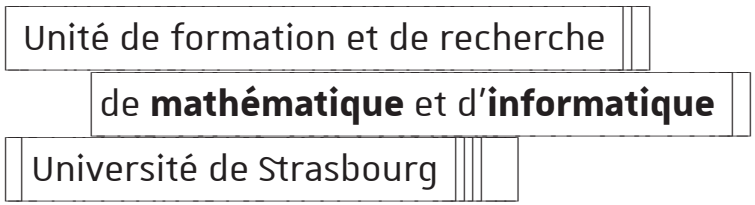
Vérification mécanique des preuves en géométrie

Julien Narboux
Collaborations avec Michael Beeson, Pierre Boutry, Gabriel Braun, Charly Gries, Pascal Schreck, Freek Wiedijk



École Thématique MPHC Mathématiques et Philosophie Contemporaines

Saint-Flour, 27-30 Juin 2018

Plan

Plan

Bugs connus

Ariane Vol 501 (1996)

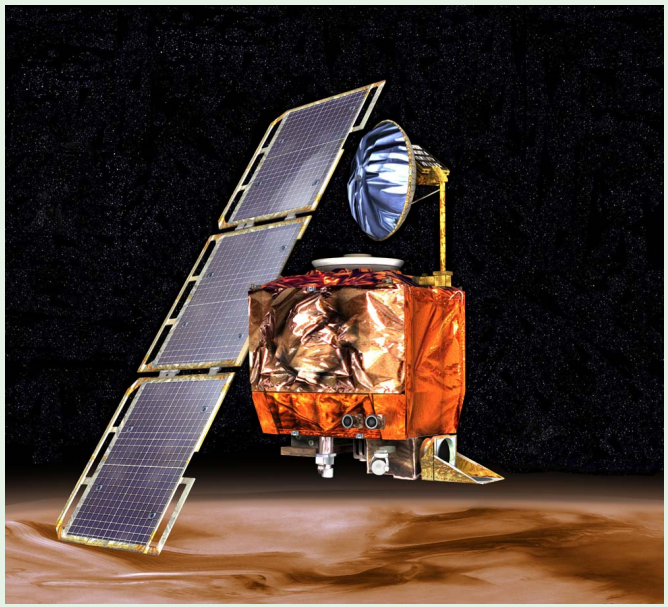
”The software exception was caused during execution of a data conversion from 64-bit floating point to 16-bit signed integer value. The floating point number which was converted had a value greater than what could be represented by a 16-bit signed integer. [...] The value was much higher than expected because the early part of the trajectory of Ariane 5 differs from that of Ariane 4 and results in considerably higher horizontal velocity values.”

Ariane 501 Inquiry Board report :
`http://esamultimedia.esa.int/docs/esa-x-1819eng.pdf`

Mars Climate Orbiter (1999)

”The ’root cause’ of the loss of the spacecraft was the failed translation of English units into metric units in a segment of ground-based, navigation-related mission software.”

Cost : $327 600 000.



Un petit exemple

Exercice : écrire un programme qui renvoie la valeur absolue d'un entier relatif x [a].

```
int abs(int x)
  {
   int z;
   if (x<0)
    z=-x;
   else
    z=x;
   return z;
}
```

a. Source : David Mentré

Un petit exemple

Exercice : écrire un programme qui renvoie la valeur absolue d'un entier relatif x [a].

```
int abs(int x)
  {
   int z;
   if (x<0)
    z=-x;
   else
    z=x;
   return z;
}
```

a. Source : David Mentré

Ce programme ne fonctionne pas !

Si $x = -2^{31}$, sont opposé n'est pas représentable.

Table des matières

Plan

De nombreuses preuves incorrectes du postulat des parallèles :

En 1763, dans sa thèse Klügel fournit une liste de 30 preuves incorrectes.

- Ptolemée admet l'unicité des parallèles.
- Proclus admet qu'étant donné deux droite parallèles, toute droite qui intersecte l'une intersecte l'autre.
- Legendre a publié plusieurs preuves incorrectes dans son 'best-seller' "Éléments de géométrie".
- ...

Postulat du Triangle

$$\widehat{A} + \widehat{B} + \widehat{C} = 180°$$

Adrien-Marie Legendre

(caricature

Julien Léopold Boilly)

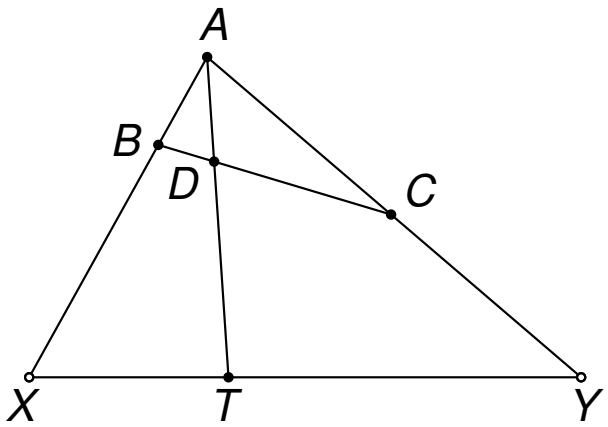
Postulat du Triangle

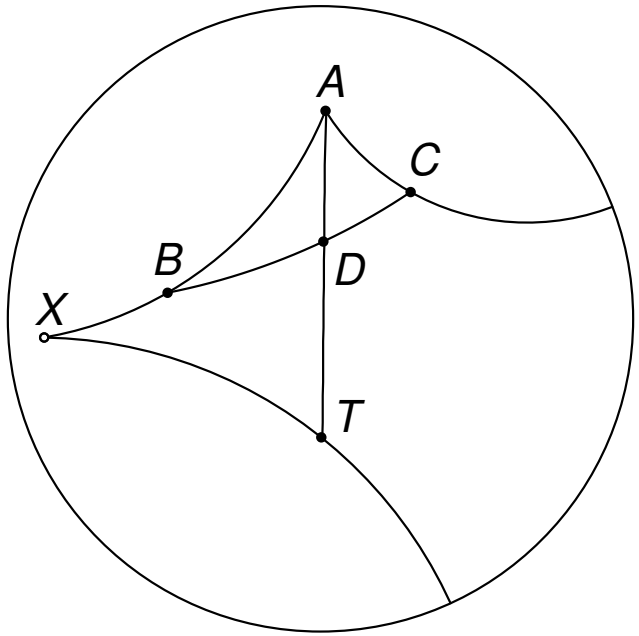
“Il n’en est pas moins certain que le théorème sur la somme des trois angles du triangle doit être regardé comme l’une de ces vérités fondamentales qu’il est impossible de contester [...].”

Adrien-Marie Legendre

(caricature

Julien Léopold Boilly)


A
B
D
C
X
T
Y


A
C
B
D
X
T

Plan

Un exemple plus récent

”In October, 1998, Carlos Simpson submitted to the arXiv preprint server a paper called “Homotopy types of strict 3-groupoids”. It claimed to provide an argument that implied that the main result of the ”∞-groupoids” paper, which M. Kapranov and I had published in 1989, can not be true. However, Kapranov and I had considered a similar critique ourselves and had convinced each other that it did not apply. I was sure that we were right until the Fall of 2013 (! !).”

Vladimir Voevodsky

Source : `http://www.math.ias.edu/vladimir/files/2014_IAS.pdf`, page 9.

”It soon became clear that the only real long-term solution to the problems that I encountered is to start using computers in the verification of mathematical reasoning. ”

Vladimir Voevodsky (field medalist 2002)

Source : `http://www.math.ias.edu/vladimir/files/2014_IAS.pdf`, page 13.

Bugs dans les vérificateurs de preuves

Coq CHANGES :

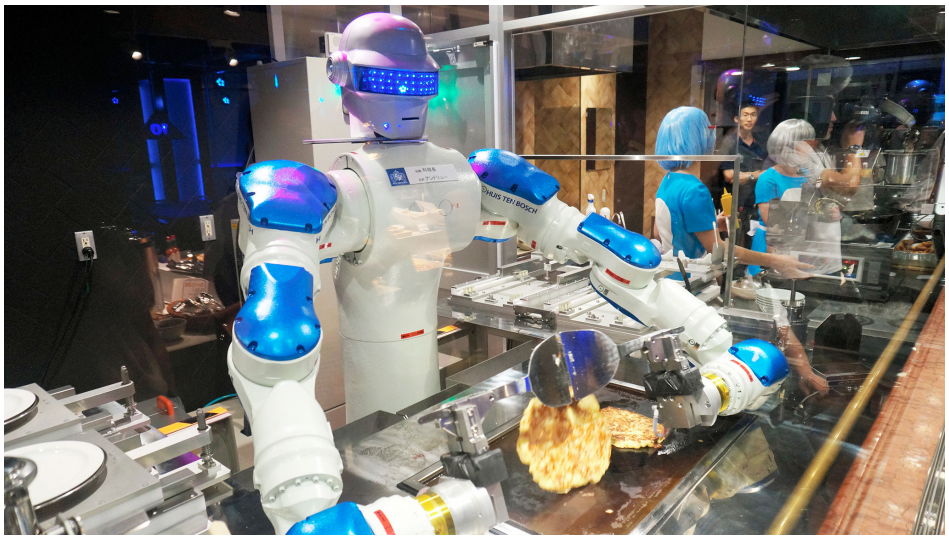
```
Changes from V8.5pl2 to V8.5pl3
===============================

Critical bugfix

- #4876: Guard checker incompleteness when using primitive projections

Changes from 8.7.1 to 8.7.2
===========================

Fixed a critical bug in the VM handling of universes (#6677). This bug
affected all releases since 8.5.
```

On pouvait prouver faux !

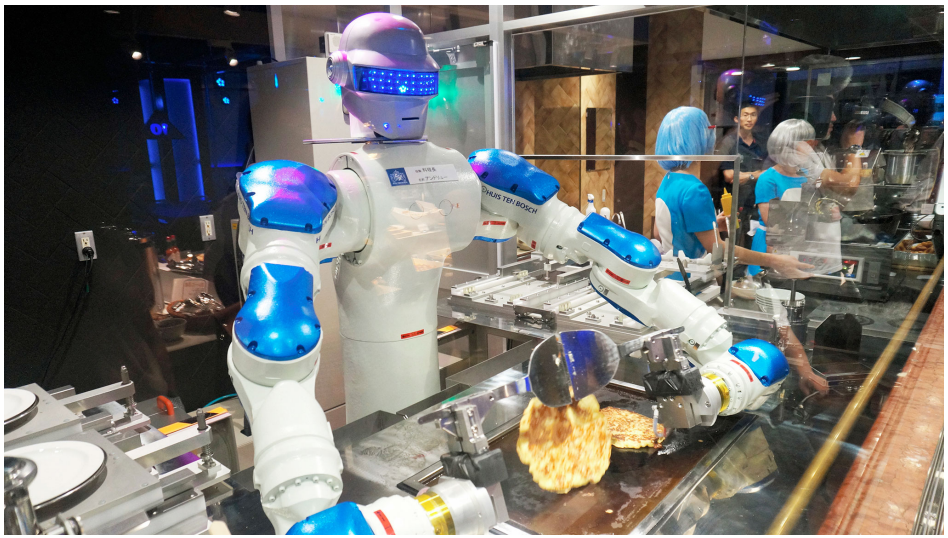
Plan

- Un nom relativement mal choisi :
  - Ils n'aident pas à trouver une preuve, seulement à *vérifier* qu'une preuve est correcte.
  - Comme c'est difficile d'obtenir une preuve formelle, on la construit de manière *interactive* (ITP Interactive Theorem Proving)
- Le domaine frère est celui de la preuve automatique (ATP : Automated Theorem Proving) :la machine qui transforme les cochons en saucisses.
- Des frères siamois :
  - L'automatisation est intégrée à la preuve interactive :
    - ★ A petite échelle (hachoir à viande + poussoir à saucisses).
    - ★ A échelle moyenne (machine à saucisses).
  - La preuve automatique est souvent un peu interactive (choix de l'algo et de ses paramètres, encodage, *hints*,. . .).

Automatisation



Automatisation



Assistants de preuve

- Automath (1967)
- Coq (1984)
- HOL-Light (90s)
- HOL (1988)
- Isabelle (1986)
- Lean (2013)
- Matita (1999)
- Mizar (1973)
- ...

Quelques exemples de théorèmes

- ”Si les portes sont ouvertes le train est en face d’un quai”.
- $$\sum_{0}^{n} i = \frac{n(n+1)}{2}$$

Example

We want to show that :

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$$

Example

We want to show that :

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$$

We will show that :

$$2 * \sum_{i=0}^{n} i = n(n+1)$$

Example

We want to show that :

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$$

We will show that :

$$2 * \sum_{i=0}^{n} i = n(n+1)$$

In Coq :

```
Lemma sun_n : forall n:nat, 2*(sum_int n)=n*(n+1).
```

Example

We want to show that :

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$$

We will show that :

$$2 * \sum_{i=0}^{n} i = n(n+1)$$

In Coq :

```
Lemma sun_n : forall n:nat, 2*(sum_int n)=n*(n+1).
```

Definition of $\sum$?

Example

We want to show that :

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$$

We will show that :

$$2 * \sum_{i=0}^{n} i = n(n+1)$$

In Coq :

```
Lemma sun_n : forall n:nat, 2*(sum_int n)=n*(n+1).
```

Definition of $\sum$?

$$\sum_{i=0}^{0} i = 0$$

$$\sum_{i=0}^{n} i = n + \sum_{i=0}^{n-1} i$$

Un assistant preuve fournit plusieurs langages

1. Un langage pour décrire les axiomes/énoncés/définitions.
2. Un langage pour décrire les preuves.
3. Un ou des méta-langages pour décrire les générateurs de preuves.

Un compromis

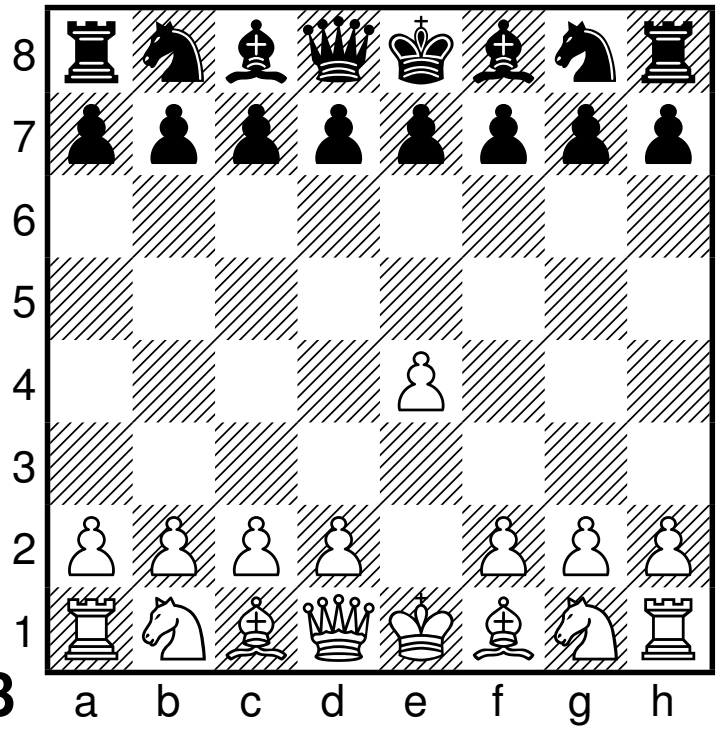
Un langage informatique est un compromis entre pouvoir d'expressivité et capacité d'exécution.

Première étape

Formaliser les *énoncés* serait déjà une avancée majeure.
Projet *formal abstracts* initié par Tom Hales :
Donner une version formelle des énoncés des textes mathématiques.
`https://github.com/formalabstracts/formalabstracts`

Pour décrire les preuves

1. Langages procéduraux.
2. Langages déclaratifs.



1 e4 Z2.Nf3

Lisibilité d'une preuve formelle

- Les preuves en langage procédural sont difficiles à lire *sans ordinateur*.
- Les preuves en langage déclaratif sont plus facile à relire.

Caractère explicatif d'une preuve formelle

- Une preuve formelle explique *plus* parce qu'elle contient potentiellement tous les détails.
- Une preuve formelle explique souvent *moins* car elle ne dit pas *ce qui est de l'ordre du détail*.
- Une preuve informelle explique *moins* car elle peut se tromper sur ce qui est de l'ordre du détail (exemple de la somme des angles).

Automatisation vs explication

- Parfois l'automatisation rend la preuve plus lisible car plus courte : On sait que A d'après les lemmes B,C,D.
- On pourrait dire qu'une preuve partiellement automatisée est plus proche de la preuve informelle. Un preuve automatisée est plus proche de l'idée de la preuve car plus maintenable.
- Mais parfois l'automatisation peut rendre la preuve *moins maintenable* (sensible aux modifications du démonstrateur automatique).

Preuve informelle	Preuve formelle	Preuve formelle mécanisée
Objet sémantique	Objet syntaxique	Objet syntaxique
	Correcte par définition	Correcte par définition
Vérification souvent sémantique et avec accord commun	Vérification difficile	Vérification facile si on a le bon logiciel
Possibilité d'arbitrer en cas de désaccords		
		Peut être vendue

Les preuves via la correspondance de Curry-Howard

Preuve informelle	Preuve formelle	Preuve formelle mécanisée
Idée d'algorithme	Algorithme	Programme

Avantage/inconvénient preuve formelle

Avantage de la preuve formelle vérifiée mécaniquement :

- On se ramène à des hypothèses générales.
- Le travail du relecteur est plus léger.
- Permet de clarifier les hypothèses, définitions utilisées.
- Peut être revérifiée quand on change les définitions ou les énoncés.

Inconvénient :

- C'est un objet syntaxique pas une idée, donc valide dans un contexte précis : Euclide vs Euclide vérifié par rapport à certaines définitions en utilisant Coq version 8.8 qui tourne sur MacOS 10.11.16. $\rightarrow$ problème de la portabilité des preuves.

Les trous dans les preuves informelles

- des branches sans feuilles,
- des branches auxquelles on ne peut pas rajouter de feuilles,
- des nœuds avec pas le bon nombre de branches,
- des branches mal connectées,
- des cycles dans l'arbre.

Les défauts du processus de validation des preuves informelles

Pourquoi la possibilité d'arbitrage en cas de dés-accord çà ne suffit pas :

- Parce que l'absence de désaccord n'implique pas que c'est vrai :
  - Parce que çà n'intéresse personne.
  - Parce que personne ne pense que vous puissiez avoir tort.
  - Parce que personne n'ose dire que vous avez tort.
  - Parce que tout le monde pense que c'est vrai.
- Parce que çà limite aux preuves que les humains peuvent vérifier, ce qui donc exclu des preuves et des théorèmes (voir exemples plus loin).

Qualités essentielles pour vérifier une preuve formelle :

- savoir ne pas utiliser son intuition
- être rapide
- être ”courageux”

$\rightarrow$ facile pour un ordinateur

Quelles hypothèses ?

Il faut faire confiance à :

- la logique sous-jacente à l'assistant de preuve et

Quelles hypothèses ?

Il faut faire confiance à :

- la logique sous-jacente à l'assistant de preuve et
- que l'implantation correspond bien à la théorie et

Quelles hypothèses ?

Il faut faire confiance à :

- la logique sous-jacente à l'assistant de preuve et
- que l'implantation correspond bien à la théorie et
- au compilateur et

Quelles hypothèses ?

Il faut faire confiance à :

- la logique sous-jacente à l'assistant de preuve et
- que l'implantation correspond bien à la théorie et
- au compilateur et
- au microprocesseur et

Quelles hypothèses ?

Il faut faire confiance à :

- la logique sous-jacente à l'assistant de preuve et
- que l'implantation correspond bien à la théorie et
- au compilateur et
- au microprocesseur et
- à vos définitions et énoncés et

Quelles hypothèses ?

Il faut faire confiance à :

- la logique sous-jacente à l'assistant de preuve et
- que l'implantation correspond bien à la théorie et
- au compilateur et
- au microprocesseur et
- à vos définitions et énoncés et
- à vos axiomes.

Quelles hypothèses ?

Il faut faire confiance à :

- la logique sous-jacente à l'assistant de preuve et
- que l'implantation correspond bien à la théorie et
- au compilateur et
- au microprocesseur et
- à vos définitions et énoncés et
- à vos axiomes.

Quelles hypothèses ?

Il faut faire confiance à :

- la logique sous-jacente à l'assistant de preuve et
- que l'implantation correspond bien à la théorie et
- au compilateur et
- au microprocesseur et
- à vos définitions et énoncés et
- à vos axiomes.

Critère de de Bruijn

- Les preuves sont certifiée par un *noyau*.
  - Isabelle (très petit)
  - HOL (très petit)
  - Coq (relativement petit)

  En revanche, ni Mizar, ni PVS n'ont une notion de noyau.

Noyau

- On doit faire confiance au noyau.
- le reste du système peut contenir des bugs : notations, coercion, automatisation . . . sont là pour aider à générer des preuves formelles (atomisation relative).

La réflexion

Idée : Convaincre Coq que l'algorithme qui génère une démonstration est correct, plutôt que la démonstration en elle-même.
ou bien :
Un algorithme correct qui génère une démonstration appliqué à un argument est aussi une démonstration.
Exemple :

$$x^2 + 1 + 2x = (x + 1)^2$$

En développant de chaque côté et réordonnant les termes on obtient la même chose à gauche et à droite donc l'égalité est vérifiée (car l'algorithme transforme une expression en une autre égale).
Plutôt qu'une longue liste de distributivité/associativité/commutativité.

Plan

Calculs

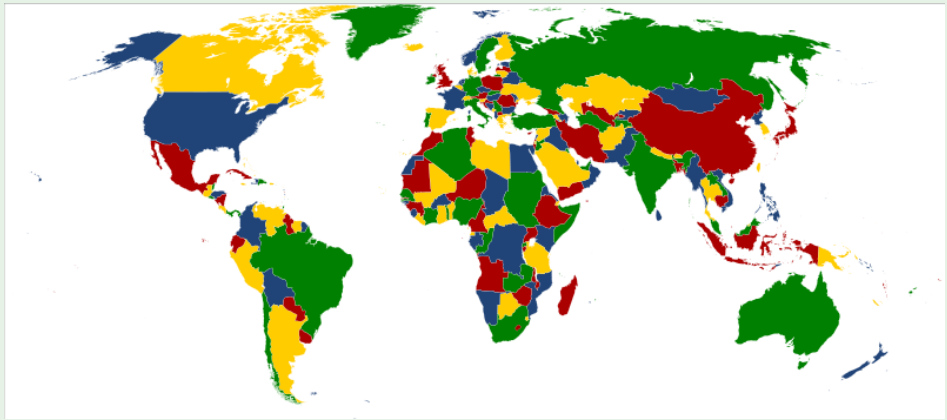
Le théorème des quatre couleurs

1879 Preuve incorrecte par Kempe

1890 Heaywood trouve l'erreur

1976 Appel and Hake (1478 configurations)

2004 Formalisation en Coq par Gonthier



Conjecture de Kepler $\rightarrow$ théorème de Hales

Picture by Robert Cudmore

1998 Proof by Thomas Hales
Robert MacPherson, the editor :

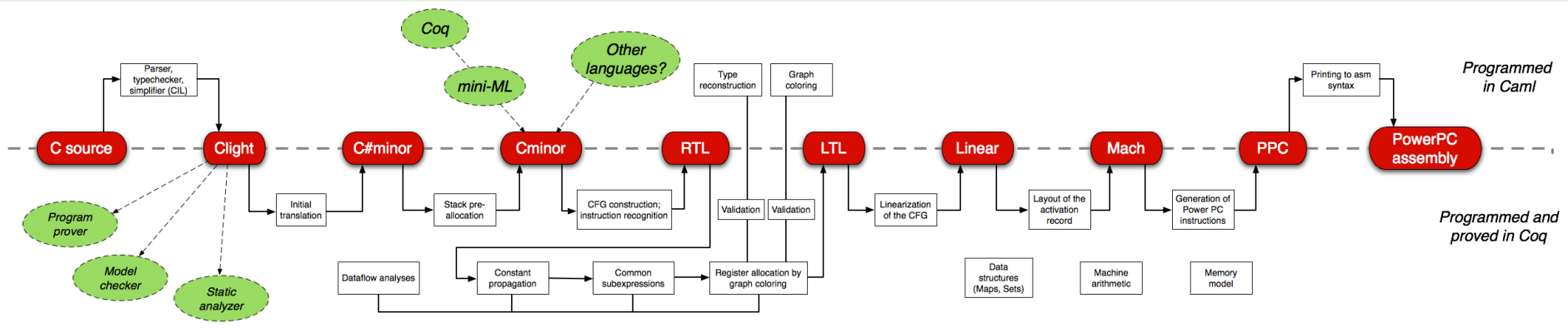
"The news from the referees is bad, from my perspective. They have not been able to certify the correctness of the proof, and will not be able to certify it in the future, because they have run out of energy to devote to the problem. This is not what I had hoped for. The referees put a level of energy into this that is, in my experience, unprecedented."

2004 - 2014 Projet Flyspeck : formalisation en HOL-light avec des contributions en Coq et Isabelle

Des systèmes complexes

Un compilateur

CompCert un compilateur certifié (Xavier Leroy).



Détails techniques

Ligne de métro

- Méthode B
- Paris (line 14, 1998), Paris (ligne 1, 2005), Lyon (ligne D), ...

Détails techniques

Un système d'exploitation

sel4 : Micro noyau (Isabelle/HOL).
Preuve : 165000 lignes, 11 années pers.
Code : 15000 lignes, 2.5 années pers.

La taille de la preuve I

Feit-Thompson

```
Theorem Feit_Thompson (gT:finGroupType)
                      (G:{group gT}):
odd ##|G| -> solvable G.
```

Preuve par l'équipe Mathematical Components (Septembre 2012) [a] : 170 000 lignes, 4 200 théorèmes

---

a. http://ssr2.msr-inria.inria.fr/~jenkins/current/progress.html

Détails techniques

Cartes à puce

Gemalto : certification niveau EAL7.

Limites

- La preuve formelle coûte cher.
- La preuve s'applique au modèle forcement abstrait qui peut être insensible à certains problèmes (ex : attaques par canaux cachés).
- La preuve formelle ne s'applique qu'aux problèmes qu'on peut *spécifier*.

Plan

Euclid (−325-−265) *Les Elements.*

Hilbert (1862-1943) *Die Grundlagen der Geometrie.*

Tarski (1902-1983) *Metamathematische Methoden in der Geometrie*.

Euclid (−325-−265) *Les Elements.*

Hilbert (1862-1943) *Die Grundlagen der Geometrie.*

Tarski (1902-1983) *Metamathematische Methoden in der Geometrie*.

Euclid (−325-−265) *Les Elements.*

Hilbert (1862-1943) *Die Grundlagen der Geometrie.*

Tarski (1902-1983) *Metamathematische Methoden in der Geometrie*.

GeoCoq

- Une bibliothèque de preuves
- Michael Beeson, Gabriel Braun, Pierre Boutry, Charly Gries, Julien Narboux, Pascal Schreck
- Taille : $>$ 3900 Lemmes, $>$ 130000 lignes
- Licence LGPL3

Objectifs

- Enseignement
- Preuve d'algorithmes
- Applications à la physique

Fondements de la géométrie

1. Approche synthétique
2. Approche analytique
3. Approche métrique
4. Approche à partir de groupes de transformations

Approche synthétique

Des objets géométriques primitifs + des prédicats géométriques + et des axiomes . . .

> *On peut remplacer les points, les droites et les plans, par des tables, des chaises et des tasses.* *David Hilbert*

- Axiomes de Hilbert :

types : points, droites et plans
prédicats : incidence, entre-deux, congruence, congruence des angles

- Axiomes de Tarski :

types : points
prédicats : entre-deux, congruence

- . . .des nombreuses variantes

Approche Analytique

On suppose que l'on a un corps $\mathbb{F}$.
Points := $\mathbb{F}^n$

Approche Métrique

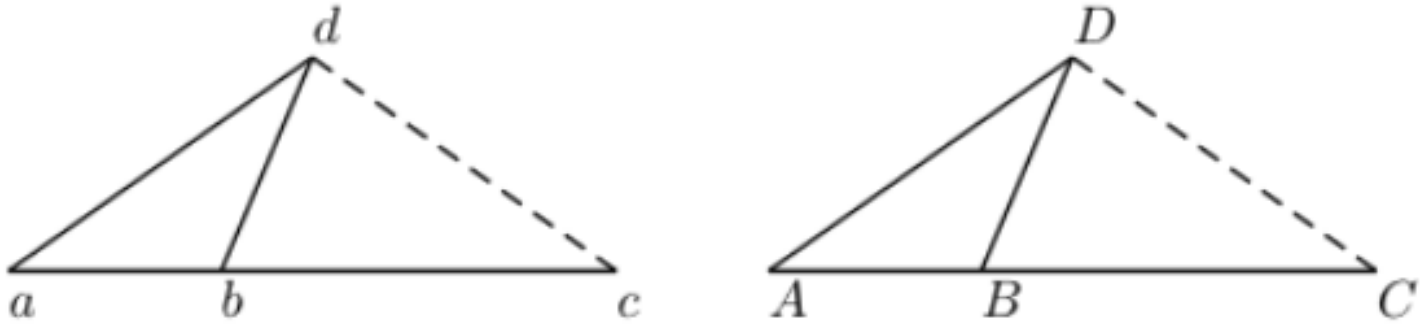
On suppose à la fois :

- des nombres (un corps)
- des objets géométriques
- des axiomes

Les axiomes de Tarski

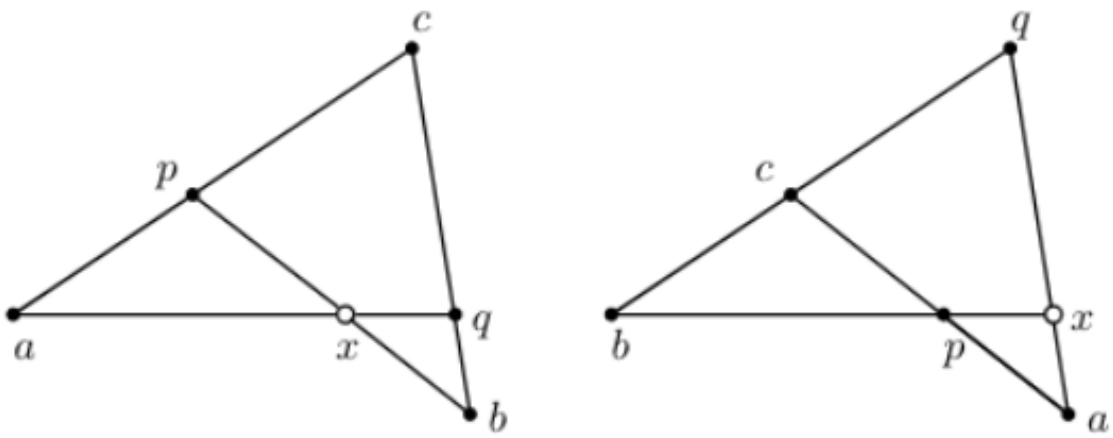
A1	Symmetry	$AB \equiv BA$
A2	Pseudo-Transitivity	$AB \equiv CD \wedge AB \equiv EF \rightarrow CD \equiv EF$
A3	Cong Identity	$AB \equiv CC \rightarrow A = B$
A4	Segment construction	$\exists E, \mathrm{Bet}\ A\ B\ E \wedge BE \equiv CD$
A6	Between Identity	$\mathrm{Bet}\ A\ B\ A \rightarrow A = B$
A8	Lower Dimension	$\exists ABC, \neg\mathrm{Bet}\ A\ B\ C \wedge \neg\mathrm{Bet}\ B\ C\ A \wedge \neg\mathrm{Bet}\ C\ A\ B$

Cinq segments



Side-angle-side sans angles !

Pasch



A7 Inner Pasch

$$\text{Bet } A\,P\,C \wedge \text{Bet } B\,Q\,C \rightarrow \exists X, \text{Bet } P\,X\,B \wedge \text{Bet } Q\,X\,A$$

Un développement sans “axiome”

Axiome = variable globale
On utilise à la place des hypothèses “implicites” :

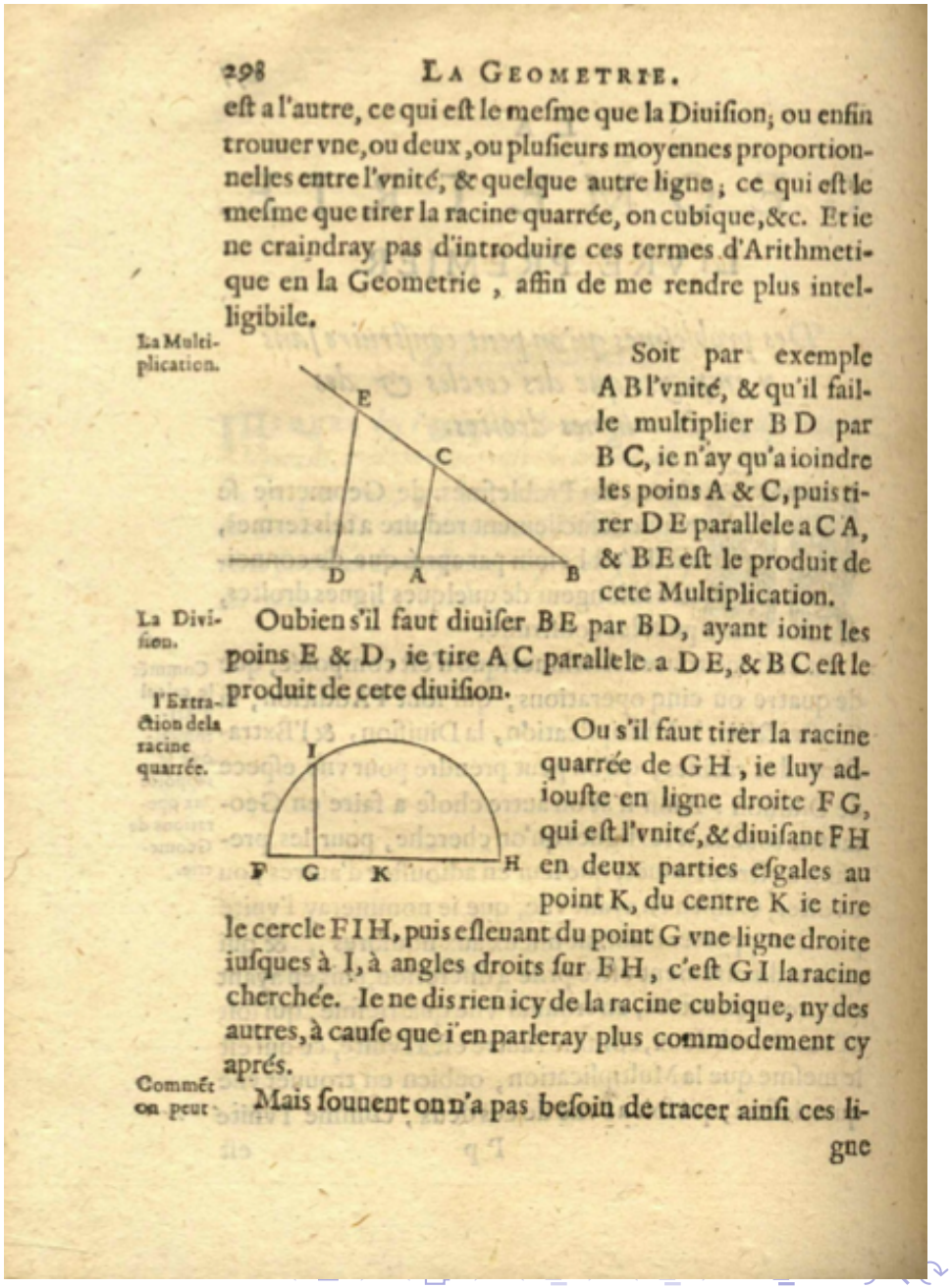
```
Class Tarski_neutral_dimensionless :=
{
 Tpoint : Type;
 Bet : Tpoint -> Tpoint -> Tpoint -> Prop;
 Cong : Tpoint -> Tpoint -> Tpoint -> Tpoint -> Prop;
 cong_pseudo_reflexivity : forall A B, Cong A B B A;
 cong_inner_transitivity : forall A B C D E F,
   Cong A B C D -> Cong A B E F -> Cong C D E F;
 cong_identity : forall A B C, Cong A B C C -> A = B;
 segment_construction : forall A B C D,
   exists E, Bet A B E /\ Cong B E C D;
   ...
```

Alors on peut faire de la méta-théorie

```
Instance Hilbert_euclidean_follows_from_Tarski_euclidean :
  Hilbert_euclidean
  Hilbert_neutral_follows_from_Tarski_neutral.
```

Arithmétisation de la géométrie

René DESCARTES (1925). *La géométrie*.



298 LA GEOMETRIE.

eſt a l'autre, ce qui eſt le meſme que la Diuiſion; ou enfin trouuer vne, ou deux, ou pluſieurs moyennes proportionnelles entre l'vnité, & quelque autre ligne; ce qui eſt le meſme que tirer la racine quarrée, ou cubique, &c. Et ie ne craindray pas d'introduire ces termes d'Arithmetique en la Geometrie, affin de me rendre plus intelligibile.

La Multiplication.

Soit par exemple A B l'vnité, & qu'il faille multiplier B D par B C, ie n'ay qu'a ioindre les poins A & C, puis tirer D E parallele a C A, & B E eſt le produit de cete Multiplication.

La Diuiſion.

Ou bien s'il faut diuiſer B E par B D, ayant ioint les poins E & D, ie tire A C parallele a D E, & B C eſt le produit de cete diuiſion.

L'Extraction de la racine quarrée.

Ou s'il faut tirer la racine quarrée de G H, ie luy adiouſte en ligne droite F G, qui eſt l'vnité, & diuiſant F H en deux parties eſgales au point K, du centre K ie tire le cercle F I H, puis eſleuant du point G vne ligne droite iuſques à I, à angles droits ſur F H, c'eſt G I la racine cherchée. Ie ne dis rien icy de la racine cubique, ny des autres, à cauſe que i'en parleray plus commodement cy aprés.

Comment on peut

Mais ſouuent on n'a pas beſoin de tracer ainſi ces ligne

Il n'y a que des points

```
Lemma characterization_of_congruence_F : forall A B C D,
  Cong A B C D <->
  let (Ac, _) := coordinates_of_point_F A in
  let (Ax, Ay) := Ac in
  let (Bc, _) := coordinates_of_point_F B in
  let (Bx, By) := Bc in
  let (Cc, _) := coordinates_of_point_F C in
  let (Cx, Cy) := Cc in
  let (Dc, _) := coordinates_of_point_F D in
  let (Dx, Dy) := Dc in
  (Ax - Bx) * (Ax - Bx) + (Ay - By) * (Ay - By) -
  ((Cx - Dx) * (Cx - Dx) + (Cy - Dy) * (Cy - Dy)) =F= 0.
```

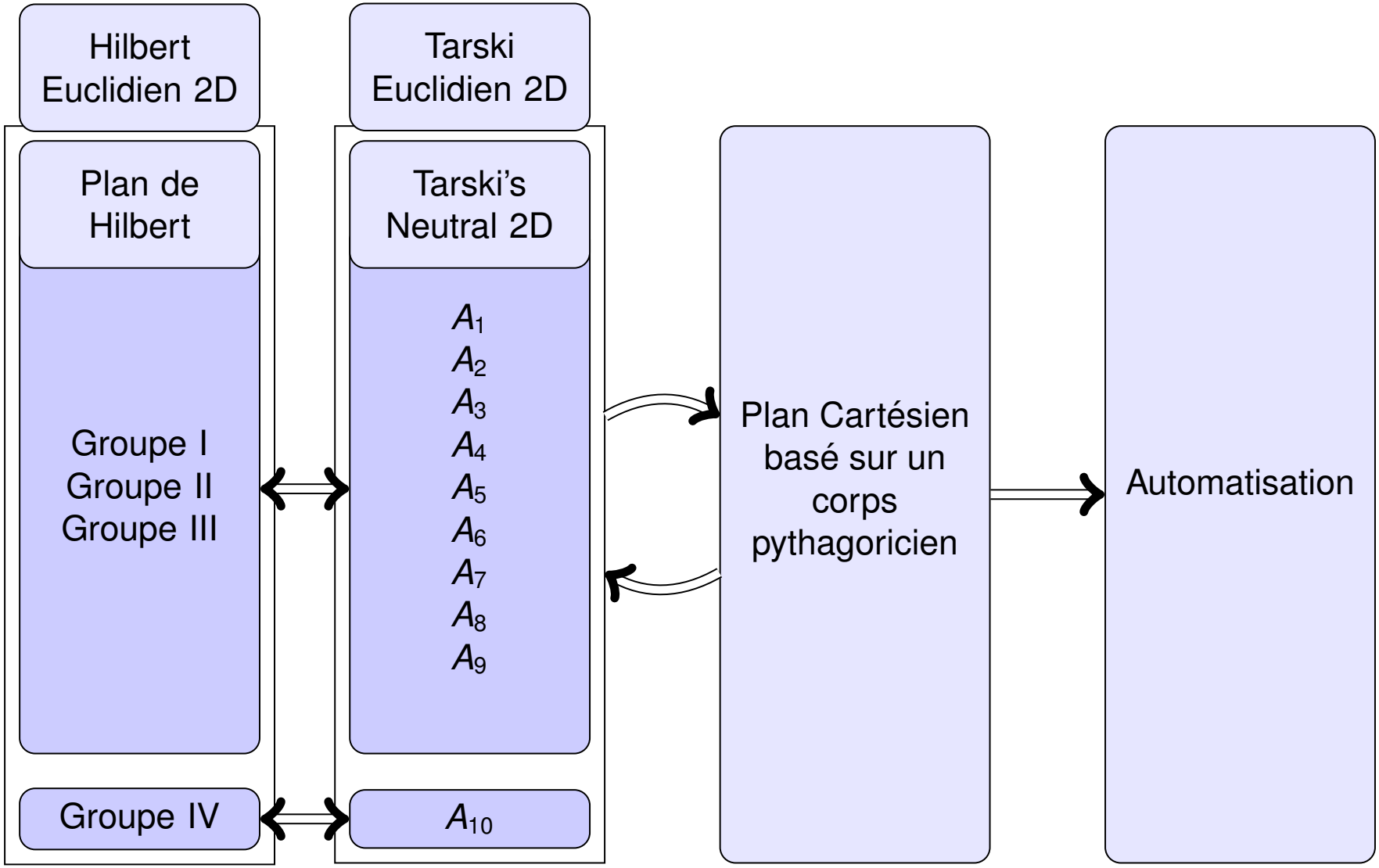
Automatisation en Géométrie

Ceci n'est pas un théorème à propos de polynômes :

```
Lemma centroid_theorem : forall A B C A1 B1 C1 G,
  Midpoint A1 B C ->
  Midpoint B1 A C ->
  Midpoint C1 A B ->
  Col A A1 G ->
  Col B B1 G ->
  Col C C1 G \/ Col A B C.
Proof.
intros A B C A1 B1 C1 G; convert_to_algebra; decompose_coordinates.
intros; spliter. express_disj_as_a_single_poly; nsatz.
Qed.
```

Techniques de formalisation

- Un mélange de preuve automatique et intéractive.
- Bootstraping : prouver des prouveurs automatiques avec d'autres prouveurs automatiques, on alors enrichir le prouveur avec le prouveur.


Hilbert
Euclidien 2D
Tarski
Euclidien 2D
Plan de
Hilbert
Tarski's
Neutral 2D
Groupe I
Groupe II
Groupe III
A_1
A_2
A_3
A_4
A_5
A_6
A_7
A_8
A_9
Groupe IV
A_{10}
Plan Cartésien
basé sur un
corps
pythagoricien
Automatisation

Interpretation mutuelle

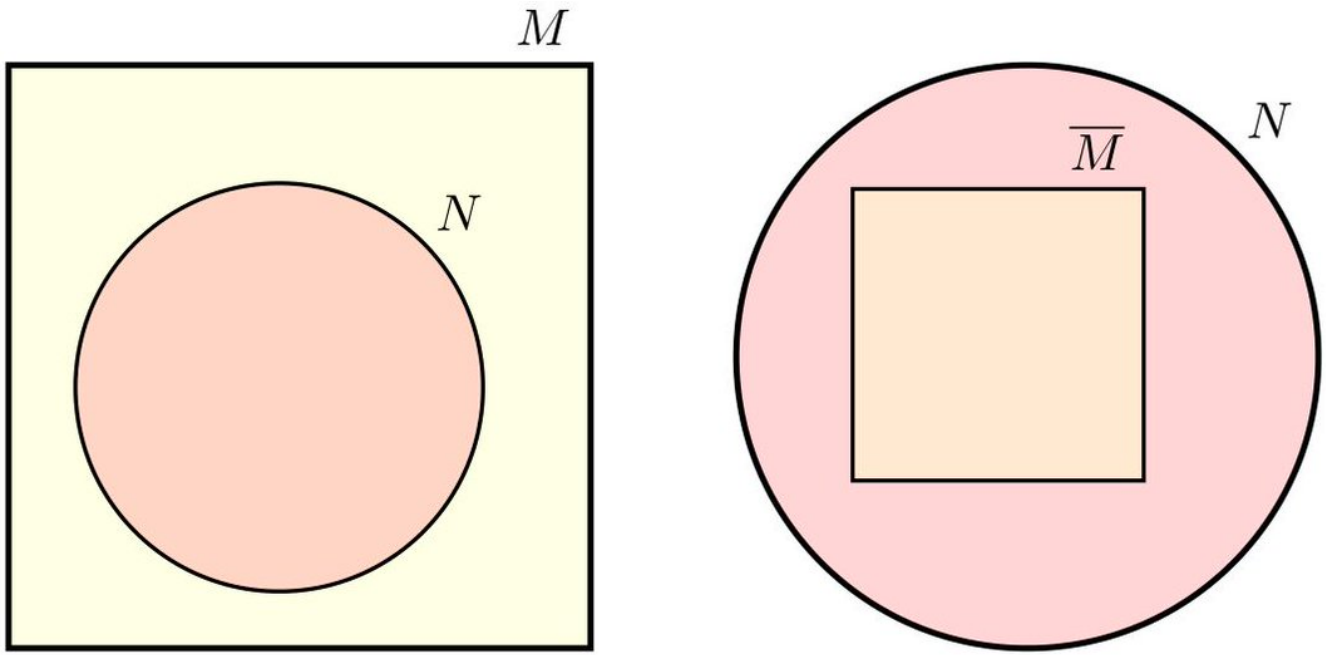


FIGURE 1. Mutual interpretation

Source : Joel David Hamkins

Continuité

Axiome de Dedekind du second-ordre A_{11}^*

$$\forall \alpha\beta\ (\exists a\ \forall xy\ (x \in \alpha \wedge y \in \beta \rightarrow \mathrm{Bet}\ a\, x\, y)) \rightarrow$$

$$(\exists b\ \forall xy\ (x \in \alpha \wedge y \in \beta \rightarrow \mathrm{Bet}\ x\, b\, y))$$

Schema d'axiomes de Dedekind A_{11}

$$(\exists a\ \forall xy\ (\alpha(x) \wedge \beta(y) \rightarrow \mathrm{Bet}\ a\, x\, y)) \rightarrow$$

$$(\exists b\ \forall xy\ (\alpha(x) \wedge \beta(y) \rightarrow \mathrm{Bet}\ x\, b\, y))$$

where $\alpha(x)$ and $\beta(y)$ stand for any first-order formulae in the language of Tarski's axiom system which does not contain any free occurrence of a, b, y in α and a, b, x in β.

Du premier ordre

```
Inductive FOF : Prop -> Prop :=
| eq_fof : forall A B:Tpoint, FOF (A = B)
| bet_fof : forall A B C, FOF (Bet A B C)
| cong_fof : forall A B C D, FOF (Cong A B C D)
| not_fof : forall P, FOF P -> FOF (~ P)
| and_fof : forall P Q, FOF P -> FOF Q -> FOF (P /\ Q)
| or_fof : forall P Q, FOF P -> FOF Q -> FOF (P \/ Q)
| implies_fof : forall P Q, FOF P -> FOF Q -> FOF (P -> Q)
| forall_fof : forall P, (forall (A:Tpoint), FOF (P A)) ->
                                              FOF (forall A, P A)
| exists_fof : forall P, (forall (A:Tpoint), FOF (P A)) ->
                                              FOF (exists A, P A).
```

Plongement

```
Inductive tFOF :=
| eq_fof1 : Tpoint -> Tpoint -> tFOF
| bet_fof1 : Tpoint -> Tpoint -> Tpoint -> tFOF
| cong_fof1 : Tpoint -> Tpoint -> Tpoint -> Tpoint ->
| not_fof1 : tFOF -> tFOF
| and_fof1 : tFOF -> tFOF -> tFOF
| or_fof1 : tFOF -> tFOF -> tFOF
| implies_fof1 : tFOF -> tFOF -> tFOF
| forall_fof1 : (Tpoint -> tFOF) -> tFOF
| exists_fof1 : (Tpoint -> tFOF) -> tFOF.
```

Les deux définitions coïncident

```
Lemma fof1__fof : forall F1:tFOF, FOF (fof1_prop F1).

Lemma fof__fof1 : FunctionalChoice_on Tpoint tFOF ->
  forall F:Prop, FOF F ->
  exists F1:tFOF,  F <-> fof1_prop F1.
```

Encodage du schema

```
Definition first_order_dedekind := forall Alpha Beta,
  (forall X, FOF (Alpha X)) ->
  (forall Y, FOF (Beta Y)) ->
  (exists A, forall X Y, Alpha X -> Beta Y -> Bet A X Y) ->
  (exists B, forall X Y, Alpha X -> Beta Y -> Bet X B Y).
```

Hilbert's own completeness axiom, added in other editions as V.2, takes the somewhat awkward form of requiring that it be impossible to properly extend the sets and relations satisfying the other axioms so that all the other axioms still hold.

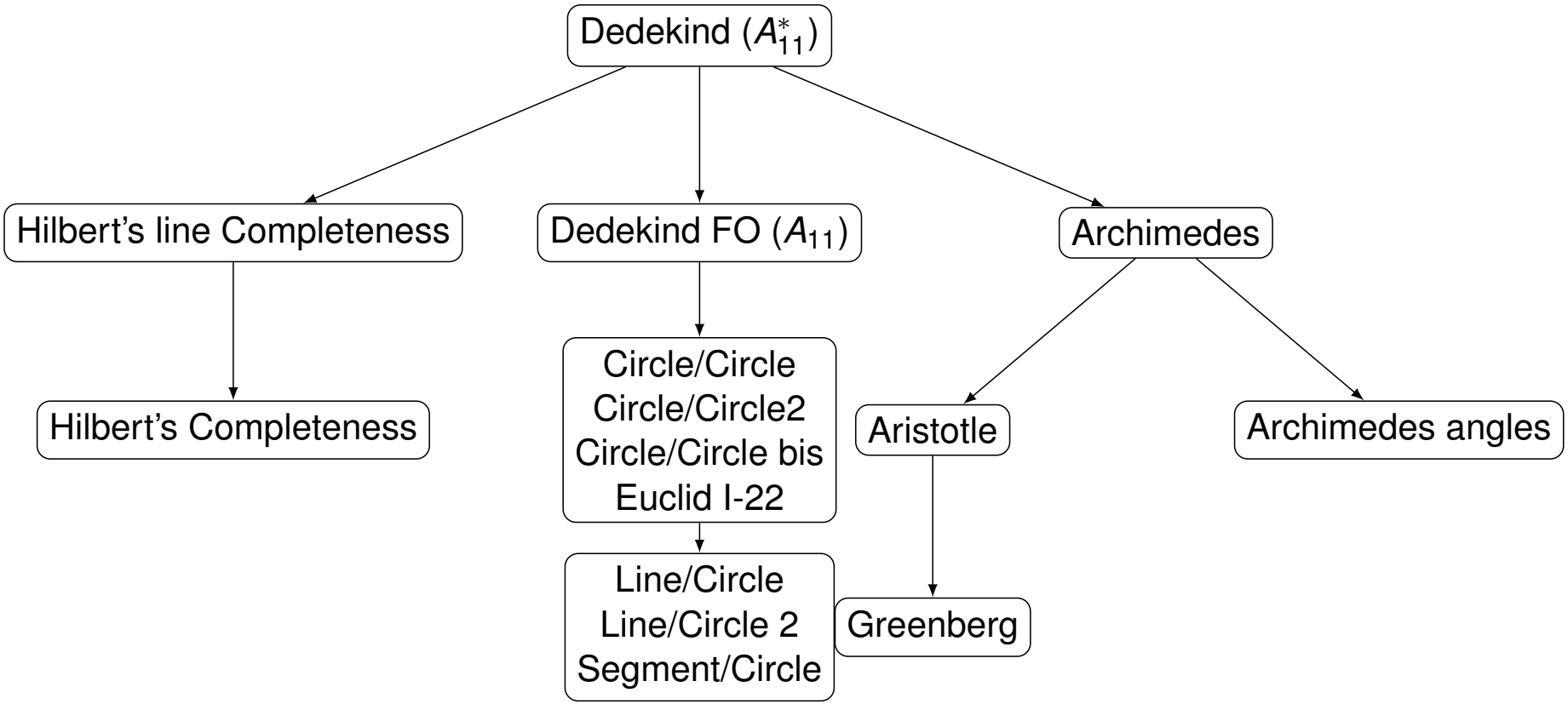
Martin MARTIN 1998, p. 175

Complétude à la Hilbert

“L’ensemble des points d’une droite, soumis aux relations d’ordre et de congruence, n’est susceptible d’aucune extension dans laquelle restent valides les relations précédentes et les axiomes I à III et V.1”

Formalisation de V2

```
Definition inj {T1 T2:Type} (f:T1->T2) := forall A B, f A = f B -> A = B.

Definition pres_bet {Tm: Tarski_neutral_dimensionless}
  (f : @Tpoint Tn -> @Tpoint Tm) := forall A B C, Bet A B C ->
                                                  Bet (f A) (f B) (f C).

Definition pres_cong {Tm: Tarski_neutral_dimensionless}
  (f : @Tpoint Tn -> @Tpoint Tm) := forall A B C D, Cong A B C D ->
                                                    Cong (f A) (f B) (f C) (f D).

Definition extension {Tm: Tarski_neutral_dimensionless} f :=
 inj f /\ pres_bet f /\ pres_cong f.

Definition completeness_for_planes := forall (Tm: Tarski_neutral_dimensior
  (Tm2 : Tarski_neutral_dimensionless_with_decidable_point_equality Tm)
  (M : Tarski_2D Tm2)
  (f : @Tpoint Tn -> @Tpoint Tm),
  @archimedes_axiom Tm ->
  extension f ->
  forall A, exists B, f B = A.
```


Dedekind (A_{11}^*)
Hilbert's line Completeness
Dedekind FO (A_{11})
Archimedes
Hilbert's Completeness
Circle/Circle
Circle/Circle2
Circle/Circle bis
Euclid I-22
Aristotle
Archimedes angles
Line/Circle
Line/Circle 2
Segment/Circle
Greenberg

Plan

Vérifions Euclide

Deux approches :

1. Essayer de vérifier les preuves d'Euclide
2. Vérifier les énoncés d'Euclide en faisant le moins d'hypothèses possible.

Exemple : Euclide I.1 l'existence d'un triangle équilatéral : la preuve d'Euclide utilise l'axiome de continuité Cercle-Cercle mais pas l'axiome des parallèles (trivial).
Mais il est aussi possible de formaliser une preuve utilisant l'axiome des parallèles mais pas la continuité Cercle-Cercle (non trivial).
Pambuccian a montré qu'on ne peux pas se passer des deux.

Les deux approches sont disponibles dans GeoCoq, aujourd'hui je parle de la première.
C'est une collaboration avec Beeson et Wiedijk.
En résumé :

- Un choix d'axiomes.
- Des preuves formelles des propositions du livre I

Notre cadre de travail

- Une théorie du premier ordre avec des variables de deux sortes différentes : points et des cercles.
- Les angles sont représentés par trois points. Comme Euclide, on parle de l'angle "ABC".
- Les droites sont données par deux points.
- Les relations primitives sont la "congruence" et l'entre deux.
- La congruence est une relation d'arité 4 entre points, $AB = CD$. Comme Euclide on utilise le mot égalité plutôt que "congruence".
- On a choisi de nommer les cercles, même si Euclide ne le fait pas. Euclide nomme les cercles par trois points, sans prouver que les points existent. On dit "Soit K le cercle de centre C et de rayon AB."

Nos axiomes (on a sélectionné les axiomes, mais ce sont des énoncés bien connus)

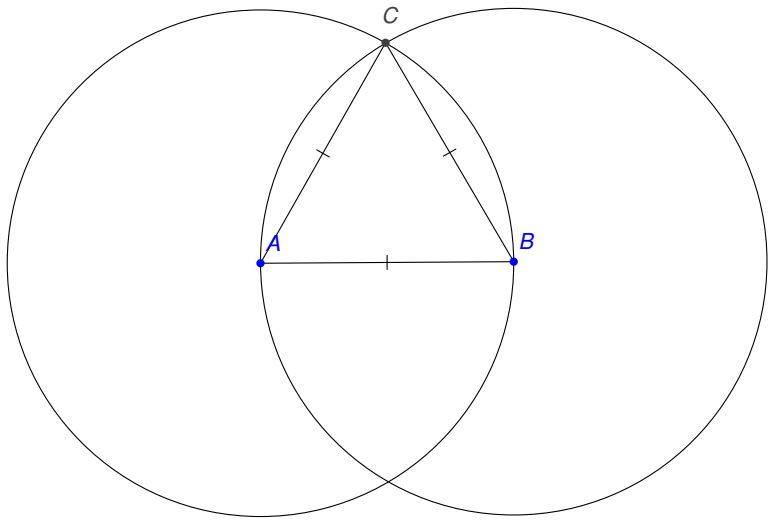
- Axiomes d'entre deux
- Axiomes de congruence, cela inclue l'extension de segments.
- Deux formes de l'axiome de Pasch, "Pasch interne" et "Pasch externe", introduites par Peano en 1890.
- L'axiome des 5-segments de Tarski, qui permet de prouver SAS.
- Continuité droite-cercle et cercle-cercle
- Euclide 5
- Nous n'avons pas Euclide 4 (les angles droits sont égaux) car il peut être prouvé.
- Un compas pas trop puissant.
- Des axiomes sur la congruence des aires.
- On a essayé de rajouter ce qu'il manquait pour les preuves d'Euclide, pas plus.

Un exemple

Proposition (Livre I, Prop. 1)

Soient A et B deux points, construire un triangle equilateral sur AB.

Preuve : Soit $\mathcal{C}_1$ et $\mathcal{C}_2$ les cercles de centre *A* et *B* et de rayon *AB*. Soit *C* l'intersection $\mathcal{C}_1$ et $\mathcal{C}_2$. La distance *AB* est égale à *AC* et *AB* est égale *BC*. Donc *ABC* est équilateral.

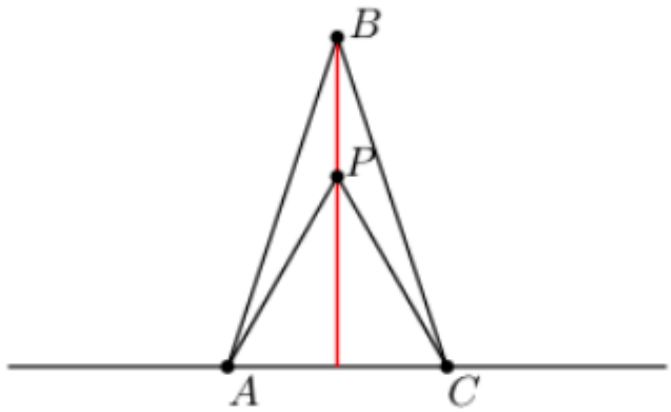


Deux des ‘trous’ dans Euclide

Problèmes

- Les postulats d’Euclide ne permettent pas de prouver que C existe.
- Euclide ne prouve pas que le triangle n’est pas dégénéré.

Prop. I.9, Bisection de l'angle



- Construire P par I.1 tel que ACP est équilateral.
- Alors BP est la bissectrice.
- Mince ! Et si B et P sont le même point ?

Prop. I.9 (suite)

- On pourrait prendre un axiome cercle-cercle plus fort.
- De toute façon comment on sait que la demie droite coupe AC ?
- Euclide s'en sert dans I.10 (Milieu) sans l'avoir prouvé.
- On s'en sort en construisant le milieu grâce à une preuve de Gupta.

Un preuve syntaxique de l'indépendance de l'axiome des parallèles.

Un exemple jouet

Exemple

Le langage :

Un prédicat : R (arité 2)
Une constante : $\blacksquare$
Un symbole de fonction : μ (arité 1)

Une axiome : $R(\blacksquare, \blacksquare)$

Une règle : $\forall x, R(x, x) \Rightarrow R(\mu(x), \mu(x))$

Question

Est-ce que $R(\mu(\mu(\blacksquare)), \mu(\blacksquare))$ est un théorème ?

Réponse 1 (preuve syntaxique)

Non, car :

1. Ce n'est pas un axiome.
2. La règle ne s'applique qu'une fois.

Réponse 2 (preuve sémantique)

Non, car on peut interpréter :

- R par l'égalité $=$
- $\blacksquare$ par 0
- μ par la fonction $x \mapsto x + 1$

On a bien $0 = 0$ et $\forall x, x = x \Rightarrow x + 1 = x + 1$ mais pas $2 = 1$.

Tarski

Cinq axiomes avec des quantifications existentielles :

1. Lower dimension
2. Segment construction
3. Pasch
4. Parallel postulate
5. Continuity : Dedekind cuts or line-circle continuity

Main idea

Study the maximum distance between the points in the axioms with existential quanti fication :

Lower dim Initial Constant.

Inner Pasch The distance is conserved.

Segment Construction The distance is at most doubled.

Line Circle Continuity The distance is preserved.

Euclid We can build points arbitrarily far.

The proof

- Skolemize the axiom system : replace existential quantification with function symbols.
- Apply Herbrand's theorem.

Herbrand's theorem

Herbrand's theorem says that under some assumptions (the theory is first-order and does not contains existential), if the theory proves an existential theorem $\exists y\, \phi(a, y)$, with ϕ quantifier-free, then there exist finitely many terms $t_1, \ldots, t_n$ such that the theory proves

$$\phi(a, t_1(a)) \vee \phi(a, t_2(a)) \ldots \vee \ldots \phi(a, t_n(a)).$$

Example in geometry

Dropping or erecting a perpendicular.

Conclusion

GeoCoq

On a une bibliothèque partant des fondements (Tarski, Hilbert, Euclide) et allant jusqu'à l'arithmétisation et l'automatisation.

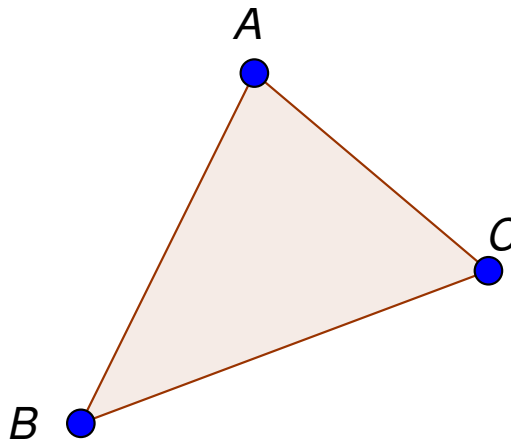
Euclide

- On a du rajouter des axiomes sur la congruence des aires.
- On a formalisé le livre I avec des preuves classiques du premier ordre.
- On a du prouver les propositions dans un ordre différent et utiliser une preuve de Gupta.

Questions ?

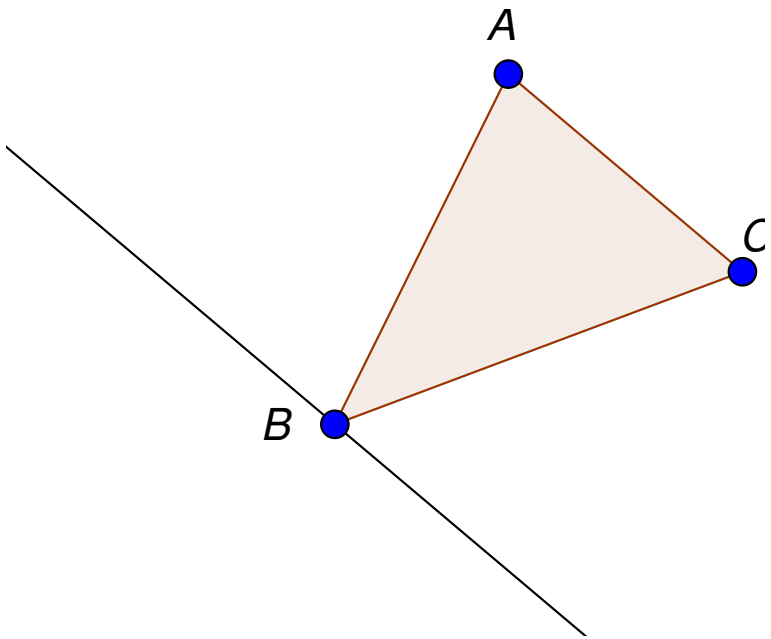
La somme des angles d'un triangle

Soit l une parallèle à AC passant par B.



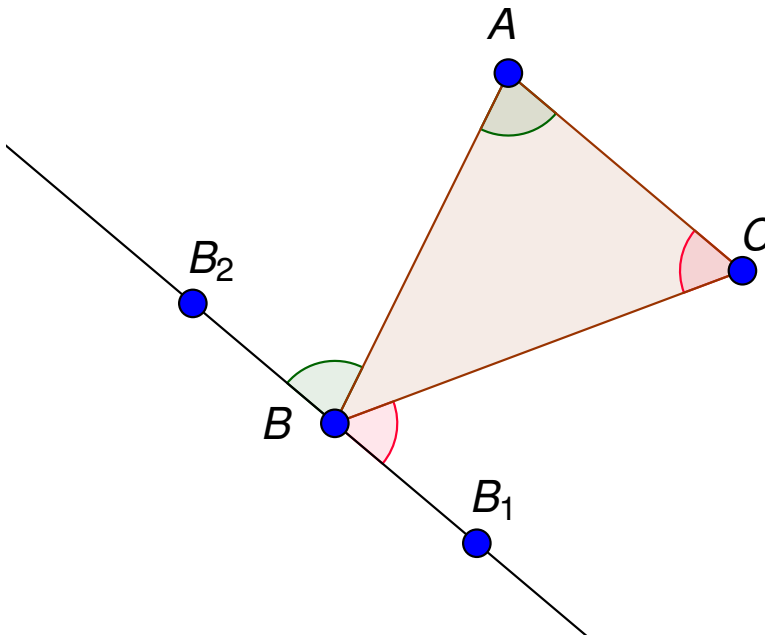
La somme des angles d'un triangle

Soit l une parallèle à AC passant par B.



La somme des angles d'un triangle

Soit l une parallèle à AC passant par B.

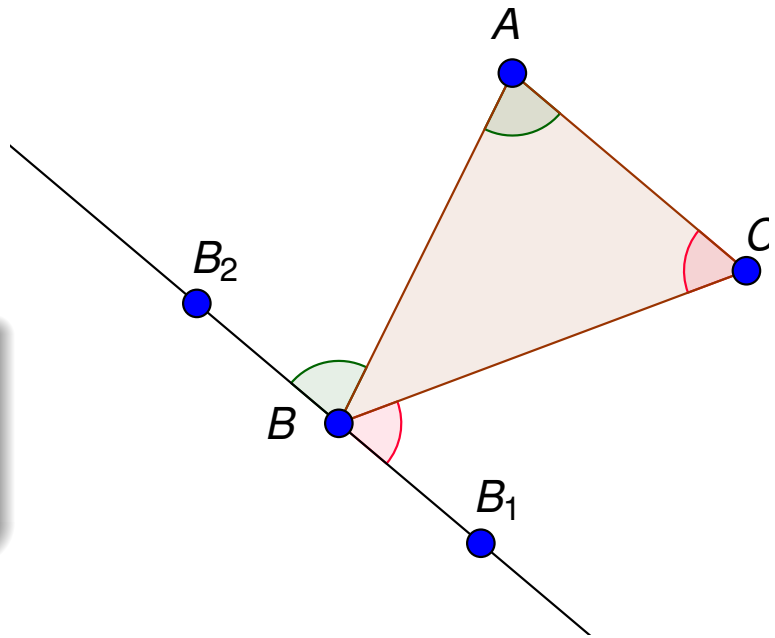


La somme des angles d'un triangle

Soit l une parallèle à AC passant par B.

Problème !

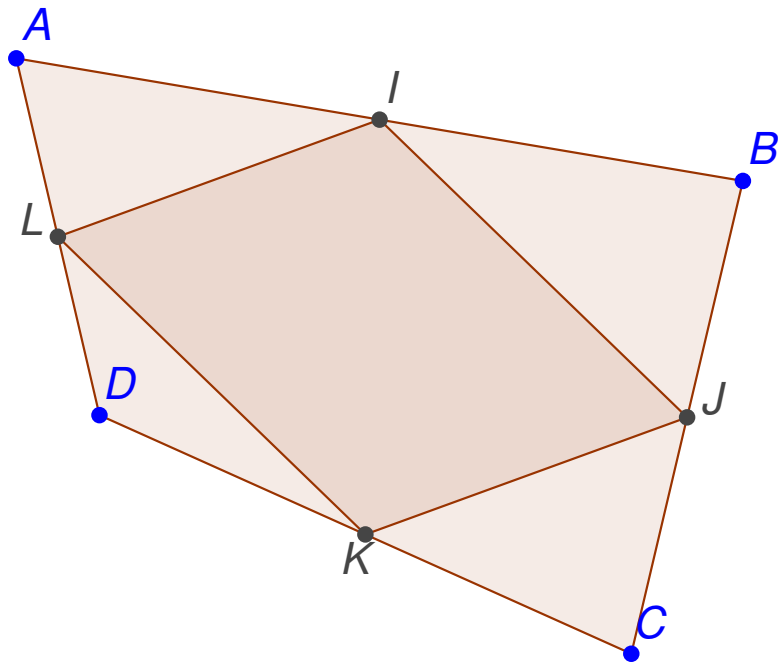
Il faut prouver que les angles sont bien alternes/internes.



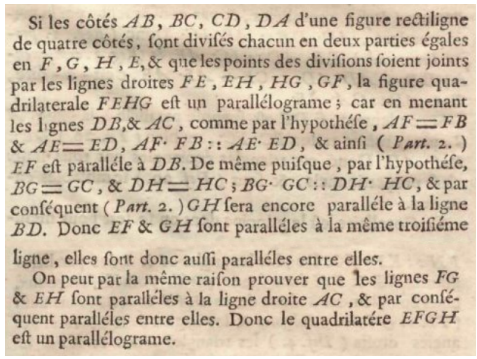
Théorème de Varignon

Theorem

Soit ABCD un quadrilatère. Soient I, J, K et L les milieux de AB, BC, CD, et AD, alors IJKL est un parallèlogramme.



D'après le théorème de la droite des milieux. Dans le triangle ABC on a $AC \parallel IJ$. On a aussi $AC \parallel LK$. Donc $LK \parallel IJ$.
De manière analogue, $IL \parallel JK$.

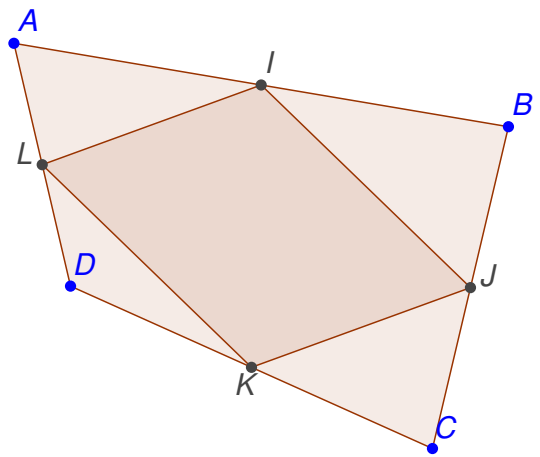


Si les côtés AB, BC, CD, DA d'une figure rectiligne de quatre côtés, sont divisés chacun en deux parties égales en F, G, H, E, & que les points des divisions soient joints par les lignes droites FE, EH, HG, GF, la figure quadrilaterale $FEHG$ est un parallélograme ; car en menant les lignes DB, & AC, comme par l'hypothèse, $AF = FB$ & $AE = ED$, $AF \cdot FB :: AE \cdot ED$, & ainsi (*Part.* 2.) EF est parallèle à DB. De même puisque, par l'hypothèse, $BG = GC$, & $DH = HC$; $BG \cdot GC :: DH \cdot HC$, & par conséquent (*Part.* 2.) GH sera encore parallèle à la ligne BD. Donc EF & GH sont parallèles à la même troisiéme ligne, elles sont donc aussi parallèles entre elles.

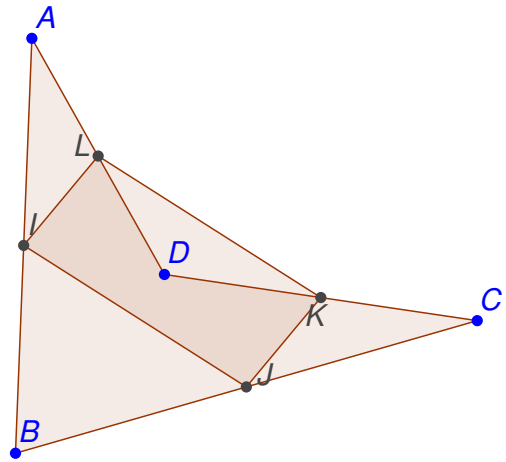
On peut par la même raison prouver que les lignes FG & EH sont parallèles à la ligne droite AC, & par conséquent parallèles entre elles. Donc le quadrilatére $EFGH$ est un parallélograme.

Preuve originale

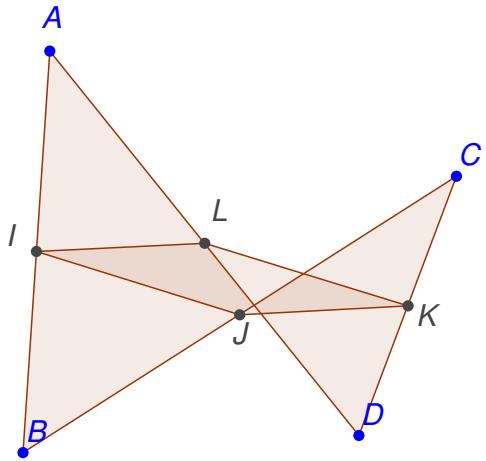
Théorème de Varignon



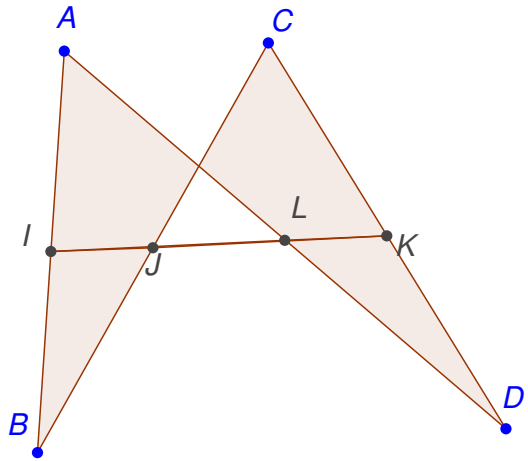
(a) Cas Convexe



(b) Cas Concave



(c) Cas d'auto-intersection



(d) Cas particulier