# LES TROIS DIMENSIONS DES DÉMONSTRATIONS

**Yves GUIRAUD**

Institut de mathématiques de Luminy

http ://iml.univ-mrs.fr/~guiraud

Laboratoire de sûreté des logiciels

Saclay – 2 mars 2006

# Les deux dimensions des formules

# Les formules de SKS

Les *formules of SKS* sont les (classes d'équivalence de) termes :

- à deux sortes : une pour les *atomes* ($a$, $b$, etc.) et une pour les *formules* ($f$, $g$, etc.) ;
- engendrés par la grammaire suivante :

$$a ::= x_a \mid \bar{a} \,,$$

$$f ::= x_f \mid \bot \mid \top \mid a \mid f \wedge f \mid f \vee f \,;$$

- équipés des relations *structurelles* :
  - associativité et commutativité de $\wedge$ et de $\vee$,
  - unités : $\top \wedge f = f, \quad \bot \vee f = f, \quad \bot \wedge \bot = \bot, \quad \top \vee \top = \top,$
  - involutivité de $\bar{\cdot}$ : $\bar{\bar{a}} = a.$

## Les formules en tant qu'objets de dimension 2

Les formules de SKS sont remplacées par tous les « circuits » engendrés par :

- deux couleurs de « fils » : vert pour les atomes, orange pour les formules ;
- quatorze « composants », représentés ainsi :

Six « composants » pour la structure des formules de SKS plus huit pour la *gestion explicite des ressources* : duplication, effacement, échange.

Chaque « circuit » représente une famille de formules de SKS :

$((\bot \vee f) \wedge a), \overline{a})$ $\quad$ $\top$ $\quad$ $a \wedge a$ $\quad$ $a \wedge \overline{a}$

# Un peu de terminologie sur les polygraphes

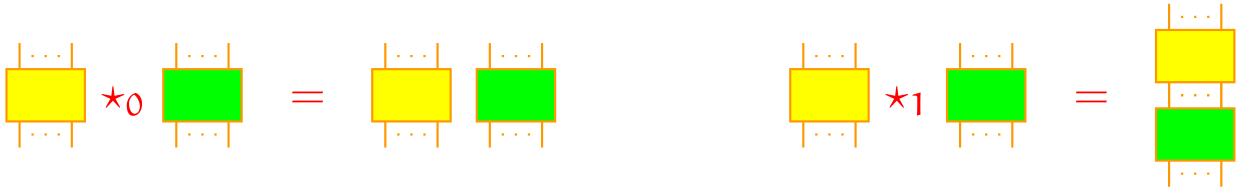
Les « circuits » forment un *2-polygraphe* :

– les deux sortes de « fils » sont ses *1-cellules*,

– les quatorze « composants » sont ses *2-cellules*,

– les « circuits » sont ses *2-chemins* ou *2-flèches*.

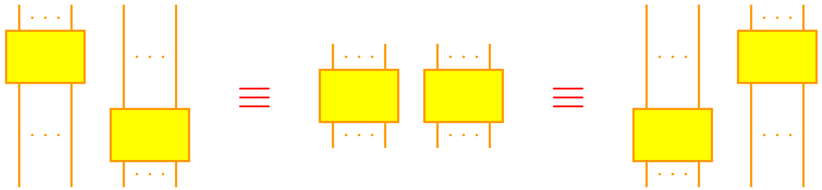
Le « 2 » représente les deux *compositions* possibles, une par dimension/direction :




La deuxième composition $f \star_1 g$ n'est définie que si le *1-but* de $f$ et la *1-source* de $g$ coïncident, ce qui s'écrit : $f_1^+ = g_1^-$.

# La relation d'échange $\equiv_{01}$

Les circuits sont considérés *modulo déformation topologique* :



Ces mouvements sont contrôlés par la *relation d'échange* $\equiv_{01}$ :

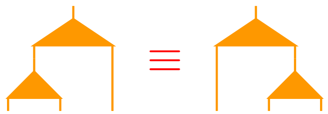
$$(f \star_0 g_1^-) \star_1 (f_1^+ \star_0 g) \ \equiv_{01}\ f \star_0 g \ \equiv_{01}\ (f_1^- \star_0 g) \star_1 (f \star_0 g_1^+)$$

Cette relation est invisible sur les formules.

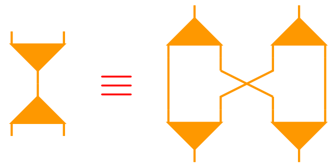
# Équivalence de $2$-chemins

Chaque famille de formules de SKS est représentée par plusieurs $2$-chemins car :

- La gestion des ressources est désormais explicite :

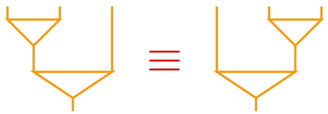


$(x, x, x) = (x, x, x)$

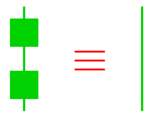


$(x \wedge y, x \wedge y) = (x \wedge y, x \wedge y)$

- Les formules de SKS sont munies des relations structurelles :



$(x \vee y) \vee z \equiv x \vee (y \vee z)$



$\bar{\bar{a}} \equiv a$

Ces équivalences sont des objets de dimension $3$, de même que les démonstrations.

# Les trois dimensions des démonstrations

# Les démonstrations de SKS

Les *démonstrations de SKS* sont tous les chemins de réécriture sur les formules engendrés par :

• les huit *règles de déduction de SKS* :

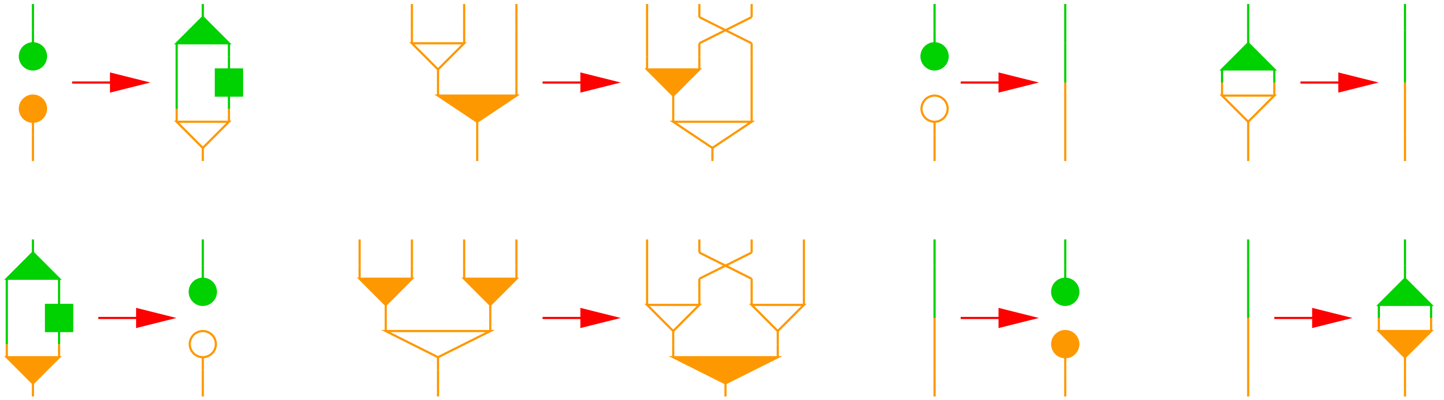
$$\frac{\top}{a \vee \bar{a}} \qquad \frac{(x \vee y) \wedge z}{(x \wedge z) \vee y} \qquad \frac{\bot}{a} \qquad \frac{a \vee a}{a}$$

$$\frac{a \wedge \bar{a}}{\bot} \qquad \frac{(x \wedge y) \vee (z \wedge t)}{(x \vee z) \wedge (y \vee t)} \qquad \frac{a}{\top} \qquad \frac{a}{a \wedge a}$$

• les relations structurelles, vues comme des règles utilisables dans les deux sens.

# Les règles de déduction en dimension 3

Les huit règles de déduction de SKS sont remplacées par des règles de réécriture portant sur les 2-chemins :

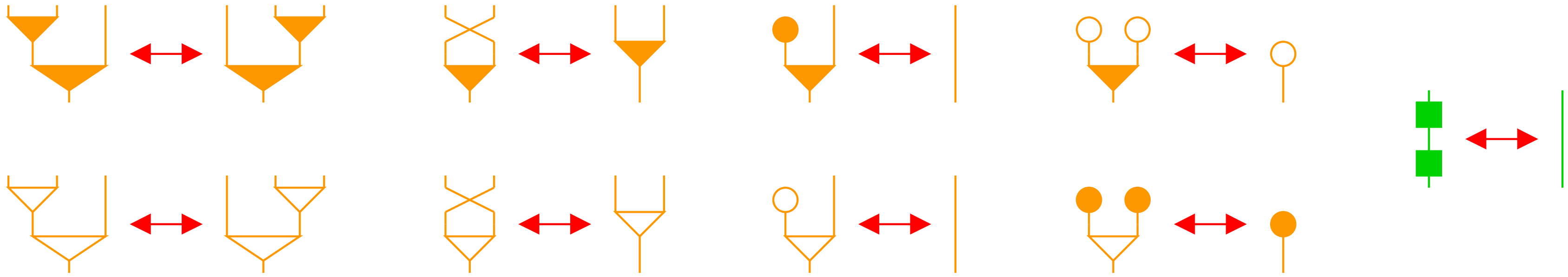


Ces objets sont des *3-cellules* sur le 2-polygraphe des formules.

Mais ces 3-cellules ne sont pas suffisantes pour décrire toutes les démonstrations de SKS : il faut encore leur ajouter des 3-cellules correspondant aux relations structurelles et aux opérations de gestion des ressources.

# Les $3$-cellules structurelles

Les relations structurelles sont remplacées par les $2 \times 9 = 18$ cellules suivantes :



Il y en a deux pour chacune des neuf équations : une dans chaque direction.

C'est une manière, parmi d'autres, de représenter une équation entre formules.

On peut, au choix, remplacer une telle équation par :

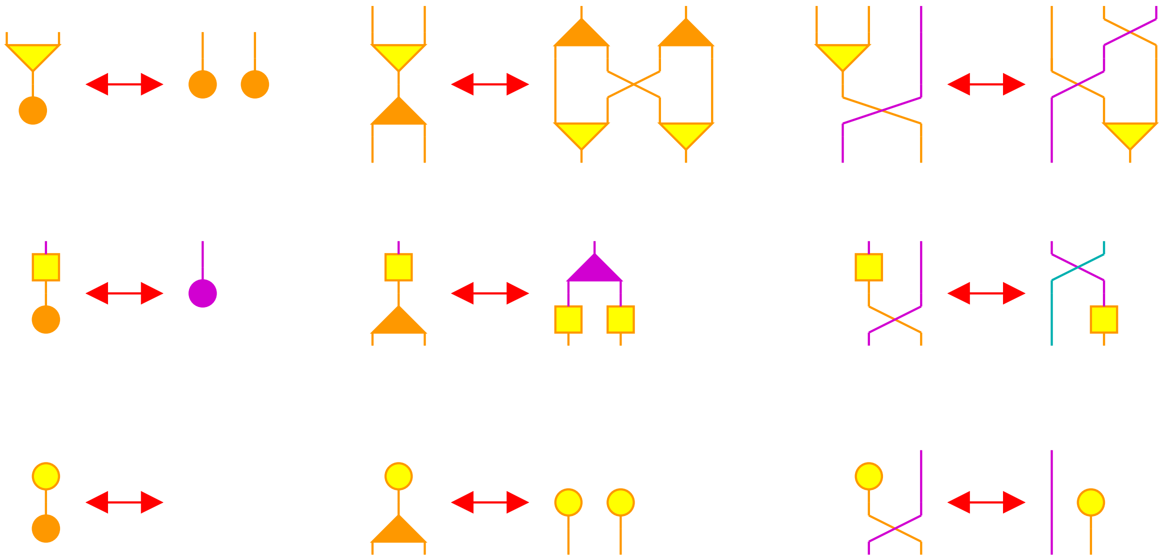
- une équation entre les $2$-chemins correspondant (on travaille dans un quotient),
- un couple de $3$-cellules (comme ici),
- une seule $3$-cellule (si l'on dispose d'une présentation convergente équivalente).

Il y a d'autres possibilités comme nous le verrons plus loin.

# Les 3-cellules de gestion des ressources

Elles sont divisées en deux familles :

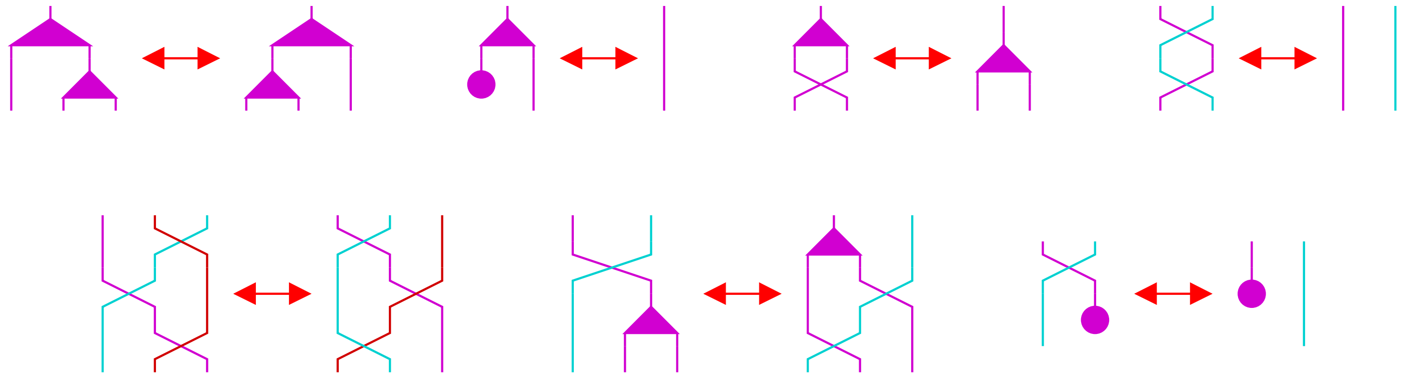
- une première famille avec $2 \times 24 = 48$ cellules :



# Les $3$-cellules de gestion des ressources

Elles sont divisées en deux familles :

- une seconde famille avec $2 \times 26 = 52$ cellules :



Si on ne considère que ces $3$-cellules de gestion des ressources, on peut les présenter de manière convergente.

On peut ainsi calculer un représentant canonique pour tous les $2$-chemins qui représentent la même formule de SKS (sans les relations structurelles).

Mais si on ajoute les $3$-cellules de déduction, cela crée des problèmes de confluence.

## The $3$-polygraph of proofs

En ajoutant toutes ces $3$-cellules au $2$-polygraphe des formules, on obtient un *3-polygraphe* avec :

- deux $1$-cellules (atome et formule),
- quatorze $2$-cellules (opérations de la structure),
- cent vingt-six $3$-cellules, dont cent pour la gestion des ressources.

On démontre que :

- Chaque chemin de réécriture engendré par les $3$-cellules représente une démonstration de SKS.
- Chaque démonstration de SKS peut être représentée par au moins un chemin de réécriture.

Mais ces chemins de réécriture possèdent une structure : *ce sont des $3$-chemins.*

Révélons cette structure et voyons ce qui se passe...

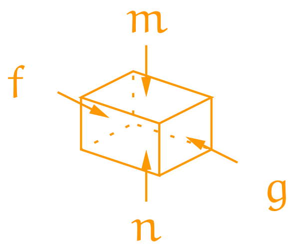
# La structure des 3-chemins

# Les $3$-chemins d'un polygraphe

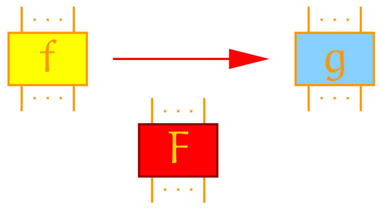
Les *3-chemins* d'un polygraphe sont définis par récurrence ainsi :

• Une $3$-cellule $F : f \longrightarrow g$ est aussi un $3$-chemin, de $f$ (sa *2-source*) vers $g$ (son *2-but*).

On représentera temporairement $F$ comme un « bloc » :



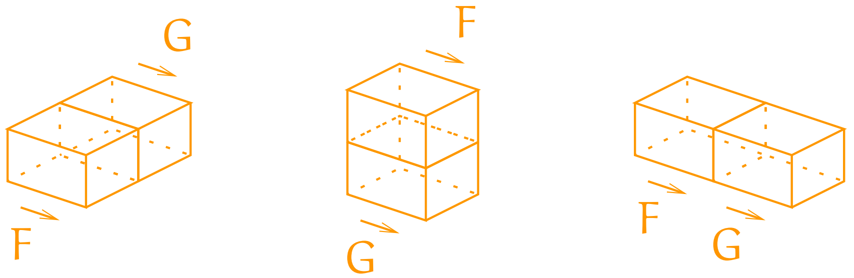

On peut couper verticalement ce bloc en trois endroits pour obtenir :




• Chaque $2$-chemin $f$ est un $3$-chemin de $f$ dans $f$.

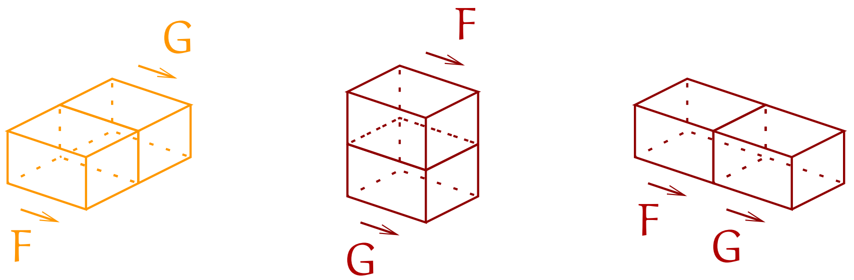
# Les $3$-chemins d'un polygraphe

• Si $F : f \to f'$ et $G : g \to g'$ sont des $3$-chemins, on peut les composer de trois manières différentes :



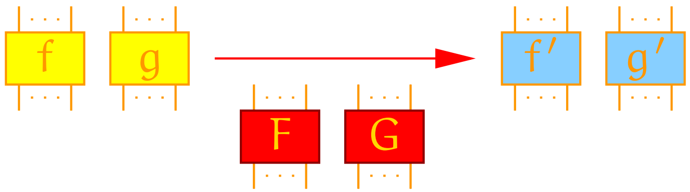
# Les $3$-chemins d'un polygraphe

• Si $F : f \longrightarrow f'$ et $G : g \longrightarrow g'$ sont des $3$-chemins, on peut les composer de trois manières différentes :



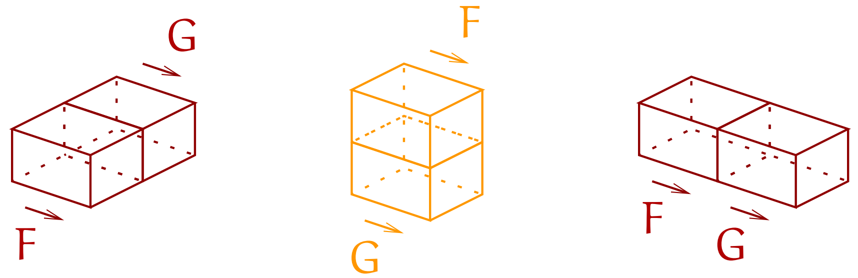

La première opération donne $F \star_0 G : f \star_0 g \longrightarrow f' \star_0 g'$.

En coupe :



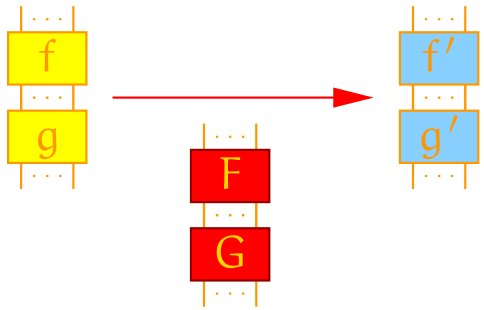
# Les 3-chemins d'un polygraphe

• Si $F : f \longrightarrow f'$ et $G : g \longrightarrow g'$ sont des 3-chemins, on peut les composer de trois manières différentes :



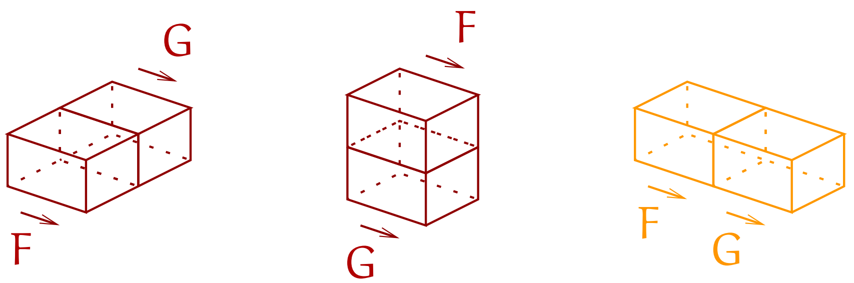

La seconde opération donne $F \star_1 G : f \star_1 g \longrightarrow f' \star_1 g'$ (seulement si $F_1^+ = G_1^-$).

En coupe :



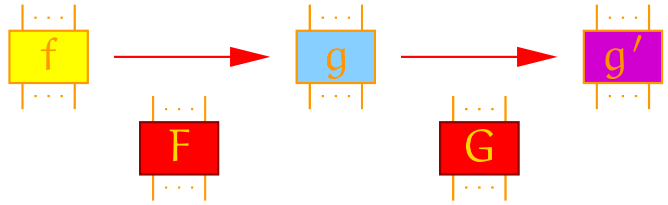
# Les $3$-chemins d'un polygraphe

• Si $F : f \to f'$ et $G : g \to g'$ sont des $3$-chemins, on peut les composer de trois manières différentes :



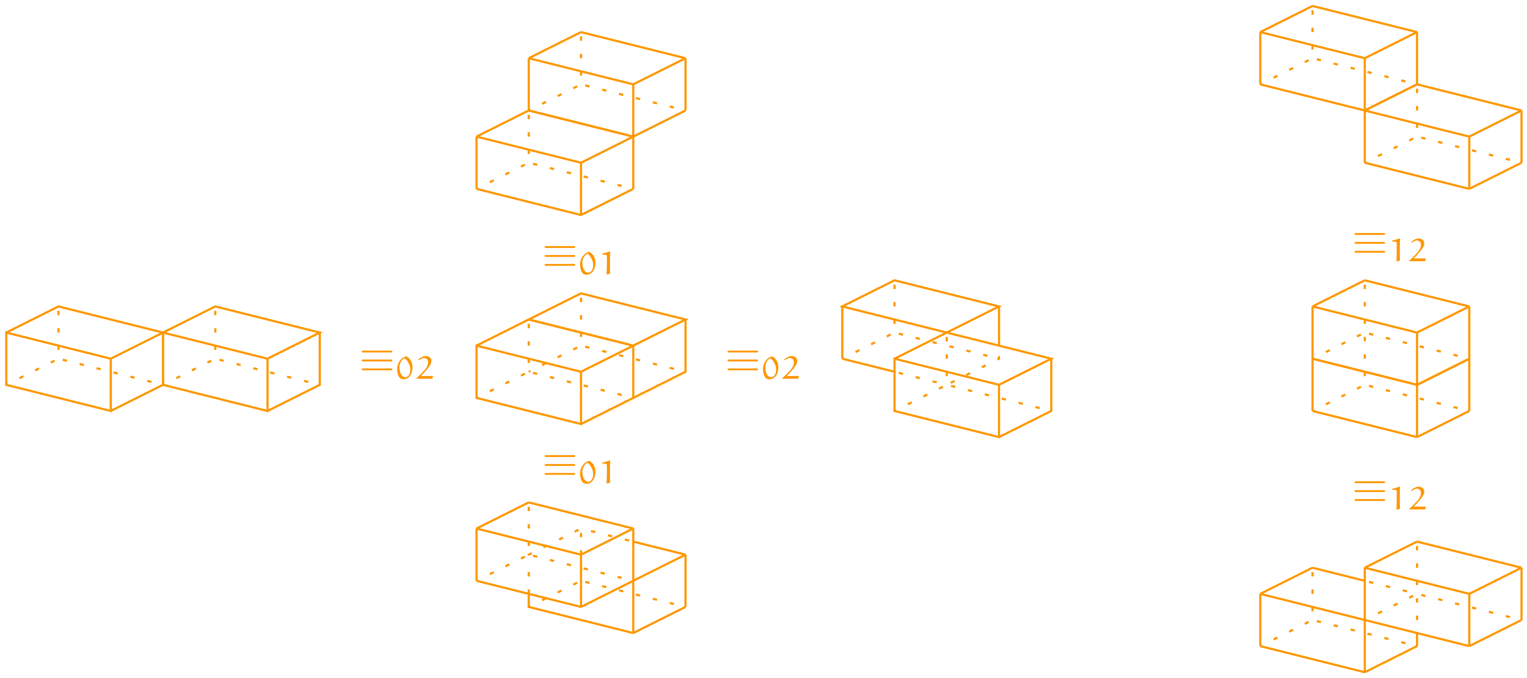

La troisième opération donne $F \star_2 G : f \to g'$ (seulement si $F_2^+ = G_2^-$).

En coupe :



# Relations d’échange

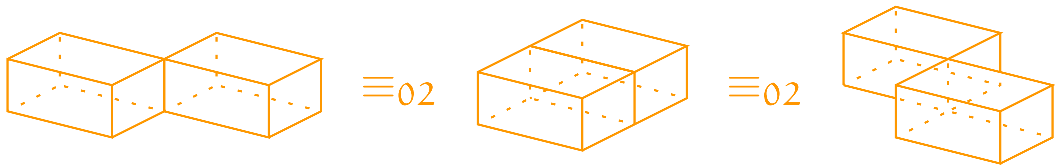
Dans un polygraphe, on identifie les 3-chemins *modulo relations d’échange* :




La relation $\equiv_{01}$ est un « fantôme » provenant de la dimension 2 (ou l’inverse). Mais les deux autres sont nouvelles et elles ont une interprétation logique : elles identifient les 3-flèches qui représentent la même démonstration mais qui sont distinguées par la syntaxe utilisée pour écrire les formules (« bureaucratie »).

# La relation $\equiv_{02}$

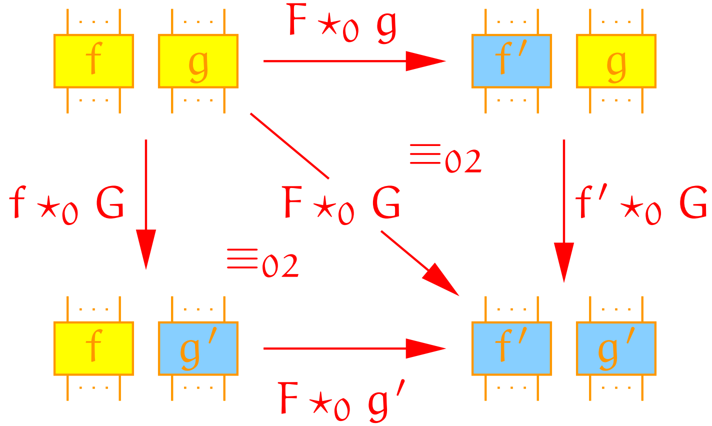
Regardons :




On peut aussi l'écrire :

$$(F \star_0 G_2^-) \star_2 (F_2^+ \star_0 G) \;\equiv_{02}\; F \star_0 G \;\equiv_{02}\; (F_2^- \star_0 G) \star_2 (F \star_0 G_2^+).$$

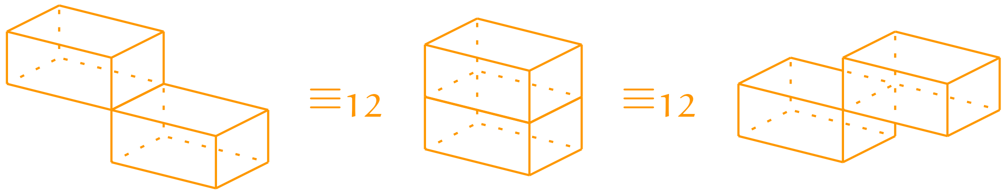
Ou en coupe :




La relation $\equiv_{02}$ identifie les démonstrations qui utilisent les deux mêmes arguments, dans deux sous-formules distinctes, mais dans un ordre différent (« bureaucratie de type A »).

# La relation $\equiv_{12}$

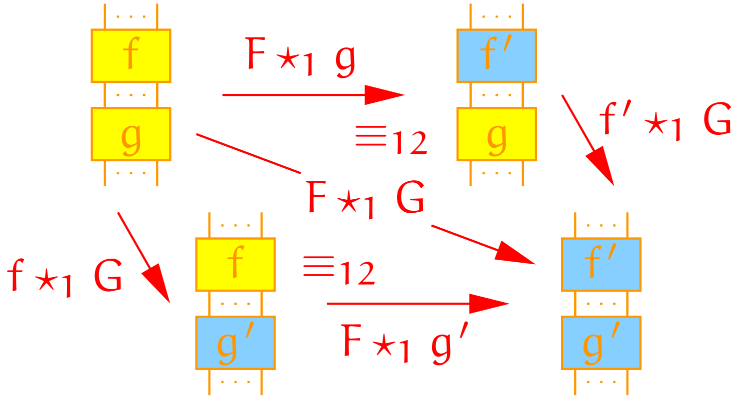
Regardons :




On peut aussi l'écrire :

$$(F \star_1 G_2^-) \star_2 (F_2^+ \star_1 G) \;\equiv_{12}\; F \star_1 G \;\equiv_{12}\; (F_2^- \star_1 G) \star_2 (F \star_1 G_2^+).$$

Ou en coupe :




La relation $\equiv_{12}$ identifie les démonstrations qui utilisent les deux mêmes arguments, l'un « suffisamment à l'intérieur de l'autre », mais dans un ordre différent (« bureaucratie de type B »).

# Comparaison entre termes et polygraphes

Si l'on utilise des termes pour décrire les formules :

- les deux types de « bureaucratie » apparaîssent très différents par essence ;
- on peut écrire des équations qui décrivent le type A (technique) ;
- il est *très* difficile d'en écrire pour le type B.

Si les formules sont les 2-chemins d'un polygraphe :

- les deux types de « bureaucratie » sont similaires et contrôlés par :

$$(F \star_i G_j^-) \star_j (F_i^+ \star_i G) \equiv_{ij} F \star_i G \equiv_{ij} (F_j^- \star_i G) \star_j (F \star_i G_j^+) \qquad \text{pour } i < j;$$

- ces équations ont une interprétation « géométrique » : ce sont des déformations.

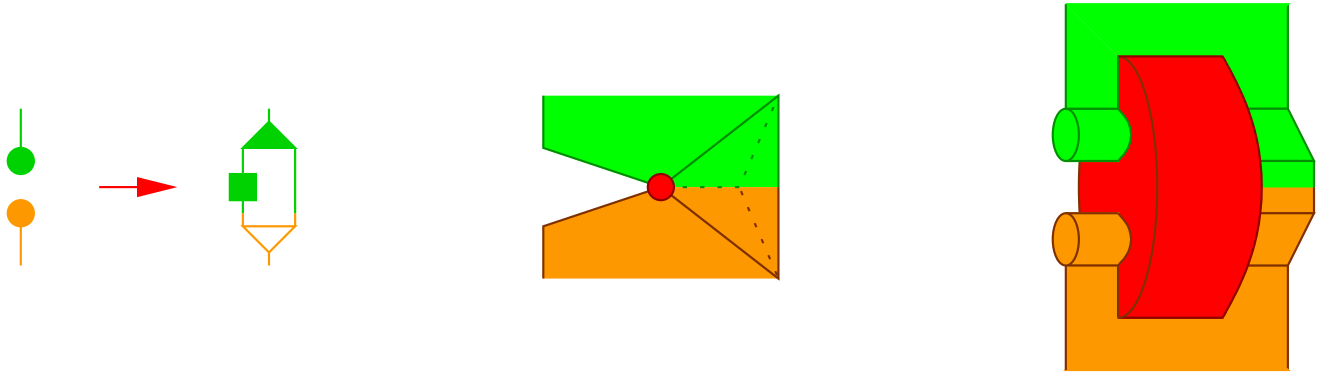
# Dimensions supérieures

## Démonstrations en trois dimensions

La représentation « bloc » n'est pas fidèle. À la place, on utilise un analogue tridimensionnel de la dualité qui a donné la représentation « circuit » des $2$-chemins :

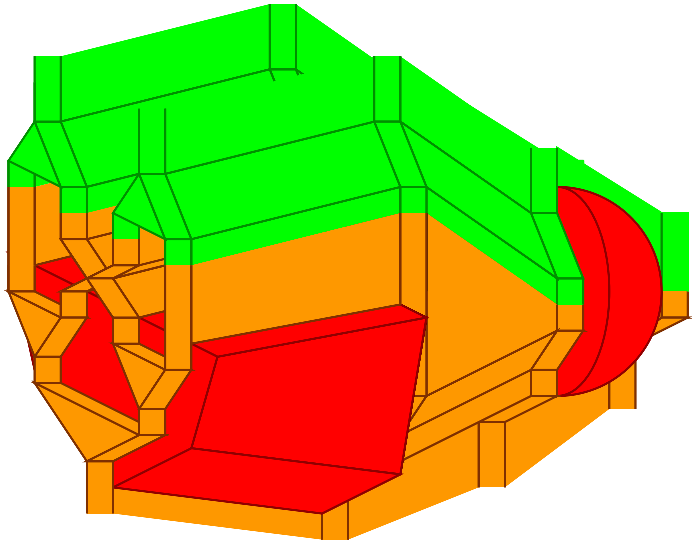
- chaque $i$-cellule est dessinée comme un objet de dimension $(3 - i)$ ;
- puis les $2$ et $3$-cellules sont « gonflées » pour être mises en valeur.

Appliquons cette recette sur la $3$-cellule suivante :

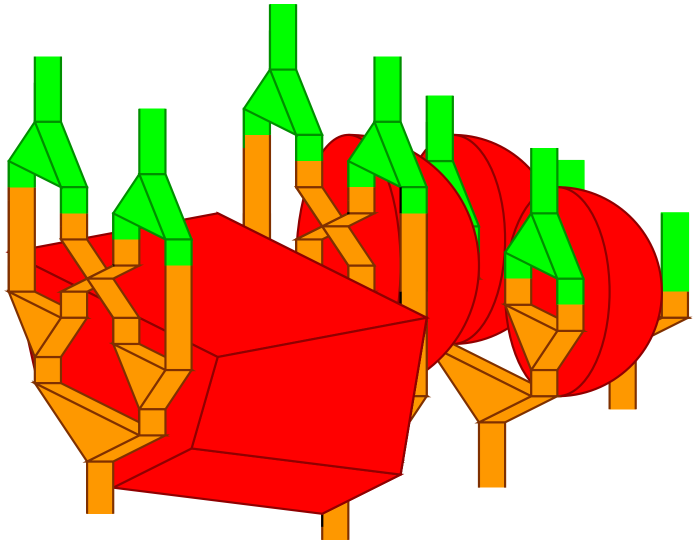


Les démonstrations sont tous les LEGO que l'on peut construire à l'aide de ces composants élémentaires, *modulo* les déformations topologiques correspondant aux relations d'échange.

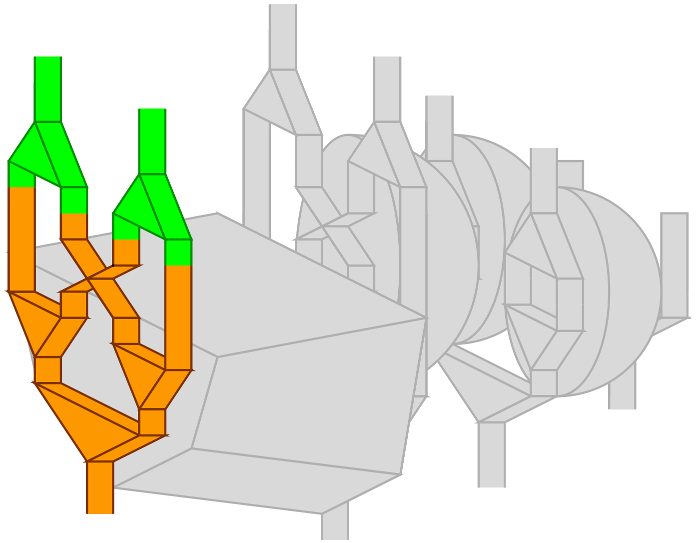
# Une démonstration en trois dimensions



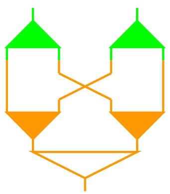
## Une démonstration en trois dimensions



# Une démonstration en trois dimensions

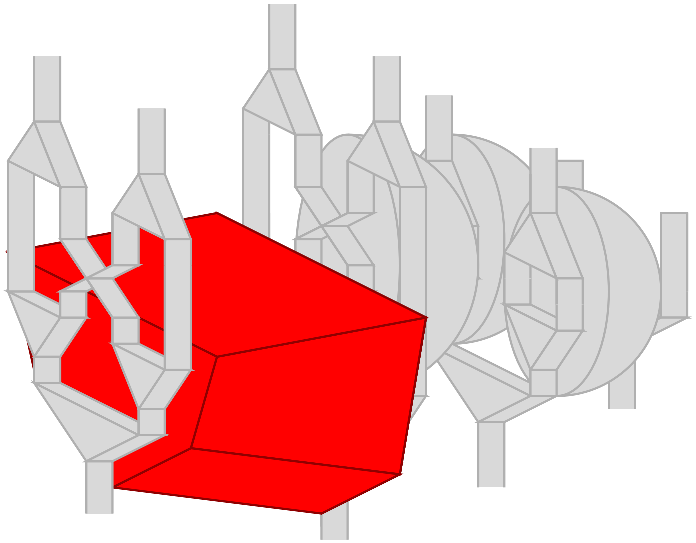


En coupe :

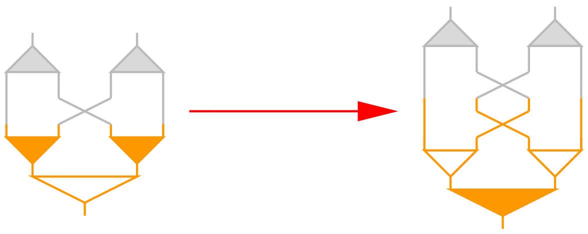


$(a \wedge b) \vee (a \wedge b)$

## Une démonstration en trois dimensions

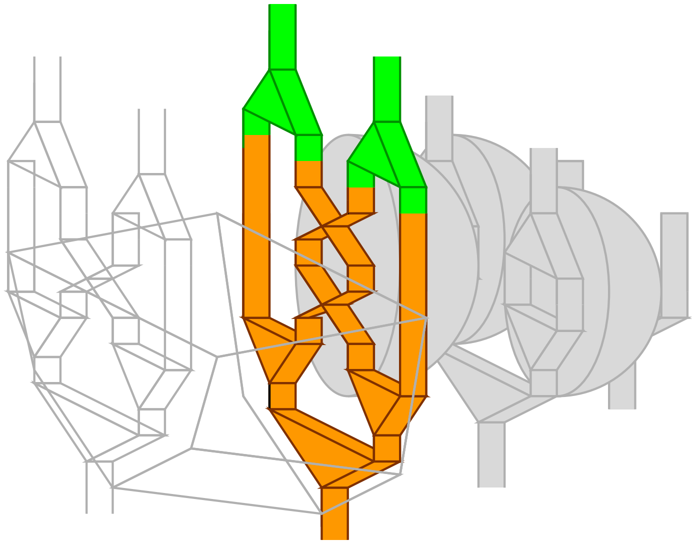


En coupe :

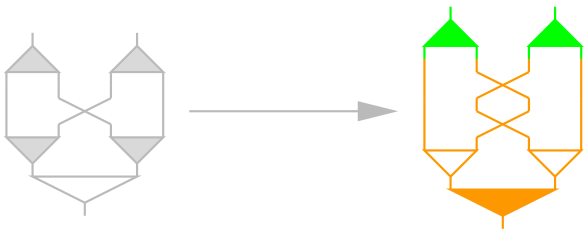


$(a \wedge b) \vee (a \wedge b)$

# Une démonstration en trois dimensions

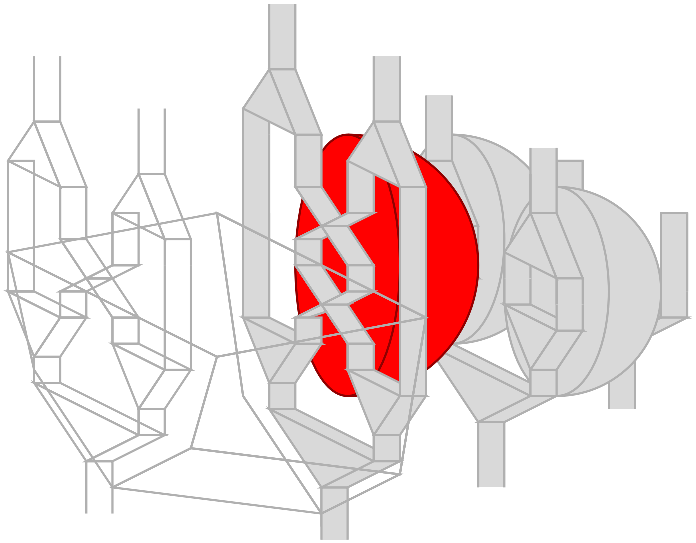


En coupe :

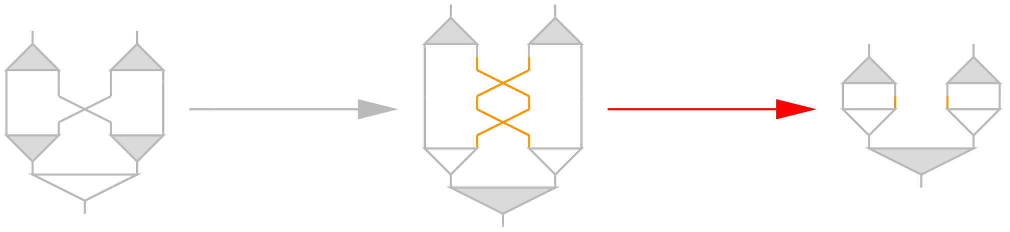


$(a \wedge b) \vee (a \wedge b)$ $(a \vee a) \wedge (b \vee b)$

# Une démonstration en trois dimensions

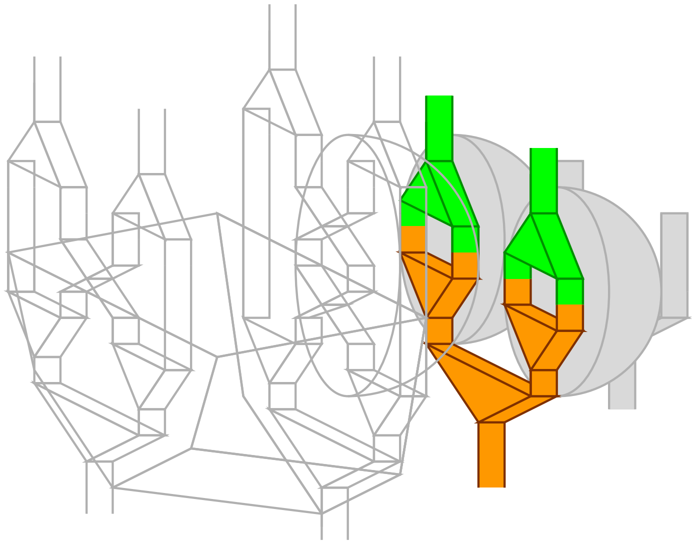


En coupe :

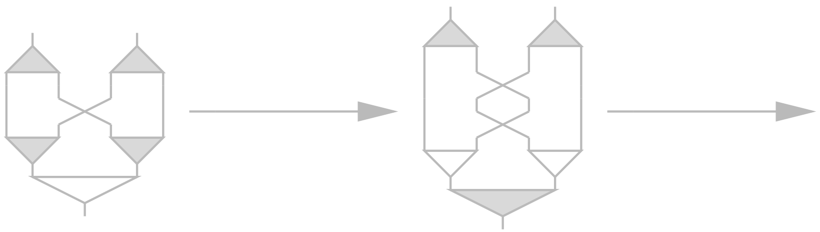


$(a \wedge b) \vee (a \wedge b)$ $(a \vee a) \wedge (b \vee b)$

# Une démonstration en trois dimensions

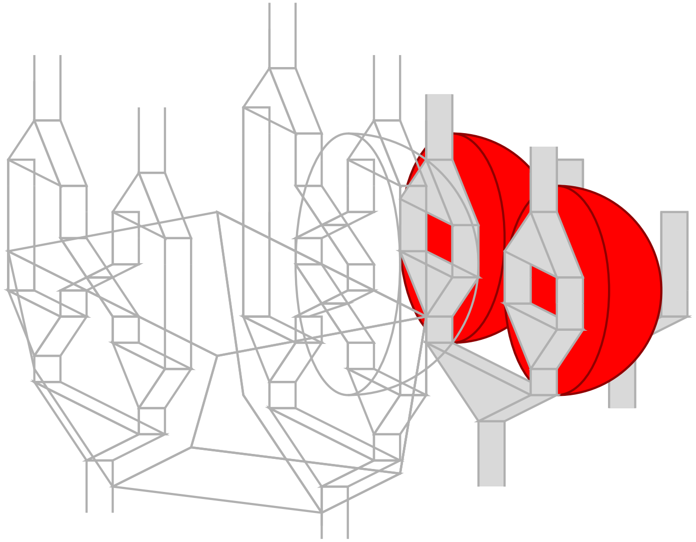


En coupe :

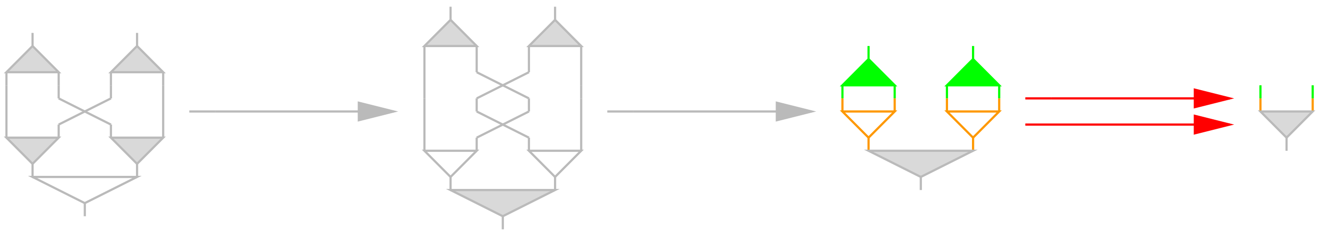


$(a \wedge b) \vee (a \wedge b)$ $\quad$ $(a \vee a) \wedge (b \vee b)$ $\quad$ $(a \vee a) \wedge (b \vee b)$

## Une démonstration en trois dimensions

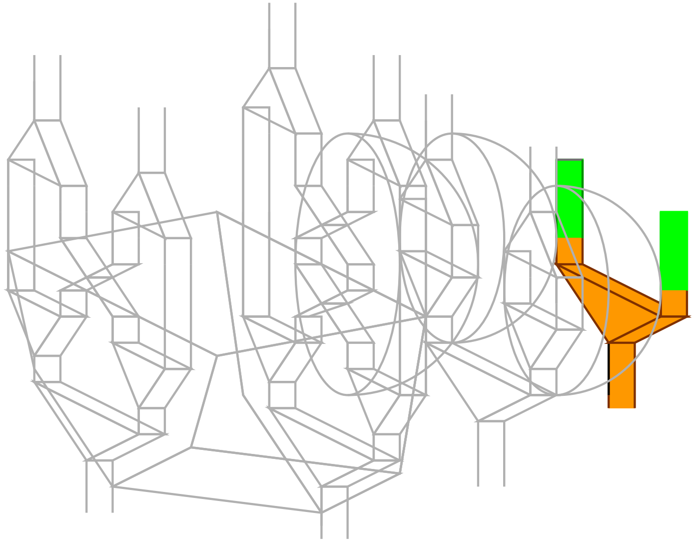


En coupe :

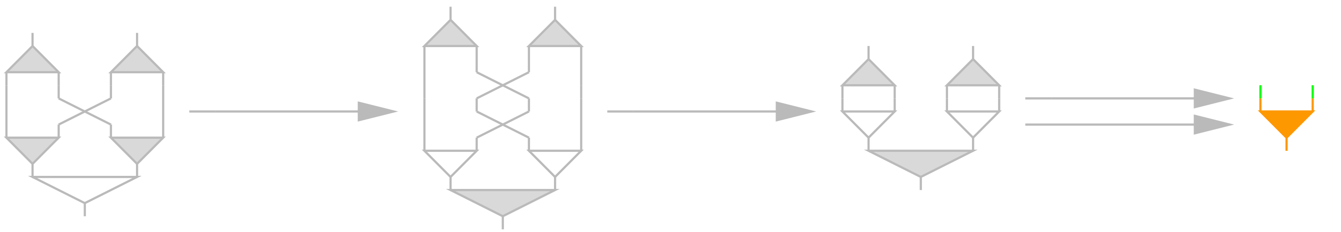


$(a \wedge b) \vee (a \wedge b)$ $\quad$ $(a \vee a) \wedge (b \vee b)$ $\quad$ $(a \vee a) \wedge (b \vee b)$

# Une démonstration en trois dimensions

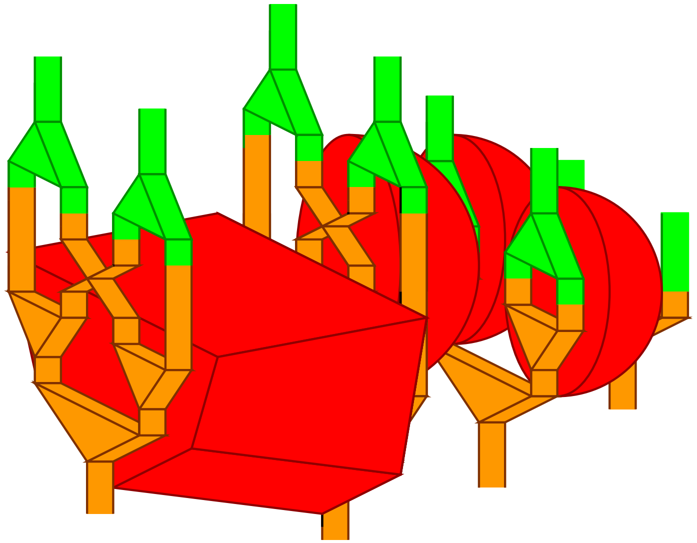


En coupe :

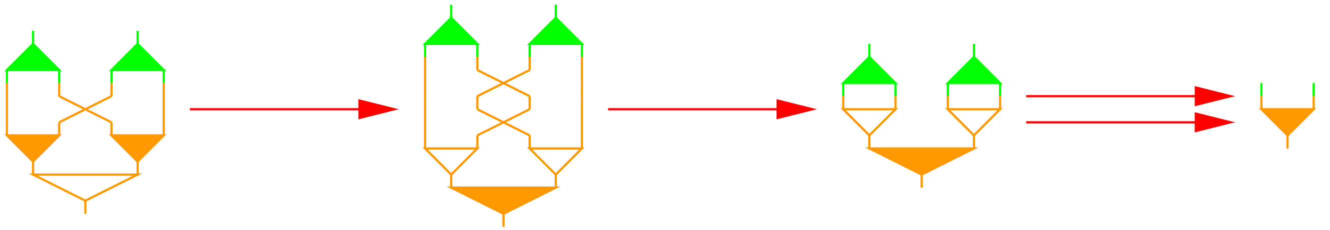


$(a \wedge b) \vee (a \wedge b)$ $\quad$ $(a \vee a) \wedge (b \vee b)$ $\quad$ $(a \vee a) \wedge (b \vee b)$ $\quad$ $a \wedge b$

## Une démonstration en trois dimensions

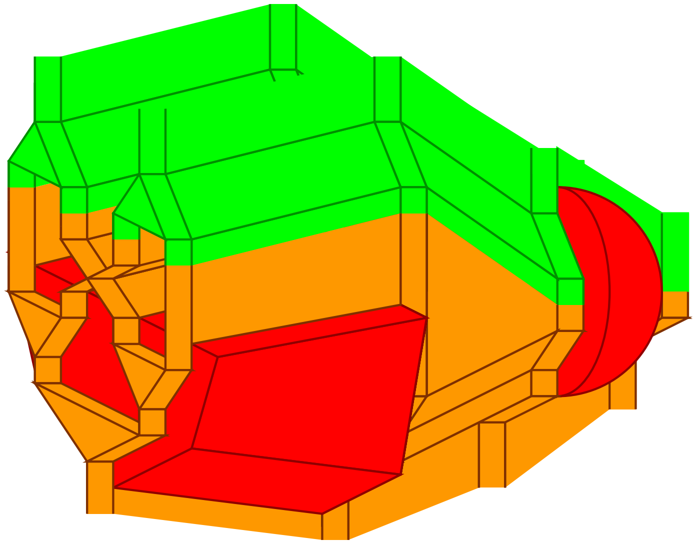


En coupe :

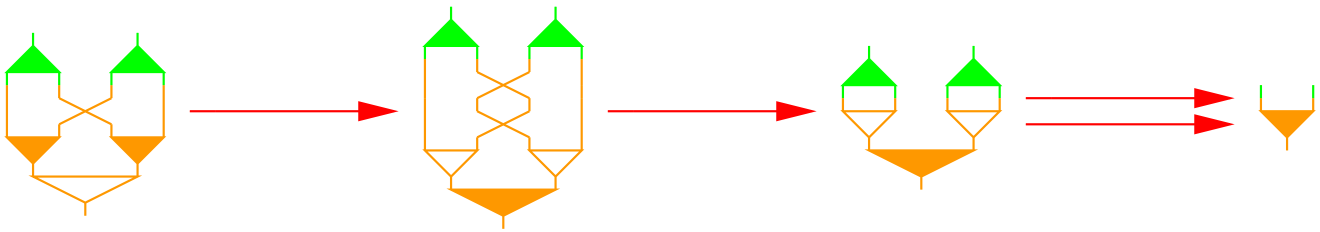


$(a \wedge b) \vee (a \wedge b)$ $\quad (a \vee a) \wedge (b \vee b)$ $\quad (a \vee a) \wedge (b \vee b)$ $\quad a \wedge b$

# Une démonstration en trois dimensions

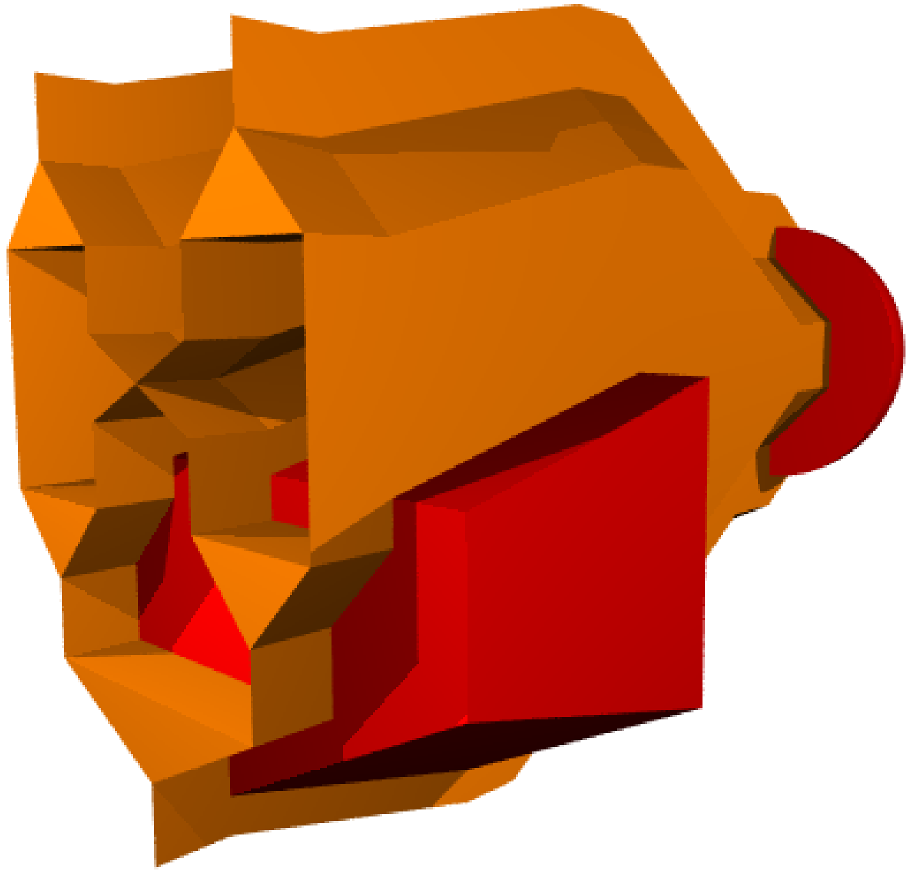


En coupe :

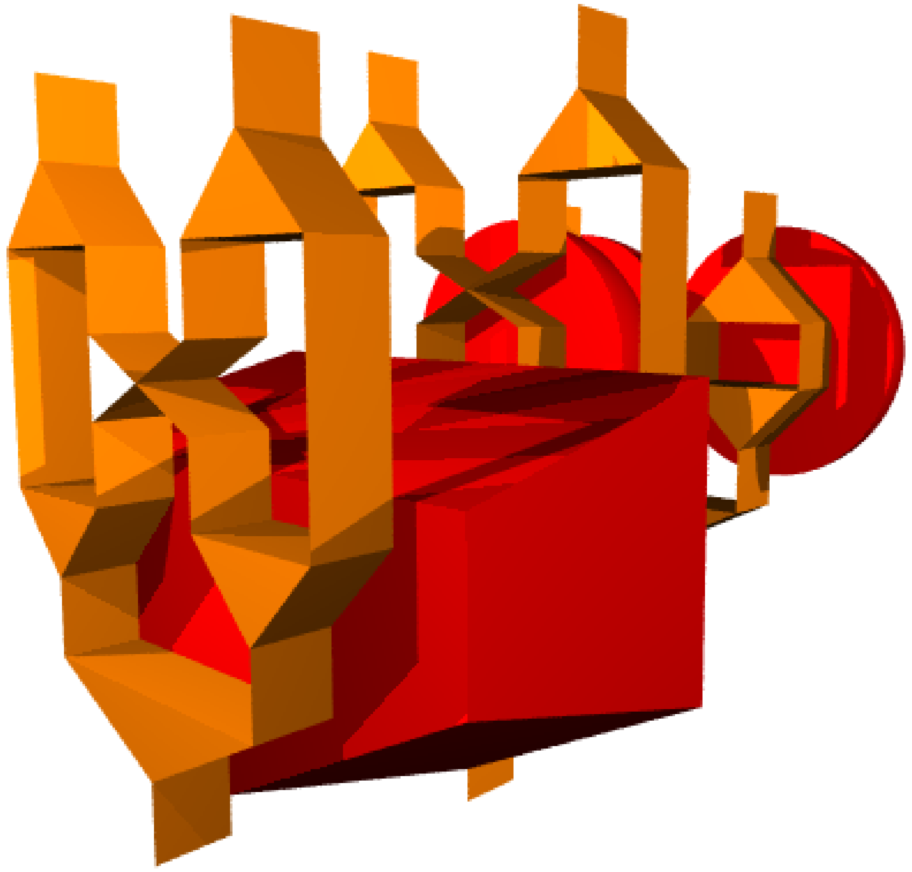


$(a \wedge b) \vee (a \wedge b)$ $\quad$ $(a \vee a) \wedge (b \vee b)$ $\quad$ $(a \vee a) \wedge (b \vee b)$ $\quad$ $a \wedge b$

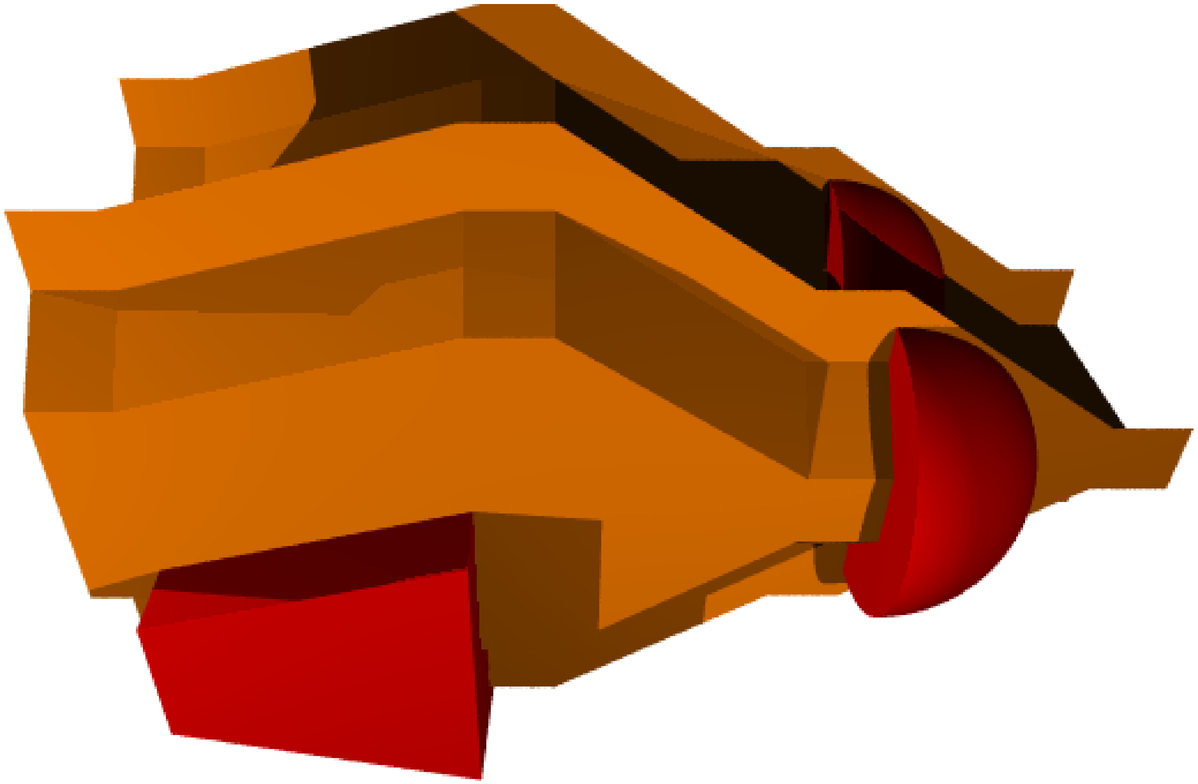
## Une démonstration en trois dimensions (version 2)



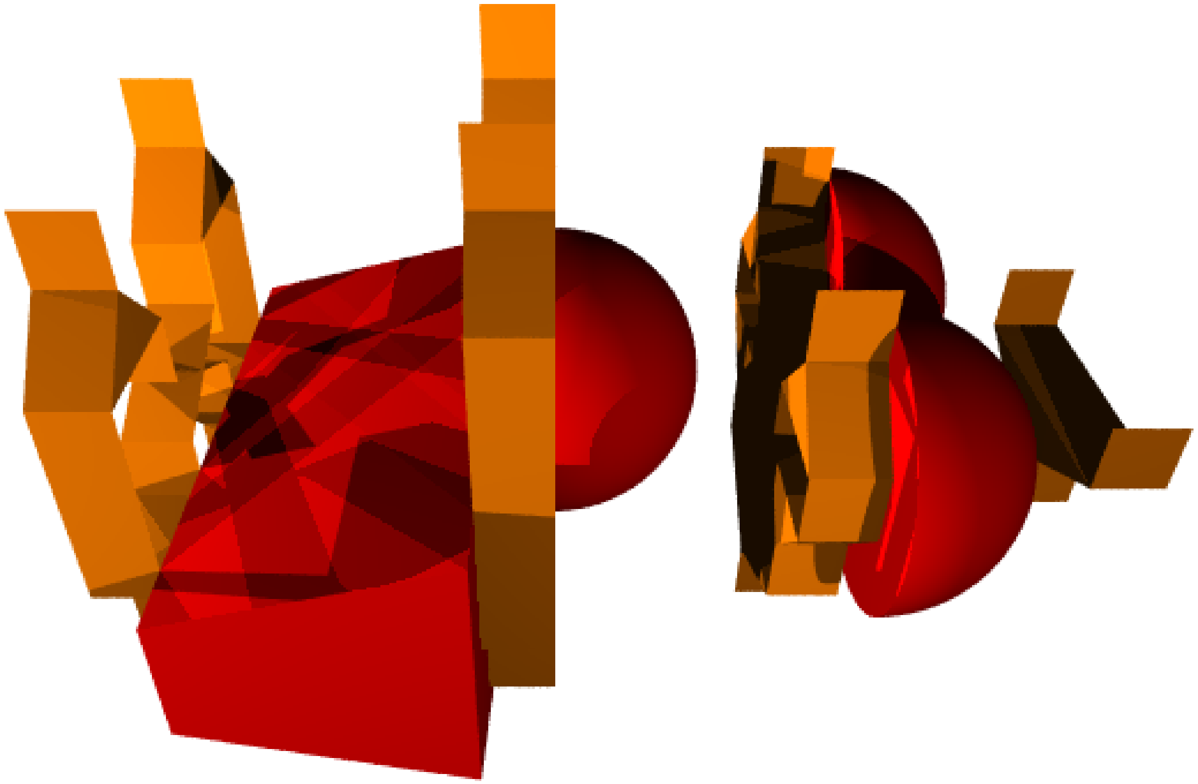
# Une démonstration en trois dimensions (version 2)



# Une démonstration en trois dimensions (version 2)



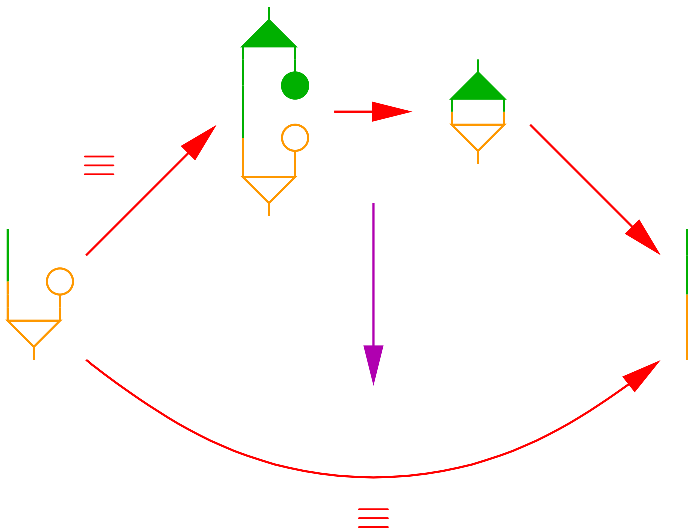
# Une démonstration en trois dimensions (version 2)



# La quatrième dimension

Les polygraphes fournissent aussi une structure algébrique aux *démonstrations portant sur des démonstrations*, dès qu'elles sont produites par des règles locales.

Par exemple :




C'est une *4-cellule* sur le 3-polygraphe des démonstrations...

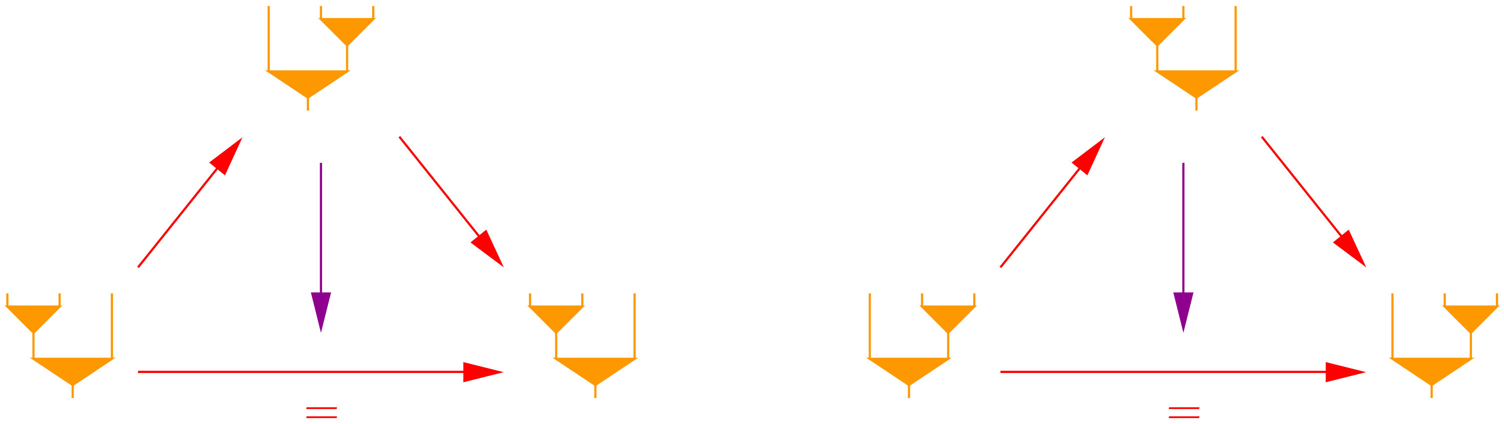
... les calculs qu'elle engendre sont des *4-chemins*.

# La quatrième dimension

Un autre exemple : les relations entre formules. Elles peuvent être vues comme :

- un couple de 3-cellules, une dans chaque direction plus
- un couple de 4-cellules (preuves que les 3-cellules sont un 3-isomorphisme).

Par exemple, la relation d'associativité de $\wedge$ devient :




Dans ce cadre, les calculs locaux sur les démonstrations sont des objets de dimension 4, donc munis de la structure suivante :

- 4 compositions, les trois anciennes plus $\star_3$,
- 6 types de « bureaucratie », les trois anciens plus $\equiv_{03}$, $\equiv_{13}$ et $\equiv_{23}$.

## Conclusion

Ainsi les polygraphes proposent un cadre alternatif pour la théorie de la démonstration.

Ses principaux avantages sont les suivants :

- Exhiber les dimensions cachées des formules et des démonstrations permet de contrôler les différents types de bureaucratie à l'aide des relations d'échange, qui ont toutes la même forme.

- Les démonstrations ont des représentations tridimensionnelles, dans lesquelles les relations d'échange apparaîssent comme des mouvements topologiques.

- Les calculs locaux portant sur les démonstrations ont une place et une structure naturelles, en dimension 4.

*À suivre...*

# LES TROIS DIMENSIONS DES DÉMONSTRATIONS

**Yves GUIRAUD**

Institut de mathématiques de Luminy

http ://iml.univ-mrs.fr/~guiraud

Laboratoire de sûreté des logiciels

Saclay – 2 mars 2006