Alain Giorgetti

Résumé de la séance du 24/10/2013 :

- problème des démonstrations longues (et de la relecture)
- problème des erreurs : comment les limiter ?
- exp. personnelle : un logiciel (un code) remplace-t-il une preuve ?

Dém longue ne veut pas dire difficile ou compliquée.

ex de la formalisation du th des 4 couleurs
de Feit-Thompson } (sur les groupes finis, le th est décidable)

Si démontrer = calculer + raisonner,
- calculer : logiciel de calcul formel
- raisonner : assistant de preuve formelle.

B : il faut un bon bagage (bcp de choses évidentes difficiles à formaliser → capacité d'abstraction du cerveau humain)

+ : on a une assurance supplémentaire

Jusqu'à présent, il n'y a pas de preuve nouvelle ! (ou très rarement).

Comment vérifier une démonstration ?

- avant publi, par l'auteur
- après publi, par le rapporteur

cf Dowek, Métamorphoses 2007

Idée : soumettre simultanément une démonstration formelle exécutable.

Étude de cas : Décomposition bijective des cartes pointées de genre donné.

une carte est un graphe plongé dans une surface, telle que chaque composante connexe du complément est homéomorphe à un disque ouvert.

- sommets
- faces
- arêtes
- genre

} formule d'Euler.

À isomorphisme près de la surface préservant l'orientation et du graphe, il y a unicité quand on précise 3 des 4 données.

carte pointée : carte avec un brin.

Avantage : elles n'ont pas d'automorphisme non trivial.

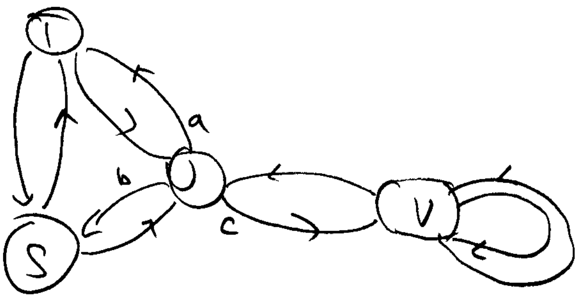
Description combinatoire : triplet (D,R,L)
ensemble fini ; permutation ; involution sans pt fixe. et $\langle R,L\rangle$ agit transitivement sur D.

D : les brins = darts = arêtes orientées

R : rotation autour d'un sommet

L : échange d'un brin en son inverse

$D = \{a, \dots, j\}$



$$R = \underset{\text{pour } U}{(abc)}\ \underset{\text{pour } T}{(de)}\ \underset{\text{pour } S}{(f\ g)}\ \underset{\text{pour } V}{(i\ j)}$$

$$L = (ad)(ef)(gb)(ch)(ij)$$

mais on ne voit pas la surface.

On définit un automorphisme de la carte : permutation p telle que $M^p = M$.
$(D, p^{-1}Rp, p^{-1}Lp)$.

Tout automorphisme déterminé par l'image d'un brin.

formule du genre d'Euler : $v - e + f = 2 - 2g$.

La q. est de calculer le # de cartes pointées de genre g avec v sommets f faces.

Idée : stocker plus de choses : prendre plus d'infos pour calculer ce #.

Formalisation : pb : les cartes pointées ne se décomposent pas en c.p. plus petites.
on se place dans le cadre des cartes séparées : k sommets distingués.
voire r brins pointés. $(r \geq 1)$.

cp : $k = 0$, $r = 1$.

On a alors une formule de récurrence.

Formellement, comment la certifier ?

- éq fonctionnelle
- relations entre polynômes.

1er pb : comment définir ce qu'est un ensemble fini ?
et les actions transitives.
et les permutations.

. . . .

Q publication = logiciel ?

- exécutable ?
- versions ...