ISSN : 2795-9104
Version numérique

MaSciProûve

Vol. 1 Num. 2

La revue de l'association sans but lucratif "cafr-MSA2P"

Siège social :
Rue de la Brasserie 5
7100 La Louvière, Belgique
Numéro d'entreprise : 0777.770.751
Registre des Personnes Morales : Hainaut division Mons
IBAN : BE79 3632 1778 3733

Editeur responsable Roland Coghetto

Avril-Mai-Juin 2022

Les articles de ce périodique ne sont pas des articles scientifiques : ils ne sont pas soumis à un protocole de relecture et de validation avec comité de lecture scientifique. Nous ne publions pas d'articles scientifiques dans ce périodique : le cas échéant, nous vous invitons à contacter directement les revues scientifiques.
De plus, certains ne sont pas à strictement parler des articles de vulgarisation : en effet, ils n'en respectent ni la forme ni le contenu.
Sauf exception, les numéros de version des logiciels et bibliothèques associées à ces logiciels ne sont volontairement pas explicités. Si besoin, nous invitons le lecteur à vérifier au cas par cas l'état actuel des modifications apportées à ces logiciels ou bibliothèques.

Par contre, les articles ont pour objectif de présenter, de susciter votre intérêt, d'alimenter votre curiosité et votre réflexion au sujet de l'utilisation de logiciels *assistant interactif de preuve* ou *assistant automatique de preuve.*
Soyez également libre de nous proposer vos articles non scientifiques. Dans la limite de nos moyens, l'association soutient ses membres pour la préparation d'articles utilisant des assistants de preuves pour des revues scientifiques : aide à l'utilisation des logiciels, compréhension des bibliothèques,. . .

"Proûve" signifie "preuve" (dialecte wallon de Liège - Dictionnaire liégeois de Jean Haust)

Editeur responsable de la revue "MaSciProûve" : Roland Coghetto

"cafr-MSA2P" ASBL est l'abréviation de *"Centre autonome de formation et de recherche en mathématiques et sciences avec assistants de preuve"* association sans but lucratif (non-profit organisation)
Siège social : Rue de la Brasserie 5, 7100 La Louvière - Belgique
Numéro d'entreprise : 0777.770.751
Registre des Personnes Morales : Hainaut division Mons
IBAN : BE79 3632 1778 3733

L'association ne délivre pas de diplômes. (cf. Art. 3 §3. du *Décret définissant le paysage de l'enseignement supérieur et l'organisation académique des études* : "Les établissements d'enseignement supérieur [. . .] sont seuls habilités à délivrer les titres, grades académiques, diplômes et certificats correspondant aux niveaux 5 à 8 du cadre francophone des certifications.")

Auteur : Roland Coghetto

Remerciements : Denise C. (pour son soutien à la version imprimée), Predrag Janičić (pour les précisions apportées au logiciel **GCLC** ainsi qu'au logiciel **ArgoTriCS** de Vesna Marinković (née Pavlovic)), Pascal Fontaine (pour l'entretien).

Relecture des articles : Catherine Marbaix.

Ce périodique ne peut être vendu.

Table des matières

1 Le coin des logiciels

1.1 GCLC

Dans cette section nous allons aborder notre premier assistant automatique de preuve. Ce n'est probablement pas le plus représentatif de tous les assistants automatiques, mais il est intéressant à plus d'un égard.

Voici comment l'auteur du logiciel, Predrag Janičić, professeur à l'Université de Belgrade, présente **GCLC**[17] [1] [2] :

> GCLC (from "Geometry Constructions -> LaTeX Converter") is a tool for visualizing geometry, and for producing mathematical illustrations. Its main purposes are :
> — producing digital mathematical illustrations of high quality ;
> — use in teaching geometry ;
> — use in studying geometry with the help of automated theorem provers.

Le logiciel est téléchargeable à l'adresse suivante : `https://github.com/janicicpredrag/gclc`. Il est sous licence *Creative Commons licence CC BY-ND*[3] : Attribution-NoDerivatives 4.0 International, autrement dit : attribution mais pas de modification.

Initialement **GCLC** n'est pas un assistant de preuve. Il s'agit d'un logiciel en ligne de commande (également disponible avec une version fenêtrée "gui") qui permet d'encoder des figures géométriques dans plusieurs formats, dont principalement ceux utilisés dans LaTeX.

Prenons un exemple tiré du manuel d'utilisateur[4] afin d'illustrer notre propos (voir le Listing 1) .

Ce code essaye d'être le plus proche d'une pratique mathématique quotidienne ; ainsi la plupart des notations parlent d'elle-même. (Pour plus de précision : `med a C B` est la construction de la médiatrice a du segment $[CB]$ et `intersec O a b` est la construction du point O comme point d'intersection de deux droites sécantes a et b. [5])

Le manuel de l'utilisateur précise :

> Geometrical constructions are the main area of GCLC. A geometrical construction is a sequence of specific, primitive construction steps. These primitive construction steps are also called elementary constructions and they are :
> — [...]
> — construction of a point such that it is the intersection of two lines (if such a point exist) ;
> — [...]

).

En compilant ce fichier avec la commande appropriée [6], nous obtenons le résultat représenté par la Figure 2.

Même si les fonctions de **GCLC** pour dessiner des graphiques sont très intéressantes, nous ne les aborderons pas en profondeur dans cette section.

Notre intérêt se portera plutôt sur les fonctionnalités suivantes :

— la capacité à placer un point aléatoirement sur un segment (`onsegment`), sur une droite (`online`), sur un cercle (`oncircle`) ;
— la capacité de pouvoir affirmer, dans certaines situations particulières, si un énoncé est vrai (`prove`).
  Cet énoncé peut être prouvé uniquement si les constructions utilisent les termes suivants :
  — `point`
  — `line`

[1] `http://poincare.matf.bg.ac.rs/~janicic//gclc/`

[2] Trad. : **GCLC** est un outil permettant de visualiser la géométrie et de produire des illustrations mathématiques. Ses principaux objectifs sont les suivants
— la production d'illustrations mathématiques numériques de haute qualité ;
— utilisation dans l'enseignement de la géométrie ;
— l'étude de la géométrie à l'aide de la démonstration automatique de théorèmes.

[3] This license allows for redistribution, commercial and non-commercial, as long as it is passed along unchanged and in whole, with credit to the author.

[4] `https://github.com/janicicpredrag/gclc/blob/master/samples/basic_samples/sample01_triangle.gcl`

[5] Il est à noter que si $a \parallel b$ ou si $a = b$, le logiciel vous signale qu'il ne peut pas déterminer l'intersection de ce point. En effet, l'intersection est vide ou bien est la droite a : `Run-time error: Bad definition. Can not determine intersection. (Line: XX, position: YY)`.

[6] Par exemple, `gclc sample01_triangle.gcl -eps`

sample01_triangle.gcl

```
point A 50 65
point B 45 35
point C 90 35
cmark_lt A
cmark_lb B
cmark_rb C
drawsegment A B
drawsegment B C
drawsegment C A
med a C B
med b A C
intersec O a b
drawcircle O A
```

FIGURE 1 – Listing sample01_triangle

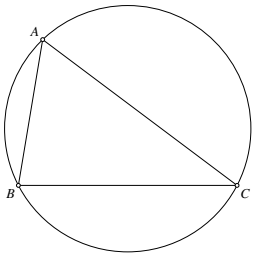

FIGURE 2 – sample01_triangle.eps

— `intersec`
— `midpoint`
— `med`
— `perp`
— `foot`
— `parallel`
— `online`,
— `translate` [7],
— `towards` [8].

On peut constater que l'assistant de preuve n'est pas adapté dans le cas de construction avec `oncircle`. Cela paraît étonnant de retrouver dans la liste des constructions autorisées la construction `midpoint`, alors que celle-ci peut être construite avec `oncircle`. Il ne s'agit pas d'une erreur. L'assistant de preuve utilise des algorithmes qui ne sont pas tout-à-fait similaire à des constructions règles/compas.

Mais dans ce cas l'assistant de preuve est-il utile ?

Si l'on désire une preuve automatique, il faut respecter les constructions permises, ce qui limite de fait les possibilités puisqu'on ne peut réaliser certaines constructions nécessitant un compas, la construction `oncircle` plus précisement. Ce serait comme utiliser une calculatrice donnant le résultat correct lorsqu'on additione 2 nombres pairs mais elle ne donnerait pas le résultat correct dans les autres situations. Faut-il jeter cette calculatrice à la poubelle ? Je pense que

[7] `translate P A B C` : le point P est égal à $C + \overrightarrow{AB}$
[8] `towards P A B n` : le point P est égal à $A + n * \overrightarrow{AB}$

non car :
- Il n'existe pas à ma connaissance d'assistant de preuve automatique qui validerait n'importe quelle construction du type règle/compas, dans un délai raisonnable.
- Certaines constructions, qui sont limitées par le mode d'emploi de **GCLC** peuvent ne pas être triviale : par exemple, les constructions possédant des configurations de type "théorème de Pappus".
- il est parfois utile lorsqu'on prépare l'énoncé d'un exercice avec un diagramme d'avoir une certitude sur un hypothèse du dessin que l'on prépare : par exemple "est-il vrai que les points sont alignés ? y-a-t-il des cas auxquels je ne pense pas où ces points ne sont plus alignés ?". L'assistant de preuve peut nous aider en nous donnant une réponse. Si elle est positive, alors nous pouvons raisonnablement nous fier à cette réponse. Bien entendu, nous pouvons vérifier nos hypothèses à la main par du calcul classique (calcul vectoriel, algébrique, ...) ou un par un raisonnement de géométrie classique.

Voici le type de questions à laquelle **GCLC** peut répondre :
- deux points P et Q sont-ils identiques ?
- trois points P, Q et R sont-ils alignés ?
- $AB \perp CD$?
- $AB \parallel CD$?
- O est-il le milieu de deux points donnés P et Q ?
- la distance (euclidienne) entre les points A et B est-elle la même qu'entre les points C et D ?
- les points A, B, C et D sont-ils dans un rapport harmonique ?

Si **GCLC** ne répond pas ou ne répond pas positivement à une question, cela ne signfie pas que la négation de l'énoncé est vrai. C'est juste que l'assistant de preuve n'a pas nécessairement trouvé une preuve.

Pour être plus précis,
- **GCLC** peut[9] :
  1. Dire qu'il est hors du champ d'application de la méthode choisie.
  2. Prouver la conjecture donnée.
  3. Réfuter la conjecture donnée.
  4. Atteindre une limite de temps.
- **GCLC** possède trois méthodes attachées à son assistant de preuves qu'il faut activer par les options `-a`, `-w` et `-g`. (l'option `-a` est activée par défaut).

Le mode par défaut (`-a`) est utile pour la préparation de graphiques contenant des éléments aléatoires comme `online`. En effet, comme nous l'avons déjà signalé plus haut, il est possible alors de
- Vérifier qu'une propriété est valide pour toutes les configurations aléatoires créés par `online` et qu'elle n'est pas vérifiée pour certaines configurations seulement. Dans le cas, où l'on propose des exercices en lien avec un graphique, et que ce graphique contient des éléments aléatoires, notre degré de confiance augmente si l'assistant de preuve nous confirme qu'un énoncé que nous lui proposons de prouver est vrai.
- Permettre un prototypage plus rapide de certains exercices. En effet, dans certains cas, une preuve (ou une vérification de la configuration des points) manuelle peut-être beaucoup plus longue qu'une vérification avec l'assistant de preuve.

Pour illustrer notre propos, prenons deux exemples particuliers :
- Le théorème de Pappus et
- La trisection d'un segment.

Dans la suite, l'ordre de succession de construction des points des figures est le même que l'ordre lexicographique : A,B,C,D,E,...

1.1.1 Théorème de Pappus

Le théorème de Pappus est un théorème classique de la géométrie projective. Un énoncé est :

[9] GCLC may :
- say that it is out of the scope of the chosen method
- prove the given conjecture
- disprove the given conjecture
- reach a time limit

"Dans un plan euclidien, soit A_1, B_1, C_1 trois points distincts alignés sur une droite (d), et soit A_2, B_2, C_2 trois autres points distincts alignés sur une autre droite (d') alors les points
— A : intersection de (B_2C_1) avec (C_2B_1)
— B : intersection de (A_2C_1) avec (C_2A_1)
— C : intersection de (A_2B_1) avec (B_2A_1)
sont alignés "[31].

La Figure 4 est une illustration du théorème de Pappus dont les points sont construits suivant le Listing 3. Il est à noter que nous avons délibérément commenté les lignes `online C A B`, `online F E D`. Celles-ci sont remplacées par `onsegment C A B` et `onsegment F E D`. En effet, la fonction `online` peut construire un point qui peut être visuellement hors de la portée de notre affichage. Cela peut rapidement devenir incompréhensible pour le lecteur si certains points lui sont hors de vue. Cette restriction volontaire ne diminue en rien notre propos.

pappus1.gcl

```
point A 10 20
point B 50 80
onsegment C A B
%online C A B
cmark_lt A
cmark_lt B
cmark_lt C
drawline A B
point D 60 15
point E 100 75
onsegment F D E
%online F D E
cmark_lt D
cmark_lt E
cmark_lt F
drawline D E
line lAE A E
line lAF A F
line lBD B D
line lBF B F
line lCD C D
line lCE C E
drawdashline lAE
drawdashline lAF
drawdashline lBD
drawdashline lBF
drawdashline lCD
drawdashline lCE
intersec P lBF lCE
intersec Q lAF lCD
intersec R lAE lBD
cmark_lt P
cmark_lt Q
cmark_lt R
drawline P Q
%prove { collinear P Q R }
```

FIGURE 3 – Listing pappus1

Nous n'avons pas encore utilisé les fonctions de *theorem prover* de **GCLC**. En effet, si visuellement nous pouvons imaginer que les trois points P, Q et R sont alignés, le sont-ils réellement ? Peut-être ne sont-ils pas alignés et notre perception erronée. Comment en être sûr ? Bien entendu, dans ce cas, notre connaissance du théorème de Pappus nous apporte la réponse. Mais que faire si nous ne reconnaissons ni le théorème de Pappus, ni la configuration ? C'est à ce moment que l'assistant de preuve peut venir à notre secours.

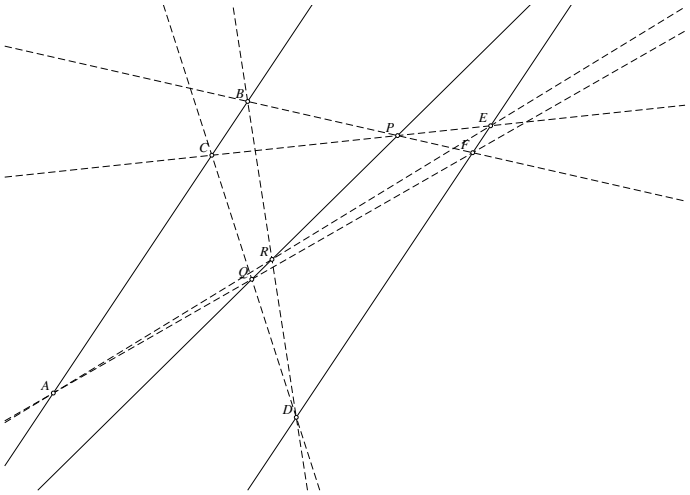

FIGURE 4 – pappus1.eps

De façon générale, il y a non pas une méthode mais trois méthodes attachées à l'assistant de preuve intégré à **GCLC** :

There are three theorem provers built into GCLC :
— a theorem prover based on the Chou's area method ; the prover produces traditional (i.e., geometric, not algebraic, coordinate-based), readable proofs ; the proofs are expressed in terms of higher-level geometry lemmas and expression simplifications.
— theorem provers based
  — on the Wu's method and
  — on the Gröbner bases method :
  these provers are algebraic theorem provers ; they are based on manipulating polynomials and they do not produce traditional geometrical proofs.

The theorem prover to be used is selected in the following way in the command line version, by an appropriate parameter :
— `-a` for the area method (default),
— `-w` for the Wu's method,
— `-g` for the Gröbner bases method.

Dans ce numéro, nous ne détaillerons pas les différentes méthodes. Par contre une introduction utile peut être trouvée (en anglais) : [21]. Pour en savoir plus sur
— la méthode des aires (en anglais) : [23, 16].
— la méthode Wu (en anglais) : [8, 10],
— la méthode des bases de Gröbner et de l'algorithme Buchberger (en français : [22] , en anglais :[14])

La dernière ligne du Listing 3 (`prove { collinear P Q R }`) est commentée par l'ajout du symbole % Supprimons ce symbole et relançons **GCLC** avec une des options `-a`, `-w` ou `-g`. Peut-être aurons nous une réponse positive ? Le fichier `pappus1.gcl` a été arbitrairement renommé `pappus1proof.gcl` : ce n'est pas nécessaire mais utile pour l'illustration ci-dessous :
— Recherche d'une preuve par la méthode des aires (option `-a`) :

```
gclc pappus1proof.gcl -a

GCLC 2022 (GC language (R) -> LaTeX Converter)
Copyright (c) 1995-2022 by Predrag Janicic, University of Belgrade.
Licensed under the MIT Licence.

Input file: pappus1proof.gcl
Output file: pappus1proof.pic
Log file: gclc.log

Starting point number: 1

The theorem prover based on the area method used.
```

```
Number of elimination proof steps:     23
Number of geometric proof steps:       54
Number of algebraic proof steps:      274
Total number of proof steps:          351

Time spent by the prover: 0.007 seconds
The conjecture successfully proved.
The prover output is written in the file pappus1proof_proof.tex.

File 'pappus1proof.gcl' successfully processed.
Ending point number: 941

Transcript written on gclc.log.
```

— Recherche d'une preuve par la méthode **Wu** (option `-w`) :

```
GCLC 2022 (GC language (R) -> LaTeX Converter)
Copyright (c) 1995-2022 by Predrag Janicic, University of Belgrade.
Licensed under the MIT Licence.

Input file: pappus1proof.gcl
Output file: pappus1proof.pic
Log file: gclc.log

Starting point number: 1

The theorem prover based on the Wu's method used.
The largest polynomial obtained during the proof process contains 18 terms.


Time spent by the prover: 0.003 seconds
The conjecture successfully proved.
The prover output is written in the file pappus1proof_proof.tex.

File 'pappus1proof.gcl' successfully processed.
Ending point number: 891

Transcript written on gclc.log.
```

— Recherche d'une preuve par la méthode des bases de Gröbner (option `-g`) :

```
GCLC 2022 (GC language (R) -> LaTeX Converter)
Copyright (c) 1995-2022 by Predrag Janicic, University of Belgrade.
Licensed under the MIT Licence.

Input file: pappus1proof.gcl
Output file: pappus1proof.pic
Log file: gclc.log

Starting point number: 1

The theorem prover based on the Groebner bases method used.
The largest polynomial obtained during the proof process contains 680 terms.


Time spent by the prover: 0.169 seconds
The conjecture successfully proved.
The prover output is written in the file pappus1proof_proof.tex.

File 'pappus1proof.gcl' successfully processed.
Ending point number: 889
```

Nous pouvons constater que dans les trois cas nous avons la confirmation que l'énoncé à prouver est vrai : `The conjecture successfully proved.`

En pratique, il arrive que les trois assistants de preuve ne confirment pas simultanément l'énoncé, mais au moins un des trois. Dans ce cas, l'énoncé peut-être considéré comme vrai.

Poursuivons notre expérimentation avec le théorème de Pappus en supposant qu'un diagramme (cf. Figure 6 du Listing 5) contient non pas une mais deux configurations de Pappus[10] : l'assistant de preuve peut-il distinguer les deux configurations séparément ? La réponse est affirmative.

Il est à noter que la conjecture `prove { collinear P Q R }` a été vérifiée avec les trois options `-a`,`-w`,`-g` tandis que la conjecture `prove { collinear P2 Q2 R2 }` a été vérifiée rapidement avec l'option `-a`, plus lentement avec l'option `-w` et sans résultat avec l'option `-g`.

Etant donné qu'au moins une des trois méthodes a pu prouver la conjoncture
`prove { collinear P2 Q2 R2 }`, celle-ci est validée.

Poursuivons notre expérimentation en considérant maintenant qu'une troisième configuration est construire à partir des 2 autres, autrement dit les points alignés P, Q et R et P_2, Q_2 et R_2 sont utilisés pour construire les trois points P_3, Q_3 et R_3. (Voir la Figure 8. Le listing est donné à titre indicatif : 7).

Malheureusement, nous n'avons pas pu obtenir une affirmation `prove { collinear P3 R3 Q3 }` par l'une des trois méthodes de l'assistant de preuve. Peut-être une configuration particulière serait nécessaire ?

CHALLENGE 1 : Réussir à prouver `prove { collinear P3 R3 Q3 }`.

CHALLENGE 2 : Allons plus loin : le théorème de Pascal qui est une généralisation du théorème de Pappus[11] :

Proposer une modification au logiciel **GCLC** afin de prouver, dans la configuration du théorème de **Pascal** : `prove { collinear X Y Z }`. (cf. Listing 9 , 11 et 13). Attention : le théorème de Pascal est valide uniquement si la conique n'est pas dégénérée en une seule droite.

De plus, comme le théorème de Pappus est un cas particulier du théorème de Pascal lorsque la conique est dégénérée en deux droites d_1 et d_2 distinctes,

CHALLENGE 3 : Proposer une modification au logiciel **GCLC** permettant de dessiner une conique dégénérée en deux droites sécantes ou parallèles distinctes ou non directement à partir de droites et non pas avec une approximation de points (cf. Listing 15 ,17). Par exemple étant donné que :

> "A conic `<conic_id>` is determined by the given parameters a, b, c, d, e and f in the following form : $ax^2 + 2bxy + cy^2 + 2dx + 2ey + f = 0$"

— la conique déterminée par les valeurs (1,0,-1,0,-10,-25) càd d'équation $x^2 - y^2 - 10y - 25 = 0$ est dégénérée en deux droites sécantes ;

— la conique déterminée par les valeurs (1,-1,1,0,0,-1) càd d'équation $x^2 - 2xy + y^2 - 1 = 0$ est dégénérée en deux droites parallèles.

Nous espérons vous avoir convaincu par ces exemples simples de l'utilité potentielle de l'assistant de preuve annexé à un logiciel de dessin de diagramme de géométrie élémentaire.

Si, dans des situations simples, il est possible de vérifier par un calcul vectoriel l'énoncé (par exemple l'alignement), dans d'autres exemples ce calcul vectoriel augmente en complexité. Même si l'appel à la fonction `prove` peut ne pas donner une réponse, si la réponse est positive, elle peut nous donner une information utile et parfois non négligeable.

[10] La première configuration est basée sur les points A, B, C, D, E et F située en bas de l'image tandis que la seconde configuration est basée sur les points $A2$, $B2$, $C2$, $D2$, $E2$ et $F2$ située en haut de l'image

[11] Le théorème de Cayley–Bacharach est une généralisation du théorème de Pascal. Pour en savoir plus (en anglais) :[31]. Nous n'utiliserons pas cette généralisation.

pappus2.gcl

```
dim 200 200
point A 10 20
point B 50 80
onsegment C A B
%online C A B
cmark_lt A
cmark_lt B
cmark_lt C
drawline A B
point D 60 15
point E 100 75
onsegment F D E
%online F D E
cmark_lt D
cmark_lt E
cmark_lt F
drawline D E
line lAE A E
line lAF A F
line lBD B D
line lBF B F
line lCD C D
line lCE C E
drawdashline lAE
drawdashline lAF
drawdashline lBD
drawdashline lBF
drawdashline lCD
drawdashline lCE
intersec P lBF lCE
intersec Q lAF lCD
intersec R lAE lBD
cmark_lt P
cmark_lt Q
cmark_lt R
drawdashline P Q
point A2 10 120
point B2 50 180
onsegment C2 A2 B2
%online C2 A2 B2
cmark_lt A2
cmark_lt B2
cmark_lt C2
drawline A2 B2
point D2 60 115
point E2 100 175
onsegment F2 D2 E2
%online F2 D2 E2
cmark_lt D2
cmark_lt E2
cmark_lt F2
drawline D2 E2
line lAE2 A2 E2
line lAF2 A2 F2
line lBD2 B2 D2
line lBF2 B2 F2
line lCD2 C2 D2
line lCE2 C2 E2
drawdashline lAE2
drawdashline lAF2
drawdashline lBD2
drawdashline lBF2
drawdashline lCD2
drawdashline lCE2
intersec P2 lBF2 lCE2
intersec Q2 lAF2 lCD2
intersec R2 lAE2 lBD2
cmark_lt P2
cmark_lt Q2
cmark_lt R2
drawdashline P2 Q2
%prove { collinear P Q R }
%prove { collinear P2 Q2 R2 }
```

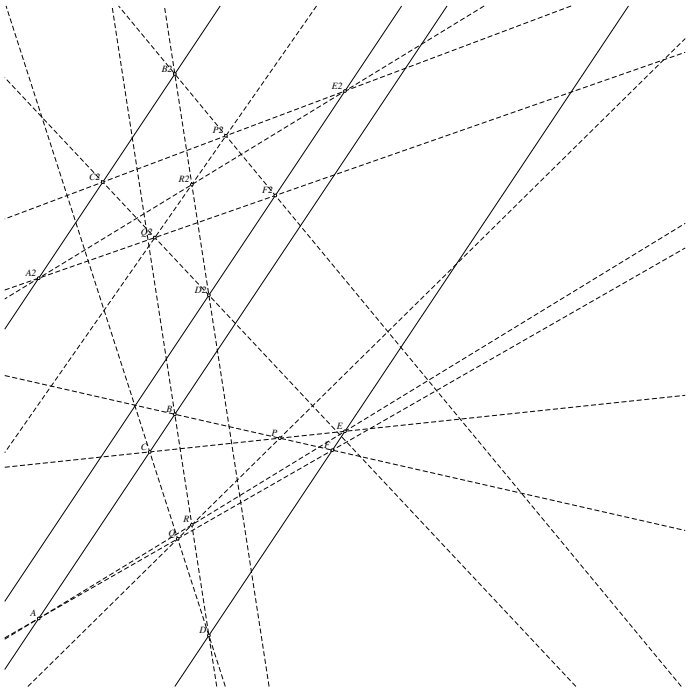

FIGURE 6 – pappus2.eps

pappus3.gcl

```
dim 200 200
point A 10 20
point B 50 80
onsegment C A B
%online C A B
cmark_lt A
cmark_lt B
cmark_lt C
drawline A B
point D 60 15
point E 100 75
onsegment F D E
%online F D E
cmark_lt D
cmark_lt E
cmark_lt F
drawline D E
line lAE A E
line lAF A F
line lBD B D
line lBF B F
line lCD C D
line lCE C E
intersec P1 lBF lCE
intersec Q1 lAF lCD
intersec R1 lAE lBD
cmark_lt P1
cmark_lt Q1
cmark_lt R1
drawdashline P1 Q1
point A2 10 120
point B2 50 180
onsegment C2 A2 B2
%online C2 A2 B2
cmark_lt A2
cmark_lt B2
cmark_lt C2
drawline A2 B2
point D2 60 115
point E2 100 175
onsegment F2 D2 E2
%online F2 D2 E2
cmark_lt D2
cmark_lt E2
cmark_lt F2
drawline D2 E2
line lAE2 A2 E2
line lAF2 A2 F2
line lBD2 B2 D2
line lBF2 B2 F2
line lCD2 C2 D2
line lCE2 C2 E2
intersec P2 lBF2 lCE2
intersec Q2 lAF2 lCD2
intersec R2 lAE2 lBD2
cmark_lt P2
cmark_lt Q2
cmark_lt R2
drawdashline P2 Q2
line lAE3 P1 Q2
line lAF3 P1 R2
line lBD3 Q1 P2
line lBF3 Q1 R2
line lCD3 R1 P2
line lCE3 R1 Q2
intersec P3 lBF3 lCE3
intersec Q3 lAF3 lCD3
intersec R3 lAE3 lBD3
cmark_lt P3
cmark_lt Q3
cmark_lt R3
drawline P3 Q3
%prove { collinear P3 Q3 R3 }
```

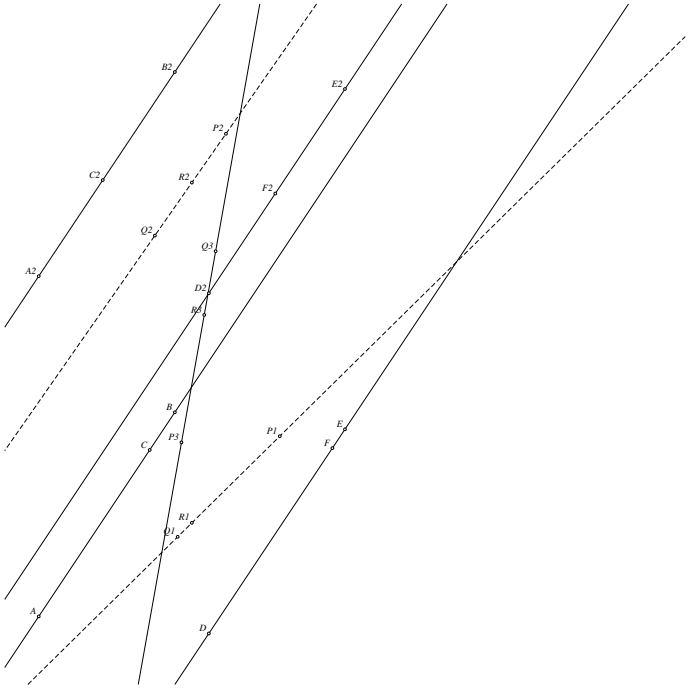

FIGURE 8 – pappus3.eps

pascal1.gcl

```
dim 80 80
ang_picture 2.5 2.5 80 80
ang_origin 20.0 35.0
%ang_drawsystem

ang_conic h 1 -1 2 -1 -0 -1
ang_conicprecision 300
ang_drawconic h

ang_point A1 0.5 0
ang_point A2 1 1
line lA A1 A2
ang_intersec2 P1 P2 h lA
cmark_lt P1
cmark_lt P2

ang_point B1 1.5 0
ang_point B2 2 1
line lB B1 B2
ang_intersec2 Q1 Q2 h lB
cmark_lt Q1
cmark_lt Q2

ang_point C1 3.0 0
ang_point C2 3.1 1
line lC C1 C2
ang_intersec2 R1 R2 h lC
cmark_lt R1
cmark_lt R2

line l1 R1 Q2
line l2 R2 Q1
line l3 P1 Q2
line l4 P2 Q1
line l5 P1 R2
line l6 P2 R1
drawdashline l1
drawdashline l2
drawdashline l3
drawdashline l4
drawdashline l5
drawdashline l6

intersec X l1 l2
intersec Y l3 l4
intersec Z l5 l6
cmark_lt X
cmark_lt Y
cmark_lt Z
drawline X Y
%prove { collinear X Y Z }
```

FIGURE 9 – Listing pascal1

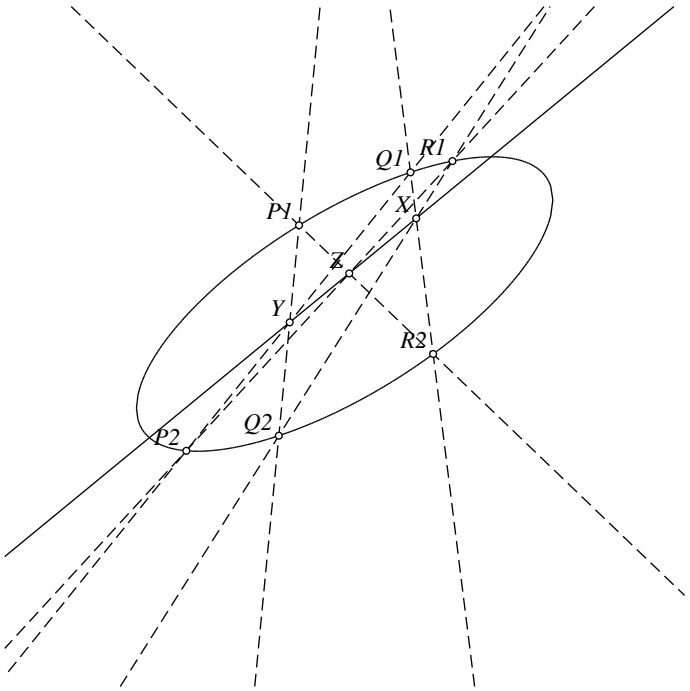

FIGURE 10 – pascal1.eps

pascal2.gcl

```
dim 80 80
ang_picture 2.5 2.5 80 80
ang_origin 20.0 35.0
%ang_drawsystem

ang_conic h 1 -1 -2 -1 -0 -1
ang_conicprecision 300
ang_drawconic h

ang_point A1 -1 0
ang_point A2 -1 1
line lA A1 A2
ang_intersec2 P1 P2 h lA
cmark_lt P1
cmark_lt P2

ang_point B1 2.1 0
ang_point B2 2.0 -1
line lB B1 B2
ang_intersec2 Q1 Q2 h lB
cmark_lt Q1
cmark_lt Q2

ang_point C1 3.0 0
ang_point C2 3.1 1
line lC C1 C2
ang_intersec2 R1 R2 h lC
cmark_lt R1
cmark_lt R2

line l1 R1 Q2
line l2 R2 Q1
line l3 P1 Q2
line l4 P2 Q1
line l5 P1 R2
line l6 P2 R1
drawdashline l1
drawdashline l2
drawdashline l3
drawdashline l4
drawdashline l5
drawdashline l6

intersec X l1 l2
intersec Y l3 l4
intersec Z l5 l6
cmark_lt X
cmark_lt Y
cmark_lt Z
drawline X Y
%prove { collinear X Y Z }
```

FIGURE 11 – Listing pascal2

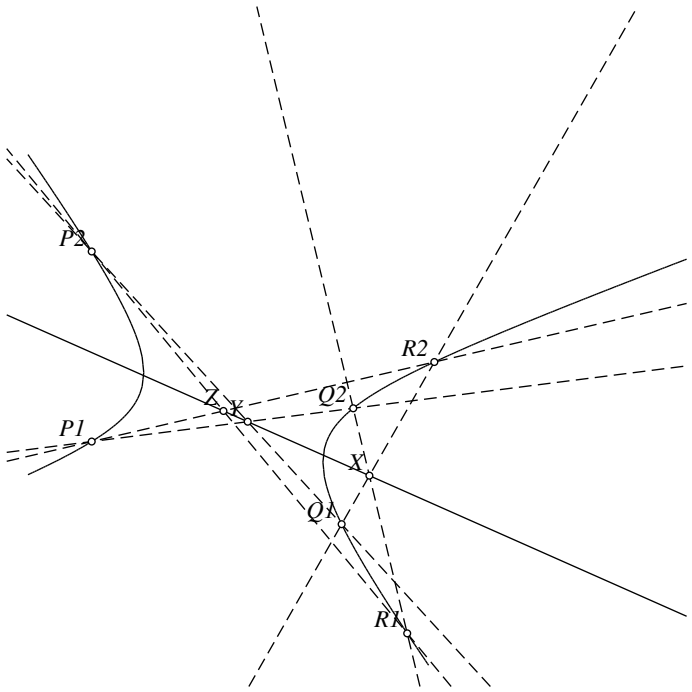

FIGURE 12 – pascal2.eps

pascal3.gcl

```
dim 80 80
ang_picture 2.5 2.5 80 80
ang_origin 20.0 35.0
%ang_drawsystem

ang_conic h 0 0 2 -1 -1 -1
ang_conicprecision 300
ang_drawconic h


ang_point A1 0.5 0
ang_point A2 1 1
line lA A1 A2
ang_intersec2 P1 P2 h lA
cmark_lt P1
cmark_lt P2


ang_point B1 1.5 0
ang_point B2 2 1
line lB B1 B2
ang_intersec2 Q1 Q2 h lB
cmark_lt Q1
cmark_lt Q2


ang_point C1 3.0 0
ang_point C2 3.1 1
line lC C1 C2
ang_intersec2 R1 R2 h lC
cmark_lt R1
cmark_lt R2


line l1 R1 Q2
line l2 R2 Q1
line l3 P1 Q2
line l4 P2 Q1
line l5 P1 R2
line l6 P2 R1
drawdashline l1
drawdashline l2
drawdashline l3
drawdashline l4
drawdashline l5
drawdashline l6


intersec X l1 l2
intersec Y l3 l4
intersec Z l5 l6
cmark_lt X
cmark_lt Y
cmark_lt Z
drawline X Y
%prove { collinear X Y Z }
```

FIGURE 13 – Listing pascal3

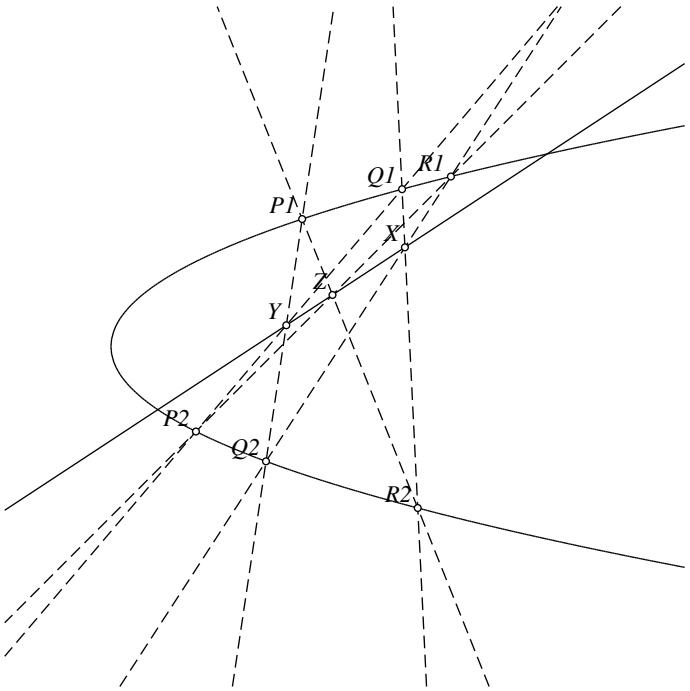

FIGURE 14 – pascal3.eps

pascal4.gcl

```
dim 80 80
ang_picture 2.5 2.5 80 80
ang_origin 20.0 35.0
ang_drawsystem

ang_conic h 1 -1 1 -0 0 -1
ang_conicprecision 10
ang_drawconic h

ang_point A1 0.5 0
ang_point A2 1 1
line lA A1 A2
ang_intersec2 P1 P2 h lA
cmark_lt P1
cmark_lt P2

ang_point B1 2.5 0
ang_point B2 2 1
line lB B1 B2
ang_intersec2 Q1 Q2 h lB
cmark_lt Q1
cmark_lt Q2

ang_point C1 6.5 0
ang_point C2 3.1 1
line lC C1 C2
ang_intersec2 R1 R2 h lC
cmark_lt R1
cmark_lt R2

line l1 R1 Q2
line l2 R2 Q1
line l3 P1 Q2
line l4 P2 Q1
line l5 P1 R2
line l6 P2 R1
drawdashline l1
drawdashline l2
drawdashline l3
drawdashline l4
drawdashline l5
drawdashline l6

intersec X l1 l2
intersec Y l3 l4
intersec Z l5 l6
cmark_lt X
cmark_lt Y
cmark_lt Z
drawline X Y
%prove { collinear X Y Z }
```

FIGURE 15 – Listing pascal4

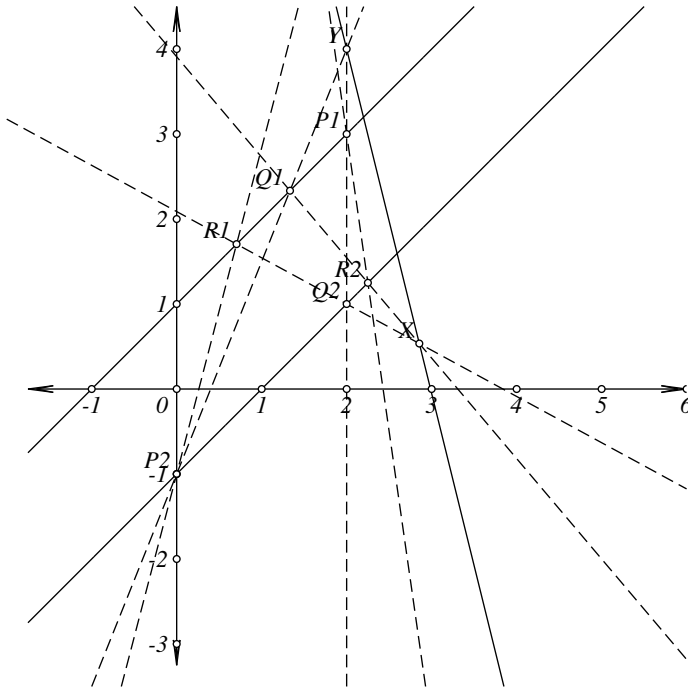

FIGURE 16 – pascal4.eps

pascal5.gcl

```
dim 80 80
ang_picture 2.5 2.5 80 80
ang_origin 20.0 80.0
%ang_drawsystem

ang_conic h 1 0 -1 0 -4 -16
ang_conicprecision 100
ang_drawconic h

ang_point A1 1 0
ang_point A2 1 1
line lA A1 A2
ang_intersec2 P1 P2 h lA
cmark_lt P1
cmark_lt P2

ang_point B1 2 0
ang_point B2 2 1
line lB B1 B2
ang_intersec2 Q1 Q2 h lB
cmark_lt Q1
cmark_lt Q2

ang_point C1 3.0 0
ang_point C2 3.1 1
line lC C1 C2
ang_intersec2 R1 R2 h lC
cmark_lt R1
cmark_lt R2

line l1 R1 Q2
line l2 R2 Q1
line l3 P1 Q2
line l4 P2 Q1
line l5 P1 R2
line l6 P2 R1
drawdashline l1
drawdashline l2
drawdashline l3
drawdashline l4
drawdashline l5
drawdashline l6

intersec X l1 l2
intersec Y l3 l4
intersec Z l5 l6
cmark_lt X
cmark_lt Y
cmark_lt Z
drawline X Y
%prove { collinear X Y Z }
```

FIGURE 17 – Listing pascal5

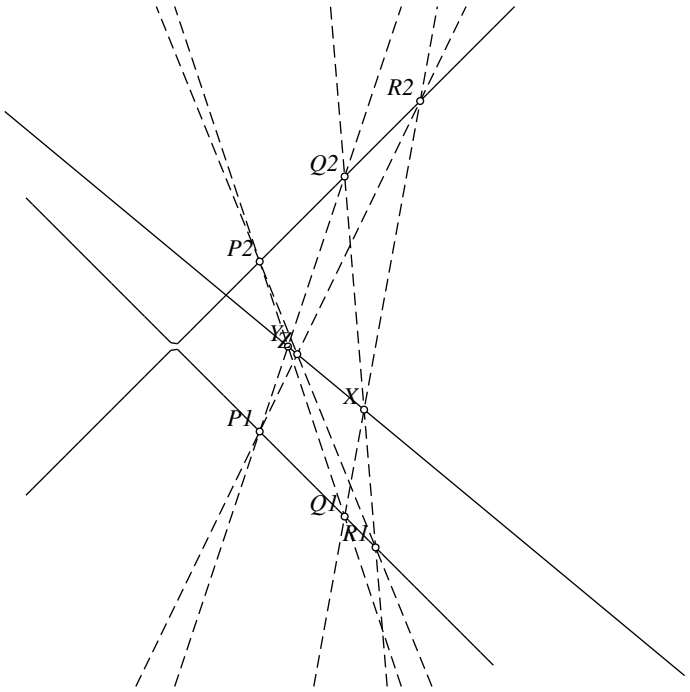

FIGURE 18 – pascal5.eps

1.1.2 Trisection d'un segment

Il est bien connu que la trissection d'un angle à l'aide de la règle et du compas est impossible. Par contre la trissection d'un segment est un problème de géométrie élémentaire.

Il existe plusieurs solutions à ce problème de construction. Nous laissons le lecteur expérimenter par lui-même le logiciel **GCLC** en décochant le symbole `%` de la dernière ligne des listings pris en compte et en lançant une des trois options `-a`, `-w` et `-g` avec les options par défaut.

1. Méthode 1 (Listing 19)
2. Méthode 2 (Listing 21)
3. Méthode 3 (Listing 23)
4. Méthode 4 (Listing 25)
5. Méthode 5 (Listing 27)

Résultats : (✓= proved)

Construction	option `-a`	option `-w`	option `-g`
	Méthode des aires	Méthode "Wu"	Méthodes des bases de Groebner
Méthode 1	out of scope	✓	✓
Méthode 2	✓	not proved	not proved
Méthode 3	out of scope	not proved	not proved
Méthode 4	not proved timeout (default 10 sec)	✓	✓
Méthode 5	out of scope	out of scope	out of scope

En conclusion, actuellement, les *méthodes 1, 2 et 4* sont validées par l'assistant de preuve de **GCLC**, puisqu'au moins une des trois méthodes (méthodes aires, méthode "Wu", méthodes des bases de Groebner) effectue une vérification valide.

Il est intéressant de lire les *non-degeneracy conditions* (ngd-conditions) signalée dans le fichier ".tex" produit par **GCLC** à la suite de la vérification avec l'option `-a`, que nous avons repris en Annexes ("GCLC Prover Output for conjecture "trisect2proof " - Area method used" - 7.4) et que nous reprenons ci-dessous (7.4)

— $S_{CAB} \neq S_{EAB}$ i.e., lines CE and AB are not parallel (construction based assumption)
— $S_{CAEB} \neq 0$ (cancellation assumption)
— $CB \neq 0$ (cancellation assumption)
— $S_{CAB} \neq 0$ i.e., points C, A and B are not collinear (cancellation assumption)

Que retenir de l'analyse de ces conditions ? Cela confirme notre *intuition* : il faut choisir le point C n'appartenant pas sur la ligne AB.

Cela signifie-t-il que nécessairement les autres méthodes de construction sont erronées ? Pas du tout ! Cela signifie soit que les conditions d'utilisation ne sont pas remplies (cf. mode d'emploi), soit les paramètres de recherches par défaut ne sont pas les bons, soit **GCLC** n'est pas encore en état de valider ces constructions [12].

A titre d'exemple, voici une preuve que la Méthode 5 (Listing 27) est une trisection d'un segment AB

Démonstration. Sur base du diagramme 28 créé à partir du Listing 27, on a la démonstration suivante : Soit $(0, 0)$ les coordonnées du point A (resp. $(l, 0)$ celles du point B, avec $0 < l$). Les coordonnées des points C et D sont $(\frac{l}{2}, 0)$ et $(\frac{3l}{2}, 0)$. Les coordonnées (x_p, y_p) du point P vérifient

$$\begin{cases} x_p^2 + y_p^2 = l^2 \\ (x_p - \dfrac{3l}{2})^2 + y_p^2 = (\dfrac{3l}{2})^2 \end{cases} \tag{1}$$

Ainsi, x_p vérifie l'équation suivante :

$$(x_p - \frac{3l}{2})^2 - x_p^2 = (\frac{5l^2}{4})$$

[12] Ce n'est pas un aveux d'échec : le développement de ces outils peut se poursuivre.

qui admet la solution $x_p = \frac{l}{3}$. Les coordonnées du point Q sont alors $(\frac{l}{3}, 0)$. □

CHALLENGE 4 : Proposer des paramètres de recherches ou une modification de **GCLC** permettant de prouver la méthode 3, 5 (Listing 23,27).

Une question naturelle se pose : pourquoi ne peut-on pas montrer qu'un point est entre deux autres ? Autrement dit, pourquoi pas un énoncé de la sorte : "proof between A B C " ? Il semble évident que `midpoint C A B` implique `same_length A C C B` et `between C A B` réciproquement ? Une réponse peut-être trouvée (*A New Axiom System for the Area Method*) in [16] :

> The axiom system used by Chou, Gao and Zhang [...] is a semi-analytic axiom system with (only) points as primitive objects (lines are not primitive objects as in Hilbert's axiom system). The axiom system contains the axioms of field, so the system uses the concept of numbers, but it is still coordinate free. The field is not assumed to be ordered, hence the axiom system has the property of representing an unordered geometry. This means that, for instance, one cannot express the concept of a point being between two points (unlike in Hilbert's system).

[13]

`trisect1.gcl`

```
dim 100 80
point A 10 10
point B 70 10
cmark_lt A
cmark_rt B
line lAB A B
drawsegment A B
point C 15 20
cmark_lt C
line lAC A C
drawdashline A C
circle cCA C A
intersec2 D D2 cCA lAC
cmark_t D
circle cDC D C
intersec2 E E2 cDC lAC
cmark_t E
line lEB E B
drawdashline E B
parallel lD D lEB
drawdashline lD
intersec F lD lAB
cmark_rt F
parallel lC C lEB
drawdashline lC
intersec G lC lAB
cmark_rt G
prove { same_length F B G F }
```

FIGURE 19 – Listing trisect1

[13] Trad. Le système axiomatique utilisé par Chou, Gao et Zhang est un système axiomatique semi-analytique avec (seulement) des points comme objets primitifs (les lignes ne sont pas des objets primitifs comme dans le système de Hilbert). Le système d'axiomes contient les axiomes des Corps, donc le système utilise le concept de nombres, mais il est toujours sans coordonnées. Le Corps n'est pas supposé être nécessairement ordonné, le système d'axiomes a la propriété de représenter une géométrie non ordonnée. Cela signifie que, par exemple, on ne peut pas exprimer le concept d'un point situé entre deux points (contrairement au système de Hilbert).

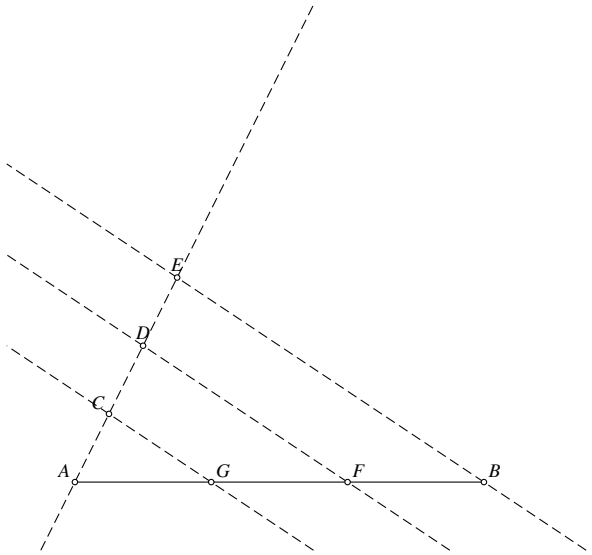

FIGURE 20 – trisect1.eps

trisect2.gcl

```
point A 10 10
point B 80 10
cmark_lt A
cmark_rt B
line lAB A B
drawsegment A B
point C 10 55
cmark_lt C
drawdashsegment C B
midpoint D C B
cmark_rt D
drawdashsegment A D
midpoint E A D
cmark_lt E
line lCE C E
drawline C E
intersec F lCE lAB
cmark_rt F
midpoint G F B
cmark_rt G
prove { same_length A F F G }
```

FIGURE 21 – Listing trisect2

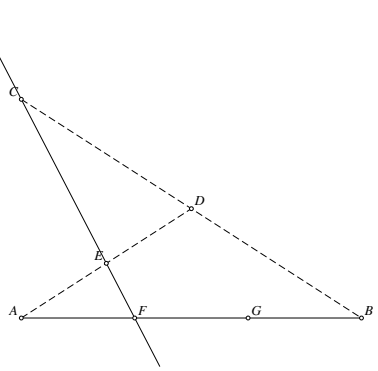

FIGURE 22 – trisect2.eps

trisect3.gcl

```
point A 10  40
point B 80 40
cmark_lt A
cmark_rt B
line lAB A B
drawsegment A B
point C 25 50
cmark_lt C
line lC  A C
drawdashline A C
parallel lB B lC
drawdashline lB
midpoint D A B
cmark_rt D
line lCD C D
drawdashline lCD
intersec E lB lCD
line lBE B E
cmark_lt E
circle cCA C A
intersec2 F F2 cCA lC
cmark_lt F
circle cEB E B
intersec2 G2 G lBE cEB
cmark_lt G
line lEF E F
drawdashline lEF
intersec H lEF lAB
cmark_rt H
line lCG C G
drawdashline lCG
intersec J lCG lAB
mark_lt J
%prove { same_length H B J H }
```

FIGURE 23 – Listing trisect3

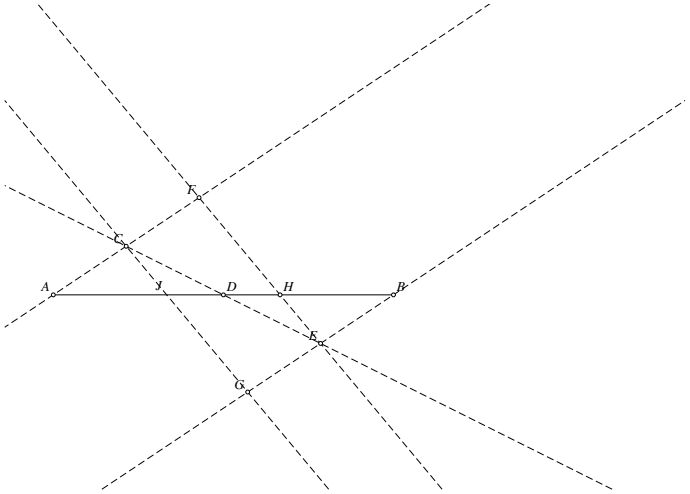

FIGURE 24 – trisect3.eps

trisect4.gcl

```
point A 10 40
point B 80 40
cmark_lt A
cmark_lt B
line lAB A B
drawsegment A B
point C 30 70
cmark_lt C
line lAC A C
drawdashline lAC
parallel lB B lAC
drawdashline lB
midpoint D A B
cmark_rt D
line lCD C D
drawdashline lCD
intersec E lCD lB
cmark_lt E
midpoint F A C
cmark_lt F
midpoint G B E
cmark_rt G
line lCG C G
drawline lCG
intersec H lCG lAB
cmark_rt H
line lEF E F
drawline lEF
intersec I lEF lAB
cmark_rt I
%prove { same_length I A I H }
%prove { same_length I H H B }
```

FIGURE 25 – Listing trisect4

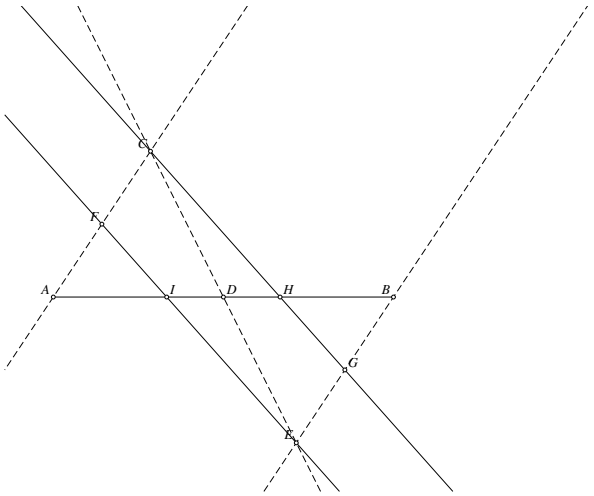

FIGURE 26 – trisect4.eps

trisect5.gcl

```
point A 10 10
point B 40 10
cmark_lt A
cmark_lt B
line lAB A B
drawsegment A B
drawdashline lAB
midpoint C A B
cmark_lt C
circle cBC B C
drawdashcircle cBC
intersec2 D D2 lAB cBC
cmark_lt D
circle cDA D A
drawdashcircle cDA
circle cAB A B
drawdashcircle cAB
intersec2 P2 P cAB cDA
cmark_t P
foot Q P lAB
cmark_lt Q
drawdashline P Q
midpoint R Q B
cmark_lt R
%prove { same_length A Q R B }
```

FIGURE 27 – Listing trisect5

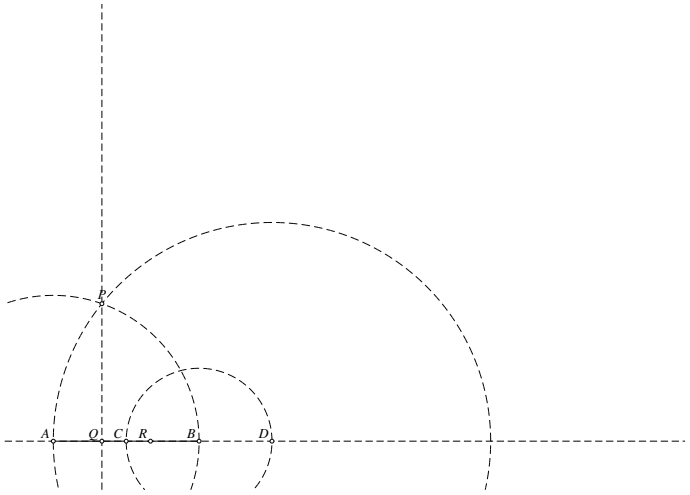

FIGURE 28 – trisect5.eps

2 Le coin des bibliothèques

Dans cette section, nous choisissons de vous présenter un extrait d'une bibliothèque *open source*. Le choix du système est à notre discrétion mais il est souvent également possible de trouver des développements semblables dans un autre langage ou avec le support d'une autre logique. Nous vous invitons à comparer et à nous transmettre vos observations et commentaires, que nous publierons, le cas échéant, dans un prochain numéro.

2.1 Bienvenue dans la Matrix...

Bon blague à part, il ne s'agit pas de présenter dans cette section le film bien connu du même nom mais une très brève présentation de l'utilisation des matrices avec **Isabelle**/**Hol**. Plus particulièrement, il s'agit de vérifier que

$$\begin{pmatrix} 1 & 2 & 1 \\ 1 & -1 & 3 \\ 1 & 0 & 1 \end{pmatrix} . \begin{pmatrix} 0 & -1 & -1 \\ 3 & 1 & 2 \\ -1 & 2 & 0 \end{pmatrix} = \begin{pmatrix} 5 & 3 & 3 \\ -6 & 4 & -3 \\ -1 & 1 & -1 \end{pmatrix}$$

Pour être complet, voici le résultat dans **maxima** :

```
$ maxima

Maxima 5.44.0 http://maxima.sourceforge.net
using Lisp GNU Common Lisp (GCL) GCL 2.6.12
Distributed under the GNU Public License. See the file COPYING.
Dedicated to the memory of William Schelter.
The function bug_report() provides bug reporting information.
(%i1) A:matrix([1,2,1],[1,-1,3],[1,0,1]);
                                [ 1   2   1 ]
                                [           ]
(%o1)                           [ 1  - 1  3 ]
                                [           ]
                                [ 1   0   1 ]
(%i2) B:matrix([0,-1,-1],[3,1,2],[-1,2,0]);
                               [  0   - 1  - 1 ]
                               [               ]
(%o2)                          [  3    1    2  ]
                               [               ]
                               [ - 1   2    0  ]
(%i3) A.B;
                                [  5   3   3  ]
                                [             ]
(%o3)                           [ - 6  4  - 3 ]
                                [             ]
                                [ - 1  1  - 1 ]
```

Il peut sembler que l'usage du calcul matriciel est fréquent dans les théories incluses dans la bibliothèque ouverte comme l'**A.F.P.**[14] d'**Isabelle** ou même dans la bibliothèque intégrée[15] à **Isabelle**. Il n'en est rien.

Un assistant de preuve n'est pas un logiciel de calcul formel comme, par exemple, **Maxima**. Dans l'état actuel des assistants de preuve, ceux-ci ne savent pas prévoir un résultat : ils ne peuvent pas calculer la somme ou le produit de deux matrices. Par contre, la vérification d'un résultat est possible.

Cette vérification est "parfaite" mathématiquement mais elle n'est pas toujours possible dans tous les cas et parfois elle n'est ni évidente, ni directe.

Nous n'allons pas nous attarder à ces cas, mais nous ne ferons pas non plus l'impasse sur ces

[14] Archive Formal Proofs :`https://www.isa-afp.org/`
[15] Par exemple : `~~/src/HOL/Analysis`

difficultés. Il vaut peut-être mieux connaître les limites actuelles d'un assistant de preuve pour mieux cerner son utilisation.

Dans le cas de l'utilisation d'**Isabelle/HOL**, voici une piste d'utilisation en deux étapes :

1. exprimer des énoncés matriciels corrects,
2. (tenter de) prouver ces énoncés.

En effet, il est important de pouvoir écrire des énoncés corrects.

Commençons par un simple vecteur de $\mathbb{R}^2$:

$$\begin{pmatrix} 1 \\ 2 \end{pmatrix}$$

peut être traduit par `vector [1,2] :: real^2`, avec `vector` définit dans le fichier `Catersian_Space.thy` du répertoire `src/HOL/Analysis` .

Nous pouvons aussi avoir un vecteur contenant des variables :

$$\begin{pmatrix} \frac{a^2}{a^2+b^2} \\ \frac{b^2}{a^2+b^2} \end{pmatrix}$$

traduit par `vector [a^2/(a^2 + b^2),b^2/(a^2+b^2)]`.

Pour la matrice carrée nulle, on peut écrire `mat 0`, pour la matrice identité : `mat 1`. La matrice

$$\begin{pmatrix} r & 0 & 0 \\ 0 & r & 0 \\ 0 & 0 & r \end{pmatrix}$$

sera représentée par `mat r` avec parfois une indication sur la dimension de cette matrice carrée.

```
theory TEST1
  imports "HOL-Analysis.Cartesian_Space"
begin

lemma T1:
 fixes M :: "real^3^3" and r :: real
 assumes "M = mat r"
 shows "M = M" by blast

end
```

est valide. Par contre

```
theory TEST1
  imports "HOL-Analysis.Cartesian_Space"
begin

lemma T1:
 fixes M :: "real^3^2" and r :: real
 assumes "M = mat r"
 shows "M = M" by blast

end
```

n'est plus valide : l'assistant de preuve a constaté que la matrice n'est pas carrée.

L'exemple précédent montre comment utiliser une matrice *localement* à une proposition. Si nous désirons que la matrice ait une portée plus importante, nous pouvons l'introduire dans une définition comme ci-dessous :

```
definition M2a :: "real^2^2" where
  "M2a <equiv> vector [
  vector [1, 2],
  vector [2, 3]]"
```

ou par exemple,

```
definition M :: "real^3^3" where
  "M <equiv> vector [
  vector [1, 0, 0],
  vector [0, 1, 0],
  vector [0, 0, -1]]"
```

Une autre façon de définir une matrice est d'utiliser le symbole χ (à ne pas confondre avec le symbole λ). Un exemple : `definition K :: "real^3^3" where "K ≡ χ i j. (if i = j then 1 else 0)"` représente la matrice

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

on a d'ailleurs la preuve suivante :

```
lemma T3:
  shows "K = mat 1"
  by (simp add: K_def mat_def)
```

De la même façon,
`definition K2 :: "real=>real^3^3" where "(K2 r) ≡ χ i j. (if i = j then r else 0)"`
représente la matrice

$$\begin{pmatrix} r & 0 & 0 \\ 0 & r & 0 \\ 0 & 0 & r \end{pmatrix}$$

Pour s'en convaincre, on a la preuve suivante :

```
lemma T3b:
  shows "(K2 r) = mat r"
  by (simp add: K2_def mat_def)
```

Nous voyons ici, que l'assistant de preuve a immédiatemment inféré que r est un réel et que `mat r` est une matrice réelle avec 3 lignes et 3 colonnes.

Par contre il existe également une autre façon de définir une matrice, qui figure dans une *theory* disponible dans l'**Archive Formal Proof** : *Jordan_ Normal_ Form/Matrix.thy*. Par exemple, il est possible de traduire la matrice suivante :

$$\begin{pmatrix} 2 & 4 & 1 \\ -1 & 0 & 1 \\ 1 & 3 & 2 \end{pmatrix}$$

par `abbreviation J :: "complex Matrix.mat" where "J ≡ mat_of_cols_list 3 [[2, 4, 1],[-1,0,1],[1,3,2]]"`

La matrice unité est définie, dans le fichier, de cette façon :
`definition one_mat :: "nat ⇒ 'a :: {zero,one} mat" ("1 ⇓m ") where "1 ⇓m n ≡ mat n n ( λ (i,j). if i = j then 1 else 0)"`

Par exemple, on peut avoir :

```
theory TEST2
  imports Jordan_Normal_Form.Matrix

abbreviation M1 :: "complex Matrix.mat" where
"M1 <EQUIV> mat_of_cols_list 3  [[2,4,1],
                           [-1,0,1],
                           [1,3,2]]"
lemma M1R:
  shows "M1 * (one_mat 3) = (one_mat 3) * M1"
proof -
  let ?X = "M1 * (one_mat 3)"
  let ?Y = "(one_mat 3) * M1"
```

```
  {
    fix i j
    assume a0:"i < dim_row ?X" and a1:"j < dim_col ?X"
    have "?X $$ (i,j) = ?Y $$ (i,j)"
      by (simp add: mat_of_cols_list_def)
  }
  moreover
  have "dim_row ?X = dim_row ?Y"
    by (simp add: mat_of_cols_list_def)
  moreover
  have "dim_col ?X = dim_col ?Y"
    by (simp add: mat_of_cols_list_def)
  ultimately
  show ?thesis
    by (metis eq_matI)
qed
```

On note ici que les indices des lignes et des colonnes varient entrent 0 et 2.

Par contre, nous allons déchanter si nous voulons, par exemple, montrer que les deux matrices ci-dessous commutent :

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

et

$$\begin{pmatrix} a & 0 & 0 & c \\ 0 & a & 0 & 0 \\ 0 & d & e & 0 \\ 0 & 0 & 0 & e \end{pmatrix}$$

Cette commutation peut être facilement montrée avec `maxima` :

```
$ maxima

Maxima 5.44.0 http://maxima.sourceforge.net
using Lisp GNU Common Lisp (GCL) GCL 2.6.12
Distributed under the GNU Public License. See the file COPYING.
Dedicated to the memory of William Schelter.
The function bug_report() provides bug reporting information.
(%i1) A:matrix([0,1,0,0],[0,0,0,0],[0,0,0,1],[0,0,0,0]);
                                [ 0  1  0  0 ]
                                [            ]
                                [ 0  0  0  0 ]
(%o1)                           [            ]
                                [ 0  0  0  1 ]
                                [            ]
                                [ 0  0  0  0 ]
(%i2) B:matrix([a,0,0,c],[0,a,0,0],[0,d,e,0],[0,0,0,e]);
                                [ a  0  0  c ]
                                [            ]
                                [ 0  a  0  0 ]
(%o2)                           [            ]
                                [ 0  d  e  0 ]
                                [            ]
                                [ 0  0  0  e ]
(%i3) A.B-B.A;
                                [ 0  0  0  0 ]
                                [            ]
                                [ 0  0  0  0 ]
```

```
(%o3)                                [           ]
                                     [ 0  0  0  0 ]
                                     [           ]
                                     [ 0  0  0  0 ]
(%i4)
```

par contre le preuve avec **Isabelle/Hol** n'est pas encore possible, de façon simple. En effet, un code assez simple[16] :

```
theory TEST2
  imports Jordan_Normal_Form.Matrix
begin

abbreviation M1 :: "complex Matrix.mat" where
"M1 <EQUIV> mat_of_cols_list 4  [[0,1,0,0],
                          [0,0,0,0],
                          [0,0,0,1],
[0,0,0,0]]"
abbreviation M2 :: "complex'=>'complex'=>'complex'=>'complex'=>'complex Matrix.mat" where
"M2 a c d e <EQUIV> mat_of_cols_list 4  [[a,0,0,c],
                                         [0,a,0,0],
                                         [0,d,e,0],
                                         [0,0,0,e]]"

lemma M2R:
  fixes a c d e :: complex
  shows "M1 * (M2 a c d e) = (M2 a c d e) * M1" sorry
```

n'admet pas un preuve dans le même schéma que dans les preuves précédentes.

CHALLENGE 5 : Proposer une preuve à ce lemme.

Comme nous avons pu le voir ci-dessus, dans l'état actuel d'**Isabelle/HOL**, il n'est vraiment pas toujours facile de prouver les énoncés matriciels.

Ainsi un énoncé aussi trivial que :

$$\begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} = r \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

traduit par

```
lemma T2:
fixes M :: "real^2^2" and r :: real
assumes "M = mat r"
shows "M = r *_R mat 1" sledgehammer
```

n'admet pas de preuve en moins d'une minute dans notre configuration PC, alors qu'un énoncé plus général comme `lemma T3: "transpose (mat n) = mat n" by simp` est directement prouvé.

Paradoxalement, les énoncés suivant peuvent être prouvés :

```
definition M :: "real^3^3" where
  "M <equiv> vector [
  vector [1, 0,0],
  vector [0, 1,0],
   vector[0,0,-1]]"


lemma R5:
  shows "transpose M = M"
  unfolding transpose_def and M_def
  by (simp add: vec_eq_iff forall_3)
```

[16] Dans cette situation il est possible de remplacer `definition` par `abbreviation`

```
lemma R6: "M ** M = mat 1"
  unfolding M_def and matrix_matrix_mult_def and mat_def and vector_def
  by (simp add: sum_3 vec_eq_iff forall_3)
```

La périmètre d'utilisation de cette réprésentation me semble donc très limité. Après quelques expérimentations, je n'ai pas pu effectué la somme des 2 matrices de nombres quelconques.

Par contre, il existe une autre méthode pour la réprésentation matricielle. Celle-ci peut-être trouvée dans le fichier `SQ_MTX.thy` de la théorie `Matrices_for_ODEs`.

Mais revenons à notre exemple initial. Dans la nouvelle représentation, la solution est immédiate :

Le fichier `VERFI1.thy` est une solution :

```
theory VERFI1

imports Matrices_for_ODEs.SQ_MTX

begin

lemma test1:
  shows
"mtx
  ([1,  2, 1] #
   [1, -1, 3] #
   [1,  0, 1] # []) *
mtx
  ([ 0, -1, -1] #
   [ 3,  1,  2] #
   [-1,  2,  0] # []) = (
mtx
  ([ 5, 3,  3] #
   [-6, 4, -3] #
   [-1, 1, -1]#[]):: 3 sq_mtx)"
  unfolding sq_mtx_times_eq UNIV_3
  by (simp add: sq_mtx_eq_iff)
```

La ligne de vérification[17] est

```
  unfolding sq_mtx_times_eq UNIV_3
  by (simp add: sq_mtx_eq_iff)
```

Soyons hardi, trouvons une vérification de l'énoncé suivant, où a, b et c sont des nombres réels quelconques :

$$\begin{pmatrix} 1 & 2 & 1 \\ 1 & -1 & 3 \\ 1 & 0 & 1 \end{pmatrix}.\begin{pmatrix} 0 & -1 & a \\ 3 & 1 & b \\ -1 & 2 & c \end{pmatrix} = \begin{pmatrix} 5 & 3 & a+2b+c \\ -6 & 4 & a-b+3c \\ -1 & 1 & a+c \end{pmatrix}$$

Maxima donne le même résultat :

```
$ maxima

Maxima 5.44.0 http://maxima.sourceforge.net
using Lisp GNU Common Lisp (GCL) GCL 2.6.12
Distributed under the GNU Public License. See the file COPYING.
Dedicated to the memory of William Schelter.
The function bug_report() provides bug reporting information.
(%i1) A:matrix([1,2,1],[1,-1,3],[1,0,1]);
                                [ 1   2   1 ]
```

[17] Dans un premier temps, nous ne donnerons pas d'explication sur cette vérification. Cela peut sembler incompréhensible. Il est à retenir que `sq_mtx_times`, `UNIV_3` et `sq_mtx_eq_iff` sont les justifications utiles. Nous reviendrons ultérieurement sur ces notations et leur signification.

```
                                  [          ]
(%o1)                             [ 1  - 1  3 ]
                                  [          ]
                                  [ 1   0   1 ]
(%i2) B:matrix([0,-1,a],[3,1,b],[-1,2,c]);
                                  [  0   - 1  a ]
                                  [             ]
(%o2)                             [  3    1   b ]
                                  [             ]
                                  [ - 1   2   c ]
(%i3) A.B;
                              [  5   3  c + 2 b + a ]
                              [                     ]
(%o3)                         [ - 6  4  3 c - b + a ]
                              [                     ]
                              [ - 1  1     c + a    ]
(%i4)
```

Une solution possible (en l'ajoutant à la fin du fichier `VERFI1.thy`)

```
lemma test2:
  shows
"mtx
  ([1,  2, 1] #
   [1, -1, 3] #
   [1,  0, 1] # []) *
mtx
  ([ 0, -1, a] #
   [ 3,  1, b] #
   [-1,  2, c] # []) = (
mtx
  ([ 5, 3,  a + 2 * b +     c] #
   [-6, 4,  a -     b + 3 * c] #
   [-1, 1,  a         +     c]#[]):: 3 sq_mtx)"
  unfolding sq_mtx_times_eq unfolding UNIV_3
  by (simp add: sq_mtx_eq_iff)
```

Nous pouvons constater que la justification est identique :

```
  unfolding sq_mtx_times_eq unfolding UNIV_3
  by (simp add: sq_mtx_eq_iff)
```

Finalement, peut-on *tout* vérifier ? Non.

Voici un exemple qui montre que nous pouvons faire l'impasse sur certaines justifications qui sont déjà nécessaires dans des calculs algébriques simples.

La simple vérification de l'égalité (avec $1 - ab \neq 0$) suivante :

$$b.\frac{-a}{1-ab} + 1.\frac{1}{1-ab} = \frac{1-ab}{1-ab}$$

nécessite, en utilisant sledgehammer, des *vérifications consommatrices de temps* de la forme [18] :

```
by (smt (verit, ccfv_threshold) add.commute diff_divide_distrib
   divide_divide_eq_left divide_minus1 frac_diff_eq1 minus_divide_left
   mult.commute mult_1 times_divide_eq_right)
```

En tenant compte de cette égalité, nous pouvons montrer l'égalité suivante :

$$\begin{pmatrix} 1 & a \\ b & 1 \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{1-ab} & \frac{-a}{1-ab} \\ \frac{-b}{1-ab} & \frac{1}{1-ab} \end{pmatrix} = \begin{pmatrix} \frac{1-ab}{1-ab} & 0 \\ 0 & \frac{1-ab}{1-ab} \end{pmatrix}$$

Ceci met clairement en évidence que la solution simple présentée dans les deux exemples précédents ne peut être mise en oeuvre ici. En effet, même si la méthode utilise la représentation matricielle précédente, la méthode pour prouver l'égalité nécessite beaucoup plus d'étapes manuelles. Celles-ci doivent être adaptées à l'énoncé.

```
lemma test3:
shows
  "mtx
  ([ 1, a] #
   [ b, 1] # []) *
mtx
  ([ 1/(1-a*b) , -a/(1-a*b)] #
   [ -b/(1-a*b),  1/(1-a*b)] # []) = (
mtx
  ([ (1-a*b)/(1-a*b), 0              ] #
   [ 0              , (1-a*b)/(1-a*b)] #[]):: 2 sq_mtx)"
proof -
  have M1: "a * b = b * a" by force
  have "mtx
  ([1, a] #
   [ b,1] # []) *
mtx
  ([1/(1-a*b),-a/(1-a*b)] #
   [ -b/(1-a*b),1/(1-a*b)] # []) = (
mtx([1 * (1/(1-a*b)) + a * (-b/(1-a*b)),1 * (-a/(1-a*b))+a*(1/(1-a*b))] #
    [b * (1/(1-a*b)) + 1 * (-b/(1-a*b)),b * (-a/(1-a*b))+1*(1/(1-a*b))] #[])::2 sq_mtx)"
    unfolding sq_mtx_times_eq unfolding UNIV_2
    by (simp add: sq_mtx_eq_iff)
  also have "... = (mtx([(1/(1-a*b)) - a * b/(1-a*b),(-a+a)/(1-a*b)] #
    [(b-b) * (1/(1-a*b)),1/(1-a*b)  -(b * a)/(1-a*b)] #[])::2 sq_mtx)"
    by force
  also have "... = (mtx([(1/(1-a*b)) - a * b/(1-a*b),(-a+a)/(1-a*b)] #
    [(b-b) * (1/(1-a*b)),1/(1-a*b)  -(a * b)/(1-a*b)] #[])::2 sq_mtx)"
    using M1 by presburger
  also have "... = (mtx([(1/(1-a*b)) - a * b/(1-a*b),(-a+a)/(1-a*b)] #
    [(b-b) * (1/(1-a*b)),(1-a*b)/(1-a*b)] #[])::2 sq_mtx)"
    by (metis diff_divide_distrib)
```

[18] Cette solution n'est pas unique : **Sledgehammer** peut aussi proposer :

```
by (metis (no_types, opaque_lifting) diff_divide_distrib mult.commute mult_1
   mult_minus_right times_divide_eq_right uminus_add_conv_diff)
```

ou

```
by (metis (no_types, opaque_lifting) diff_divide_distrib mult.commute
   mult_cancel_right2 mult_minus_right times_divide_eq_right uminus_add_conv_diff)
```

ou

```
by (smt (verit, ccfv_threshold) diff_divide_distrib mult.commute
   mult_minus_right times_divide_eq_left)
```

```
  also have "... = (mtx([((1-a*b)/(1-a*b)),(-a+a)/(1-a*b)] #
    [(b-b) * (1/(1-a*b)),(1-a*b)/(1-a*b)] #[])::2 sq_mtx)"
    by (metis diff_divide_distrib)
  also have "... = (mtx([((1-a*b)/(1-a*b)),0/(1-a*b)] #
    [0 * (1/(1-a*b)),(1-a*b)/(1-a*b)] #[])::2 sq_mtx)"
    by force
  also have "... = (mtx([((1-a*b)/(1-a*b)),0] #
    [0,(1-a*b)/(1-a*b)] #[])::2 sq_mtx)"
    by force
  thus ?thesis
    using calculation by presburger
qed

lemma test4:
  assumes "1 - a * b \<noteq> 0"
  shows
"mtx
  ([1, a] #
   [b, 1] # []) *
mtx
  ([  1/(1-a*b),-a/(1-a*b)] #
   [ -b/(1-a*b), 1/(1-a*b)] # []) = (
mtx
  ([1, 0] #
   [0,1] #[]):: 2 sq_mtx)"
  using test3 assms by force
```

Au final, certains énoncés sont rapidement vérifiés, d'autres moins. Si vous avez besoin de vérifier un énoncé "un peu plus complexe" comme le troisième exercice, vous devez prévoir plusieurs étapes. **Isabelle** ne peut pas (encore ?) effectué automatiquement tous les résultats proposés par **Maxima**.

Il est à noter que la théorie `imports Matrices_for_ODEs.SQ_MTX` de Jonathan Julian Huerta y Munive a été postée seulement en 2020[20] dans l'**Archive Formal Proofs**...

En conclusion : que tout cela nous vous empêche pas de vérifier une égalité ou une propriété matricielle. Certains énoncés peuvent être prouvés plus rapidement que d'autres alors que ces mêmes énoncés n'étaient pas encore accessibles à la démonstration (dans un temps raisonnable) il y a quelques années.

Si tout ceci vous paraît un peu "exagéré", alors *il faut qu'on en parle....*

2.2 Le théoreme de Fubini, version Mizar

Le théorème de Fubini est un théorème classique en analyse. Dans cette section, nous n'aborderons ni sa démonstration ni ses applications mais les éléments qui vont nous permettre de comprendre l'énoncé telle que prouvée par Noboru Endou dans [11].

Avant de présenter la forme qui apparaît dans la MML [19], un premier détour vers des énoncés communs sont présentés ci-dessous : celui de Wikipédia, une version de mon cours de Licence, une version plus *professionnelle*.

Voici la version Wikipédia[30] :

[19] `http://www.mizar.org` `http://www.mizar.org/version/current/html/`

Théorème de Fubini-Tonelli[1] — Soient $(X, \mathcal{A}, \mu)$ et $(Y, \mathcal{B}, \nu)$ deux espaces mesurés tels que les deux mesures soient σ-finies et soit $(X \times Y, \mathcal{A} \times \mathcal{B}, \mu \times \nu)$ l'espace mesurable produit muni de *la* mesure produit. Si

$$f : X \times Y \to [0, +\infty]$$

est une application $\mathcal{A} \times \mathcal{B}$-mesurable, alors les applications

$$x \mapsto \int_Y f(x,y)\, \mathrm{d}\nu(y) \quad \text{et} \quad y \mapsto \int_X f(x,y)\, \mathrm{d}\mu(x)$$

sont respectivement $\mathcal{A}$- et $\mathcal{B}$-mesurables et

$$\int_{X\times Y} f(x,y)\, \mathrm{d}(\mu \times \nu)(x,y) = \int_X \left[\int_Y f(x,y)\, \mathrm{d}\nu(y)\right] \mathrm{d}\mu(x) = \int_Y \left[\int_X f(x,y)\, \mathrm{d}\mu(x)\right] \mathrm{d}\nu(y).$$

FIGURE 29 – Théorème de Fubini (Version Wikipedia)

Le théorème de Fubini, Théorie de la Mesure, cours de Lic. Math[25] n'est pas tout-à-fait le même [20].

En effet, des conventions particulières doivent être rappelées :

Convention. Dans ce paragraphe,

a) X_1 et X_2 sont deux ensembles non vides et nous posons $X = X_1 \times X_2$,

b) $\mathcal{S}_1$ et $\mathcal{S}_2$ sont des semi-anneaux sur X_1 et X_2 respectivement, et nous posons $\mathcal{S} = \mathcal{S}_1 \times \mathcal{S}_2$.

Rappelons qu'alors $\mathcal{S}$ est un semi-anneau sur X.

FIGURE 30 – Semi-anneau

Les semi-anneaux d'ensembles sont définis :

Définition. Un *semi-anneau sur* X est une partie $\mathcal{S}$ de $\wp(X)$ qui vérifie les quatre conditions suivantes:

(sa1) $\emptyset \in \mathcal{S}$,

(sa2) il existe une suite $(S_m)_{m\in\mathbb{N}_0}$ de $\mathcal{S}$ telle que $X = \cup_{m=1}^{\infty} S_m$,

(sa3) pour tous S_1, $S_2 \in \mathcal{S}$, il existe une $\mathcal{S}$-partition finie de $S_1 \cap S_2$,

(sa4) pour tous S_1, $S_2 \in \mathcal{S}$, il existe une $\mathcal{S}$-partition finie de $S_1 \setminus S_2$.

Remarque. La condition **(sa2)** est introduite pour des raisons de commodité. Pour une large partie de la théorie, elle n'est pas nécessaire. Son intervention permet d'alléger certains énoncés. De plus, elle est souvent réalisée en pratique; elle l'est toujours pour les mesures de probabilité (définies sur $(X, \mathcal{A})$ où $\mathcal{A}$ est une σ-algèbre de parties de X).□

FIGURE 31 – Semi-anneau

Le théorème de Fubini s'énonce ainsi :

Théorème 4.5.3 (Fubini) *Si f est une fonction $\mu_1 \times \mu_2$-intégrable, alors*

a) *pour μ-presque tout $x_2 \in X_2$, $f(., x_2)$ est μ_1-intégrable,*

b) *$\int f\, d\mu_1$ est une fonction μ_2-intégrable,*

c) *on a*

$$\int \left(\int f\, d\mu_1\right) d\mu_2 = \int f\, d(\mu_1 \times \mu_2).$$

FIGURE 32 – Théorème de Fubini (Version Jean Schmets)

[20] Note de cours Jean Schmets : `http://www.anmath.ulg.ac.be/js/ens.html`

Pour les professionnels, l'énoncé du théorème de Fubini dans *Measure Theory*[3] :

> **3.4.4. Theorem.** *Let μ and ν be σ-finite nonnegative measures on the spaces X and Y. Suppose that a function f on $X \times Y$ is integrable with respect to the product measure $\mu \otimes \nu$. Then, the function $y \mapsto f(x,y)$ is integrable with respect to ν for μ-a.e. x, the function $x \mapsto f(x,y)$ is integrable with respect to μ for ν-a.e. y, the functions*
>
> $$x \mapsto \int_Y f(x,y)\,\nu(dy) \quad \text{and} \quad y \mapsto \int_X f(x,y)\,\mu(dx)$$
>
> *are integrable on the corresponding spaces, and one has*
>
> $$\int_{X\times Y} f\,d(\mu\otimes\nu) = \int_Y \int_X f(x,y)\,\mu(dx)\,\nu(dy) = \int_X \int_Y f(x,y)\,\nu(dy)\,\mu(dx). \tag{3.4.3}$$

FIGURE 33 – Théorème de Fubini (Version Vladimir Igorevich Bogachev and Maria Aparecida Soares Ruas)

Il apparaît qu'il est donc nécessaire de préciser clairement l'énoncé.

La bibliothèque mathématique de Mizar (MML) contient les définitions d'un **semi-anneau d'ensemble**[9] (`SRINGS_1.MIZ`) :

```
definition
let X be set ;
mode semiring_of_sets of X is
     with_empty_element
     cap-finite-partition-closed
     diff-c=-finite-partition-closed
  Subset-Family of X;
end;
```

Il existe une autre définition[13], plus conventionnelle mathématiquement, de la notion de **semi-anneau d'ensemble**(`SRINGS_3.MIZ`) :

```
definition
  let X be set ;
  mode Semiring of X is
     with_empty_element
     cap-closed
     semi-diff-closed Subset-Family of X;
end;
```

La différence est minime. D'ailleurs tout `Semiring of X` est un `semiring_of_sets of X`. L'inverse n'est pas vrai [21].

Nous sommes prêts pour aborder la version MML du l'énoncé théorème de Fubini[11] (`MESFUN13:30`) :

```
theorem :: MESFUN13:30
for X1, X2 being non empty set
for S1 being SigmaField of X1
for S2 being SigmaField of X2
for M1 being sigma_Measure of S1
for M2 being sigma_Measure of S2
for f being PartFunc of [:X1,X2:],ExtREAL
for SX1 being Element of S1 st
    M1 is sigma_finite &
    M2 is sigma_finite &
```

`http://www.anmath.ulg.ac.be/js/ens/tm.pdf`

[21] Pourquoi ces deux définitions apparaissent dans la MML ? Je pense qu'il s'agit d'un pur hasard, les auteurs travaillaient indépendamment avec des motivations différentes. Les relecteurs ont accepté la présence de ces deux définitions.

```
    f is_integrable_on Prod_Measure (M1,M2) &
    X1 = SX1 holds
ex U being Element of S1 st
   ( M1 . U = 0 &
   ( for x being Element of X1 st x in U ‘ holds
            ProjPMap1 (f,x) is_integrable_on M2 ) &
            (Integral2 (M2,|.f.|)) | (U ‘) is PartFunc of X1,REAL &
            Integral2 (M2,f) is SX1 \ U -measurable &
            (Integral2 (M2,f)) | (U ‘) is_integrable_on M1 &
            (Integral2 (M2,f)) | (U ‘) in L1_Functions M1 &
            ex g being Function of X1,ExtREAL st
                ( g is_integrable_on M1 &
                  g | (U ‘) = (Integral2 (M2,f)) | (U ‘) &
                  Integral ((Prod_Measure (M1,M2)),f) = Integral (M1,g) ) )
```

Cet énoncé est beaucoup plus long. En effet, toute formalisation nécessite beaucoup de précision.

En particulier la proposition `X1=SX1` peut paraître une erreur ou un oubli de suppression, il n'en est rien. Il est nécessaire à la ligne `Integral2 (M2,f) is SX1 \ U -measurable` car le système **Mizar** attend précisément un élément de `S1` devant `-measurable`. Si l'auteur de l'énoncé avait simplement écrit `X1 \ U -measurable`, Mizar n'aurait pas compris de suite que `X1 \ U` est bien un élément de S_1 (ce qui est mathématiquement trivial).[22]

Si on tente de retranscrire sous une forme mathématique cet énoncé, il aurait la forme raccourcie suivante :

Théoreme 2.1. *Soit $(\mu_1, \mathcal{S}_1, X_1)$, $(\mu_2, \mathcal{S}_2, X_2)$ deux σ-mesures sur les espaces non vides X_1 et X_2. Supposons que la fonction f définie sur $X_1 \times X_2$ et à valeurs dans $\overline{\mathbb{R}}$ est $\mu_1 \times \mu_2$-intégrable alors il existe U un élement de $\mathcal{S}_1$ de μ_1-mesure nulle tel que*

- *$\forall x \in X_1 \backslash U$, $f(x,.)$ soit μ_2-intégrable ;*
- *$\left(\int |f| d\mu_2\right)|_{X_1 \backslash U}$ est une fonction définie sur une partie de X_1 et à valeur dans $\mathbb{R}$;*
- *$\int f d\mu_2$ est $X_1 \backslash U$-mesurable ;*
- *$\left(\int f d\mu_2\right)|_{X_1 \backslash U}$ est μ_1-intégrable et*
- *$\exists g$ fonction μ_1-intégrable sur X_1 tel que*
  - *$g|_{X_1 \backslash U} = \left(\int f d\mu_2\right)|_{X_1 \backslash U}$ et*
  - *$\int f d(\mu_1 \times \mu_2) = \int g d\mu_1$.*

Nous pouvons voir clairement l'introduction d'un ensemble U de $\mathcal{S}_1$ de μ_1-mesure nulle qui est implicitement contenu dans les autres énoncés plus classiques.

De plus l'introduction de la fonction g est nécessaire pour clarifier la définition. Il aurait aussi été probablement possible de définir une fonction `#` définie sur $X_1 \backslash U$ tel que `#(f,M2,X1,U):=Integral2 (M2,f)`.

Au final, on retrouve bien le théorème de Fubini. Nous laissons le soin au lecteur de naviguer directement dans la fichier `mesfun13.html`[23] afin de vérifier les définitions utilisées.

Nous n'aborderons pas ici, ni la démonstration, ni les applications de ce théorème à l'aide de **Mizar**.

Par contre il est peut-être utile de présenter une forme plus classique du théorème de Fubini, également démontrée précédemment par Endou[12][24] :

```
theorem :: MESFUN12:84
for X1, X2 being non empty set
for S1 being SigmaField of X1
for S2 being SigmaField of X2
for M1 being sigma_Measure of S1
```

[22] Techniquement, cette façon de faire n'est pas unique. Il est aussi possible d'utiliser une injection $i : SETS|_{\mathcal{S}_1} \to \mathcal{S}_1 : X \mapsto X$, notée et définie par exemple avec le symbole `#`, ainsi `SX1` peut être remplacé par `#X1`.

[23] `http://www.mizar.org/version/current/html/mesfun13.html`

[24] `http://www.mizar.org/version/current/html/mesfun12.html`

```
for M2 being sigma_Measure of S2
for A being Element of sigma (measurable_rectangles (S1,S2))
for f being PartFunc of [:X1,X2:],ExtREAL st
  M1 is sigma_finite & M2 is sigma_finite &
  ( f is nonnegative or f is nonpositive ) &
  A = dom f & f is A -measurable
holds
( Integral ((Prod_Measure (M1,M2)),f) = Integral (M2,(Integral1 (M1,f))) &
  Integral ((Prod_Measure (M1,M2)),f) = Integral (M1,(Integral2 (M2,f))) )
```

avec [25]

```
definition
let X1, X2 be set ;
let S1 be Field_Subset of X1;
let S2 be Field_Subset of X2;
func measurable_rectangles (S1,S2) -> semialgebra_of_sets of [:X1,X2:]
equals :: MEASUR10:def 5
{ [:A,B:] where A is Element of S1, B is Element of S2 : verum } ;
```

et[26]

```
 definition
let Omega be non empty set ;
let X be Subset-Family of Omega;
func sigma X -> SigmaField of Omega means :: PROB_1:def 9
( X c= it & ( for Z being set st X c= Z & Z is SigmaField of Omega holds
it c= Z ) );
```

avec[27]

```
definition
let X be set ;
mode SigmaField of X is
   non empty
   compl-closed
   sigma-multiplicative Subset-Family of X;
```

et[28]

```
 definition
let X be set ;
let IT be Subset-Family of X;
attr IT is compl-closed means :Def1: :: PROB_1:def 1
for A being Subset of X st A in IT holds
A ‘ in IT;
end;
```

et enfin[29]

```
 definition
let X be set ;
let F be Subset-Family of X;
attr F is sigma-multiplicative means :Def6: :: PROB_1:def 6
for A1 being SetSequence of X st rng A1 c= F holds
Intersection A1 in F;
end;
```

Il est à noter le travail très récent réaliser avec **Coq** sur le théorème de “Tonelli”[4] :

[25] http://www.mizar.org/version/current/html/measur10.html#K3
[26] http://www.mizar.org/version/current/html/prob_1.html#K9
[27] http://www.mizar.org/version/current/html/prob_1.html#NM3
[28] http://www.mizar.org/version/current/html/prob_1.html#V1
[29] http://www.mizar.org/version/current/html/prob_1.html#V4

Theorem 1: Tonelli

Let (X_1, Σ_1, μ_1) and (X_2, Σ_2, μ_2) be measure spaces. Assume that μ_1 and μ_2 are σ-finite. Let $f \in \mathcal{M}_+(X_1 \times X_2, \Sigma_1 \otimes \Sigma_2)$. Then, we have

$$(1) \qquad \left(\forall x_1 \in X_1,\ f_{x_1} \in \mathcal{M}_+(X_2, \Sigma_2)\right) \quad \wedge \quad \int_{X_2} f_{x_1}\, d\mu_2 \in \mathcal{M}_+(X_1, \Sigma_1),$$

$$(2) \qquad \left(\forall x_2 \in X_2,\ f^{x_2} \in \mathcal{M}_+(X_1, \Sigma_1)\right) \quad \wedge \quad \int_{X_1} f^{x_2}\, d\mu_1 \in \mathcal{M}_+(X_2, \Sigma_2),$$

$$(3) \qquad \int_{X_1 \times X_2} f\, d(\mu_1 \otimes \mu_2) = \int_{X_1} \left(\int_{X_2} f_{x_1}\, d\mu_2 \right) d\mu_1 = \int_{X_2} \left(\int_{X_1} f^{x_2}\, d\mu_1 \right) d\mu_2.$$

FIGURE 34 – Théorème de “Tonelli”, version **Coq**

3 Il faut qu’on en parle...

Les assistants de preuve, qu’ils soient interactifs ou automatiques, sont des outils. Nous vous préconisons leur emploi en “personne prudente et raisonnable” avec un regard critique : c’est le but de cette section. Comme nous ne pouvons être exhaustifs, soyez libre également d’y apporter vos avis et vos opinions.

Nous refusons de publier des opinions, avis ou positions contraires à la loi, par exemple propos haineux et racistes, injures, calomnies, propos diffamatoires,...
De plus, chaque assistant de preuve a ses avantages et ses inconvénients et ils s’inscrivent dans des contextes de développement, de logique, ou d’histoires,... souvent différents. La revue n’est pas et ne doit pas être un lieu de dénigrement d’un assistant de preuve ou d’une logique en particulier.

Deux sujets abordés dans cette section.

3.1 La Géométrographie

Si vous êtes intéressé, le sujet est toujours d’actualité. En effet, même si on trouve des traces de la Géométrographie (ou Art des constructions géométriques)[30] dans le livre d’Emile Lemoine [31] de 1892, le sujet se poursuit, par exemple avec le projet [2] de compétition ou avec le projet "Open Library of Geometry Automatic Theorem Provers"[1]`https://github.com/opengeometryprover/OpenGeometryProver`. Ce projet-ci a été présenté lors de la conférence annuelle "International Workshop on Theorem Proving Components for Educational Software (ThEdu)"[32] qui est une mine d’or. Plus d’info sur : `https://dblp.org/db/conf/thedu/index.html` Nous avons vu que les constructions ne se valent pas : certaines admettent peu d’étapes d’autres en demandent plus. Il est parfois utile d’établir une cartographie des méthodes de construction géométrique. Une lecture intéressante : "Taxonomies of geometric problems"[24] ?

Sans oublier des constructions suprenantes dans le plan hyperbolique : comment construire un cercle hyperbolique[27][33].

Si un article de cette revue est consacrée à la découverte de quelques aspects du logiciel **GCLC**, il est à noter que celui-ci est utilisé dans deux expérimentations pour les moins étonnantes et intéressantes.

Dans les 2 présentation ci-dessous, ce n’est pas **GCLC** qui est mis à l’honneur mais le logiciel **ArgoTriCS**, implémenté[34] par Madame Vesna Marinković (née Pavlovic), auteure principale et membre

[30] Accessible en ligne sur Gallica : `https://gallica.bnf.fr/ark:/12148/bpt6k68143p.r.notice`
[31] Les symédianes : c’est lui !. Emile Lemoine (wikipedia) : `https://fr.wikipedia.org/wiki/%C3%89mile_Lemoine`
[32] `https://www.uc.pt/en/congressos/thedu`
[33] Hyperbolic Constructions in Geometer’s Sketchpad. L’auteur, Steve Szydlik, signale sur son site internet que les constructions n’ont pas été prouvées exactes
[34] en PROLOG et ayant environ 6000 lignes de code

du groupe ARGO (Automated Reasoning Group[35]), lors de sa thèse de doctorat [36] [18, 26].

3.1.1 Recueil en ligne de problèmes de construction de positions triangulaires

Connaissez vous la liste de problème de Wernick[28] ?
Connaissant 3 points des 16 points de la liste suivante :
— Les sommets A, B et C ;
— Le centre de gravité G du triangle ABC ;
— Le centre du cercle circonscrit O au triangle ABC ;
— Le centre du cercle inscrit I au triangle ABC ;
— L'orthocentre du triangle ABC : H.
— Les milieux M_{AB}, M_{AC} et M_{BC} des côtés du triangle ABC ;
— Les pieds P_A, P_B, P_C des hauteurs issues des sommets du triangle ABC ;
— Les pieds B_A, P_B et P_C des bissectrices :
construire à la règle et au compas, *quand cela est possible*, le triangle ABC.

Des chercheurs français (P. Schreck et P. Mathis) et serbes (V. Marinkovič[37] et P. Janičič) ont étudié de façon systématique ces problèmes (voir [26, 19]) grâce à l'assistant automatique de preuve **ArgoTriCS**.

La particuliarité du logiciel n'est pas d'indiquer seulement s'il y a une solution mais d'indiquer, quand cela est possible, la suite des étapes nécessaires pour construire le triangle ABC [38].

C'est assez impressionnant ! Pour chaque solution proposée, il y a une version en *langage naturel* et une version **GCLC**.

Par exemple, voici une méthode pour – ayant les point O, M_C et H – reconstruire le triangle ABC (35) avec les indications concernant les cas dégénérés possibles [39] :

La version en langage naturel[40] :

1. Using the point O and the point H, construct a point G (rule W01) ;
2. Using the point Mc and the point G, construct a point C (rule W01) ;
3. Using the point O and the point Mc, construct a line mc (rule W02) ;
   `% DET: points O and Mc are not the same`
4. Using the point C and the point O, construct a circle k(O,C) (rule W06) ;
   `% NDG: points C and O are not the same`
5. Using the point Mc and the line mc, construct a line c (rule W10a) ;
6. Using the circle k(O,C) and the line c, construct a point A and a point B (rule W04) ;
   `% NDG: line c and circle k(O,C) intersect`

La version utilisable avec **GCLC** :

```
dim 120 120

point O 65 51.14
point M_{c} 50 67.5
point H 80 72.73

color 220 0 0
fontsize 11

cmark_t O
cmark_lt M_{c}
cmark_rt H
color 0 0 0
fontsize 10
```

[35] http ://argo.matf.bg.ac.rs/
[36] En serbe : `http://poincare.matf.bg.ac.rs/~vesnam/radovi/teza.pdf`
[37] `http://poincare.matf.bg.ac.rs/~vesnap/`
[38] `http://poincare.matf.bg.ac.rs/~vesnap/animations/compendiums.html`
[39] `http://poincare.matf.bg.ac.rs/~vesnap/animations/construction_0300.html`
[40] N.d.E : En anglais : il s'agit de la sortie originale.

```
% Constructing a line L_{\_G32009} which passes through point O and point H
line L_{\_G32009} O H

color 200 200 200
drawline L_{\_G32009}
color 0 0 0

% Constructing a point P_{\_G32110} with coordinates (0,0)
point P_{\_G32110} 0 0
cmark_r P_{\_G32110}

% Constructing a point P_{\_G32034} such that OP_{\_G32034}/OP_{\_G32110}=1
towards P_{\_G32034} O P_{\_G32110} 1
cmark_r P_{\_G32034}
color 200 200 200
drawsegment O P_{\_G32034}
color 0 0 0

% Constructing a point P_{\_G32079} such that OP_{\_G32079}/OP_{\_G32110}=3
towards P_{\_G32079} O P_{\_G32110} 3
cmark_r P_{\_G32079}
color 200 200 200
drawsegment O P_{\_G32079}
color 0 0 0

% Constructing a line L_{\_G32040} which passes through point H and point P_{\_G32079}
line L_{\_G32040} H P_{\_G32079}

color 200 200 200
drawline L_{\_G32040}
color 0 0 0

% Constructing a line L_{\_G32003} which contains the point P_{\_G32034} and
  is parallel to the line L_{\_G32040} parallel L_{\_G32003} P_{\_G32034} L_{\_G32040}

color 200 200 200
drawline L_{\_G32003}
color 0 0 0

% Constructing a point G which belongs to line L_{\_G32003} and line L_{\_G32009}
intersec G L_{\_G32003} L_{\_G32009}
cmark_t G

% Constructing a point C such that M_{c}C/M_{c}G=3
towards C M_{c} G 3
cmark_b C
color 200 200 200
drawsegment M_{c} C
color 0 0 0

% DET:  points O and M_{c} are not the same
% Constructing a line m_{c} which passes through point O and point M_{c}
line m_{c} O M_{c}

color 200 200 200
drawline m_{c}
color 0 0 0
```

```
% NDG:  points C and O are not the same
% Constructing a circle k(O,C) whose center is at point O and
% which passes through point C circle k(O,C) O C

color 200 200 200
drawcircle k(O,C)
color 0 0 0

% Constructing a line c which is perpendicular to line m_{c} and
% which passes through point M_{c} perp c M_{c} m_{c}

color 200 200 200
drawline c
color 0 0 0

% NDG:  line c and circle k(O,C) intersect
% Constructing points A and B which are in intersection of k(O,C) and c
intersec2 A B k(O,C) c
cmark_t A
cmark_b B

drawsegment A B
drawsegment A C
drawsegment B C

% Non-degenerate conditions:  line c and circle k(O,C) intersect;
%                             points C and O are not the same
% Determination conditions:  points O and M_{c} are not the same
```

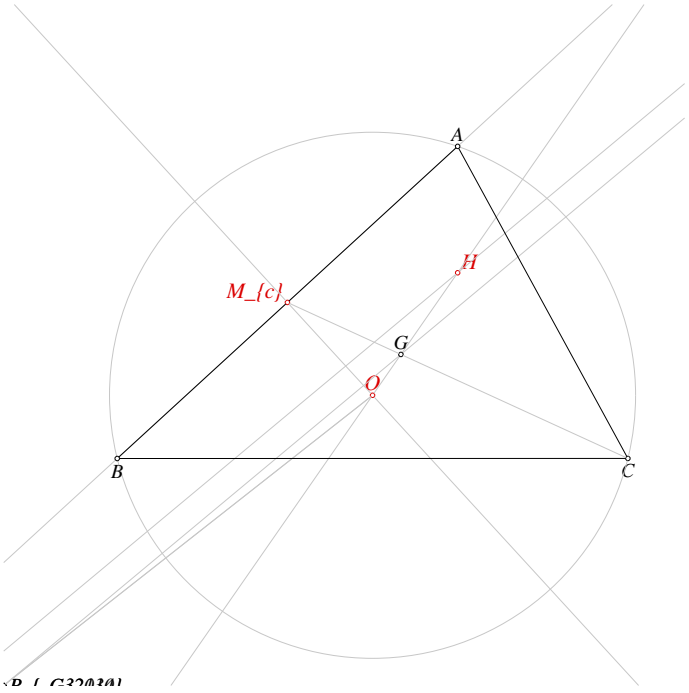

FIGURE 35 – gclc300.eps

[41] On Automating Triangle Constructions in Absolute and Hyperbolic Geometry https://arxiv.org/pdf/2201.00534.pdf

[42] http://poincare.matf.bg.ac.rs/~vesnap//animations_hyp/compendium_wernick_hyperbolic.html

3.1.2 Sur l'automatisation des constructions de triangles en géométrie absolue et hyperbolique

Ce travail - en cours de réalisation (2022)[41] par Mesdames Marinkovic̀ et Šukilovic̀ et M. Maric̀ - porte probablement sur les mêmes questions que la section précédente mais [42] avec des constructions dans le modèle du disque de Poincaré.

Nous ne manquerons pas de revenir ultérieurement sur ce sujet.

3.2 Isabelle dans la matrix...

Cet "il faut qu'on en parle" est en lien direct avec une rubrique précédente, concernant l'utilisation des matrices avec l'assistant interactif de preuve **Isabelle**[43].

Avant d'écrire la rubrique sur les matrices, mon attention avait été attirée par le travail d'Anthony Bordg, Hanna Lachnitt et Yijun He : "Isabelle Marries Dirac : a Library for Quantum Computation and Quantum Information"[7] et l'article "Certified quantum computation in Isabel/HOL"[6].

Le titre de l'article fait rêver : Informatique quantique... Mais je m'égare. L'équipe résume son travail par :

> his work is an effort to formalise some quantum algorithms and results in quantum information theory. Formal methods being critical for the safety and security of algorithms and protocols, we foresee their widespread use for quantum computing in the future. We have developed a large library for quantum computing in Isabelle based on a matrix representation for quantum circuits, successfully formalising the no-cloning theorem, quantum teleportation, Deutsch's algorithm, the Deutsch-Jozsa algorithm and the quantum Prisoner's Dilemma.

[44] Ce travail utilise le calcul matriciel et il a nécessité une adaptation de la bibliothèque existante : Un des fichiers (Tensor.thy)[45] :

> There is already a formalization of tensor products in the Archive of Formal Proofs, namely Matrix_Tensor.thy in Tensor Product of Matrices [...] by T.V.H. Prathamesh, but it does not build on top of the formalization of vectors and matrices given in Matrices, Jordan Normal Forms, and Spectral Radius Theory[2] by René Thiemann and Akihisa Yamada. In the present theory our purpose consists in giving such a formalization. Of course, we will reuse Prathamesh's code as much as possible, and in order to achieve that we formalize some lemmas that translate back and forth between vectors (resp. matrices) seen as lists (resp. lists of lists) and vectors (resp. matrices) as formalized in [...].

[46]

Pourtant c'est moins l'aspect matriciel qui nous intéresse ici mais une conclusion de l'article :

> Indeed, the Letter [...] of Eisert et al. is a pioneering and highly cited article published in Physical Review Letters, a high-profile physics journal. The error uncovered therein is a notable unexpected outcome of our library. Indeed, this error had gone unnoticed in the field until our work and we found at least one subsequent published paper that reproduced it. After a private communication Eisert et al. acknowledged their error and they actually found a fix to re- establish their conclusions regarding what they call the "miracle move". An erratum was published by Physical Review Letters [...].

[47]

[43] `https://isabelle.in.tum.de/`

[44] NdE. Traduction : Ce travail est un effort pour formaliser certains algorithmes et résultats quantiques en théorie de l'information quantique. Les méthodes formelles étant essentielles pour la sûreté et la sécurité des algorithmes et des protocoles, nous prévoyons leur utilisation généralisée pour l'informatique quantique à l'avenir. Nous avons développé une grande bibliothèque pour l'informatique quantique en Isabelle, basée sur une représentation matricielle des circuits quantiques, et formalisé avec succès le théorème de non-clonage, la téléportation quantique, l'algorithme de Deutsch, l'algorithme de Deutsch-Jozsa et le dilemme du prisonnier quantique.

[45] `https://www.isa-afp.org/browser_info/current/AFP/Isabelle_Marries_Dirac/Tensor.html`

[46] NdE. Traduction : Il existe déjà une formalisation des produits tensoriels dans l'Archive of Formal Proofs, à savoir Matrix_Tensor.thy dans Tensor Product of Matrices [1] par T.V.H. Prathamesh, mais elle ne s'appuie pas sur la formalisation des vecteurs et des matrices donnée dans Matrices, Jordan Normal Forms, and Spectral Radius Theory [2]. Spectral Radius Theory [2] par René Thiemann et Akihisa Yamada. Dans la présente théorie, notre but consiste à donner une telle formalisation. Bien entendu, nous réutiliserons le code de Prathamesh autant que possible, et pour ce faire, nous formalisons quelques lemmes qui permettent de faire des allers-retours entre les vecteurs (resp. matrices) vus comme des listes (resp. listes de listes) et les vecteurs (resp. matrices) tels que formalisés dans [2].

[47] NdE Traduction : En effet, la lettre [...] d'Eisert et al. est un article pionnier et très cité publié dans Physical

Cela ne signifie pas qu'il faille formaliser au fur et à mesure tous les articles paraissant actuellement, ce qui est de toute façon *humainenemnt* impossible. D'ailleurs il arrive que des erreurs locales dans une démonstration n'impactent pas la démonstration globale.

De plus, que serait-il arrivé si Einstein avait arrêté ses travaux de recherches sur la relativité générale parce des erreurs détectées l'aurait fait abandonné toute ambition ?

Extrait France Culture du 23 novembre 2021 (Éric Chaverou et Diane Berger)[48] :

> "Les deux amis et confrères s'attaquent à l'un des problèmes auquel la communauté scientifique se heurtait depuis des décennies : l'anomalie de l'orbite de la planète Mercure. Le périhélie de Mercure, c'est-à-dire le point de son orbite le plus proche du Soleil, se déplace lentement au fil du temps, sous l'effet d'autres corps dans le système solaire. Un décalage infinitésimal existe entre les équations de Newton, et ce qui était observé, sans que personne n'ait pu fournir d'explication irréfutable. Pour Einstein et Besso, si leurs équations donnent pour résultat le décalage observé, la théorie sera validée." précise Adrien Legendre, Directeur du département des Livres Rares et Manuscrits de la maison de ventes aux enchères française Aguttes, à l'origine de la vente de ce mardi. D'ajouter : "Les calculs du manuscrit Einstein-Besso comportent toutefois un certain nombre d'erreurs passées inaperçues, et dans les mois suivants, Einstein mit de côté cette première approche. Besso quitte Zurich, emportant avec lui le document."

Extrait du journal "Le Soir" du 21 novembre 2021[49] :

> Début 1913, lui et Besso "s'attaquent à l'un des problèmes auxquels la communauté scientifique se heurtait depuis des décennies : l'anomalie de l'orbite de la planète Mercure", rappelle Christie's. Les deux scientifiques résoudront cette énigme.
>
> Ce n'est pas dans les calculs couchés sur ce manuscrit, qui comptent "un certain nombre d'erreurs passées inaperçues". Quand Einstein les repéra, il ne se préoccupa plus de ce manuscrit, emporté par Besso.

Il n'est pas le lieu de dire qu'il faille accepter des erreurs dans les articles au nom d'une soi-disant simple liberté du processus de découverte scientifique. Bien entendu, tout article se doit d'être correct ou corrigé rapidement le cas échéant et nul ne désire que l'utilisation d'articles non corrigés provoque des conséquences dommageables.

Devant les enjeux de certaines applications, une vérification formelle est un plus.

Anthony Bordg propose son point de vue dans "The Mathematical Intelligencer n° 43, 2021" [5] que je résume personnellement de cette façon : [50].

- Vers une crise d'évaluation par les pairs, obligeant les mathématiques à se réinventer ;
- Il est possible de réduire le risque d'erreur dans les preuves mathématiques ;
- Les assistants de preuve pourraient permettre aux mathématiciens d'être plus fidèles à leur idéal de rigueur ;
- L'examen par les pairs restera nécessaire. Les humains resteront donc des acteurs clés pour décider quels résultats méritent d'être publiés ;
- Les preuves formelles obligent les mathématiciens à faire des choix techniques et à traiter des détails de très bas niveau ;
- Beaucoup de progrès reste à faire pour rendre les assistants de preuve plus conviviaux[51].
- Il est intéressant de continuer à progresser dans la formalisation des mathématiques à l'aide d'assistants de preuve, afin de rendre plus efficace le processus d'évaluation par les pairs.

Promis, on en reparle dans un autre numéro.

Review Letters, une revue de physique très en vue. L'erreur qui y a été découverte est un résultat inattendu notable de notre bibliothèque. En effet, cette erreur était passée inaperçue dans le domaine jusqu'à notre travail. et nous avons trouvé au moins un article publié ultérieurement qui la reproduisait. Après une communication privée, Eisert et al. ont reconnu leur erreur et ont trouvé un correctif pour rétablir leurs conclusions concernant ce qu'ils appellent le "système d'échange de données". Un erratum a été publié par Physical Review Letters [...].

[48] https://www.franceculture.fr/sciences/102-millions-deuros-pour-un-manuscrit-dalbert-einstein-qui-prepare-la-relativite-generale

[49] https://www.lesoir.be/407721/article/2021-11-21/de\protect\discretionary{\char\hyphenchar\font}{}{}encheres-astronomiques-un-manuscrit-deinstein-vendu-paris

[50] En open access : `https://link.springer.com/content/pdf/10.1007/s00283-020-10037-7.pdf`

[51] user-friendly

4 Interview de M. Pascal Fontaine - WG Automated theorem provers - CA20111

Depuis quelques années, des chercheurs s'investissent dans la recherche ayant pour thème les assistants de preuve automatiques et ils se réunissent annuellement, en autre, durant

— la *Conference on Artificial Intelligence and Theorem Proving - AITP* [52] et

— l'*International Conference on Automated Deduction* [53] [54] organisée par l'association "Association for Automated Reasoning"[55].

De plus, cette année, débute grâce au **COST**[56] [57], le programme **EuroProfNet**[58] c'est-à-dire l'"European Research Network on Formal Proofs" (CA20111)).

La description de ce programme est disponible sur le site (voir [59])[60] :

> Si les tests peuvent révéler des erreurs dans les programmes informatiques, seule la vérification formelle peut garantir leur absence. Les niveaux d'assurance d'évaluation les plus élevés des critères communs d'évaluation de la sécurité des technologies de l'information exigent des preuves mathématiques d'exactitude vérifiées automatiquement. Les preuves sont également à la base des mathématiques et de nombreuses sciences, et sont donc très importantes dans l'enseignement et la recherche.
>
> Dans de nombreuses technologies informatiques, les développeurs et les utilisateurs s'appuient sur des langages et des protocoles standard pour échanger des données et permettre l'interopérabilité des outils : TCP/IP pour la communication réseau, HTML pour les pages web, etc. Ce n'est toutefois pas le cas pour les preuves formelles, ce qui constitue un obstacle majeur à leur adoption par l'industrie. La raison principale est qu'actuellement, les systèmes de preuve utilisent des fondements logiques mutuellement incompatibles. Heureusement, seules de petites parties des preuves développées dans un système utilisent des caractéristiques incompatibles avec d'autres systèmes.
>
> L'Europe est un acteur majeur dans le domaine des preuves formelles : environ 65% des systèmes de preuve du monde sont développés en Europe, y compris les deux assistants de preuve les plus utilisés, Coq et Isabelle.
>
> Cette action vise à stimuler l'interopérabilité et la facilité d'utilisation des systèmes de preuve et à faire entrer les preuves formelles dans une nouvelle ère. Pour la première fois, elle rassemble tous les développeurs et utilisateurs de systèmes de preuve en Europe. Pour rendre les preuves échangeables, ils exprimeront, dans un cadre logique commun, les fondements logiques de leurs systèmes et développeront des outils pour l'inter-translation des preuves développées dans les systèmes individuels vers et depuis ce cadre logique commun.

Mon attention a été attirée par la présence, dans ce programme, de chercheurs belges, dont des wallons, et en particulier le Chef du groupe de travail "Automated theorem provers" de **EuroProfNet** : Pascal Fontaine, professeur à l'Université de Liège[61].

Il a accepté de répondre à mes questions.

MaSciProûve : Si un professeur de l'école secondaire désire illustrer son cours par les assistants automatiques de preuves, quelles sources lui conseillerais-tu ? Dans le numéro de cette revue, un article est consacré au logiciel GCLC intégrant un assistant de preuve permettant de prouver certains énoncés en lien avec la construction de diagrammes de géométrie élémentaire. Ton travail porte-t-il aussi sur ce genre de logiciel et ce genre de problème ?

Pascal : En ce qui concerne l'école secondaire, je n'ai pas grand-chose à dire, excepté le fait

[52] http://aitp-conference.org

[53] http://www.cadeinc.org/

[54] https://en.wikipedia.org/wiki/Conference_on_Automated_Deduction

[55] http://aarinc.org/

[56] https://www.cost.eu/

[57] COST (Coopération européenne en science et technologie) est un organisme de financement des réseaux de recherche et d'innovation. Nos actions contribuent à relier les initiatives de recherche en Europe et au-delà et permettent aux chercheurs et aux innovateurs de développer leurs idées dans tous les domaines scientifiques et technologiques en les partageant avec leurs pairs. Les actions COST sont des réseaux ascendants d'une durée de quatre ans qui stimulent la recherche, l'innovation et les carrières.

[58] https://europroofnet.github.io/

[59] https://www.cost.eu/actions/CA20111/#tabs+Name:Description

[60] N.d. E : traduction en français

[61] https://www.uliege.be/cms/c_11399834/fr/pascal-fontaine

que la rigueur mathématique a quand même tendance à se perdre au bénéfice des résultats et de la quantité de choses apprises. Les assistants de preuve sont des outils qui imposent la rigueur. Même les mathématiciens de haut vol font de temps en temps des erreurs et certains se retournent alors vers les assistants de preuve. Comme les élèves qui sortent actuellement du secondaire ont de moins en moins cette rigueur mathématique, au bénéfice d'une quantité de matière, il est peut-être intéressant de commencer à réfléchir à la façon dont on va faire des preuves assistées par ordinateur aussi au niveau du secondaire. Mais je peux difficilement proposer un outil adapté et stable. Il faudrait que ce soit quelque chose autour de la géométrie, je crois, donc ton choix de GCLC me semble judicieux. C'est par la géométrie que j'ai appris la rigueur mathématique quand j'ai commencé à faire des démonstrations en deuxième et troisième année de secondaire. Les recherches actuelles dans les assistants automatiques sont très dirigées vers la vérification de programmes ; il serait nécessaire, je crois, de développer un outil adapté à la pédagogie.

MaSciProûve : Et de journal, de revue, de livre ? Pour, par exemple un étudiant, qui voudrait dire : « voilà j'aimerai bien présenter en classe pendant une heure 'c'est quoi un assistant automatique de preuve' ». A part Wikipédia il n'y a rien pour le moment ?

Pascal : En livre... je n'ai pas vraiment de livre très précis mais Gilles Dowek[62] est un spécialiste de tout ce qui est assistant de preuve - et des preuves rigoureuses - et c'est aussi un excellent vulgarisateur. Il a plusieurs livres à son actif. Et même si ce ne sont pas des livres sur les assistants de preuve, je pense que dans ses livres transparaît une certaine idée de la rigueur qu'on peut avoir dans les assistants de preuve, parce que c'est au cœur de son domaine de recherche. Si quelqu'un veut un petit peu découvrir nos aspects, je crois que les livres de Gilles Dowek peuvent être un bon point d'entrée. Par exemple, son dernier livre que j'ai lu de lui est : « le temps des algorithmes »[63].

MaSciProûve : Une section de cette revue est consacrée à la vérification Isabelle d'énoncés contenant du calcul matriciel. Sledgehammer est un outil communiquant avec des assistants automatiques de preuves externes (E, cvc4, spass, z3, veriT et zipperposition) afin de leur demander des propositions de vérification. Penses-tu que ces assistants automatiques soient utiles ? Sont-ils perfectibles ? D'autres assistants de preuve pourraient également être utiles ?

Pascal : Les assistants de preuve permettent de traiter avec rigueur de très grandes preuves très complexes : chaque étape de la preuve est revérifiée par l'ordinateur. Mais revérifiée à un niveau de granularité[64] très très fin. La probabilité qu'il y ait une erreur dans une preuve vérifiée par ordinateur est infime.

Par contre, cela a un coût. La personne qui va utiliser l'assistant de preuve doit aussi écrire sa preuve à un niveau de granularité qui est très très fin de manière à ce que cela passe dans l'ordinateur. Donc nous, au niveau des provers[65] automatiques, on essaye de faire en sorte que ce qui est simple pour l'humain soit aussi fait automatiquement par ordinateur, c'est-à-dire que l'utilisateur de l'assistant de preuve puisse écrire sa preuve dans un niveau de granularité qui correspond plus au niveau du mathématicien.

Et on n'est pas encore à un état satisfaisant mais on progresse. Les progrès sont vraiment manifestes ces 20, 30 dernières années et chaque année, les outils deviennent meilleurs. Donc on peut imaginer que dans environ 20 ans, on puisse utiliser les assistants de preuve de la même manière qu'un mathématicien utiliserait du papier pour écrire une preuve et que les détails de preuve soient écrits automatiquement par des algorithmes, des provers automatiques. Je contribue[66] à ces provers automatiques[67].

MaSciProûve : Les assistants automatiques de preuve sont-ils des outils dans la même continuité que la calculatrice, le logiciel de calcul formel et le logiciel de programmation logique ?

Pascal : Je crois, et il y a beaucoup de mathématiciens dont le cœur de métier est vraiment les mathématiques, pas l'informatique, pas les assistants de preuve, pas la logique, qui utilisent les assistants de preuve pour prouver leur théorème pour éviter les erreurs. Je dirais que l'assistant de preuve correspond à la feuille de tableur, et l'assistant automatique de preuve serait la calculette. Quand on travaille plusieurs semaines ou plusieurs mois sur une preuve, et qu'on trouve une erreur, ce sont des semaines ou des mois qui sont perdus. Quand on utilise l'assistant de preuve, on doit payer cela par des preuves beaucoup plus détaillées, mais l'avantage c'est qu'on avance sur un sol beaucoup

[62] G. Dowek, Laboratoire Spécification et Vérification, ENS Paris-Saclay : `http://www.lsv.fr/~dowek/index.html.fr`

[63] «Le temps des algorithmes » de Gilles Dowek et Serge Abiteboul. Ed. Essai le Pommier, 2017

[64] N. d. E : Granularité = niveau de détails (`https://fr.wikipedia.org/wiki/Granularit%C3%A9`)

[65] N. D. E : Prononcez « prouveur ». Provers = des assistants de preuve. (`https://en.wikipedia.org/wiki/Proof_assistant`)

[66] «VeriT an open, trustable and efficient SMT-solver », voir : `https://verit-solver.org/`

[67] N. d. E. : Il y a plusieurs types d'assistants de preuve. VeriT fait partie de la catégorie des « SMT » : `https://fr.wikipedia.org/wiki/Satisfiability_modulo_theories`

plus stable. Chaque fois qu'on écrit quelque chose, on a un degré de certitude qui est plus grand. Là où on peut encore se tromper, c'est en écrivant un théorème qui ne correspond pas exactement à ce qu'on a en tête, et qui ne permettra pas à la fin de vérifier ce qu'on veut vraiment vérifier. Mais cela est un peu le jeu des mathématiques ; de toute façon on peut revenir aussi dans l'assistant de preuve et réécrire. Donc oui, je pense que c'est dans la continuité mais on a quand même encore une vingtaine d'années de retard sur les logiciels de calcul formel, que tu mentionnes aussi, et qui ont aussi assez bien modifié la façon dont on fait des mathématiques avec des intégrales ou de l'algèbre. Une personne qui fait de l'algèbre de façon intensive connaît des logiciels comme Mapple, Mathematica,...

MaSciProûve : Je t'interromps : tu as mis en évidence qu'en mathématiques les choses ne se démontrent pas de façon linéaire, que le mathématicien travaille : il commence sa démonstration... on pourrait toujours avoir cette impression qu'on a un énoncé, on démontre et on passe au suivant. As-tu l'impression que depuis une vingtaine d'années les choses se sont compliquées et que le mathématicien doit faire plus attention quand il avance que dans les années 1970, que la rigueur a changé parce que les concepts, les mathématiques aussi ont évolués ?

Pascal : Je crois que oui, mais je ne suis pas un mathématicien, donc je ne peux pas commenter le travail du mathématicien. Par contre, j'ai déjà entendu plusieurs mathématiciens discuter du sujet : les mathématiques se compliquent aussi, comme tout devient extrêmement technique. Le mathématicien est obligé de se spécialiser. Il prend ses informations de plusieurs sources et chaque fois qu'on change de source, finalement, on change les notations, le contexte et on peut se tromper aussi dans ces contextes. Telle personne aura démontré tel théorème dans le cas fini. Telle autre personne va le réutiliser dans le cas dénombrable et cela ne sera pas du tout la même chose. Donc il n'est pas impossible que quelque chose devienne faux quand on l'étend un peu trop. Cette extension dangereuse, on peut la faire de façon totalement obscure quand on récupère un résultat qui provient de gauche ou droite. Donc effectivement il y a des choses qui peuvent se cacher là. Les assistants de preuve ne laisseraient pas passer ce genre d'erreur. Mais encore une fois, je ne suis pas un mathématicien : je vois juste autour de moi des mathématiciens qui se disent maintenant « oui, il faut que j'utilise un assistant de preuve pour développer les mathématiques parce que je me suis trompé trop souvent et je n'ai pas envie de me tromper ; je préfère créer les choses de façon sûre, même si cela a un surcoût. » Il y a aussi un aspect presque métaphysique dans l'utilisation des assistants de preuve : on recrée dans la machine les vérités du monde et cela a quelque chose de très motivant, presque mystique.

MaSciProûve : C'est un monde qui peut rester figé comme ça... Une fois qu'il est créé, on a l'impression qu'on est sûr de soi et donc il va devenir immuable, un peu comme un code source qui va être utilisable dans 1000 ans.

Pascal : Oui, oui, tout-à-fait.

MaSciProûve : En pratique en fait, c'est pas tout-à-fait vrai. J'aurai peut-être l'occasion d'en parler une autre fois...

Pascal : Oui mais finalement, tu en connais plus que moi sur le développement de théories mathématiques dans les assistants de preuve, puisque tu as toi-même écrit des preuves dans la librairie Mizar.... et donc tu sais comment les choses évoluent. Tu vois aussi de temps en temps que les gens développent une théorie mais d'autres personnes développent la même théorie en utilisant d'autres conventions, d'autres définitions.

MaSciProûve : Il y a toute une sociologie, il y a des modes qui viennent et des gens qui veulent recommencer tout. C'est toute une sociologie historique intéressante. On n'a jamais fini même sur des choses hyper-élémentaires et cela est génial. C'est pour cela que les questions portent sur les assistants automatiques, qui est ton domaine à toi. Je ne veux pas t'emmener vers les interactifs[68] qui sont plutôt – je ne suis pas expert- , mais utilisateur ...

Pascal : Tu es beaucoup plus expert que moi.

MaSciProûve : ... et un automatique, pour moi, c'est comme la calculatrice qui nous aide à résoudre un problème, et puis le logiciel de calcul formel qui nous permettait il y a un trentaine d'année d'avoir une intégrale ou une dérivée (valable ou pas, cela est un autre problème...), et puis la résolution de Sodoku et tout cela... et puis on arrive... aux assistants automatiques, on ne connaissait pas il y a vingt ans. C'est un support pour résoudre certains problèmes (mais pas tous). On est vraiment au début...

— *** —

L'entretien s'est déroulé à distance, en raison de la situation sanitaire. J'avais encore quelques

[68] Assistant interactif de preuve (`https://fr.wikipedia.org/wiki/Assistant_de_preuve`)

autres questions à poser mais, malheureusement, le temps était limité de mon côté. J'espère pouvoir retrouver M. Pascal Fontaine pour poursuivre cet échange, dans un prochain numéro.

5 L'association sur internet...

L'association loue un serveur privé virtuel debian et un serveur web.
L'adresse du serveur web est `www.cafr-msa2p.be` (en http ou https) avec les sous-domaines :

— la revue *MaSciProûve* est disponible à l'adresse `masciprouve.cafr-msa2p.be`. Les anciens numéros sont téléchargeables. Attention : les fichiers pdf contiennent des liens externes actifs.
— le *centre de documentation* est disponible à l'adresse `cd.cafr-msa2p.be` avec la liste des livres et revues consultables.

`msa2p.be` : il s'agit du serveur de l'association contenant les répertoires gitweb. Notre serveur public *webgit* est disponible[69]. Vous pouvez y trouver les exemples de fichiers **GCLC** utilisés dans ce numéro.

6 Le centre de documentation

Le centre de documentation n'offre ni service de vente ni de prêt de livres, revues ou magazines mais la consultation sur place au siège social est possible sur rendez-vous, dans le respect des règles sanitaires en cours. Si vous désirez acquérir un livre, nous vous invitons à prendre contact avec votre libraire préféré(e).

Cette rubrique contient les dernières nouvelles, les acquisitions ainsi que des présentations de certains ouvrages en notre possession.

6.1 La convivialité

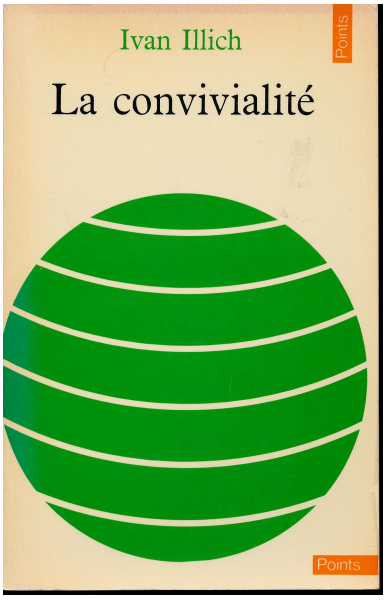

FIGURE 36 – La convivialité

De façon classique, la convivialité est, selon le dictionnaire Larousse [70] :

1. Capacité d'une société à favoriser la tolérance et les échanges réciproques des personnes et des groupes qui la composent.

[69] msa2p.be:4321
[70] `https://www.larousse.fr/dictionnaires/francais/convivialit%C3%A9/19016`

2. Facilité d'emploi d'un système informatique.

Pourtant il existe un troisième sens, associé au mot *outil*, utilisé dans son livre.
La convivialité est un livre d'Ivan Illich[71], (1973, Édition du Seuil pour la version française) [72].
Le livre contient les chapitres suivants :

1. Avant-propos
2. Introduction
3. Deux seuils de mutation
4. La reconstruction conviviale
5. L'équilibre
6. L'inversion politique : obstacles et conditions
7. L'inversion politique

Les propos du livre doivent être remis dans leurs contextes historiques et géopolitiques (fin de la guerre du Vietnam, confrontation Ouest/Est, critique de la société de consommation, des dérives médicales, etc.). Certaines thèses ont été mises en perspective (Par exemple pour la vitesse généralisée des automobilistes, Frédérice Héra note dans son article [15] qu'à l'époque Jean-Pierre DUPUY (Philosophe des sciences) concluait *Loin d'être un instrument de gain de temps, l'automobile apparaît sous cet éclairage comme un monstre chronophage*).

Si ce livre est présenté dans cette revue, c'est dans le but de mettre en évidence le concept introduit par Ivan Illich : l'**outil convivial**[29].

Extrait de l'introduction,p. 13 :

> J'appelle *société conviviale* une société où l'outil moderne est au service de la personne intégrée à la collectivité, et non au service d'un corps de spécialistes. Conviviale est la société où l'homme contrôle l'outil.
>
> Je suis conscient d'introduire un mot nouveau dans l'usage courant du langage. Je fonde ma force sur le recours au précédent. Le père de ce vocable est Brillat-Savarin, dans sa *Physiologie du goût : Méditations sur la gastronomie trascendantale.*. A moi de préciser, toutefois, que, dans l'acceptation quelque peu nouvelle que je confère au qualificatif, c'est l'outil qui est convivial et non l'homme.

Extrait, p. 45 :

> [...]
> *L'outil est convivial* dans la mesure où chacun peut l'utiliser, sans difficulté, aussi souvent ou aussi rarement qu'il le désire, à des fins qu'il détermine lui-même. L'usage que chacun en fait n'empiète pas sur la liberté d'autrui d'en faire autant. Personne n'a besoin d'un diplôme pour avoir le droit de s'en servir ; on peut le prendre ou non.
> [...]

Je vous partage mes points forts/faibles :
Points forts :

1. Comme tout assistant de preuve (automatique ou non) est un outil, certains éléments de l'analyse de Illich peuvent-ils être pertinents ? A vous de juger.
2. Ce concept d'**outil convivial** est toujours d'actualité. En témoigne l'article, à paraître de Romain Couillet, Pierre-Olivier Amblard et Denis Trystram "L'intelligence artificielle peut-elle devenir un outil convivial ? ou doit-on immédiatement arrêter toute recherche en IA ?". [73]
3. Analyse d'impact de la surconsommation et de l'utilisation excessive des ressources.
4. L'ouvrage est daté d'une cinquantaine d'année : il est intéressant d'en prendre la distance historique : certaines revendications signalées par l'auteur sont devenus des réalités politiques (cf. changement climatique, danger de la surconsommation, etc).

Points faibles :

[71] `https://fr.wikipedia.org/wiki/Ivan_Illich`
[72] La version américaine de cet ouvrage a été publiée en 1973 par Harper & Row, New York, sous le titre : Tools for conviviality, dans la collection "World Perspectives" dirigée et présentéé par Ruth Nanda Anshen.
[73] (Submitted to) Archipel 2022 : risques systémiques, trajectoires et leviers d'action. Preprint. `http://polaris.imag.fr/romain.couillet/docs/articles/IAconviviale.pdf`

1. Certains chapitres me semblent être axés, non plus sur l'outil convivial mais sur la dénonciation des problèmes socio-politiques du début des années 1970. En un demi-siècle, des avancées ont été effectuées.
2. Certaines analyses socio-politiques faites à l'époque peuvent, à mon avis, devenir difficilement défendables dans une démocratie actuelle. Pour exemple, le soutien de l'auteur à la Chine dirigée à l'époque par le dictateur Mao Tsé-toung, doit, il me semble, être relativisé : il était peut-être limité au système des médecines aux pieds nus[74]. En effet, la chute du mur de Berlin a rappelé certaines conditions inhumaines en U.R.S.S. ou en Chine. Loin de nier les difficultés liés aux périodes décrites dans le livre, une mise-à-jour avec nos problèmes contemporains serait intéressante. Je vous en laisse juger par vous-même.

7 Annexes

Ces annexes contiennent
— les preuves de l'énoncé `prove { collinear P Q R }` du diagramme 3. Nous appelons cette preuve : "pappus1proof".
  1. utilisant la méthode des aires, activée par défaut ou avec l'option `-a` ;
  2. utilisant la méthode "Wu" (option `-w`) ;
  3. utilisant la méthode des "bases de Gröbner" (option `-g`).
— la preuve[75] de l'énoncé `prove { collinear A F F G }` du diagramme 21 avec la méthode des aires (par défaut ou avec `-a`). Nous appelons cette preuve : "trisect2proof".

7.1 GCLC Prover Output for conjecture "pappus1proof" - Area method used

Let r_0 be the number such that `PRATIO` $C\ A\ A\ B\ r_0$ (for the concrete example r_0=0.689983).
Let r_1 be the number such that `PRATIO` $F\ D\ D\ E\ r_1$ (for the concrete example r_1=0.851262).

$$s_{PQR} = 0 \quad \text{by the statement} \quad (0)$$

$$\frac{\left(\left(s_{ABD} \cdot s_{PQE}\right) + \left(-1 \cdot \left(s_{EBD} \cdot s_{PQA}\right)\right)\right)}{s_{ABED}} = 0 \quad \text{by Lemma 30 (point } R \text{ eliminated)} \quad (1)$$

$$\frac{\left(\left(s_{ABD} \cdot s_{EPQ}\right) + \left(-1 \cdot \left(s_{EBD} \cdot s_{APQ}\right)\right)\right)}{s_{ABED}} = 0 \quad \text{by geometric simplifications} \quad (2)$$

$$\left(\left(s_{ABD} \cdot s_{EPQ}\right) + \left(-1 \cdot \left(s_{EBD} \cdot s_{APQ}\right)\right)\right) = 0 \quad \text{by algebraic simplifications} \quad (3)$$

$$\left(\left(s_{ABD} \cdot \frac{\left(\left(s_{ACD} \cdot s_{EPF}\right) + \left(-1 \cdot \left(s_{FCD} \cdot s_{EPA}\right)\right)\right)}{s_{ACFD}}\right) + \left(-1 \cdot \left(s_{EBD} \cdot s_{APQ}\right)\right)\right) = 0 \quad \text{by Lemma 30 (point } Q \text{ eliminated)} \quad (4)$$

$$\left(\left(\left(s_{ABD} \cdot \left(s_{ACD} \cdot s_{EPF}\right)\right) + \left(-1 \cdot \left(s_{ABD} \cdot \left(s_{FCD} \cdot s_{EPA}\right)\right)\right)\right) + \left(-1 \cdot \left(s_{EBD} \cdot \left(s_{APQ} \cdot s_{ACFD}\right)\right)\right)\right) = 0 \quad \text{by algebraic simplifications} \quad (5)$$

$$\left(\left(\left(s_{ABD} \cdot \left(s_{ACD} \cdot s_{EPF}\right)\right) + \left(-1 \cdot \left(s_{ABD} \cdot \left(s_{FCD} \cdot s_{EPA}\right)\right)\right)\right) + \left(-1 \cdot \left(s_{EBD} \cdot \left(\frac{\left(\left(s_{ACD} \cdot s_{APF}\right) + \left(-1 \cdot \left(s_{FCD} \cdot 0\right)\right)\right)}{s_{ACFD}}\right)\right)\right)\right) = 0 \quad \text{by Lemma 30 (point } Q \text{ eliminated)} \quad (6)$$

$$\left(\left(\left(s_{ABD} \cdot \left(s_{ACD} \cdot s_{FEP}\right)\right) + \left(-1 \cdot \left(s_{ABD} \cdot \left(s_{FCD} \cdot s_{AEP}\right)\right)\right)\right) + \left(-1 \cdot \left(s_{EBD} \cdot \left(\frac{\left(\left(s_{ACD} \cdot s_{FAP}\right) + \left(-1 \cdot \left(s_{FCD} \cdot 0\right)\right)\right)}{s_{ACFD}}\right)\right)\right)\right) = 0 \quad \text{by geometric simplifications} \quad (7)$$

$$\left(\left(\left(s_{ABD} \cdot \left(s_{ACD} \cdot s_{FEP}\right)\right) + \left(-1 \cdot \left(s_{ABD} \cdot \left(s_{FCD} \cdot s_{AEP}\right)\right)\right)\right) + \left(-1 \cdot \left(s_{EBD} \cdot \left(s_{ACD} \cdot s_{FAP}\right)\right)\right)\right) = 0 \quad \text{by algebraic simplifications} \quad (8)$$

$$\left(\left(\left(s_{ABD} \cdot \left(s_{ACD} \cdot \frac{\left(\left(s_{BCE} \cdot s_{FEF}\right) + \left(-1 \cdot \left(s_{FCE} \cdot s_{FEB}\right)\right)\right)}{s_{BCFE}}\right)\right) + \left(-1 \cdot \left(s_{ABD} \cdot \left(s_{FCD} \cdot s_{AEP}\right)\right)\right)\right) + \left(-1 \cdot \left(s_{EBD} \cdot \left(s_{ACD} \cdot s_{FAP}\right)\right)\right)\right) = 0 \quad \text{by Lemma 30 (point } P \text{ eliminated)} \quad (9)$$

$$\left(\left(\left(s_{ABD} \cdot \left(s_{ACD} \cdot \frac{\left(\left(s_{BCE} \cdot 0\right) + \left(-1 \cdot \left(s_{FCE} \cdot s_{FEB}\right)\right)\right)}{s_{BCFE}}\right)\right) + \left(-1 \cdot \left(s_{ABD} \cdot \left(s_{FCD} \cdot s_{AEP}\right)\right)\right)\right) + \left(-1 \cdot \left(s_{EBD} \cdot \left(s_{ACD} \cdot s_{FAP}\right)\right)\right)\right) = 0 \quad \text{by geometric simplifications} \quad (10)$$

$$\left(\left(\left(s_{ABD} \cdot \left(s_{ACD} \cdot \left(s_{FCE} \cdot s_{FEB}\right)\right)\right) + \left(s_{ABD} \cdot \left(s_{FCD} \cdot \left(s_{AEP} \cdot s_{BCFE}\right)\right)\right)\right) + \left(s_{EBD} \cdot \left(s_{ACD} \cdot \left(s_{FAP} \cdot s_{BCFE}\right)\right)\right)\right) = 0 \quad \text{by algebraic simplifications} \quad (11)$$

$$\left(\left(\left(s_{ABD} \cdot \left(s_{ACD} \cdot \left(s_{FCE} \cdot s_{FEB}\right)\right)\right) + \left(s_{ABD} \cdot \left(s_{FCD} \cdot \left(\frac{\left(\left(s_{BCE} \cdot s_{AEF}\right) + \left(-1 \cdot \left(s_{FCE} \cdot s_{AEB}\right)\right)\right)}{s_{BCFE}} \cdot s_{BCFE}\right)\right)\right)\right) + \left(s_{EBD} \cdot \left(s_{ACD} \cdot \left(s_{FAP} \cdot s_{BCFE}\right)\right)\right)\right) = 0 \quad \text{by Lemma 30 (point } P \text{ eliminated)} \quad (12)$$

$$\left(\left(\left(s_{ABD} \cdot \left(s_{ACD} \cdot \left(s_{FCE} \cdot s_{FEB}\right)\right)\right) + \left(\left(s_{ABD} \cdot \left(s_{FCD} \cdot \left(s_{BCE} \cdot s_{AEF}\right)\right)\right) + \left(-1 \cdot \left(s_{ABD} \cdot \left(s_{FCD} \cdot \left(s_{FCE} \cdot s_{AEB}\right)\right)\right)\right)\right)\right) + \left(s_{EBD} \cdot \left(s_{ACD} \cdot \left(s_{FAP} \cdot s_{BCFE}\right)\right)\right)\right) = 0 \quad \text{by algebraic simplifications} \quad (13)$$

$$\left(\left(\left(s_{ABD} \cdot \left(s_{ACD} \cdot \left(s_{FCE} \cdot s_{FEB}\right)\right)\right) + \left(\left(s_{ABD} \cdot \left(s_{FCD} \cdot \left(s_{BCE} \cdot s_{AEF}\right)\right)\right) + \left(-1 \cdot \left(s_{ABD} \cdot \left(s_{FCD} \cdot \left(s_{FCE} \cdot s_{AEB}\right)\right)\right)\right)\right)\right) + \left(s_{EBD} \cdot \left(s_{ACD} \cdot \left(\frac{\left(\left(s_{BCE} \cdot s_{FAP}\right) + \left(-1 \cdot \left(s_{FCE} \cdot s_{AEB}\right)\right)\right)}{s_{BCFE}} \cdot s_{BCFE}\right)\right)\right)\right) = 0 \quad \text{by Lemma 30 (point } P \text{ eliminated)} \quad (14)$$

$$\left(\left(\left(s_{ABD} \cdot \left(s_{ACD} \cdot \left(s_{FCE} \cdot s_{FEB}\right)\right)\right) + \left(\left(s_{ABD} \cdot \left(s_{FCD} \cdot \left(s_{BCE} \cdot s_{AEF}\right)\right)\right) + \left(-1 \cdot \left(s_{ABD} \cdot \left(s_{FCD} \cdot \left(s_{FCE} \cdot s_{AEB}\right)\right)\right)\right)\right)\right) + \left(s_{EBD} \cdot \left(s_{ACD} \cdot \left(\frac{\left(\left(s_{BCE} \cdot 0\right) + \left(-1 \cdot \left(s_{FCE} \cdot s_{AEB}\right)\right)\right)}{s_{BCFE}} \cdot s_{BCFE}\right)\right)\right)\right) = 0 \quad \text{by geometric simplifications} \quad (15)$$

[74] `https://fr.wikipedia.org/wiki/M%C3%A9decins_aux_pieds_nus`
[75] Etant donné la longueur de certaine expression, la mise en page est incorrecte. La preuve est donnée à titre indicative.

$(((S_{ABD} \cdot (S_{ACD} \cdot (S_{FCE} \cdot S_{FEB}))) + ((S_{ABD} \cdot (S_{FCD} \cdot (S_{BCE} \cdot S_{AEF}))) + (-1 \cdot (S_{ABD} \cdot (S_{FCD} \cdot (S_{CEF} \cdot S_{AEB}))))) + (-1 \cdot (S_{ABD} \cdot (S_{ACD} \cdot (S_{FCE} \cdot S_{FA}$			by algebraic simplifications (15)
$(((S_{ABD} \cdot (S_{ACD} \cdot (S_{CEF} \cdot S_{EBF}))) + ((S_{ABD} \cdot (S_{CDF} \cdot (S_{BCE} \cdot S_{AEF}))) + (-1 \cdot (S_{ABD} \cdot (S_{CDF} \cdot (S_{CEF} \cdot S_{AEB}))))) + (-1 \cdot (S_{ABD} \cdot (S_{ACD} \cdot (S_{CEF} \cdot S_{AB}$			by geometric simplifications (17)
$(((S_{ABD} \cdot (S_{ACD} \cdot ((S_{CED} + (r_1 \cdot (S_{CEE} + (-1 \cdot S_{CED})))) \cdot S_{EBF}))) + ((S_{ABD} \cdot (S_{CDF} \cdot (S_{BCE} \cdot S_{AEF}))) + (-1 \cdot (S_{ABD} \cdot (S_{CDF} \cdot (S_{CEF} \cdot S_{AEB}))))) + (-1 \cdot$			by Lemma 29 (point F eliminated) (18)
$(((S_{ABD} \cdot (S_{ACD} \cdot ((S_{CED} + (r_1 \cdot (0 + (-1 \cdot S_{CED})))) \cdot S_{EBF}))) + ((S_{ABD} \cdot (S_{CDF} \cdot (S_{BCE} \cdot S_{AEF}))) + (-1 \cdot (S_{ABD} \cdot (S_{CDF} \cdot (S_{CEF} \cdot S_{AEB}))))) + (-1 \cdot (S_{E}$			by geometric simplifications (19)
$((((S_{ABD} \cdot (S_{ACD} \cdot (S_{EBF} \cdot S_{CED}))) + (-1 \cdot (S_{ABD} \cdot (S_{ACD} \cdot (S_{EBF} \cdot (r_1 \cdot S_{CED})))))) + ((S_{ABD} \cdot (S_{CDF} \cdot (S_{BCE} \cdot S_{AEF}))) + (-1 \cdot (S_{ABD} \cdot (S_{CDF} \cdot (S_{CEF}$			by algebraic simplifications (20)
$((((S_{ABD} \cdot (S_{ACD} \cdot ((S_{EBD} + (r_1 \cdot (S_{EBE} + (-1 \cdot S_{EBD})))) \cdot S_{CED}))) + (-1 \cdot (S_{ABD} \cdot (S_{ACD} \cdot (S_{EBF} \cdot (r_1 \cdot S_{CED})))))) + ((S_{ABD} \cdot (S_{CDF} \cdot (S_{BCE} \cdot S_{AEF}))) +$			by Lemma 29 (point F eliminated) (21)
$((((S_{ABD} \cdot (S_{ACD} \cdot ((S_{EBD} + (r_1 \cdot (0 + (-1 \cdot S_{EBD})))) \cdot S_{CED}))) + (-1 \cdot (S_{ABD} \cdot (S_{ACD} \cdot (S_{EBF} \cdot (r_1 \cdot S_{CED})))))) + ((S_{ABD} \cdot (S_{CDF} \cdot (S_{BCE} \cdot S_{AEF}))) + (-1$			by geometric simplifications (22)
$(((((S_{ABD} \cdot (S_{ACD} \cdot (S_{CED} \cdot S_{EBD}))) + (-1 \cdot (S_{ABD} \cdot (S_{ACD} \cdot (S_{CED} \cdot (r_1 \cdot S_{EBD})))))) + (-1 \cdot (S_{ABD} \cdot (S_{ACD} \cdot (S_{EBF} \cdot (r_1 \cdot S_{CED})))))) + ((S_{ABD} \cdot (S_{CDF} \cdot$			by algebraic simplifications (23)
$(((((S_{ABD} \cdot (S_{ACD} \cdot (S_{CED} \cdot S_{EBD}))) + (-1 \cdot (S_{ABD} \cdot (S_{ACD} \cdot (S_{CED} \cdot (r_1 \cdot S_{EBD})))))) + (-1 \cdot (S_{ABD} \cdot (S_{ACD} \cdot ((S_{EBD} + (r_1 \cdot (S_{EBE} + (-1 \cdot S_{EBD})))) \cdot (r_1 \cdot$			by Lemma 29 (point F eliminated) (24)
$(((((S_{ABD} \cdot (S_{ACD} \cdot (S_{CED} \cdot S_{EBD}))) + (-1 \cdot (S_{ABD} \cdot (S_{ACD} \cdot (S_{CED} \cdot (r_1 \cdot S_{EBD})))))) + (-1 \cdot (S_{ABD} \cdot (S_{ACD} \cdot ((S_{EBD} + (r_1 \cdot (0 + (-1 \cdot S_{EBD})))) \cdot (r_1 \cdot S_{CE$			by geometric simplifications (25)
$(((((S_{ABD} \cdot (S_{ACD} \cdot (S_{CED} \cdot S_{EBD}))) + (-2 \cdot (S_{ABD} \cdot (S_{ACD} \cdot (S_{CED} \cdot (r_1 \cdot S_{EBD})))))) + (S_{ABD} \cdot (S_{ACD} \cdot (r_1 \cdot (S_{CED} \cdot (r_1 \cdot S_{EBD})))))) + ((S_{ABD} \cdot (S_{CDF} \cdot$			by algebraic simplifications (26)
$(((((S_{ABD} \cdot (S_{ACD} \cdot (S_{CED} \cdot S_{EBD}))) + (-2 \cdot (S_{ABD} \cdot (S_{ACD} \cdot (S_{CED} \cdot (r_1 \cdot S_{EBD})))))) + (S_{ABD} \cdot (S_{ACD} \cdot (r_1 \cdot (S_{CED} \cdot (r_1 \cdot S_{EBD})))))) + ((S_{ABD} \cdot ((S_{CDD} \cdot$			by Lemma 29 (point F eliminated) (27)
$(((((S_{ABD} \cdot (S_{ACD} \cdot (S_{CED} \cdot S_{EBD}))) + (-2 \cdot (S_{ABD} \cdot (S_{ACD} \cdot (S_{CED} \cdot (r_1 \cdot S_{EBD})))))) + (S_{ABD} \cdot (S_{ACD} \cdot (r_1 \cdot (S_{CED} \cdot (r_1 \cdot S_{EBD})))))) + ((S_{ABD} \cdot ((0 + (r_1 \cdot$			by geometric simplifications (28)
$(((((S_{ABD} \cdot (S_{ACD} \cdot (S_{CED} \cdot S_{EBD}))) + (-2 \cdot (S_{ABD} \cdot (S_{ACD} \cdot (S_{CED} \cdot (r_1 \cdot S_{EBD})))))) + (S_{ABD} \cdot (S_{ACD} \cdot (r_1 \cdot (S_{CED} \cdot (r_1 \cdot S_{EBD})))))) + ((-1 \cdot (S_{ABD} \cdot (r_1 \cdot$			by algebraic simplifications (29)
$(((((S_{ABD} \cdot (S_{ACD} \cdot (S_{CED} \cdot S_{EBD}))) + (-2 \cdot (S_{ABD} \cdot (S_{ACD} \cdot (S_{CED} \cdot (r_1 \cdot S_{EBD})))))) + (S_{ABD} \cdot (S_{ACD} \cdot (r_1 \cdot (S_{CED} \cdot (r_1 \cdot S_{EBD})))))) + ((-1 \cdot (S_{ABD} \cdot (r_1 \cdot$			by Lemma 29 (point F eliminated) (30)
$(((((S_{ABD} \cdot (S_{ACD} \cdot (S_{CED} \cdot S_{EBD}))) + (-2 \cdot (S_{ABD} \cdot (S_{ACD} \cdot (S_{CED} \cdot (r_1 \cdot S_{EBD})))))) + (S_{ABD} \cdot (S_{ACD} \cdot (r_1 \cdot (S_{CED} \cdot (r_1 \cdot S_{EBD})))))) + ((-1 \cdot (S_{ABD} \cdot (r_1 \cdot$			by geometric simplifications (31)
$(((((S_{ABD} \cdot (S_{ACD} \cdot (S_{CED} \cdot S_{EBD}))) + (-2 \cdot (S_{ABD} \cdot (S_{ACD} \cdot (S_{CED} \cdot (r_1 \cdot S_{EBD})))))) + (S_{ABD} \cdot (S_{ACD} \cdot (r_1 \cdot (S_{CED} \cdot (r_1 \cdot S_{EBD})))))) + (((-1 \cdot (S_{ABD} \cdot (r_1 \cdot$			by algebraic simplifications (32)
$(((((S_{ABD} \cdot (S_{ACD} \cdot (S_{CED} \cdot S_{EBD}))) + (-2 \cdot (S_{ABD} \cdot (S_{ACD} \cdot (S_{CED} \cdot (r_1 \cdot S_{EBD})))))) + (S_{ABD} \cdot (S_{ACD} \cdot (r_1 \cdot (S_{CED} \cdot (r_1 \cdot S_{EBD})))))) + (((-1 \cdot (S_{ABD} \cdot (r_1 \cdot$			by Lemma 29 (point F eliminated) (33)
$(((((S_{ABD} \cdot (S_{ACD} \cdot (S_{CED} \cdot S_{EBD}))) + (-2 \cdot (S_{ABD} \cdot (S_{ACD} \cdot (S_{CED} \cdot (r_1 \cdot S_{EBD})))))) + (S_{ABD} \cdot (S_{ACD} \cdot (r_1 \cdot (S_{CED} \cdot (r_1 \cdot S_{EBD})))))) + (((-1 \cdot (S_{ABD} \cdot (r_1 \cdot$			by geometric simplifications (34)
$(((((S_{ABD} \cdot (S_{ACD} \cdot (S_{CED} \cdot S_{EBD}))) + (-2 \cdot (S_{ABD} \cdot (S_{ACD} \cdot (S_{CED} \cdot (r_1 \cdot S_{EBD})))))) + (S_{ABD} \cdot (S_{ACD} \cdot (r_1 \cdot (S_{CED} \cdot (r_1 \cdot S_{EBD})))))) + (((-1 \cdot (S_{ABD} \cdot (r_1 \cdot$			by algebraic simplifications (35)
$(((((S_{ABD} \cdot (S_{ACD} \cdot (S_{CED} \cdot S_{EBD}))) + (-2 \cdot (S_{ABD} \cdot (S_{ACD} \cdot (S_{CED} \cdot (r_1 \cdot S_{EBD})))))) + (S_{ABD} \cdot (S_{ACD} \cdot (r_1 \cdot (S_{CED} \cdot (r_1 \cdot S_{EBD})))))) + (((-1 \cdot (S_{ABD} \cdot (r_1 \cdot$			by Lemma 29 (point F eliminated) (36)
$(((((S_{ABD} \cdot (S_{ACD} \cdot (S_{CED} \cdot S_{EBD}))) + (-2 \cdot (S_{ABD} \cdot (S_{ACD} \cdot (S_{CED} \cdot (r_1 \cdot S_{EBD})))))) + (S_{ABD} \cdot (S_{ACD} \cdot (r_1 \cdot (S_{CED} \cdot (r_1 \cdot S_{EBD})))))) + (((-1 \cdot (S_{ABD} \cdot (r_1 \cdot$			by geometric simplifications (37)
$(((((S_{ABD} \cdot (S_{ACD} \cdot (S_{CED} \cdot S_{EBD}))) + (-2 \cdot (S_{ABD} \cdot (S_{ACD} \cdot (S_{CED} \cdot (r_1 \cdot S_{EBD})))))) + (S_{ABD} \cdot (S_{ACD} \cdot (r_1 \cdot (S_{CED} \cdot (r_1 \cdot S_{EBD})))))) + (((-1 \cdot (S_{ABD} \cdot (r_1 \cdot$			by algebraic simplifications (38)
$(((((S_{ABD} \cdot (S_{ACD} \cdot (S_{CED} \cdot S_{EBD}))) + (-2 \cdot (S_{ABD} \cdot (S_{ACD} \cdot (S_{CED} \cdot (r_1 \cdot S_{EBD})))))) + (S_{ABD} \cdot (S_{ACD} \cdot (r_1 \cdot (S_{CED} \cdot (r_1 \cdot S_{EBD})))))) + (((-1 \cdot (S_{ABD} \cdot (r_1 \cdot$			by Lemma 29 (point F eliminated) (39)
$(((((S_{ABD} \cdot (S_{ACD} \cdot (S_{CED} \cdot S_{EBD}))) + (-2 \cdot (S_{ABD} \cdot (S_{ACD} \cdot (S_{CED} \cdot (r_1 \cdot S_{EBD})))))) + (S_{ABD} \cdot (S_{ACD} \cdot (r_1 \cdot (S_{CED} \cdot (r_1 \cdot S_{EBD})))))) + (((-1 \cdot (S_{ABD} \cdot (r_1 \cdot$			by geometric simplifications (40)
$(((((S_{ABD} \cdot (S_{ACD} \cdot S_{EBD})) + (-2 \cdot (S_{ABD} \cdot (S_{ACD} \cdot (r_1 \cdot S_{EBD}))))) + (S_{ABD} \cdot (S_{ACD} \cdot (r_1 \cdot (r_1 \cdot S_{EBD}))))) + (((-1 \cdot (S_{ABD} \cdot (r_1 \cdot (S_{BCE} \cdot S_{AED})))) + (S_{ABD} \cdot$			by algebraic simplifications (41)
$(((((S_{ABD} \cdot (S_{ACD} \cdot S_{EBD})) + (-2 \cdot (S_{ABD} \cdot (S_{ACD} \cdot (r_1 \cdot S_{EBD}))))) + (S_{ABD} \cdot (S_{ACD} \cdot (r_1 \cdot (r_1 \cdot S_{EBD}))))) + (((-1 \cdot (S_{ABD} \cdot (r_1 \cdot (S_{BCE} \cdot S_{AED})))) + (S_{ABD} \cdot$			by Lemma 29 (point F eliminated) (42)
$(((((S_{ABD} \cdot (S_{ACD} \cdot S_{EBD})) + (-2 \cdot (S_{ABD} \cdot (S_{ACD} \cdot (r_1 \cdot S_{EBD}))))) + (S_{ABD} \cdot (S_{ACD} \cdot (r_1 \cdot (r_1 \cdot S_{EBD}))))) + (((-1 \cdot (S_{ABD} \cdot (r_1 \cdot (S_{BCE} \cdot S_{AED})))) + (S_{ABD} \cdot$			by geometric simplifications (43)
$((((-1 \cdot (S_{ABD} \cdot (S_{ACD} \cdot S_{EBD}))) + (S_{ABD} \cdot (S_{ACD} \cdot (r_1 \cdot S_{EBD})))) + (((-1 \cdot (S_{ABD} \cdot (S_{BCE} \cdot S_{AED})))) + (S_{ABD} \cdot (S_{AEB} \cdot$			by algebraic simplifications (44)
$((((-1 \cdot (S_{ABD} \cdot (S_{ACD} \cdot S_{EBD}))) + (S_{ABD} \cdot (S_{ACD} \cdot (r_1 \cdot S_{EBD})))) + (((-1 \cdot (S_{ABD} \cdot (S_{BCE} \cdot S_{AED})))) + (S_{ABD} \cdot (S_{AEB} \cdot$			by Lemma 29 (point F eliminated) (45)
$((((-1 \cdot (S_{ABD} \cdot (S_{ACD} \cdot S_{EBD}))) + (S_{ABD} \cdot (S_{ACD} \cdot (r_1 \cdot S_{EBD})))) + (((-1 \cdot (S_{ABD} \cdot (S_{BCE} \cdot S_{AED})))) + (S_{ABD} \cdot (S_{AEB} \cdot$			by Symmetric simplifications (46)
$((((-1 \cdot (S_{ABD} \cdot (S_{BCE} \cdot S_{AED}))) + (S_{ABD} \cdot (S_{BCE} \cdot (r_1 \cdot S_{AED})))) + ((S_{ABD} \cdot (S_{AEB} \cdot S_{CED})) + (-1 \cdot (S_{ABD} \cdot (S_{AEB} \cdot$			by algebraic simplifications (47)
$((((-1 \cdot (S_{ABD} \cdot (S_{EBC} \cdot S_{AED}))) + (S_{ABD} \cdot (S_{EBC} \cdot (r_1 \cdot S_{AED})))) + ((S_{ABD} \cdot (S_{AEB} \cdot S_{EDC})) + (-1 \cdot (S_{ABD} \cdot (S_{AEB} \cdot$			by geometric simplifications (48)
$((((-1 \cdot (S_{ABD} \cdot ((S_{EBA} + (r_0 \cdot (S_{EBB} + (-1 \cdot S_{EBA})))) \cdot S_{AED}))) + (S_{ABD} \cdot (S_{EBC} \cdot (r_1 \cdot S_{AED})))) + ((S_{ABD} \cdot (S_{AEB} \cdot S_{EDC})) + (-1 \cdot (S_{ABD} \cdot (S_{AEB} \cdot (r_1 \cdot$			by Lemma 29 (point C eliminated) (49)
$((((-1 \cdot (S_{ABD} \cdot ((S_{EBA} + (r_0 \cdot (0 + (-1 \cdot S_{EBA})))) \cdot S_{AED}))) + (S_{ABD} \cdot (S_{EBC} \cdot (r_1 \cdot S_{AED})))) + ((S_{ABD} \cdot (S_{AEB} \cdot S_{EDC})) + (-1 \cdot (S_{ABD} \cdot (S_{EBA} \cdot (r_1 \cdot S_{EDC}$			by geometric simplifications (50)
$((((-1 \cdot (S_{ABD} \cdot (S_{AED} \cdot S_{EBA}))) + (S_{ABD} \cdot (S_{AED} \cdot (r_0 \cdot S_{EBA})))) + (S_{ABD} \cdot (S_{EBC} \cdot (r_1 \cdot S_{AED})))) + ((S_{ABD} \cdot (S_{EBA} \cdot S_{EDC})) + (-1 \cdot (S_{ABD} \cdot (S_{EBA} \cdot (r_1 \cdot$			by Algebraic Simplifications (51)
$((((-1 \cdot (S_{ABD} \cdot (S_{AED} \cdot S_{EBA}))) + (S_{ABD} \cdot (S_{AED} \cdot (r_0 \cdot S_{EBA})))) + (S_{ABD} \cdot ((S_{EBA} + (r_0 \cdot (S_{EBB} + (-1 \cdot S_{EBA})))) \cdot (r_1 \cdot S_{AED})))) + ((S_{ABD} \cdot (S_{EBA} \cdot S_{E}$			by Lemma 29 (point C eliminated) (52)
$((((-1 \cdot (S_{ABD} \cdot (S_{AED} \cdot S_{EBA}))) + (S_{ABD} \cdot (S_{AED} \cdot (r_0 \cdot S_{EBA})))) + (S_{ABD} \cdot ((S_{EBA} + (r_0 \cdot (0 + (-1 \cdot S_{EBA})))) \cdot (r_1 \cdot S_{AED})))) + ((S_{ABD} \cdot (S_{EBA} \cdot S_{EDC})) +$			by geometric simplifications (53)
$((((-1 \cdot (S_{ABD} \cdot S_{AED})) + (S_{ABD} \cdot (S_{AED} \cdot r_0))) + ((S_{ABD} \cdot (r_1 \cdot S_{AED})) + (-1 \cdot (S_{ABD} \cdot (r_1 \cdot (S_{AED} \cdot r_0)))))) + ((S_{ABD} \cdot (S_{EDA} + (r_0 \cdot (S_{EDB} + (-1 \cdot$			by algebraic simplifications (54)
$((((-1 \cdot (S_{ABD} \cdot S_{AED})) + (S_{ABD} \cdot (S_{AED} \cdot r_0))) + ((S_{ABD} \cdot (r_1 \cdot S_{AED})) + (-1 \cdot (S_{ABD} \cdot (r_1 \cdot (S_{AED} \cdot r_0)))))) + ((S_{ABD} \cdot (S_{EDA} + (r_0 \cdot (S_{EDB} + (-1 \cdot$			by Lemma 29 (point C eliminated) (55)
$((((-1 \cdot (S_{ABD} \cdot S_{AED})) + (S_{ABD} \cdot (S_{AED} \cdot r_0))) + ((S_{ABD} \cdot (r_1 \cdot S_{AED})) + (-1 \cdot (S_{ABD} \cdot (r_1 \cdot (S_{AED} \cdot r_0)))))) + ((S_{ABD} \cdot (S_{EDA} + (r_0 \cdot (S_{EDB} + (-1 \cdot S_{AED}$			by Symmetric simplifications (56)
$((((S_{ABD} \cdot (r_1 \cdot S_{AED})) + (-1 \cdot (S_{ABD} \cdot (r_1 \cdot (S_{AED} \cdot r_0))))) + ((S_{ABD} \cdot (r_0 \cdot S_{EDB})) + (-1 \cdot (S_{ABD} \cdot (r_1 \cdot S_{EBD}))))) + ((S_{EDB} \cdot (S_{DAC})) + (S_{EDB} \cdot (S_{DAC}$			by algebraic simplifications (57)
$((((S_{ABD} \cdot (r_1 \cdot S_{AED})) + (-1 \cdot (S_{ABD} \cdot (r_1 \cdot (S_{AED} \cdot r_0))))) + ((S_{ABD} \cdot (r_0 \cdot S_{EDB})) + (-1 \cdot (S_{ABD} \cdot (r_1 \cdot S_{EBD}))))) + ((S_{EDB} \cdot (S_{DAA} + (r_0 \cdot (S_{EDB} + (-1 \cdot$			by Lemma 29 (point C eliminated) (58)
$((((S_{ABD} \cdot (r_1 \cdot S_{AED})) + (-1 \cdot (S_{ABD} \cdot (r_1 \cdot (S_{AED} \cdot r_0))))) + ((S_{ABD} \cdot (r_0 \cdot S_{EDB})) + (-1 \cdot (S_{ABD} \cdot (r_1 \cdot S_{EBD}))))) + ((S_{EDB} \cdot (S_{DAA} + (r_0 \cdot (S_{EDB} + (-1 \cdot$			by Symmetric simplifications (59)
$(((S_{ABD} \cdot r_0) + (-1 \cdot (S_{ABD} \cdot (r_1 \cdot r_0)))) + ((-1 \cdot S_{DAC}) + (S_{DAC} \cdot r_1)))$			by algebraic simplifications (60)
$(((S_{ABD} \cdot r_0) + (-1 \cdot (S_{ABD} \cdot (r_1 \cdot r_0)))) + ((-1 \cdot S_{DAA}) + (r_0 \cdot (S_{DAB} + (-1 \cdot S_{DAA})))) + (S_{DAC} \cdot r_1)))$			by Lemma 29 (point C eliminated) (61)
$(((S_{ABD} \cdot r_0) + (-1 \cdot (S_{ABD} \cdot (r_1 \cdot r_0)))) + ((-1 \cdot (0 + (r_0 \cdot (S_{ABD} + (-1 \cdot 0))))) + (S_{DAC} \cdot r_1)))$			by geometric simplifications (62)
$((-1 \cdot (S_{ABD} \cdot r_0)) + S_{DAC})$	$=$	0	by algebraic simplifications (63)
$((-1 \cdot (S_{ABD} \cdot r_0)) + (S_{DAA} + (r_0 \cdot (S_{DAB} + (-1 \cdot S_{DAA})))))$			by Lemma 29 (point C eliminated) (64)
$((-1 \cdot (S_{ABD} \cdot r_0)) + (0 + (r_0 \cdot (S_{ABD} + (-1 \cdot 0)))))$	$=$	0	by geometric simplifications (65)
0	$=$	0	by algebraic simplifications (66)

Q.E.D.

NDG conditions are :
$S_{BCE} \neq S_{FCE}$ i.e., lines BF and CE are not parallel (construction based assumption)
$S_{ACD} \neq S_{FCD}$ i.e., lines AF and CD are not parallel (construction based assumption)
$S_{ABD} \neq S_{EBD}$ i.e., lines AE and BD are not parallel (construction based assumption)
$S_{CED} \neq 0$ i.e., points C, E and D are not collinear (cancellation assumption)
$r_1 \neq 0$ i.e., constant r_1 is non-zero (cancellation assumption)
$S_{EBA} \neq 0$ i.e., points E, B and A are not collinear (cancellation assumption)
$S_{EDB} \neq 0$ i.e., points E, D and B are not collinear (cancellation assumption)

Number of elimination proof steps : 23
Number of geometric proof steps : 54
Number of algebraic proof steps : 274
Total number of proof steps : 351
Time spent by the prover : 0.007 seconds

7.2 GCLC Prover Output for conjecture "pappus1proof" - Wu's method used

7.2.1 Construction and prover internal state

Construction commands :

— Point A
— Point B
— Random point on line, C : A B 0.943061
— Point D
— Point E
— Random point on line, F : D E 0.744397
— Line lAE : A E
— Line lAF : A F
— Line lBD : B D
— Line lBF : B F
— Line lCD : C D
— Line lCE : C E
— Intersection of lines, P : lBF lCE
— Intersection of lines, Q : lAF lCD
— Intersection of lines, R : lAE lBD

Coordinates assigned to the points :

— $A = (0, 0)$
— $B = (u_1, 0)$
— $C = (u_8, 0)$
— $D = (u_3, u_4)$
— $E = (u_5, u_6)$
— $F = (x_2, u_7)$
— $P = (x_4, x_3)$
— $Q = (x_6, x_5)$
— $R = (x_8, x_7)$

Conjecture(s) :

1. Given conjecture
   — **GCLC code :**
   ```
   collinear P Q R
   ```
   — **Expression :**

$collinear(P, Q, R)$

7.2.2 Resolving constructed lines

— $AB \ni A, B, C$; line is horizontal (i.e., $y(A) = y(B)$) ; line is generated by the prover
— $DE \ni D, E, F$; line is generated by the prover
— $lAE \ni A, E, R$
— $lAF \ni A, F, Q$
— $lBD \ni B, D, R$
— $lBF \ni B, F, P$
— $lCD \ni C, D, Q$
— $lCE \ni C, E, P$

7.2.3 Creating polynomials from hypotheses

— Point A
no condition
— Point B
no condition
— Random point on line, $C : A\ B$ 0.943061
— point C is on the line (A, B) — true by the construction
no condition
— Point D
no condition
— Point E
no condition
— Random point on line, $F : D\ E$ 0.744397
— point F is on the line (D, E)

$$p_1 = (-u_6 + u_4)x_2 + (u_7u_5 - u_7u_3 + u_6u_3 - u_5u_4)$$

— Line $lAE : A\ E$
— point A is on the line (A, E)
no condition
— point E is on the line (A, E)
no condition
— Line $lAF : A\ F$
— point A is on the line (A, F)
no condition
— point F is on the line (A, F)
no condition
— Line $lBD : B\ D$
— point B is on the line (B, D)
no condition
— point D is on the line (B, D)
no condition
— Line $lBF : B\ F$
— point B is on the line (B, F)
no condition
— point F is on the line (B, F)
no condition
— Line $lCD : C\ D$
— point C is on the line (C, D)
no condition
— point D is on the line (C, D)
no condition
— Line $lCE : C\ E$
— point C is on the line (C, E)
no condition

— point E is on the line (C, E)
no condition
— Intersection of lines, $P : lBF\ lCE$
— point P is on the line (B, F)

$$p_2 = -u_7x_4 + x_3x_2 - u_1x_3 + u_7u_1$$

— point P is on the line (C, E)

$$p_3 = -u_6x_4 + (-u_8 + u_5)x_3 + u_8u_6$$

— Intersection of lines, $Q : lAF\ lCD$
— point Q is on the line (A, F)

$$p_4 = -u_7x_6 + x_5x_2$$

— point Q is on the line (C, D)

$$p_5 = -u_4x_6 + (-u_8 + u_3)x_5 + u_8u_4$$

— Intersection of lines, $R : lAE\ lBD$
— point R is on the line (A, E)

$$p_6 = -u_6x_8 + u_5x_7$$

— point R is on the line (B, D)

$$p_7 = -u_4x_8 + (u_3 - u_1)x_7 + u_4u_1$$

7.2.4 Creating polynomial from the conjecture

— Processing given conjecture(s).
— point P is on the line (Q, R)

$$p_8 = -x_8x_5 + x_8x_3 + x_7x_6 - x_7x_4 - x_6x_3 + x_5x_4$$

Conjecture 1 :

$$p_9 = -x_8x_5 + x_8x_3 + x_7x_6 - x_7x_4 - x_6x_3 + x_5x_4$$

7.2.5 Invoking the theorem prover

The used proving method is Wu's method.
The input system is :

$$\begin{aligned}
p_0 &= (-u_6 + u_4)x_2 + (u_7u_5 - u_7u_3 + u_6u_3 - u_5u_4)\\
p_1 &= -u_7x_4 + x_3x_2 - u_1x_3 + u_7u_1\\
p_2 &= -u_6x_4 + (-u_8 + u_5)x_3 + u_8u_6\\
p_3 &= -u_7x_6 + x_5x_2\\
p_4 &= -u_4x_6 + (-u_8 + u_3)x_5 + u_8u_4\\
p_5 &= -u_6x_8 + u_5x_7\\
p_6 &= -u_4x_8 + (u_3 - u_1)x_7 + u_4u_1
\end{aligned}$$

Triangulation, step 1

Choosing variable : Trying the variable with index 8.

Variable x_8 selected : The number of polynomials with this variable is 2.

Minimal degrees : 6 polynomials with degree 1 and 5 polynomials with degree 1.

Polynomial with linear degree : Removing variable x_8 from all other polynomials by reducing them with polynomial p_6.

Finished a triangulation step, the current system is :

$$\begin{aligned}
p_0 &= (-u_6+u_4)x_2+(u_7u_5-u_7u_3+u_6u_3-u_5u_4)\\
p_1 &= -u_7x_4+x_3x_2-u_1x_3+u_7u_1\\
p_2 &= -u_6x_4+(-u_8+u_5)x_3+u_8u_6\\
p_3 &= -u_7x_6+x_5x_2\\
p_4 &= -u_4x_6+(-u_8+u_3)x_5+u_8u_4\\
p_5 &= (u_6u_3-u_6u_1-u_5u_4)x_7+u_6u_4u_1\\
p_6 &= -u_4x_8+(u_3-u_1)x_7+u_4u_1
\end{aligned}$$

Triangulation, step 2

Choosing variable : Trying the variable with index 7.

Variable x_7 selected : The number of polynomials with this variable is 1.

Single polynomial with chosen variable : No reduction needed.

The triangular system has not been changed.

Triangulation, step 3

Choosing variable : Trying the variable with index 6.

Variable x_6 selected : The number of polynomials with this variable is 2.

Minimal degrees : 4 polynomials with degree 1 and 3 polynomials with degree 1.

Polynomial with linear degree : Removing variable x_6 from all other polynomials by reducing them with polynomial p_4.

Finished a triangulation step, the current system is :

$$\begin{aligned}
p_0 &= (-u_6+u_4)x_2+(u_7u_5-u_7u_3+u_6u_3-u_5u_4)\\
p_1 &= -u_7x_4+x_3x_2-u_1x_3+u_7u_1\\
p_2 &= -u_6x_4+(-u_8+u_5)x_3+u_8u_6\\
p_3 &= -u_4x_5x_2+(-u_8u_7+u_7u_3)x_5+u_8u_7u_4\\
p_4 &= -u_4x_6+(-u_8+u_3)x_5+u_8u_4\\
p_5 &= (u_6u_3-u_6u_1-u_5u_4)x_7+u_6u_4u_1\\
p_6 &= -u_4x_8+(u_3-u_1)x_7+u_4u_1
\end{aligned}$$

Triangulation, step 4

Choosing variable : Trying the variable with index 5.

Variable x_5 selected : The number of polynomials with this variable is 1.

Single polynomial with chosen variable : No reduction needed.

The triangular system has not been changed.

Triangulation, step 5

Choosing variable : Trying the variable with index 4.

Variable x_4 selected : The number of polynomials with this variable is 2.

Minimal degrees : 2 polynomials with degree 1 and 1 polynomials with degree 1.

Polynomial with linear degree : Removing variable x_4 from all other polynomials by reducing them with polynomial p_2.

Finished a triangulation step, the current system is :

$$
\begin{aligned}
p_0 &= (-u_6+u_4)x_2+(u_7u_5-u_7u_3+u_6u_3-u_5u_4)\\
p_1 &= -u_6x_3x_2+(-u_8u_7+u_7u_5+u_6u_1)x_3+(u_8u_7u_6-u_7u_6u_1)\\
p_2 &= -u_6x_4+(-u_8+u_5)x_3+u_8u_6\\
p_3 &= -u_4x_5x_2+(-u_8u_7+u_7u_3)x_5+u_8u_7u_4\\
p_4 &= -u_4x_6+(-u_8+u_3)x_5+u_8u_4\\
p_5 &= (u_6u_3-u_6u_1-u_5u_4)x_7+u_6u_4u_1\\
p_6 &= -u_4x_8+(u_3-u_1)x_7+u_4u_1
\end{aligned}
$$

Triangulation, step 6

Choosing variable : Trying the variable with index 3.

Variable x_3 selected : The number of polynomials with this variable is 1.

Single polynomial with chosen variable : No reduction needed.

The triangular system has not been changed.

Triangulation, step 7

Choosing variable : Trying the variable with index 2.

Variable x_2 selected : The number of polynomials with this variable is 1.

Single polynomial with chosen variable : No reduction needed.

The triangular system has not been changed.

The triangular system is :

$$
\begin{aligned}
p_0 &= (-u_6+u_4)x_2+(u_7u_5-u_7u_3+u_6u_3-u_5u_4)\\
p_1 &= -u_6x_3x_2+(-u_8u_7+u_7u_5+u_6u_1)x_3+(u_8u_7u_6-u_7u_6u_1)\\
p_2 &= -u_6x_4+(-u_8+u_5)x_3+u_8u_6\\
p_3 &= -u_4x_5x_2+(-u_8u_7+u_7u_3)x_5+u_8u_7u_4\\
p_4 &= -u_4x_6+(-u_8+u_3)x_5+u_8u_4\\
p_5 &= (u_6u_3-u_6u_1-u_5u_4)x_7+u_6u_4u_1\\
p_6 &= -u_4x_8+(u_3-u_1)x_7+u_4u_1
\end{aligned}
$$

7.2.6 Final remainder

Final remainder for conjecture 1 Calculating final remainder of the conclusion :

$$g=-x_8x_5+x_8x_3+x_7x_6-x_7x_4-x_6x_3+x_5x_4$$

with respect to the triangular system.

1. Pseudo remainder with p_6 over variable x_8 :

$$g=-u_4x_7x_6+(u_3-u_1)x_7x_5+u_4x_7x_4+$$

$$(-u_3+u_1)x_7x_3+u_4x_6x_3-u_4x_5x_4+u_4u_1x_5-u_4u_1x_3$$

2. Pseudo remainder with p_5 over variable x_7 :

$$g=(u_6u_4u_3-u_6u_4u_1-u_5u_4^2)x_6x_3+u_6u_4^2u_1x_6+$$

$$(-u_6u_4u_3+u_6u_4u_1+u_5u_4^2)x_5x_4-u_5u_4^2u_1x_5-u_6u_4^2u_1x_4+$$

$$u_5u_4^2u_1x_3$$

3. Pseudo remainder with p_4 over variable x_6 :

$$g = (u_6u_4^2u_3 - u_6u_4^2u_1 - u_5u_4^3)x_5x_4+$$
$$(u_8u_6u_4u_3 - u_8u_6u_4u_1 - u_8u_5u_4^2 - u_6u_4u_3^2 + u_6u_4u_3u_1+$$
$$u_5u_4^2u_3)x_5x_3+$$
$$(u_8u_6u_4^2u_1 - u_6u_4^2u_3u_1 + u_5u_4^3u_1)x_5 + u_6u_4^3u_1x_4+$$
$$(-u_8u_6u_4^2u_3 + u_8u_6u_4^2u_1 + u_8u_5u_4^3 - u_5u_4^3u_1)x_3 - u_8u_6u_4^3u_1$$

4. Pseudo remainder with p_3 over variable x_5 :

$$g = -u_6u_4^4u_1x_4x_2+$$
$$(-u_8u_7u_6u_4^3u_3 + u_8u_7u_5u_4^4 + u_7u_6u_4^3u_3u_1)x_4+$$
$$(u_8u_6u_4^3u_3 - u_8u_6u_4^3u_1 - u_8u_5u_4^4 + u_5u_4^4u_1)x_3x_2+$$
$$(u_8u_7u_5u_4^3u_1 - u_7u_5u_4^3u_3u_1)x_3 + u_8u_6u_4^4u_1x_2-$$
$$u_8u_7u_5u_4^4u_1$$

5. Pseudo remainder with p_2 over variable x_4 :

$$g = (-u_8u_6^2u_4^3u_3 + u_8u_6^2u_4^3u_1 + u_8u_6u_5u_4^4 - u_8u_6u_4^4u_1)x_3x_2+$$
$$(-u_8^2u_7u_6u_4^3u_3 + u_8^2u_7u_5u_4^4 + u_8u_7u_6u_5u_4^3u_3-$$
$$u_8u_7u_6u_5u_4^3u_1 + u_8u_7u_6u_4^3u_3u_1 - u_8u_7u_5^2u_4^4)x_3+$$
$$(u_8^2u_7u_6^2u_4^3u_3 - u_8^2u_7u_6u_5u_4^4 - u_8u_7u_6^2u_4^3u_3u_1+$$
$$u_8u_7u_6u_5u_4^4u_1)$$

6. Pseudo remainder with p_1 over variable x_3 :

$$g = ($$
$$-u_8^2u_7u_6^3u_4^3u_1 + u_8^2u_7u_6^2u_4^4u_1 + u_8u_7u_6^3u_4^3u_1^2-$$
$$u_8u_7u_6^2u_4^4u_1^2)x_2+$$
$$(u_8^2u_7^2u_6^2u_5u_4^3u_1 - u_8^2u_7^2u_6^2u_4^3u_3u_1+$$
$$u_8^2u_7u_6^3u_4^3u_3u_1 - u_8^2u_7u_6^2u_5u_4^4u_1-$$
$$u_8u_7^2u_6^2u_5u_4^3u_1^2 + u_8u_7^2u_6^2u_4^3u_3u_1^2-$$
$$u_8u_7u_6^3u_4^3u_3u_1^2 + u_8u_7u_6^2u_5u_4^4u_1^2)$$

7. Pseudo remainder with p_0 over variable x_2 :

$$g = 0$$

7.2.7 Prover report

Status : The conjecture has been proved.

Space Complexity : The biggest polynomial obtained during proof process contained 18 terms.

Time Complexity : Time spent by the prover : 0.007 seconds. There are no ndg conditions.

7.3 GCLC Prover Output for conjecture "pappus1proof" - Groebner bases method used

7.3.1 Construction and prover internal state

Construction commands :

— Point A
— Point B
— Random point on line, C : A B 0.806871
— Point D
— Point E
— Random point on line, F : D E 0.0435923
— Line lAE : A E
— Line lAF : A F
— Line lBD : B D
— Line lBF : B F
— Line lCD : C D
— Line lCE : C E
— Intersection of lines, P : lBF lCE
— Intersection of lines, Q : lAF lCD
— Intersection of lines, R : lAE lBD

Coordinates assigned to the points :
— $A = (0, 0)$
— $B = (u_1, 0)$
— $C = (u_8, 0)$
— $D = (u_3, u_4)$
— $E = (u_5, u_6)$
— $F = (x_2, u_7)$
— $P = (x_4, x_3)$
— $Q = (x_6, x_5)$
— $R = (x_8, x_7)$

Conjecture(s) :

1. Given conjecture
   — **GCLC code :**
   ```
   collinear P Q R
   ```
   — **Expression :**
   $collinear(P, Q, R)$

7.3.2 Resolving constructed lines

— $AB \ni A, B, C$; line is horizontal (i.e., $y(A) = y(B)$) ; line is generated by the prover
— $DE \ni D, E, F$; line is generated by the prover
— $lAE \ni A, E, R$
— $lAF \ni A, F, Q$
— $lBD \ni B, D, R$
— $lBF \ni B, F, P$
— $lCD \ni C, D, Q$
— $lCE \ni C, E, P$

7.3.3 Creating polynomials from hypotheses

— Point A
no condition
— Point B
no condition
— Random point on line, C : A B 0.806871
   — point C is on the line (A, B) — true by the construction
   no condition
— Point D
no condition
— Point E

no condition
— Random point on line, $F : D\ E$ 0.0435923
— point F is on the line (D, E)

$$p_1 = (-u_6 + u_4)x_2 + (u_7u_5 - u_7u_3 + u_6u_3 - u_5u_4)$$

— Line $lAE : A\ E$
— point A is on the line (A, E)
no condition
— point E is on the line (A, E)
no condition
— Line $lAF : A\ F$
— point A is on the line (A, F)
no condition
— point F is on the line (A, F)
no condition
— Line $lBD : B\ D$
— point B is on the line (B, D)
no condition
— point D is on the line (B, D)
no condition
— Line $lBF : B\ F$
— point B is on the line (B, F)
no condition
— point F is on the line (B, F)
no condition
— Line $lCD : C\ D$
— point C is on the line (C, D)
no condition
— point D is on the line (C, D)
no condition
— Line $lCE : C\ E$
— point C is on the line (C, E)
no condition
— point E is on the line (C, E)
no condition
— Intersection of lines, $P : lBF\ lCE$
— point P is on the line (B, F)

$$p_2 = -u_7x_4 + x_3x_2 - u_1x_3 + u_7u_1$$

— point P is on the line (C, E)

$$p_3 = -u_6x_4 + (-u_8 + u_5)x_3 + u_8u_6$$

— Intersection of lines, $Q : lAF\ lCD$
— point Q is on the line (A, F)

$$p_4 = -u_7x_6 + x_5x_2$$

— point Q is on the line (C, D)

$$p_5 = -u_4x_6 + (-u_8 + u_3)x_5 + u_8u_4$$

— Intersection of lines, $R : lAE\ lBD$
— point R is on the line (A, E)

$$p_6 = -u_6x_8 + u_5x_7$$

— point R is on the line (B, D)

$$p_7 = -u_4x_8 + (u_3 - u_1)x_7 + u_4u_1$$

7.3.4 Creating polynomial from the conjecture

— Processing given conjecture(s).
— point P is on the line (Q, R)

$$p_8 = -x_8x_5 + x_8x_3 + x_7x_6 - x_7x_4 - x_6x_3 + x_5x_4$$

Conjecture 1 :

$$p_9 = -x_8x_5 + x_8x_3 + x_7x_6 - x_7x_4 - x_6x_3 + x_5x_4$$

7.3.5 Invoking the theorem prover

The used proving method is Buchberger's method.
Input polynomial system is :

$$\begin{aligned}
p_0 &= (-u_6 + u_4)x_2 + (u_7u_5 - u_7u_3 + u_6u_3 - u_5u_4)\\
p_1 &= -u_7x_4 + x_3x_2 - u_1x_3 + u_7u_1\\
p_2 &= -u_6x_4 + (-u_8 + u_5)x_3 + u_8u_6\\
p_3 &= -u_7x_6 + x_5x_2\\
p_4 &= -u_4x_6 + (-u_8 + u_3)x_5 + u_8u_4\\
p_5 &= -u_6x_8 + u_5x_7\\
p_6 &= -u_4x_8 + (u_3 - u_1)x_7 + u_4u_1
\end{aligned}$$

Iteration 1 Current set is S_1 =

$$\begin{aligned}
p_0 &= (-u_6 + u_4)x_2 + (u_7u_5 - u_7u_3 + u_6u_3 - u_5u_4)\\
p_1 &= -u_7x_4 + x_3x_2 - u_1x_3 + u_7u_1\\
p_2 &= -u_6x_4 + (-u_8 + u_5)x_3 + u_8u_6\\
p_3 &= -u_7x_6 + x_5x_2\\
p_4 &= -u_4x_6 + (-u_8 + u_3)x_5 + u_8u_4\\
p_5 &= -u_6x_8 + u_5x_7\\
p_6 &= -u_4x_8 + (u_3 - u_1)x_7 + u_4u_1
\end{aligned}$$

1. Creating S-polynomial from the pair (p_0, p_1).
   Skipping pair p_0 and p_1 because gcd of their leading monoms is zero.
2. Creating S-polynomial from the pair (p_0, p_2).
   Skipping pair p_0 and p_2 because gcd of their leading monoms is zero.
3. Creating S-polynomial from the pair (p_0, p_3).
   Skipping pair p_0 and p_3 because gcd of their leading monoms is zero.
4. Creating S-polynomial from the pair (p_0, p_4).
   Skipping pair p_0 and p_4 because gcd of their leading monoms is zero.
5. Creating S-polynomial from the pair (p_0, p_5).
   Skipping pair p_0 and p_5 because gcd of their leading monoms is zero.
6. Creating S-polynomial from the pair (p_0, p_6).
   Skipping pair p_0 and p_6 because gcd of their leading monoms is zero.
7. Creating S-polynomial from the pair (p_1, p_2).
   Forming S-pol of p_1 and p_2 :

   $$p_{24} = -u_6x_3x_2 + (-u_8u_7 + u_7u_5 + u_6u_1)x_3 + (u_8u_7u_6 - u_7u_6u_1)$$

   S-pol added.

8. Creating S-polynomial from the pair (p_1, p_3).
   Skipping pair p_1 and p_3 because gcd of their leading monoms is zero.
9. Creating S-polynomial from the pair (p_1, p_4).
   Skipping pair p_1 and p_4 because gcd of their leading monoms is zero.
10. Creating S-polynomial from the pair (p_1, p_5).
    Skipping pair p_1 and p_5 because gcd of their leading monoms is zero.
11. Creating S-polynomial from the pair (p_1, p_6).
    Skipping pair p_1 and p_6 because gcd of their leading monoms is zero.
12. Creating S-polynomial from the pair (p_2, p_3).
    Skipping pair p_2 and p_3 because gcd of their leading monoms is zero.
13. Creating S-polynomial from the pair (p_2, p_4).
    Skipping pair p_2 and p_4 because gcd of their leading monoms is zero.
14. Creating S-polynomial from the pair (p_2, p_5).
    Skipping pair p_2 and p_5 because gcd of their leading monoms is zero.
15. Creating S-polynomial from the pair (p_2, p_6).
    Skipping pair p_2 and p_6 because gcd of their leading monoms is zero.
16. Creating S-polynomial from the pair (p_3, p_4).
    Forming S-pol of p_3 and p_4 :

$$p_{25} = -u_4x_5x_2 + (-u_8u_7 + u_7u_3)x_5 + u_8u_7u_4$$

    S-pol added.
17. Creating S-polynomial from the pair (p_3, p_5).
    Skipping pair p_3 and p_5 because gcd of their leading monoms is zero.
18. Creating S-polynomial from the pair (p_3, p_6).
    Skipping pair p_3 and p_6 because gcd of their leading monoms is zero.
19. Creating S-polynomial from the pair (p_4, p_5).
    Skipping pair p_4 and p_5 because gcd of their leading monoms is zero.
20. Creating S-polynomial from the pair (p_4, p_6).
    Skipping pair p_4 and p_6 because gcd of their leading monoms is zero.
21. Creating S-polynomial from the pair (p_5, p_6).
    Forming S-pol of p_5 and p_6 :

$$p_{26} = (u_6u_3 - u_6u_1 - u_5u_4)x_7 + u_6u_4u_1$$

    S-pol added.

Iteration 2 Current set is $S_2 =$

$$\begin{aligned}
p_0 &= (-u_6 + u_4)x_2 + (u_7u_5 - u_7u_3 + u_6u_3 - u_5u_4)\\
p_1 &= -u_7x_4 + x_3x_2 - u_1x_3 + u_7u_1\\
p_2 &= -u_6x_4 + (-u_8 + u_5)x_3 + u_8u_6\\
p_3 &= -u_7x_6 + x_5x_2\\
p_4 &= -u_4x_6 + (-u_8 + u_3)x_5 + u_8u_4\\
p_5 &= -u_6x_8 + u_5x_7\\
p_6 &= -u_4x_8 + (u_3 - u_1)x_7 + u_4u_1\\
p_7 &= (\\
&\quad u_8u_7u_6 - u_8u_7u_4 - u_7u_6u_3 + u_7u_5u_4 + u_6^2u_3 - u_6^2u_1 - u_6u_5u_4 +\\
&\quad u_6u_4u_1)x_3 + (-u_8u_7u_6^2 + u_8u_7u_6u_4 + u_7u_6^2u_1 - u_7u_6u_4u_1)\\
p_8 &= (u_8u_7u_6 - u_8u_7u_4 - u_7u_6u_3 + u_7u_5u_4 + u_6u_4u_3 - u_5u_4^2)x_5 +\\
&\quad (-u_8u_7u_6u_4 + u_8u_7u_4^2)\\
p_9 &= (u_6u_3 - u_6u_1 - u_5u_4)x_7 + u_6u_4u_1
\end{aligned}$$

1. Creating S-polynomial from the pair (p_0, p_7).
   Skipping pair p_0 and p_7 because gcd of their leading monoms is zero.
2. Creating S-polynomial from the pair (p_0, p_8).
   Skipping pair p_0 and p_8 because gcd of their leading monoms is zero.
3. Creating S-polynomial from the pair (p_0, p_9).
   Skipping pair p_0 and p_9 because gcd of their leading monoms is zero.
4. Creating S-polynomial from the pair (p_1, p_7).
   Skipping pair p_1 and p_7 because gcd of their leading monoms is zero.
5. Creating S-polynomial from the pair (p_1, p_8).
   Skipping pair p_1 and p_8 because gcd of their leading monoms is zero.
6. Creating S-polynomial from the pair (p_1, p_9).
   Skipping pair p_1 and p_9 because gcd of their leading monoms is zero.
7. Creating S-polynomial from the pair (p_2, p_7).
   Skipping pair p_2 and p_7 because gcd of their leading monoms is zero.
8. Creating S-polynomial from the pair (p_2, p_8).
   Skipping pair p_2 and p_8 because gcd of their leading monoms is zero.
9. Creating S-polynomial from the pair (p_2, p_9).
   Skipping pair p_2 and p_9 because gcd of their leading monoms is zero.
10. Creating S-polynomial from the pair (p_3, p_7).
    Skipping pair p_3 and p_7 because gcd of their leading monoms is zero.
11. Creating S-polynomial from the pair (p_3, p_8).
    Skipping pair p_3 and p_8 because gcd of their leading monoms is zero.
12. Creating S-polynomial from the pair (p_3, p_9).
    Skipping pair p_3 and p_9 because gcd of their leading monoms is zero.
13. Creating S-polynomial from the pair (p_4, p_7).
    Skipping pair p_4 and p_7 because gcd of their leading monoms is zero.
14. Creating S-polynomial from the pair (p_4, p_8).
    Skipping pair p_4 and p_8 because gcd of their leading monoms is zero.
15. Creating S-polynomial from the pair (p_4, p_9).
    Skipping pair p_4 and p_9 because gcd of their leading monoms is zero.
16. Creating S-polynomial from the pair (p_5, p_7).
    Skipping pair p_5 and p_7 because gcd of their leading monoms is zero.
17. Creating S-polynomial from the pair (p_5, p_8).
    Skipping pair p_5 and p_8 because gcd of their leading monoms is zero.
18. Creating S-polynomial from the pair (p_5, p_9).
    Skipping pair p_5 and p_9 because gcd of their leading monoms is zero.
19. Creating S-polynomial from the pair (p_6, p_7).
    Skipping pair p_6 and p_7 because gcd of their leading monoms is zero.
20. Creating S-polynomial from the pair (p_6, p_8).
    Skipping pair p_6 and p_8 because gcd of their leading monoms is zero.
21. Creating S-polynomial from the pair (p_6, p_9).
    Skipping pair p_6 and p_9 because gcd of their leading monoms is zero.
22. Creating S-polynomial from the pair (p_7, p_8).
    Skipping pair p_7 and p_8 because gcd of their leading monoms is zero.
23. Creating S-polynomial from the pair (p_7, p_9).
    Skipping pair p_7 and p_9 because gcd of their leading monoms is zero.
24. Creating S-polynomial from the pair (p_8, p_9).
    Skipping pair p_8 and p_9 because gcd of their leading monoms is zero.

Groebner Basis Groebner basis has 10 polynomials :

$$\begin{aligned}
p_0 &= (-u_6+u_4)x_2+(u_7u_5-u_7u_3+u_6u_3-u_5u_4)\\
p_1 &= -u_7x_4+x_3x_2-u_1x_3+u_7u_1\\
p_2 &= -u_6x_4+(-u_8+u_5)x_3+u_8u_6\\
p_3 &= -u_7x_6+x_5x_2\\
p_4 &= -u_4x_6+(-u_8+u_3)x_5+u_8u_4\\
p_5 &= -u_6x_8+u_5x_7\\
p_6 &= -u_4x_8+(u_3-u_1)x_7+u_4u_1\\
p_7 &= (\\
&\quad u_8u_7u_6-u_8u_7u_4-u_7u_6u_3+u_7u_5u_4+u_6^2u_3-u_6^2u_1-u_6u_5u_4+\\
&\quad u_6u_4u_1)x_3+(-u_8u_7u_6^2+u_8u_7u_6u_4+u_7u_6^2u_1-u_7u_6u_4u_1)\\
p_8 &= (u_8u_7u_6-u_8u_7u_4-u_7u_6u_3+u_7u_5u_4+u_6u_4u_3-u_5u_4^2)x_5+\\
&\quad (-u_8u_7u_6u_4+u_8u_7u_4^2)\\
p_9 &= (u_6u_3-u_6u_1-u_5u_4)x_7+u_6u_4u_1
\end{aligned}$$

Groebner basis succesfully computed.

7.3.6 Reducing Polynomial Conjecture

Reducing with polynomial p_5, the result is :

$$p_{47} = -u_6x_8x_3-u_6x_7x_6+u_5x_7x_5+u_6x_7x_4+u_6x_6x_3-u_6x_5x_4$$

Reducing with polynomial p_5, the result is :

$$p_{48} = u_6^2x_7x_6-u_6u_5x_7x_5-u_6^2x_7x_4+u_6u_5x_7x_3-u_6^2x_6x_3+u_6^2x_5x_4$$

Reducing with polynomial p_3, the result is :

$$\begin{gathered}
p_{49} = -\\
u_6^2x_7x_5x_2+u_7u_6u_5x_7x_5+u_7u_6^2x_7x_4-u_7u_6u_5x_7x_3+\\
u_7u_6^2x_6x_3-u_7u_6^2x_5x_4
\end{gathered}$$

Reducing with polynomial p_0, the result is :

$$\begin{gathered}
p_{50} = (-u_7u_6^2u_3+u_7u_6u_5u_4+u_6^3u_3-u_6^2u_5u_4)x_7x_5+\\
(-u_7u_6^3+u_7u_6^2u_4)x_7x_4+(u_7u_6^2u_5-u_7u_6u_5u_4)x_7x_3+\\
(-u_7u_6^3+u_7u_6^2u_4)x_6x_3+(u_7u_6^3-u_7u_6^2u_4)x_5x_4
\end{gathered}$$

Reducing with polynomial p_8, the result is :
Polynomial too big for output (text size is 1628 characters, number of terms is 5)

Reducing with polynomial p_1, the result is :
Polynomial too big for output (text size is 2450 characters, number of terms is 5)

Reducing with polynomial p_0, the result is :
Polynomial too big for output (text size is 3662 characters, number of terms is 4)

Reducing with polynomial p_7, the result is :
Polynomial too big for output (text size is 8165 characters, number of terms is 3)

Reducing with polynomial p_9, the result is :
Polynomial too big for output (number of terms is 3) Reducing with polynomial p_3, the result is :
Polynomial too big for output (number of terms is 3) Reducing with polynomial p_1, the result is :

Polynomial too big for output (number of terms is 3) Reducing with polynomial p_7, the result is :
Polynomial too big for output (number of terms is 2) Reducing with polynomial p_8, the result is :

$$p_{51} = 0$$

Conclusion is reduced to zero.

7.3.7 Prover report

Status : The conjecture has been proved.

Space Complexity : The biggest polynomial obtained during proof process contained 680 terms.

Time Complexity : Time spent by the prover : 0.141 seconds. There are no ndg conditions.

7.4 GCLC Prover Output for conjecture "trisect2proof" - Area method used

$$P_{AFA} = P_{FGF} \quad \text{by the statement} \quad (67)$$

$$P_{AFA} = \left(\left(P_{FFF} + \left(\frac{1}{2} \cdot ((P_{FBF} + (-1 \cdot P_{FFF})) + (2 \cdot P_{FFF}))\right)\right) + \left(-\frac{1}{4} \cdot P_{FBF}\right) \quad \text{by Lemma 33 (point } G \text{ eliminated)} \quad (68)$$

$$P_{AFA} = \left(\left(0 + \left(\frac{1}{2} \cdot ((P_{FBF} + (-1 \cdot 0)) + (2 \cdot 0))\right)\right) + \left(-\frac{1}{4} \cdot P_{FBF}\right)\right) \quad \text{by geometric simplifications} \quad (69)$$

$$P_{AFA} = \left(\frac{1}{4} \cdot P_{FBF}\right) \quad \text{by algebraic simplifications} \quad (70)$$

$$\left(\left(\frac{\overrightarrow{CF}}{\overrightarrow{CE}} \cdot P_{AEA}\right) + \left(\frac{\overrightarrow{FE}}{\overrightarrow{CE}} \cdot P_{ACA}\right)\right) + \left(-1 \cdot \left(\left(\frac{\overrightarrow{CF}}{\overrightarrow{CE}} = \frac{\overrightarrow{FE}}{\overrightarrow{CE}}\right) \cdot P_{CHC}\right)\right)\right) \quad \text{by Lemma 32 (point } F \text{ eliminated)} \quad (71)$$

$$\left(\left(\frac{\overrightarrow{CF}}{\overrightarrow{CE}} \cdot P_{AEA}\right) + \left(\left(-1 \cdot \frac{\overrightarrow{EF}}{\overrightarrow{CE}}\right) \cdot P_{ACA}\right)\right) + \left(-1 \cdot \left(\left(\frac{\overrightarrow{CF}}{\overrightarrow{CE}} = \left(P_{FBF} \cdot \frac{\overrightarrow{EF}}{\overrightarrow{CE}}\right)\right) \cdot P_{CEC}\right)\right)\right) \quad \text{by geometric simplifications} \quad (72)$$

$$\left(\left(\frac{\overrightarrow{CF}}{\overrightarrow{CE}} \cdot P_{AEA}\right) + \left(-1 \cdot \left(\frac{\overrightarrow{EF}}{\overrightarrow{CE}} \cdot P_{ACA}\right)\right)\right) + \left(\frac{\overrightarrow{CF}}{\overrightarrow{CE}} = \left(\frac{\overrightarrow{EF}}{\overrightarrow{CE}} \cdot P_{CHC}\right)\right)\right) \quad \text{by algebraic simplifications} \quad (73)$$

$$\left(\left(\frac{S_{CAB}}{S_{CAEB}} \cdot P_{AEA}\right) + \left(-1 \cdot \left(\frac{\overrightarrow{EF}}{\overrightarrow{CE}} \cdot P_{ACA}\right)\right)\right) + \left(\frac{\overrightarrow{CF}}{\overrightarrow{CE}} = \left(\frac{\overrightarrow{EF}}{\overrightarrow{CE}} \cdot P_{CEC}\right)\right)\right) \quad \text{by Lemma 37 , second case — points } C, C, \text{ and } E \text{ are collinear (point } F \text{ eliminated)} \quad (74)$$

$$\frac{\left(((S_{CAB} \cdot P_{AEA}) + \left(-1 \cdot \left(\frac{\overrightarrow{EF}}{\overrightarrow{CE}} \cdot (P_{ACA} \cdot S_{CAEB})\right)\right)) + \left(\frac{\overrightarrow{CF}}{\overrightarrow{CE}} = \left(\frac{\overrightarrow{EF}}{\overrightarrow{CE}} \cdot (P_{CEC} \cdot S_{CAEB})\right)\right)\right)}{S_{CAEB}} = \left(\frac{1}{4} \cdot P_{FBF}\right) \quad \text{by algebraic simplifications} \quad (75)$$

$$\frac{\left(\left((S_{CAB} \cdot P_{AEA}) + \left(-1 \cdot \left(\frac{S_{EAB}}{S_{CAEB}} \cdot (P_{ACA} \cdot S_{CAEB})\right)\right)\right) + \left(\frac{\overrightarrow{CF}}{\overrightarrow{CE}} = \left(\frac{\overrightarrow{EF}}{\overrightarrow{CE}} \cdot (P_{CEC} \cdot S_{CAEB})\right)\right)\right)}{S_{CAEB}} = \left(\frac{1}{4} \cdot P_{FBF}\right) \quad \text{by Lemma 37 , second case — points } E, C, \text{ and } E \text{ are collinear (point } F \text{ eliminated)} \quad (76)$$

$$\frac{\left(((S_{CAB} \cdot P_{AEA}) + (-1 \cdot (S_{EAB} \cdot P_{ACA}))) + \left(\frac{\overrightarrow{CF}}{\overrightarrow{CE}} = \left(\frac{\overrightarrow{EF}}{\overrightarrow{CE}} \cdot (P_{CEC} \cdot S_{CAEB})\right)\right)\right)}{S_{CAEB}} = \left(\frac{1}{4} \cdot P_{FBF}\right) \quad \text{by algebraic simplifications} \quad (77)$$

$$\frac{\left(((S_{CAB} \cdot P_{AEA}) + (-1 \cdot (S_{EAB} \cdot P_{ACA}))) + \left(\frac{S_{CAB}}{S_{CAEB}} = \left(\frac{\overrightarrow{EF}}{\overrightarrow{CE}} \cdot (P_{CEC} \cdot S_{CAEB})\right)\right)\right)}{S_{CAEB}} = \left(\frac{1}{4} \cdot P_{FBF}\right) \quad \text{by Lemma 37 , second case — points } C, C, \text{ and } E \text{ are collinear (point } F \text{ eliminated)} \quad (78)$$

$$\frac{\left(((S_{CAB} \cdot P_{AEA}) + (-1 \cdot (S_{EAB} \cdot P_{ACA}))) + \left(S_{CAB} \cdot \left(\frac{\overrightarrow{EF}}{\overrightarrow{CE}} \cdot P_{CEC}\right)\right)\right)}{S_{CAEB}} = \left(\frac{1}{4} \cdot P_{FBF}\right) \quad \text{by algebraic simplifications} \quad (79)$$

$$\frac{\left(((S_{CAB} \cdot P_{AEA}) + (-1 \cdot (S_{EAB} \cdot P_{ACA}))) + \left(S_{CAB} \cdot \left(\frac{S_{EAB}}{S_{CAEB}} \cdot P_{CEC}\right)\right)\right)}{S_{CAEB}} = \left(\frac{1}{4} \cdot P_{FBF}\right) \quad \text{by Lemma 37 , second case — points } E, C, \text{ and } E \text{ are collinear (point } F \text{ eliminated)} \quad (80)$$

$$\frac{(((S_{CAEB} \cdot (S_{CAB} \cdot P_{AEA})) + (-1 \cdot (S_{CAEB} \cdot (S_{EAB} \cdot P_{ACA})))) + (S_{CAB} \cdot (S_{EAB} \cdot P_{CEC})))}{(S_{CAEB} \cdot S_{CAEB})} = \left(\frac{1}{4} \cdot P_{FBF}\right) \quad \text{by algebraic simplifications} \quad (81)$$

$$\frac{(((S_{CAEB} \cdot (S_{CAB} \cdot P_{AEA})) + (-1 \cdot (S_{CAEB} \cdot (S_{EAB} \cdot P_{ACA})))) + (S_{CAB} \cdot (S_{EAB} \cdot P_{CEC})))}{(S_{CAEB} \cdot S_{CAEB})} = \left(\frac{1}{4} \cdot \frac{((S_{CAB} \cdot P_{FBE}) + (-1 \cdot (S_{EAB} \cdot P_{FBC})))}{S_{CAEB}}\right) \quad \text{by Lemma 30 (point } F \text{ eliminated)} \quad (82)$$

$$\frac{(((S_{CAEB} \cdot (S_{CAB} \cdot P_{AEA})) + (-1 \cdot (S_{CAEB} \cdot (S_{EAB} \cdot P_{ACA})))) + (S_{CAB} \cdot (S_{EAB} \cdot P_{CEC})))}{(S_{CAEB} \cdot S_{CAEB})} = \left(\frac{1}{4} \cdot \frac{((S_{CAB} \cdot P_{FBE}) + (-1 \cdot (S_{EAB} \cdot P_{CBF})))}{S_{CAEB}}\right) \quad \text{by geometric simplifications} \quad (83)$$

$$(((S_{CAEB} \cdot (S_{CAB} \cdot P_{AEA})) + (-1 \cdot (S_{CAEB} \cdot (S_{EAB} \cdot P_{ACA})))) + (S_{CAB} \cdot (S_{EAB} \cdot P_{CEC}))) = \left(\frac{1}{4} \cdot \frac{((S_{CAB} \cdot P_{FBE}) + (-1 \cdot (S_{EAB} \cdot P_{FBC})))}{S_{CAEB}}\right) \quad \text{by algebraic simplifications} \quad (84)$$

$$(((S_{CAEB} \cdot (S_{CAB} \cdot P_{AEA})) + (-1 \cdot (S_{CAEB} \cdot (S_{EAB} \cdot P_{ACA})))) + (S_{CAB} \cdot (S_{EAB} \cdot P_{CEC}))) = \left(\frac{1}{4} \cdot \frac{((S_{CAB} \cdot P_{FBE}) + (-1 \cdot (S_{EAB} \cdot P_{FBC})))}{S_{CAEB}}\right) + \left(-\frac{1}{4}\right)(S_{CAEB} \cdot (S_{EAB} \cdot P_{CBF})) \quad \text{by Lemma 30 (point } F \text{ eliminated)} \quad (85)$$

$$(((S_{CAEB} \cdot (S_{CAB} \cdot P_{AEA})) + (-1 \cdot (S_{CAEB} \cdot (S_{EAB} \cdot P_{ACA})))) + (S_{CAB} \cdot (S_{EAB} \cdot P_{CEC}))) = \left(\frac{1}{4} \cdot \frac{((S_{CAB} \cdot P_{FBE}) + (-1 \cdot (S_{EAB} \cdot P_{FBC})))}{S_{CAEB}}\right) + \left(\frac{1}{4} \cdot (S_{CAEB} \cdot (S_{EAB} \cdot P_{CBF}))\right) \quad \text{by algebraic simplifications} \quad (86)$$

$$(((S_{CAEB} \cdot (S_{CAB} \cdot P_{AEA})) + (-1 \cdot (S_{CAEB} \cdot (S_{EAB} \cdot P_{ACA})))) + (S_{CAB} \cdot (S_{EAB} \cdot P_{CEC}))) = \left(\frac{1}{4} \cdot \frac{((S_{CAB} \cdot P_{FBE}) + (-1 \cdot (S_{EAB} \cdot P_{FBC})))}{S_{CAEB}}\right) + \left(\frac{1}{4} \cdot (S_{CAB} \cdot (S_{EAB} \cdot P_{EBC}))\right) \quad \text{by Lemma 30 (point } F \text{ eliminated)} \quad (87)$$

$$(((S_{CAEB} \cdot (S_{CAB} \cdot P_{AEA})) + (-1 \cdot (S_{CAEB} \cdot (S_{EAB} \cdot P_{ACA})))) + (S_{CAB} \cdot (S_{EAB} \cdot P_{CEC}))) = \left(\frac{1}{4} \cdot \frac{((S_{CAB} \cdot P_{FBE}) + (-1 \cdot (S_{EAB} \cdot P_{FBC})))}{S_{CAEB}}\right) + \left(\frac{1}{4} \cdot (S_{CAB} \cdot (S_{EAB} \cdot P_{EBC}))\right) \quad \text{by Geometric simplifications} \quad (88)$$

$$(((S_{CAEB} \cdot (S_{CAB} \cdot P_{AEA})) + (-1 \cdot (S_{CAEB} \cdot (S_{EAB} \cdot P_{ACA})))) + (S_{CAB} \cdot (S_{EAB} \cdot P_{CEC}))) = \left(\frac{1}{4} \cdot \frac{((S_{CAB} \cdot P_{FBE}) + (-1 \cdot (S_{EAB} \cdot P_{FBC})))}{S_{CAEB}}\right) + \left(\frac{1}{2} \cdot (S_{CAB} \cdot (S_{EAB} \cdot P_{EBC}))\right) \quad \text{by Algebraic simplifications} \quad (89)$$

$$((((S_{CAE} + S_{BCE}) \cdot (S_{CAB} \cdot P_{AEA})) + (-1 \cdot ((S_{CAE} + S_{BCE}) \cdot (S_{EAB} \cdot P_{ACA})))) + (S_{CAB} \cdot (S_{EAB} \cdot P_{CEC}))) = \left(\frac{1}{4} \cdot \frac{((S_{CAB} \cdot P_{FBE}) + (-1 \cdot (S_{EAB} \cdot P_{FBC})))}{S_{CAEB}}\right) + \left(\frac{1}{2} \cdot (S_{CAB} \cdot (S_{EAB} \cdot P_{EBC}))\right) \quad \text{by Geometric simplifications} \quad (90)$$

$((((((0.09375 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{ACA}))) + (0.03125 =$ ... (164)

$((((((0.09375 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{ACA}))) + (0.03125 =$ ... by Lemma 29 (point D eliminated) ... (165)

$((((((0.09375 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{ACA}))) + (0.03125 =$ ... by geometric simplifications ... (166)

$(((((0.09375 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{ACA}))) + (0.03125 =$ ... by algebraic simplifications ... (167)

$(((((0.09375 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{ACA}))) + (0.03125 =$ ... by Lemma 29 (point D eliminated) ... (168)

$(((((0.09375 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{ACA}))) + (0.03125 =$ ... by geometric simplifications ... (169)

$(((((0.09375 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{ACA}))) + (0.03125 =$ ... by algebraic simplifications ... (170)

$(((((0.09375 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{ACA}))) + (0.03125 =$ ... by Lemma 29 (point D eliminated) ... (171)

$(((((0.09375 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{ACA}))) + (0.03125 =$ ... by geometric simplifications ... (172)

$(((((0.03125 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{ACA}))) + (0.03125 =$ ... by algebraic simplifications ... (173)

$(((((0.03125 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{ACA}))) + (0.03125 =$ ... by Lemma 29 (point D eliminated) ... (174)

$(((((0.03125 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{ACA}))) + (0.03125 =$ ... by geometric simplifications ... (175)

$(((((0.03125 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{ACA}))) + (0.03125 =$ ... by algebraic simplifications ... (176)

$(((((0.03125 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{ACA}))) + (0.03125 =$ ... by Lemma 29 (point D eliminated) ... (177)

$(((((0.03125 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{ACA}))) + (0.03125 =$ ... by geometric simplifications ... (178)

$((((0.03125 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{ACA}))) + (0.03125 =$ ... by algebraic simplifications ... (179)

$((((0.03125 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{ACA}))) + (0.03125 =$ ... by Lemma 29 (point D eliminated) ... (180)

$((((0.03125 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{ACA}))) + (0.03125 =$ ... by geometric simplifications ... (181)

$((((0.03125 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{ACA}))) + (0.03125 =$ ... by algebraic simplifications ... (182)

$((((0.03125 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{ACA}))) + (0.03125 =$ ... by Lemma 33 (point D eliminated) ... (183)

$((((0.03125 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{ACA}))) + (0.03125 =$ ... by geometric simplifications ... (184)

$((((0.03125 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{ACA}))) + (0.03125 =$ ... by algebraic simplifications ... (185)

$((((0.03125 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{ACA}))) + (0.03125 =$ ... by Lemma 29 (point D eliminated) ... (186)

$((((0.03125 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{ACA}))) + (0.03125 =$ ... by geometric simplifications ... (187)

$((((0.03125 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{ACA}))) + (0.03125 =$ ... by algebraic simplifications ... (188)

$((((0.03125 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{ACA}))) + (0.03125 =$ ... by Lemma 33 (point D eliminated) ... (189)

$((((0.03125 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{ACA}))) + (0.03125 =$ ... by geometric simplifications ... (190)

$0 = (((((\frac{1}{8} \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{ABD}))) + (0.0625 \cdot (S_{CAB} \cdot \ldots$ by algebraic simplifications (191)

$0 = (((((\frac{1}{8} \cdot (S_{CAB} \cdot (S_{CAB} \cdot (P_{ABC} + (\frac{1}{2} \cdot (P_{ABB} + (-1 \cdot P_{ABC}))))))) + (0.0625 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{DBD} \ldots$ by Lemma 29 (point D eliminated) (192)

$0 = (((((\frac{1}{8} \cdot (S_{CAB} \cdot (S_{CAB} \cdot (P_{ABC} + (\frac{1}{2} \cdot (0 + (-1 \cdot P_{ABC}))))))) + (0.0625 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{DBD}))) \ldots$ by geometric simplifications (193)

$0 = (((0.0625 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{ABC}))) + (0.0625 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{DBD}))) + ((\frac{1}{8} \cdot (S_{CAB} \cdot (S_{ABD} \ldots$ by algebraic simplifications (194)

$0 = ((((0.0625 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{ABC}))) + (0.0625 \cdot (S_{CAB} \cdot (S_{CAB} \cdot (P_{DBC} + (\frac{1}{2} \cdot (P_{DBB} + (-1 \cdot P_{DBC} \ldots$ by Lemma 29 (point D eliminated) (195)

$0 = ((((0.0625 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{ABC}))) + (0.0625 \cdot (S_{CAB} \cdot (S_{CAB} \cdot (P_{CBD} + (\frac{1}{2} \cdot (0 + (-1 \cdot P_{CBD})))))) \ldots$ by geometric simplifications (196)

$0 = (((0.0625 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{ABC}))) + (0.03125 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{CBD}))) + ((-\frac{1}{8} \cdot (S_{CAB} \cdot (S_{ABD} \ldots$ by algebraic simplifications (197)

$0 = ((((0.0625 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{ABC}))) + (0.03125 \cdot (S_{CAB} \cdot (S_{CAB} \cdot (P_{CBC} + (\frac{1}{2} \cdot (P_{CBB} + (-1 \cdot P_{CBC} \ldots$ by Lemma 29 (point D eliminated) (198)

$0 = ((((0.0625 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{ABC}))) + (0.03125 \cdot (S_{CAB} \cdot (S_{CAB} \cdot (P_{CBC} + (\frac{1}{2} \cdot (0 + (-1 \cdot P_{CBC})))))) \ldots$ by geometric simplifications (199)

$0 = (((0.0625 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{ABC}))) + (0.015625 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{CBC})))) + ((-\frac{1}{8} \cdot (S_{CAB} \cdot (S_{ABD} \ldots$ by algebraic simplifications (200)

$$0 = \left(\left(((0.0625 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{ABC}))) + (0.015625 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{CBC})))\right) + \left(-\frac{1}{8} \cdot \left(S_{CAB} \cdot \left(\left(S_{ABC}\right.\right.\right.\right. \quad \text{by Lemma 29 (point D eliminated)} \quad (201)$$

$$0 = \left(\left(((0.0625 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{ABC}))) + (0.015625 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{CBC})))\right) + \left(-\frac{1}{8} \cdot \left(S_{CAB} \cdot \left(\left(S_{CA}\right.\right.\right.\right. \quad \text{by geometric simplifications} \quad (202)$$

$$0 = \left(\left((0.015625 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{CBC}))) + \left(-\frac{1}{8} \cdot (S_{CAB} \cdot (S_{ABD} \cdot P_{CBD}))\right)\right) + (0.0625 \cdot (S_{ABD} \cdot (S_{ABD} \cdot \right. \quad \text{by algebraic simplifications} \quad (203)$$

$$0 = \left(\left((0.015625 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{CBC}))) + \left(-\frac{1}{8} \cdot \left(S_{CAB} \cdot \left(\left(S_{ABC} + \left(\frac{1}{2} \cdot (S_{ABB} + (-1 \cdot S_{ABC}))\right)\right) \cdot P_{CB}\right.\right.\right.\right. \quad \text{by Lemma 29 (point D eliminated)} \quad (204)$$

$$0 = \left(\left((0.015625 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{CBC}))) + \left(-\frac{1}{8} \cdot \left(S_{CAB} \cdot \left(\left(S_{CAB} + \left(\frac{1}{2} \cdot (0 + (-1 \cdot S_{CAB}))\right)\right) \cdot P_{CBD}\right)\right)\right)\right. \quad \text{by geometric simplifications} \quad (205)$$

$$0 = (((0.015625 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{CBC}))) + (-0.0625 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{CBD})))) + (0.0625 \cdot (S_{ABD} \cdot (S_{ABD} \quad \text{by algebraic simplifications} \quad (206)$$

$$0 = \left(\left((0.015625 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{CBC}))) + \left(-0.0625 \cdot (S_{CAB} \cdot \left(S_{CAB} \cdot \left(P_{CBC} \cdot \left(\frac{1}{2} \cdot (P_{CBB} + (-1 \cdot P_{CB}\right.\right.\right.\right.\right. \quad \text{by Lemma 29 (point D eliminated)} \quad (207)$$

$$0 = \left(\left((0.015625 \cdot (S_{CAB} \cdot (S_{CAB} \cdot P_{CBC}))) + \left(-0.0625 \cdot \left(S_{CAB} \cdot \left(S_{CAB} \cdot \left(P_{CBC} \cdot \left(\frac{1}{2} \cdot (0 + (-1 \cdot P_{CBC}))\right)\right.\right.\right.\right.\right.\right. \quad \text{by geometric simplifications} \quad (208)$$

$$0 = ((-0.015625 \cdot (S_{CAB} \cdot S_{CAB})) + (0.0625 \cdot (S_{ABD} \cdot S_{ABD}))) \quad \text{by algebraic simplifications} \quad (209)$$

$$0 = \left((-0.015625 \cdot (S_{CAB} \cdot S_{CAB})) + \left(0.0625 \cdot \left(\left(S_{ABC} + \left(\frac{1}{2} \cdot (S_{ABB} + (-1 \cdot S_{ABC}))\right)\right) \cdot S_{ABD}\right)\right)\right) \quad \text{by Lemma 29 (point D eliminated)} \quad (210)$$

$$0 = \left((-0.015625 \cdot (S_{CAB} \cdot S_{CAB})) + \left(0.0625 \cdot \left(\left(S_{CAB} + \left(\frac{1}{2} \cdot (0 + (-1 \cdot S_{CAB}))\right)\right) \cdot S_{ABD}\right)\right)\right) \quad \text{by geometric simplifications} \quad (211)$$

$$0 = ((-0.015625 \cdot S_{CAB}) + (0.03125 \cdot S_{ABD})) \quad \text{by algebraic simplifications} \quad (212)$$

$$0 = \left((-0.015625 \cdot S_{CAB}) + \left(0.03125 \cdot \left(S_{ABC} + \left(\frac{1}{2} \cdot (S_{ABB} + (-1 \cdot S_{ABC}))\right)\right)\right)\right) \quad \text{by Lemma 29 (point D eliminated)} \quad (213)$$

$$0 = \left((-0.015625 \cdot S_{CAB}) + \left(0.03125 \cdot \left(S_{CAB} + \left(\frac{1}{2} \cdot (0 + (-1 \cdot S_{CAB}))\right)\right)\right)\right) \quad \text{by geometric simplifications} \quad (214)$$

$$0 = 0 \quad \text{by algebraic simplifications} \quad (215)$$

Q.E.D.

NDG conditions are :
$S_{CAB} \neq S_{EAB}$ i.e., lines CE and AB are not parallel (construction based assumption)
$S_{CAEB} \neq 0$ (cancellation assumption)
$CB \neq 0$ (cancellation assumption)
$S_{CAB} \neq 0$ i.e., points C, A and B are not collinear (cancellation assumption)

Number of elimination proof steps : 55
Number of geometric proof steps : 123
Number of algebraic proof steps : 542
Total number of proof steps : 720
Time spent by the prover : 0.046 seconds

Références

[1] Nuno Baeta et Pedro Quaresma. « Open Geometry Prover Community Project ». In : *arXiv preprint arXiv :2201.01375* (2022).

[2] Nuno Baeta, Pedro Quaresma et Zoltán Kovács. « Towards a geometry automated provers competition ». In : *arXiv preprint arXiv :2002.12556* (2020).

[3] Vladimir Igorevich Bogachev et Maria Aparecida Soares Ruas. *Measure theory*. T. 1. Springer, 2007.

[4] Sylvie Boldo et al. « Lebesgue Induction and Tonelli's Theorem in Coq ». In : *arXiv preprint arXiv :2202.05040* (2022).

[5] Anthony Bordg. « A Replication Crisis in Mathematics ? » In : *The Mathematical Intelligencer* (2021), p. 1-5.

[6] Anthony Bordg, Hanna Lachnitt et Yijun He. « Certified quantum computation in Isabelle/HOL ». In : *Journal of Automated Reasoning* 65.5 (2021), p. 691-709.

[7] Anthony Bordg, Hanna Lachnitt et Yijun He. « Isabelle Marries Dirac : a Library for Quantum Computation and Quantum Information ». In : *Archive of Formal Proofs* (nov. 2020). `https://isa-afp.org/entries/Isabelle_Marries_Dirac.html`, Formal proof development. ISSN : 2150-914x.

[8] Shang-Ching Chou. « An introduction to Wu's method for mechanical theorem proving in geometry ». In : *Journal of Automated Reasoning* 4.3 (1988), p. 237-267.

[9] Roland Coghetto. « Semiring of Sets ». In : *Formaliz. Math.* 22.1 (2014), p. 79-84. DOI : `10.2478/forma-2014-0008`. URL : `https://doi.org/10.2478/forma-2014-0008`.

[10] Joran Elias. « Automated Geometric Theorem Proving : Wu's Method ». In : *Montana Mathematics Enthusiast* 3.1 (), p. 3-50.

[11] Noboru Endou. « Fubini's Theorem ». In : *Formaliz. Math.* 27.1 (2019), p. 67-74. DOI : `10.2478/forma-2019-0007`. URL : `https://doi.org/10.2478/forma-2019-0007`.

[12] Noboru Endou. « Fubini's Theorem for Non-Negative or Non-Positive Functions ». In : *Formaliz. Math.* 26.1 (2018), p. 49-67. DOI : `10.2478/forma-2018-0005`. URL : `https://doi.org/10.2478/forma-2018-0005`.

[13] Noboru Endou, Kazuhisa Nakasho et Yasunari Shidama. « sigma-ring and sigma-algebra of Sets1 ». In : *Formaliz. Math.* 23.1 (2015), p. 51-57. DOI : `10.2478/forma-2015-0004`. URL : `https://doi.org/10.2478/forma-2015-0004`.

[14] Benjamin Grégoire, Loïc Pottier et Laurent Théry. « Proof certificates for algebra and their application to automatic geometry theorem proving ». In : *International Workshop on Automated Deduction in Geometry*. Springer. 2008, p. 42-59.

[15] Frédéric Héran. « À propos de la vitesse généralisée des transports. Un concept d'Ivan Illich revisité ». In : *Revue dEconomie Regionale Urbaine* 3 (2009), p. 449-470.

[16] Predrag Janicic, Julien Narboux et Pedro Quaresma. « The area method : a recapitulation ». In : *Journal of Automated Reasoning* 48.4 (2012), p. 489-532.

[17] Predrag Janičić. « GCLC—a tool for constructive euclidean geometry and more than that ». In : *International Congress on Mathematical Software*. Springer. 2006, p. 58-73.

[18] Vesna Marinkovic, Predrag Janicic et Pascal Schreck. « Solving geometric construction problems supported by theorem proving ». In : *Proceedings of the 10th International Workshop on Automated Deduction in Geometry (ADG 2014)*. 2014, p. 121-146.

[19] Vesna Marinković. « ArgoTriCS–automated triangle construction solver ». In : *Journal of Experimental & Theoretical Artificial Intelligence* 29.2 (2017), p. 247-271.

[20] Jonathan Julian Huerta y Munive. « Matrices for ODEs ». In : *Archive of Formal Proofs* (avr. 2020). `https://isa-afp.org/entries/Matrices_for_ODEs.html`, Formal proof development. ISSN : 2150-914x.

[21] Julien Narboux, Predrag Janicic et Jacques Fleuriot. « Computer-assisted theorem proving in synthetic geometry ». In : *Handbook of Geometric Constraint Systems Principles* (2018), p. 25-73.

[22] Loïc Pottier. « Preuves formelles automatiques et calcul formel ». In : *Les cours du CIRM* 2.1 (2011), p. 1-25.

[23] Pedro Quaresma et Predrag Janičić. *The area method, rigorous proofs of lemmas in Hilbert's style axiom system*. Rapp. tech. 2009.

[24] Pedro Quaresma et al. « Taxonomies of geometric problems ». In : *Journal of Symbolic Computation* 97 (2020), p. 31-55.

[25] Jean Schmets. *Théorie de la mesure*. 1989.

[26] Pascal Schreck et al. « Wernick's list : a final update ». In : *Forum Geometricorum*. T. 16. 2016, p. 69-80.

[27] Steve Szydlik. « Hyperbolic Constructions in Geometer's Sketchpad ». In : (2001).

[28] William Wernick. « Triangle constructions with three located points ». In : *Mathematics Magazine* 55.4 (1982), p. 227-230.

[29] Wikipédia. *Outil convivial — Wikipédia, l'encyclopédie libre*. [En ligne ; Page disponible le 18-mai-2021]. 2021. url : `http://fr.wikipedia.org/w/index.php?title=Outil_convivial&oldid=183035479`.

[30] Wikipédia. *Théorème de Fubini — Wikipédia, l'encyclopédie libre*. [En ligne ; Page disponible le 16-août-2020]. 2020. url : `http://fr.wikipedia.org/w/index.php?title=Th%C3%A9or%C3%A8me_de_Fubini&oldid=173858221`.

[31] Wikipédia. *Théorème de Pappus — Wikipédia, l'encyclopédie libre*. [En ligne ; Page disponible le 2-avril-2021]. 2021. url : `http://fr.wikipedia.org/w/index.php?title=Th%C3%A9or%C3%A8me_de_Pappus&oldid=181490790`.