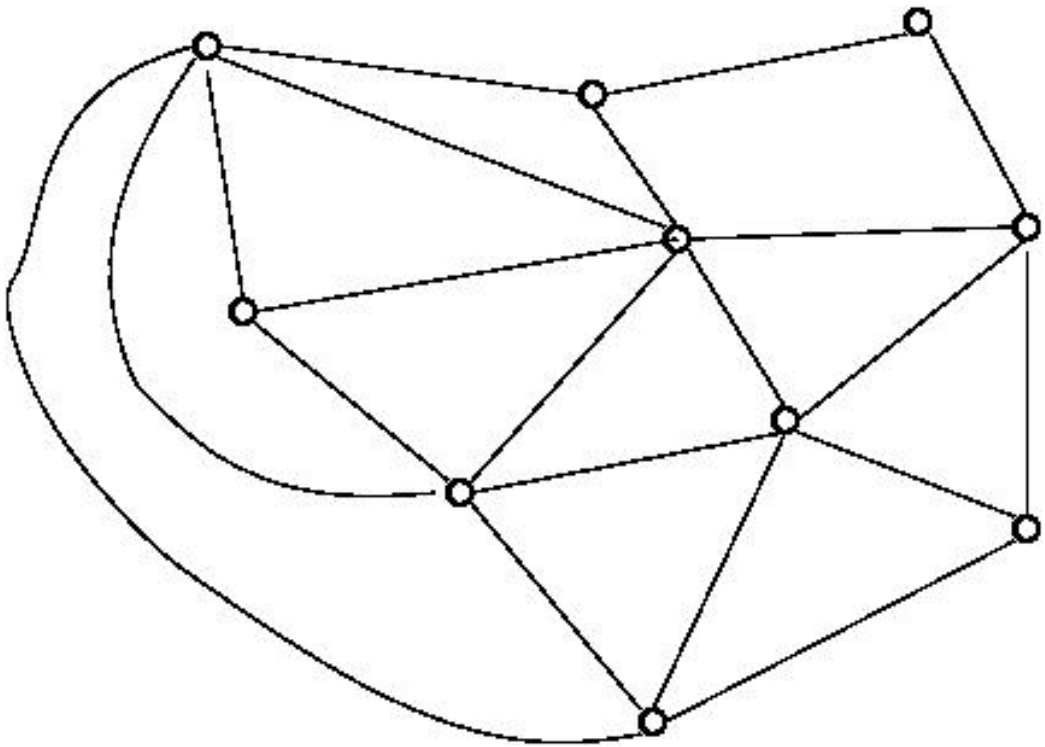
Qui peut le plus peut le moins

Première remarque : il suffit de savoir traiter les graphes triangulés



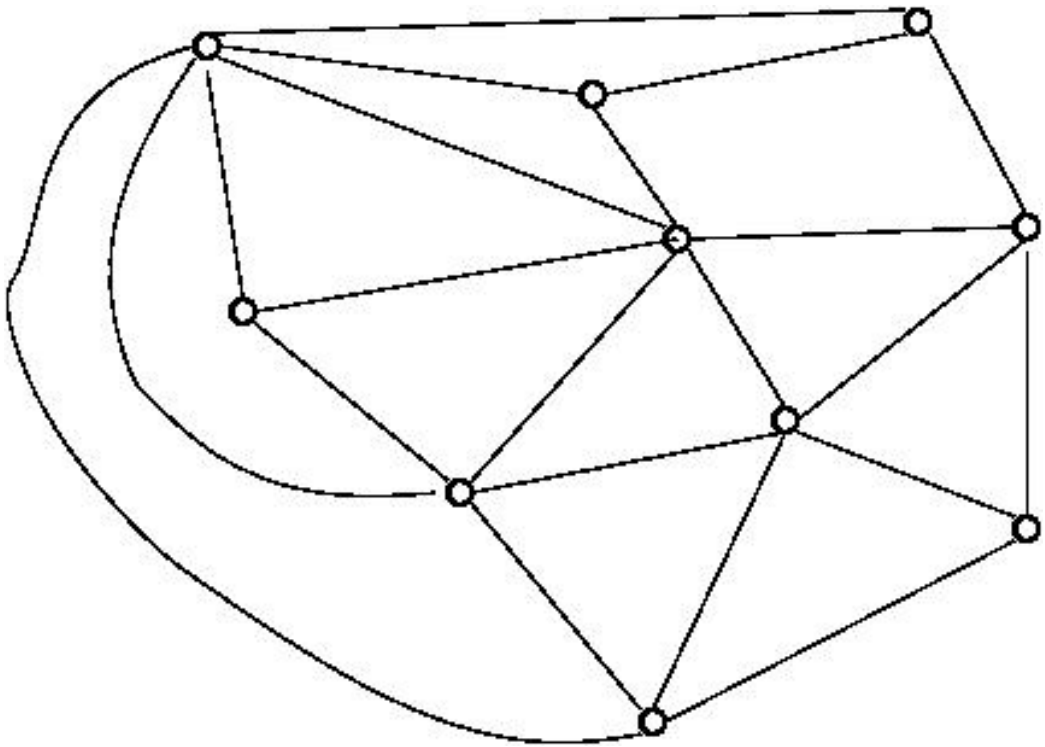
Qui peut le plus peut le moins

Première remarque : il suffit de savoir traiter les graphes triangulés



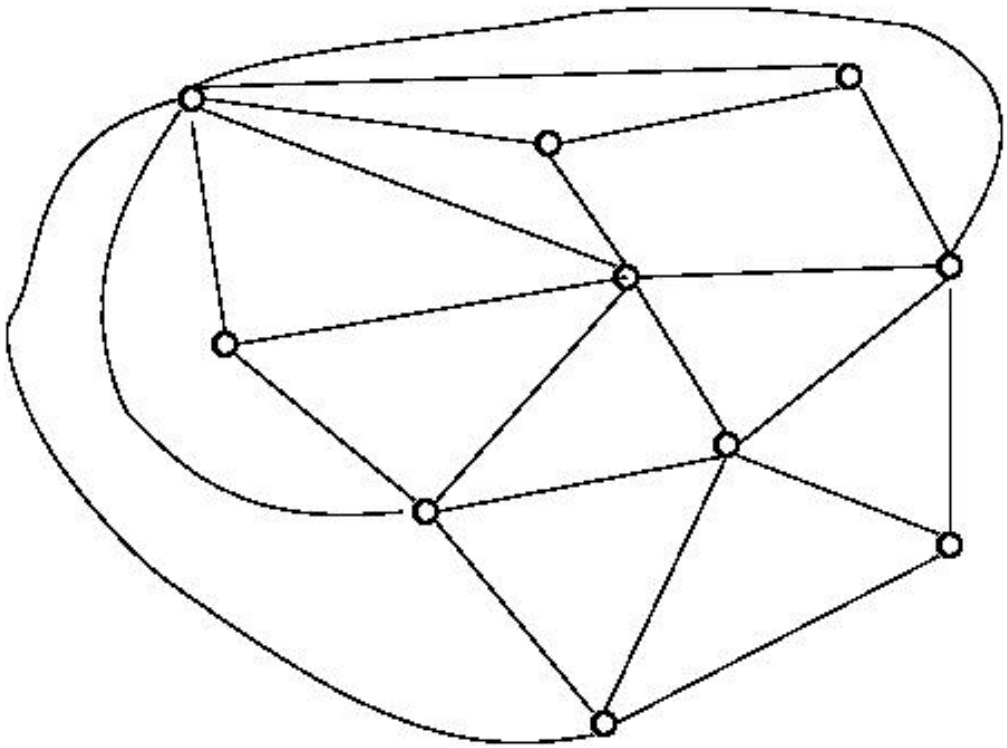
Qui peut le plus peut le moins

Première remarque : il suffit de savoir traiter les graphes triangulés



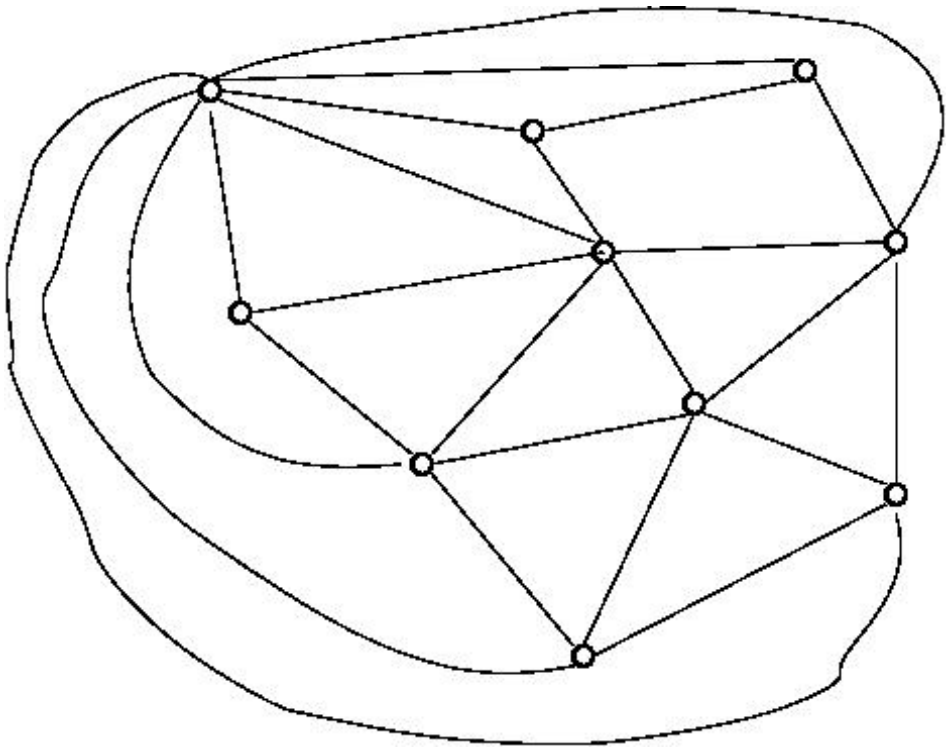
Qui peut le plus peut le moins

Première remarque : il suffit de savoir traiter les graphes triangulés



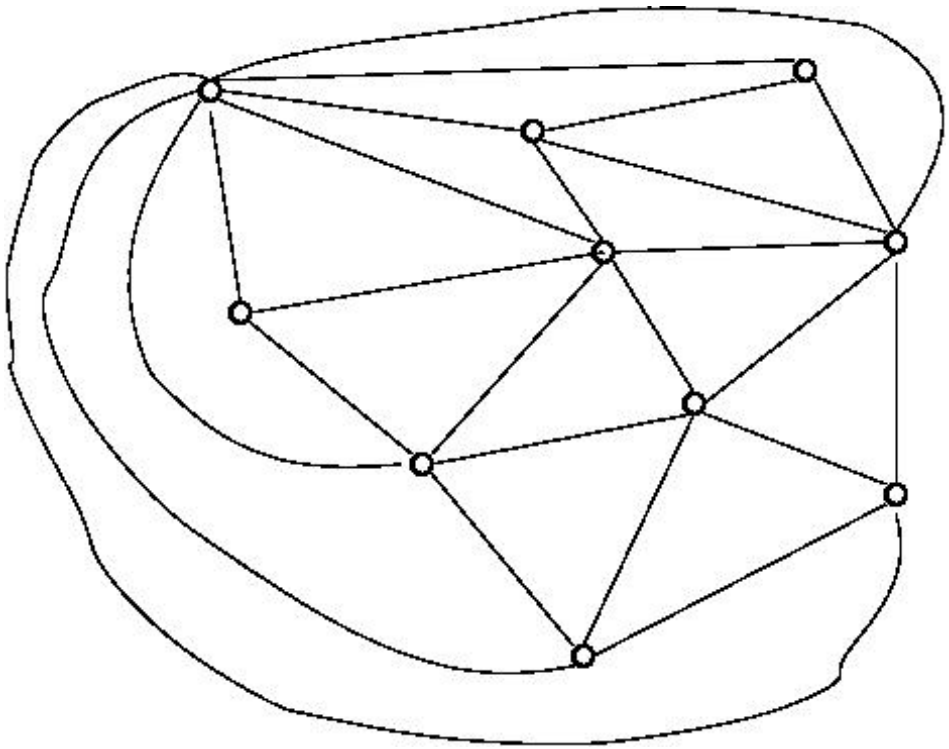
Qui peut le plus peut le moins

Première remarque : il suffit de savoir traiter les graphes triangulés



Qui peut le plus peut le moins

Première remarque : il suffit de savoir traiter les graphes triangulés



Formule d'Euler

Pour un graphe planaire :

$$2 + a = s + f$$

pour un graphe triangulé :

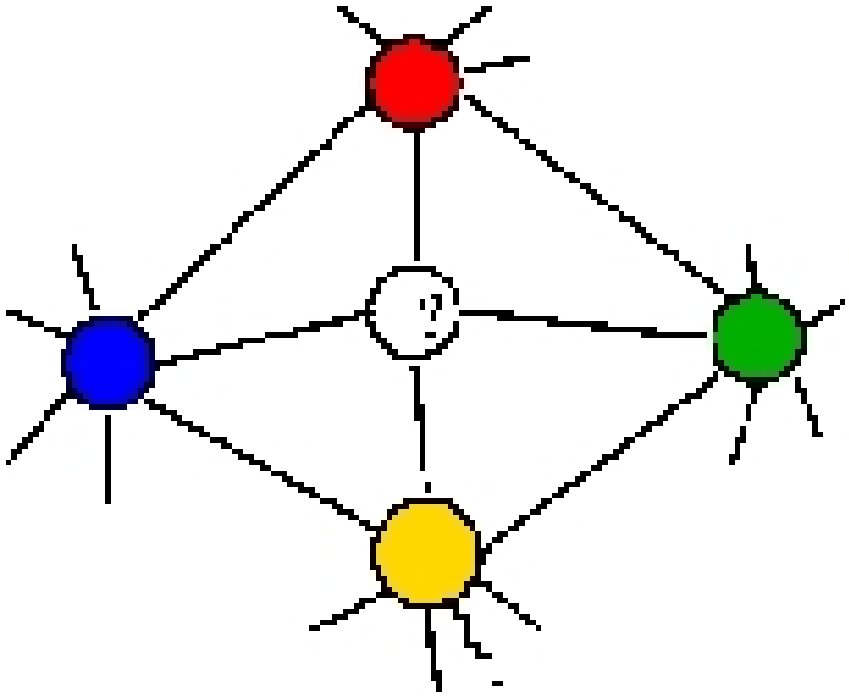
$$f = 2a/3$$

Degré moyen : $\overline{d} = 2a/s$

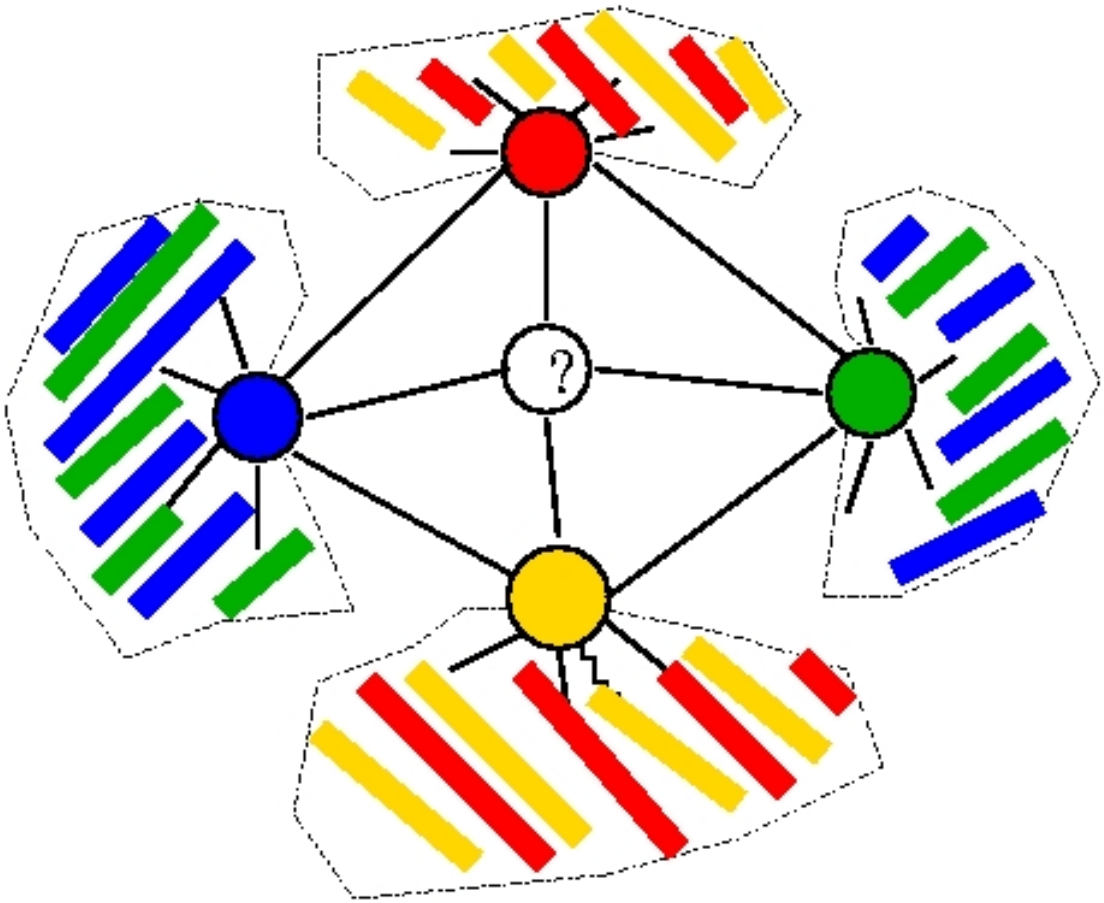
$$\overline{d} = 6 - 12/s$$

au moins un sommet a moins de 6 voisins

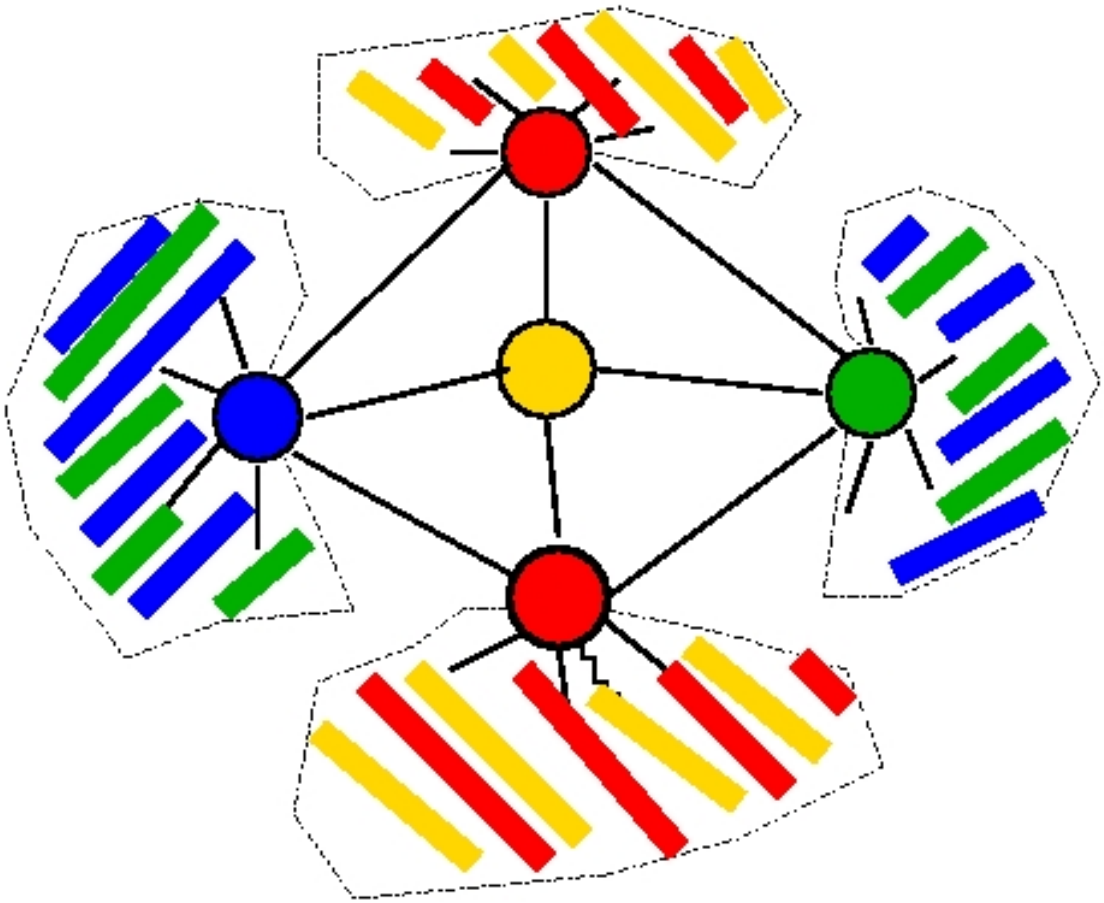
Sommet de degré 4



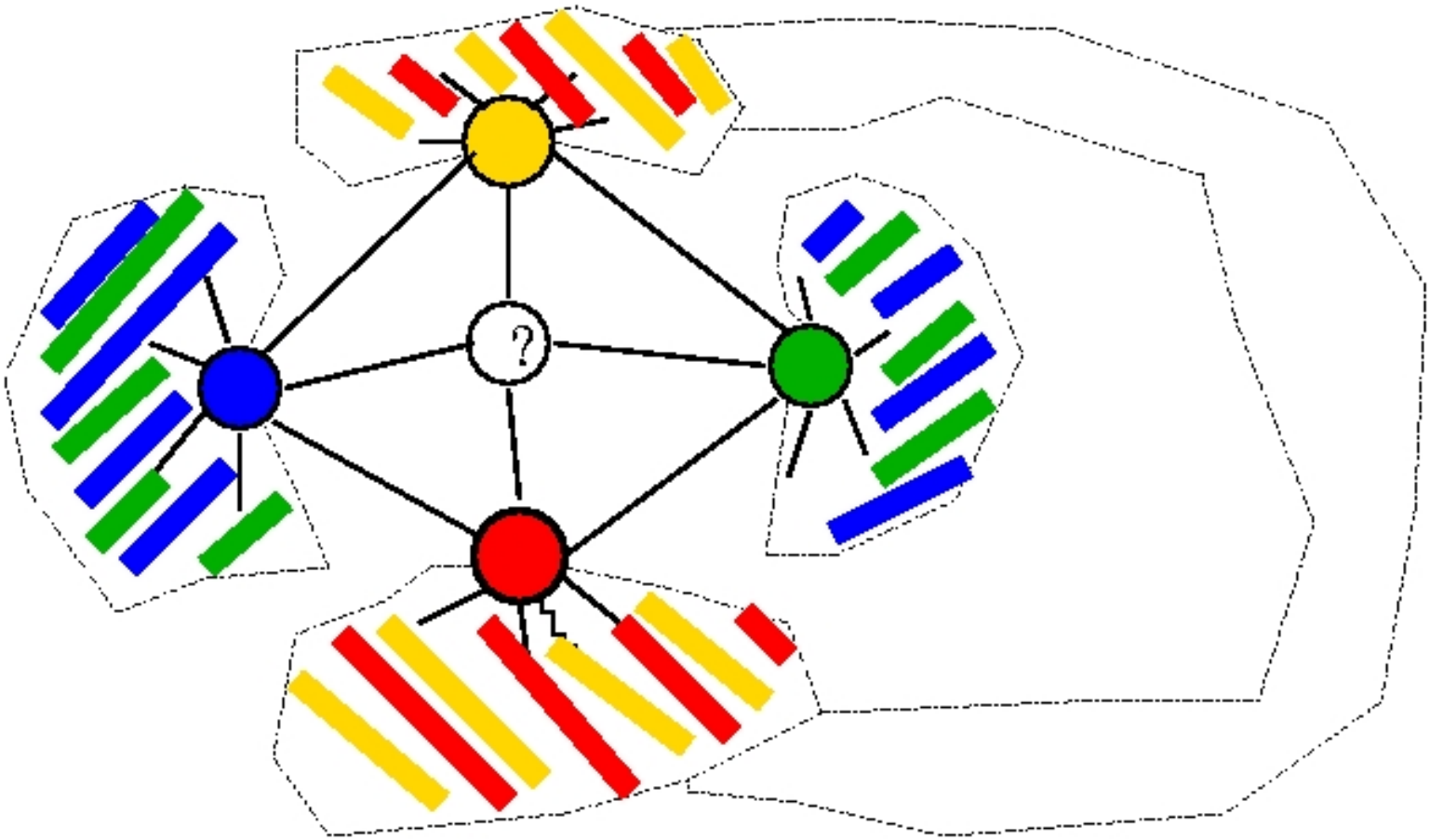
Sommet de degré 4



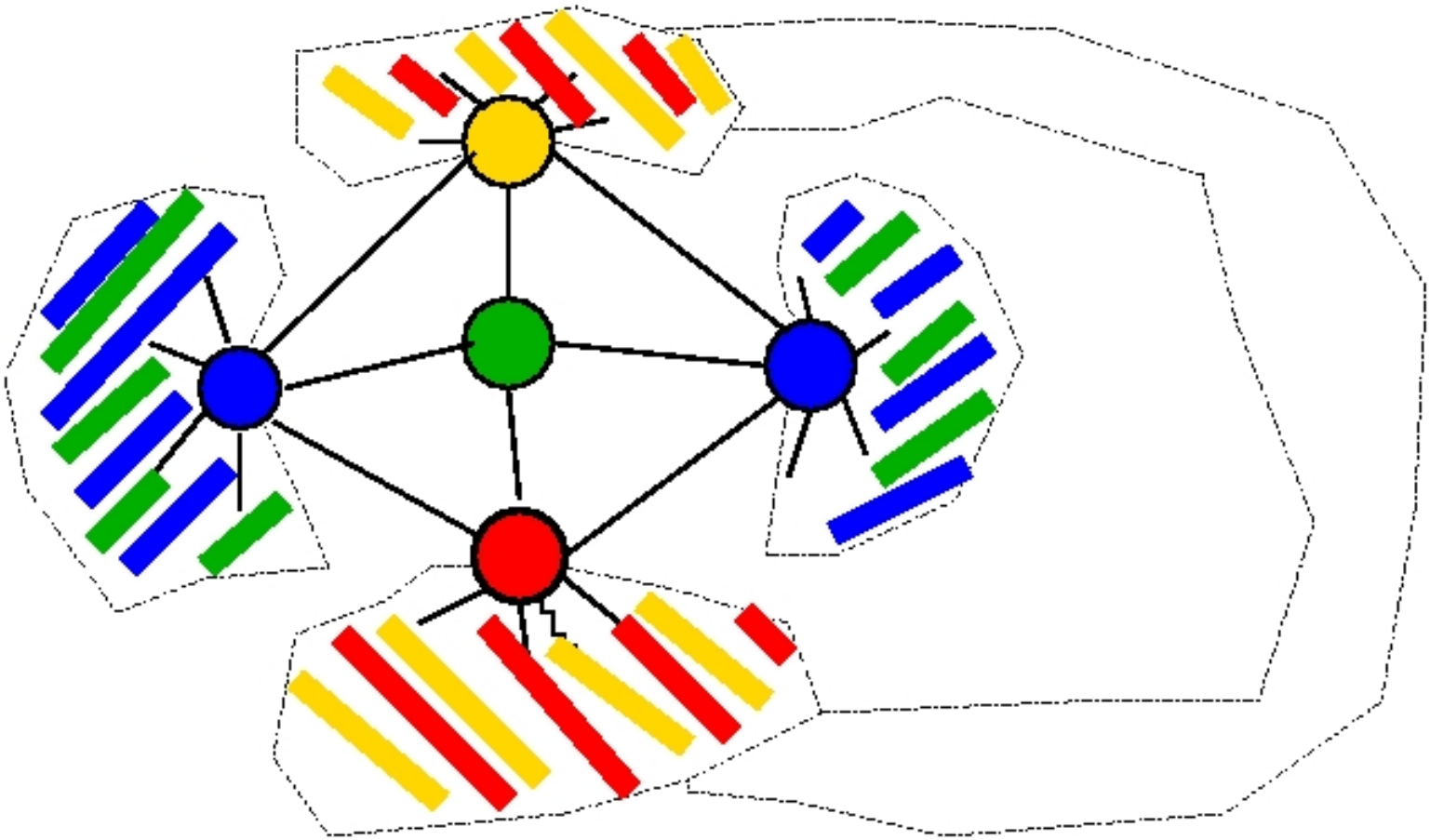
Sommet de degré 4



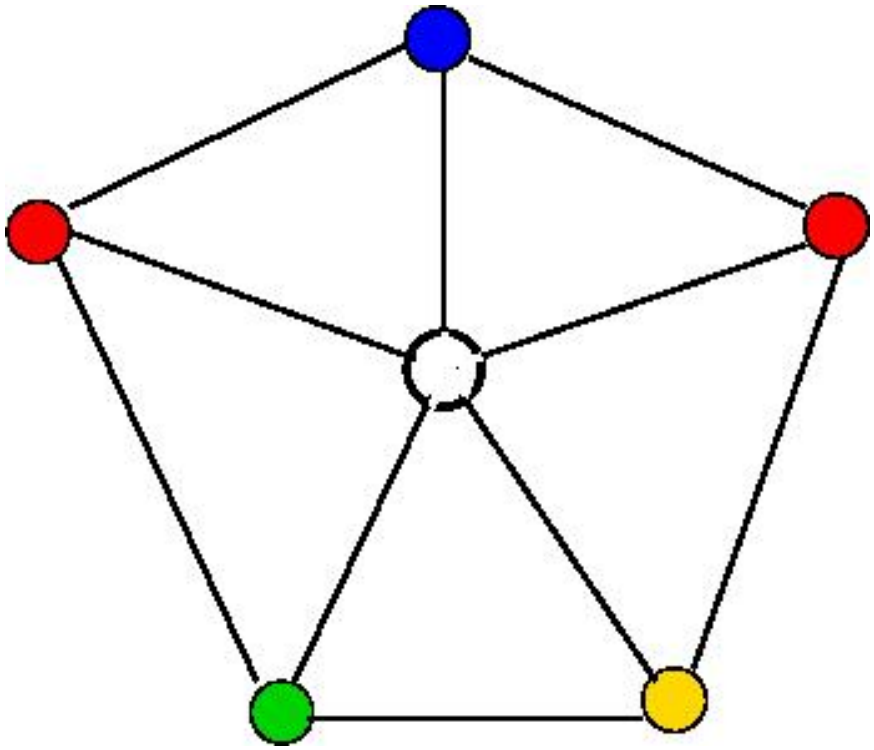
Sommet de degré 4



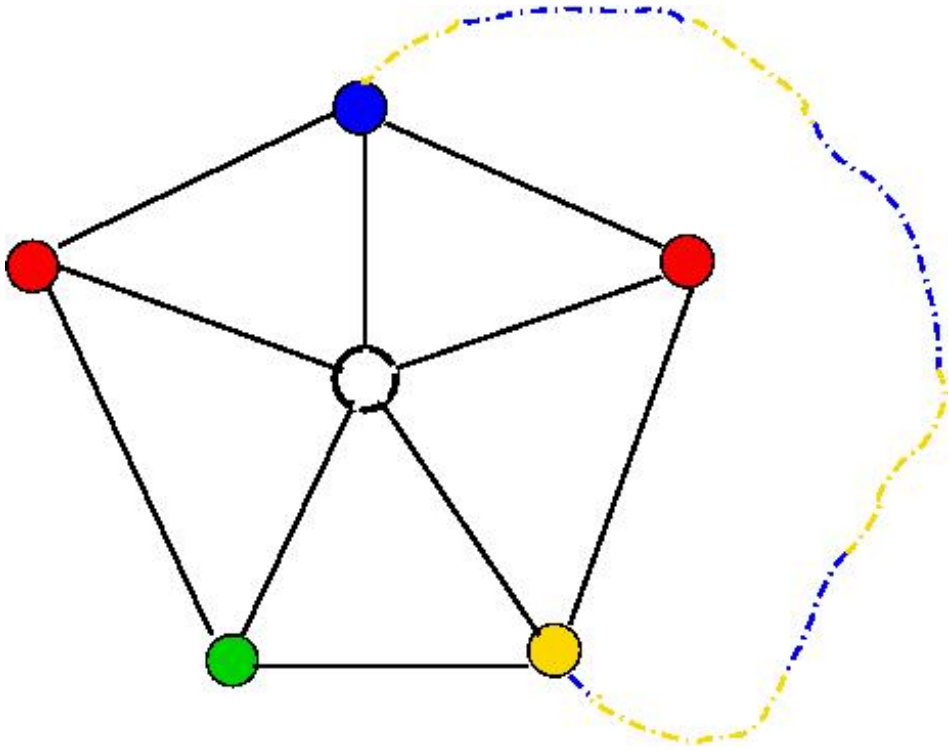
Sommet de degré 4



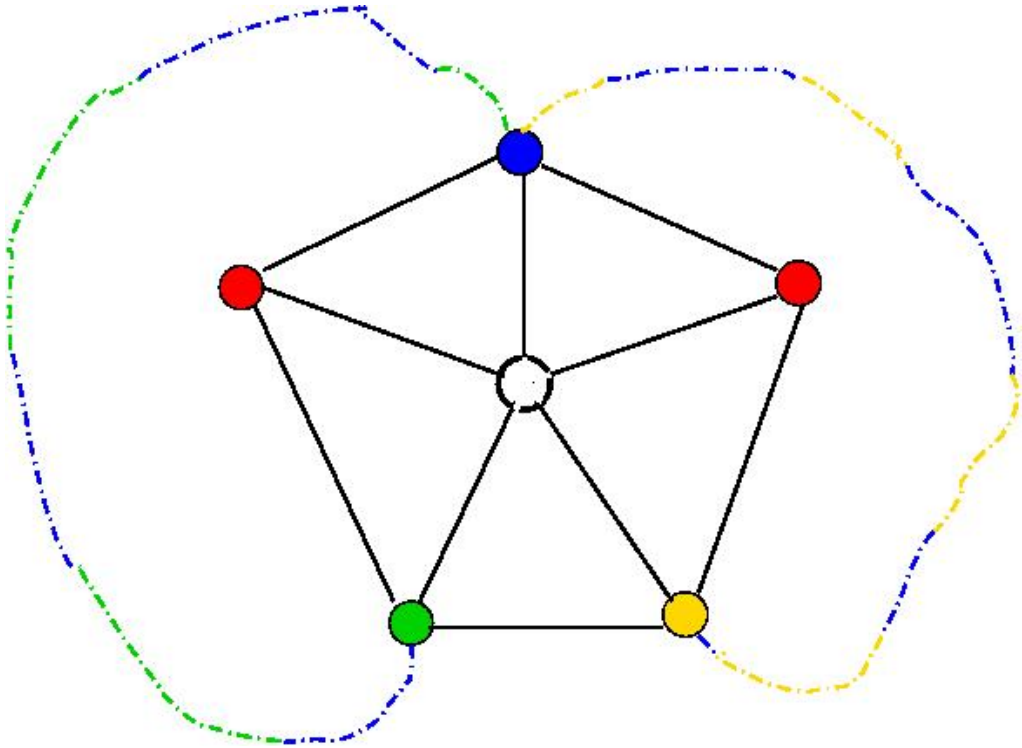
Sommet de degré 5



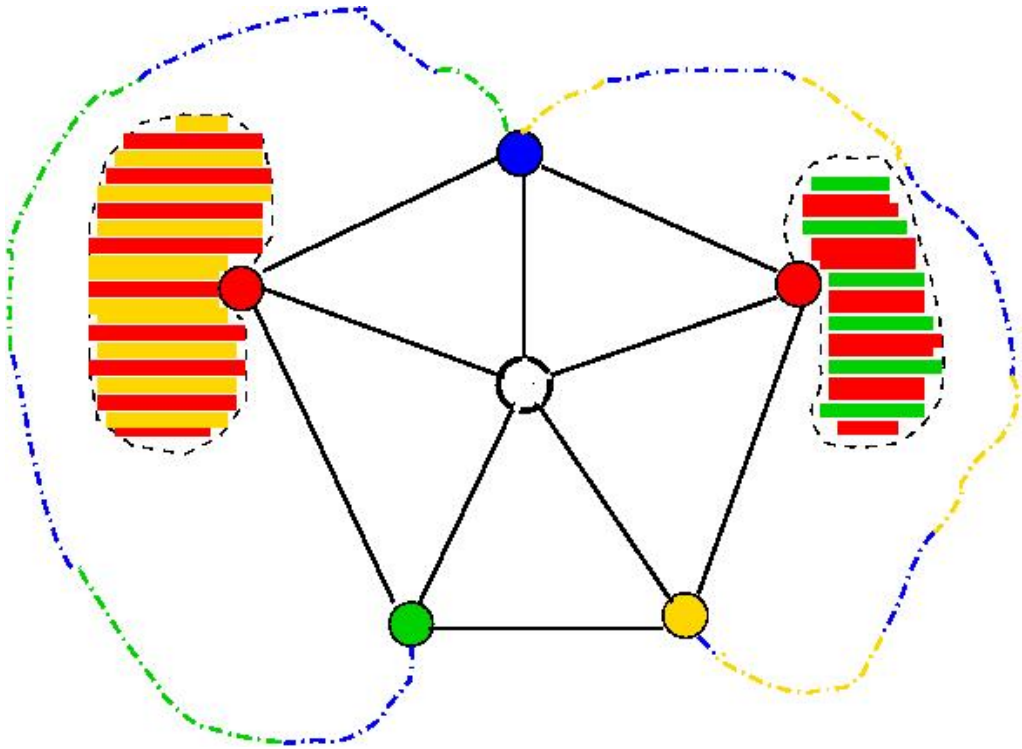
Sommet de degré 5



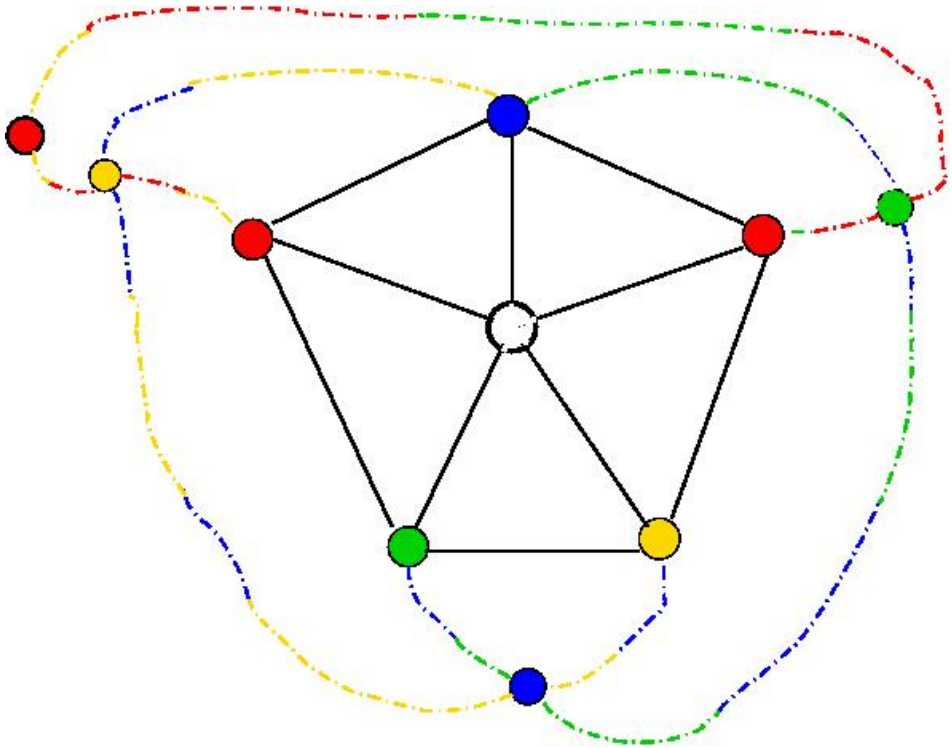
Sommet de degré 5



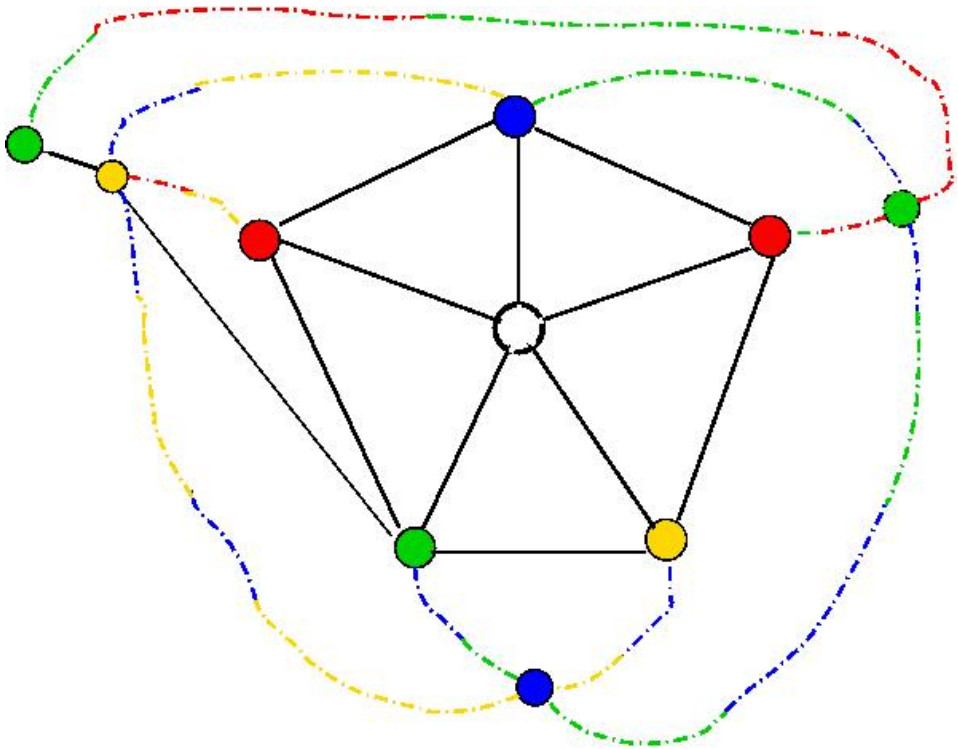
Sommet de degré 5



Sommet de degré 5

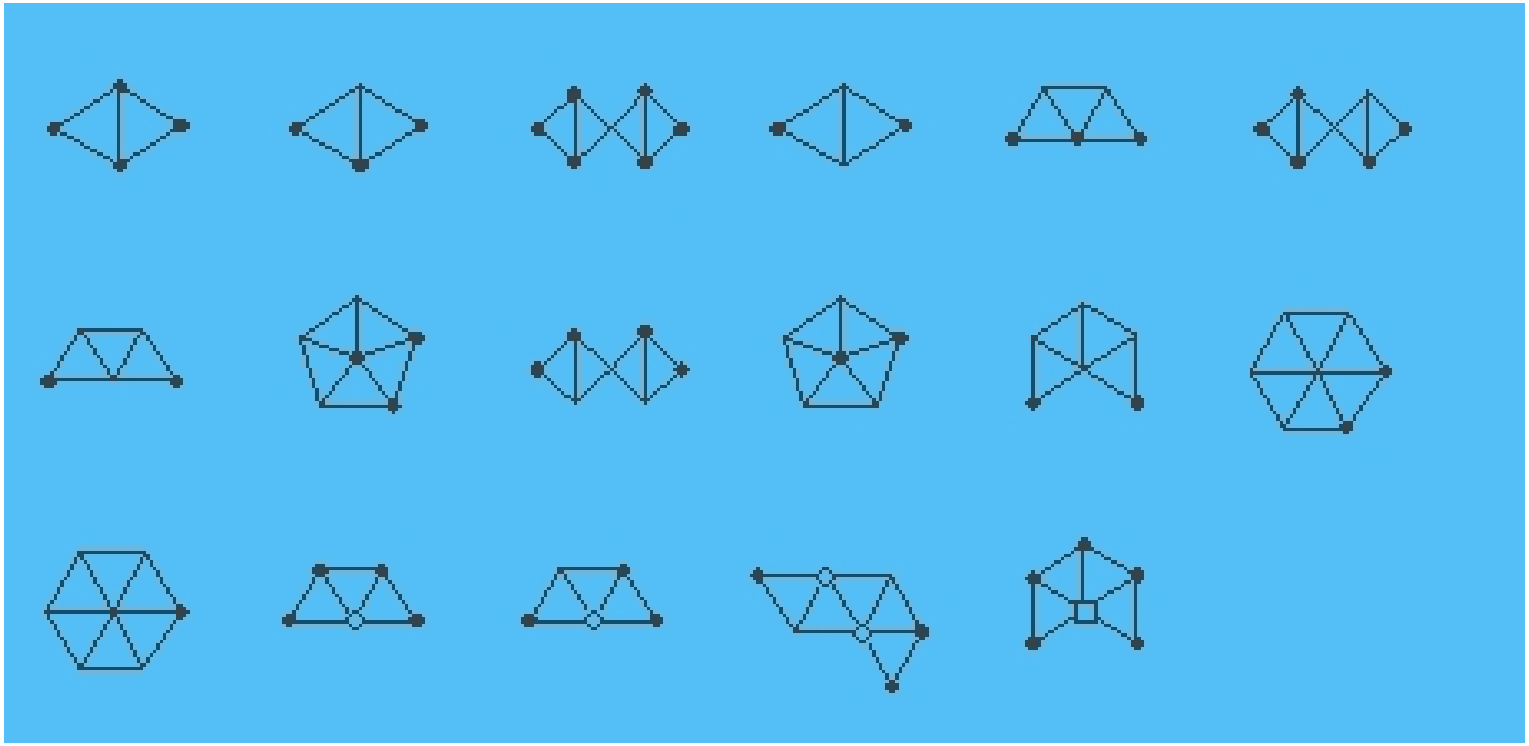


Sommet de degré 5



Configurations

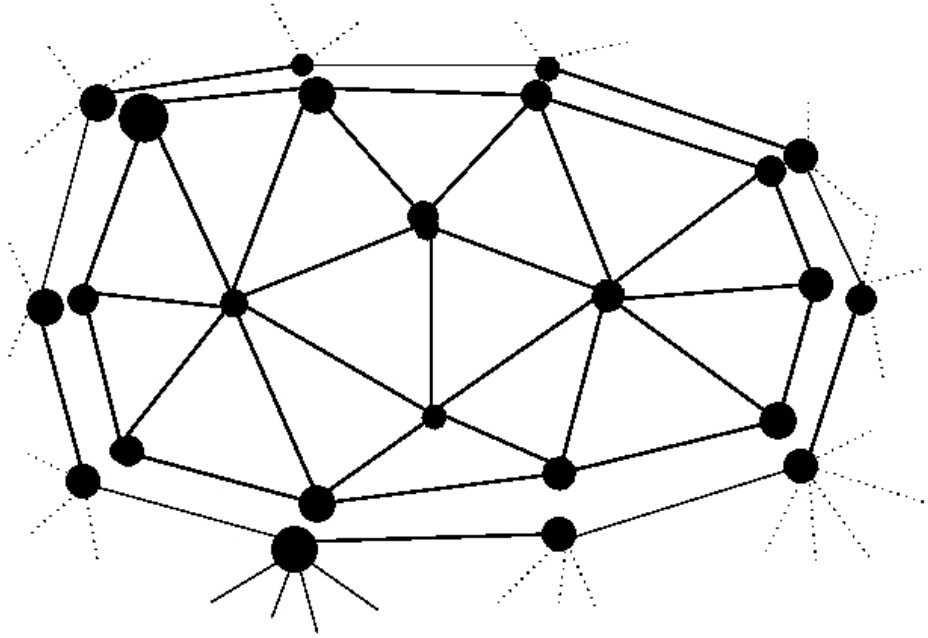
Un ensemble de graphes apparaissant dans tout graphe planaire triangulé (potentiellement problématique) :



et beaucoup d'autres (633 dans la preuve de 1995).

Reducible configuration

Principle :



configuration

= quasi-triangulation

La configuration est *réductible* s'il est possible de faire coïncider tout coloriage de l'extérieur avec un coloriage de la configuration possiblement après certains réarrangements.

explosion combinatoire

Pour chaque configuration il faut considérer :

- tous les coloriages de la frontière (jusqu'à 500.000)
- toutes les manières dont les composantes bi-colores intersectent la frontière (jusqu'à 1.500.000)

Vérifier que ces deux ensembles vérifient une condition de clôture bien choisie.
Pour chaque configuration, on arrive à faire coïncider les coloriages intérieurs et extérieurs sur la frontière. Parfois jusqu'à 25 re-coloriages sont nécessaires.

"réductibilité" = une forme de model-checking

A la limite du faisable en 1976 ; environ une pour toute la preuve avec la dernière version de Coq ; une dizaine de minutes pour le programme C.

The Future : Kepler's conjecture

The Future : Kepler's conjecture

Is there a better packing ?

The Future : Kepler's conjecture

Is there a better packing ?

Conjecture : Kepler, 1611 ..... Proof : Hales, 1998

The Future : Kepler's conjecture

Is there a better packing ?

Conjecture : Kepler, 1611 ..... Proof : Hales, 1998
"only to 99%"

The future : a small piece of Kepler's conjecture

Lemma 751442360

$$2.51^2 \leq x_1 \leq 2.696^2 \rightarrow$$
$$4 \leq x_2 \leq 2.168^2 \rightarrow$$
$$4 \leq x_3 \leq 2.168^2 \rightarrow$$
$$4 \leq x_4 \leq 2.51^2 \rightarrow$$
$$4 \leq x_5 \leq 2.51^2 \rightarrow$$
$$4 \leq x_6 \leq 2.51^2 \rightarrow$$

$$\frac{\begin{array}{c} -x_1x_3 - x_2x_4 + x_1x_5 + x_3x_6 - x_5x_6 + \\ x_2(-x_2 + x_1 + x_3 - x_4 + x_5 + x_6) \end{array}}{\sqrt{4x_2 \left(\begin{array}{c} x_2x_4(-x_2 + x_1 + x_3 - x_4 + x_5 + x_6) + \\ x_1x_5(x_2 - x_1 + x_3 + x_4 - x_5 + x_6) + \\ x_3x_6(x_2 + x_1 - x_3 + x_4 + x_5 - x_6) \\ - x_1x_3x_4 - x_2x_3x_5 - x_2x_1x_6 - x_4x_5x_6 \end{array} \right)}} < \tan\left(\frac{\pi}{2} - 0.74\right)$$

Des flottants dans les preuves

Les algorithmes permettant d'établir de telles inégalités viennent souvent de domaines plus "appliqués" (robotique, physique. . .).

Pour des calculs efficaces, on aime utiliser des *nombres flottants*.

Question habituelle : les erreurs d'arrondi !

C'est une domaine actif en informatique : L'arithmétique des ordinateurs.

On veut importer ces technologies dans nos preuves

Conclusions

- Des arguments plus complexes grâce au calcul informatique : perte de l'intuition.
  Comment être néanmoins sûr ? utiliser l'informatique !

Conclusions

- Des arguments plus complexes grâce au calcul informatique : perte de l'intuition.
  Comment être néanmoins sûr ? utiliser l'informatique !
- L'élégance mathématique n'est pas perdue ; mais elle change.

Conclusions

- Des arguments plus complexes grâce au calcul informatique : perte de l'intuition.
  Comment être néanmoins sûr ? utiliser l'informatique !
- L'élégance mathématique n'est pas perdue ; mais elle change.
- Rapport à la vérité est modifié.

Conclusions

- Des arguments plus complexes grâce au calcul informatique : perte de l'intuition.
  Comment être néanmoins sûr ? utiliser l'informatique !
- L'élégance mathématique n'est pas perdue ; mais elle change.
- Rapport à la vérité est modifié.
- Impact des méthodes formelles en mathématiques : grandissant.

Conclusions

- Des arguments plus complexes grâce au calcul informatique : perte de l'intuition.
  Comment être néanmoins sûr ? utiliser l'informatique !
- L'élégance mathématique n'est pas perdue ; mais elle change.
- Rapport à la vérité est modifié.
- Impact des méthodes formelles en mathématiques : grandissant.
- Impact des méthodes formelles en Physique : pas tout de suite.

Conclusions

- Des arguments plus complexes grâce au calcul informatique : perte de l'intuition.
  Comment être néanmoins sûr ? utiliser l'informatique !
- L'élégance mathématique n'est pas perdue ; mais elle change.
- Rapport à la vérité est modifié.
- Impact des méthodes formelles en mathématiques : grandissant.
- Impact des méthodes formelles en Physique : pas tout de suite.
- Nécessité d'une plus grande culture algorithmique

Pour en savoir plus

- Un livre : "Les Métamorphoses du Calcul", Gilles Dowek (Prix de Philosophie de l'Académie Française, 2007).
- Conférence de Gilles Kahn
  `www.inria.fr/MULTIMEDIA/Didactheque-fra.html`
- Un petit article : *Mathematics, an experimental science*, Herbert Wilff.
- Une conférence de Michel Serre
  `www.inria.fr/40ans/forum/video.fr.php`