Proof Assistant and Plane Geometry

INRIA, Marelle Project

Yves Bertot, Laurent Fuchs, Benjamin Grégoire,
Frédérique Guilhot, Tuan Minh Pham, Loïc Pottier, Laurent Théry

Motivations

8 x 24

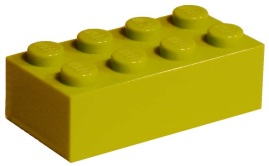
THE BULLETIN

Twenty-Eight Pages — Bend, Deschutes County, Oregon, Wednesday, January 26, 1977 — 10 Pages Cents

The answer is 546,372,891

The question is on the blackboard in the background. It says, find the 23rd root of a 201-digit number. Shakuntala Devi, a world-recognized mathematician, was shown sitting on stage at Southern Methodist University in Dallas, Texas, Tuesday working out the answer. She came up with the correct answer in 50 seconds. It took Univac more than a minute to compute. It took a professor more than four minutes to write it out on the board. (AP Wirephoto)

Motivations



Proof Assistant

Proof Assistant

Computation

$$\alpha \times \beta \to \beta \times \alpha$$

```
Compute prime 31.
  = true
```

Proof

$$p \wedge q \Rightarrow q \wedge p$$

```
Check Euclid_dvdX.
  ∀m n p : nat,
   prime p -> (p | m ^ n) = (p | m) && (0 < n)
```

Proof Assistant

Formalizing 100 Theorems

Outline

High School Geometry

Gröbner Bassis

Geometric Algebras

High School Geometry

ELSEVIER

Annals of Pure and Applied Logic 76 (1995) 169–200

ANNALS OF PURE AND APPLIED LOGIC

The axioms of constructive geometry

Jan von Plato*

University of Helsinki, Helsinki, Finland

Received 21 May 1994; revised 15 December 1994; communicated by D. van Dalen

Abstract

Elementary geometry can be axiomatized constructively by taking as primitive the concepts of the apartness of a point from a line and the convergence of two lines, instead of incidence and

High School Geometry

Deductive Reasoning : Geometry

Needs for Tools

Proof Assistant Not Yet Ready :

- Pretty Printing
- Interaction with Drawing
- More Support for Help

Pragmatic Approach

Primitive Objects

$\texttt{Parameter}\ Po : \texttt{Type}.$

$\texttt{Parameter}\ Pp : \texttt{Type}.$

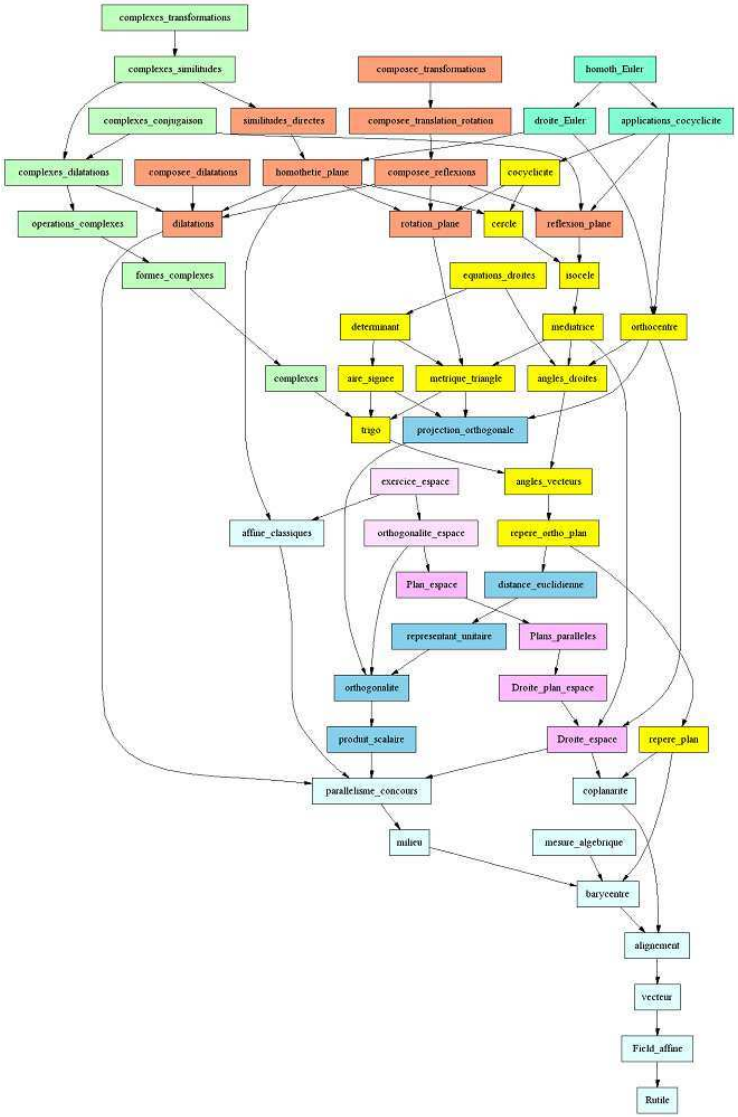
$\texttt{Parameter}\ cons_{Pp} : \mathbb{R} \to Po \to \texttt{Type}.$

$\texttt{Parameter}\ add_{Pp} : Pp \to Pp \to Pp.$

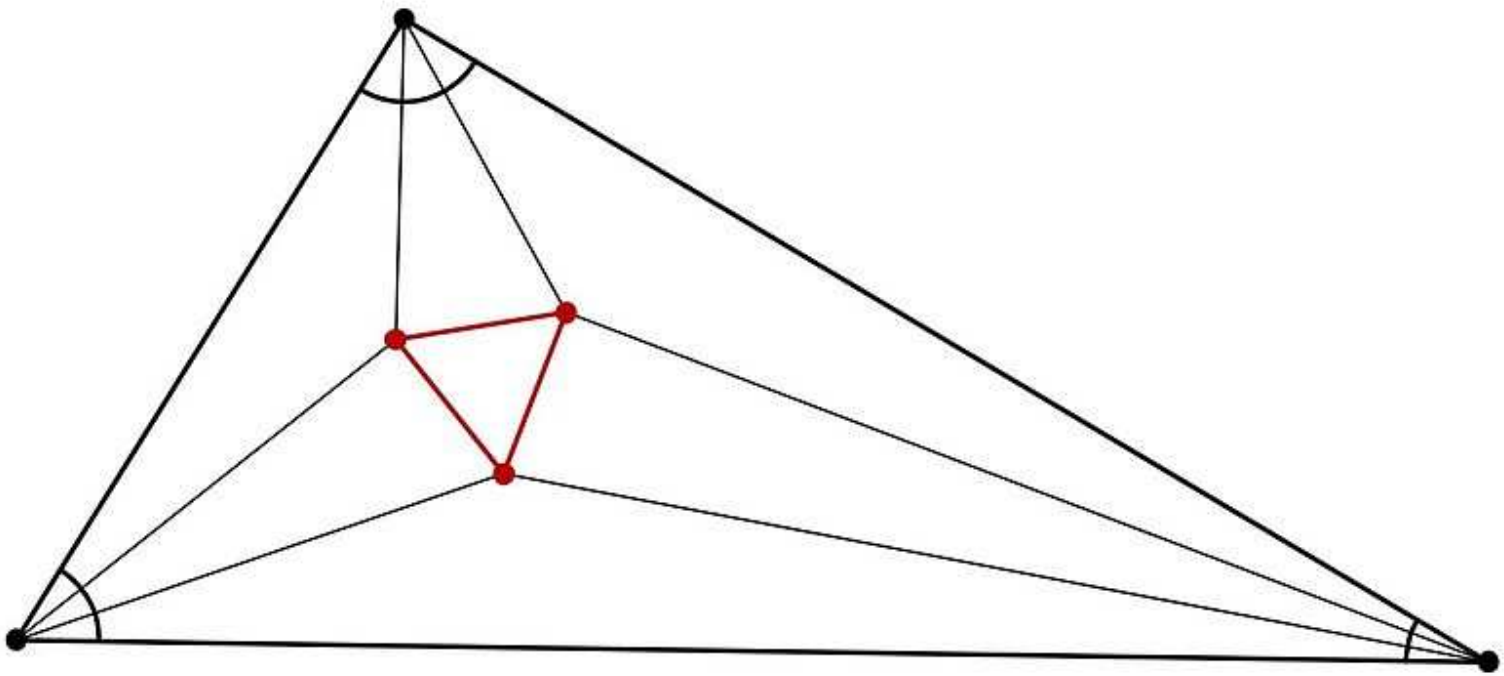
$\texttt{Parameter}\ mult_{Pp} : \mathbb{R} \to Pp \to Pp.$

$\texttt{Definition}\ vec\ p_1\ p_2 :=$
$\quad add_{Pp}\ (cons_{Pp}\ 1\ p_1)\ (cons_{Pp}\ -1\ p_2).$

Library


complexes_transformations
complexes_similitudes
composee_transformations
homoth_Euler
complexes_conjugaison
similitudes_directes
composee_translation_rotation
droite_Euler
applications_cocyclicite
complexes_dilatations
composee_dilatations
homothetie_plane
composee_reflexions
cocyclicite
operations_complexes
dilatations
rotation_plane
cercle
reflexion_plane
formes_complexes
equations_droites
isocele
determinant
mediatrice
orthocentre
complexes
aire_signee
metrique_triangle
angles_droites
trigo
projection_orthogonale
exercice_espace
angles_vecteurs
affine_classiques
orthogonalite_espace
repere_ortho_plan
Plan_espace
distance_euclidienne
representant_unitaire
Plans_paralleles
orthogonalite
Droite_plan_espace
produit_scalaire
Droite_espace
repere_plan
parallelisme_concours
coplanarite
milieu
mesure_algebrique
barycentre
alignement
vecteur
Field_affine
Rutile

Library



Proving

CoqIde

File Edit View Navigation Try Tactics Templates Queries Tools Compile Windows Help

exercice_morley.v

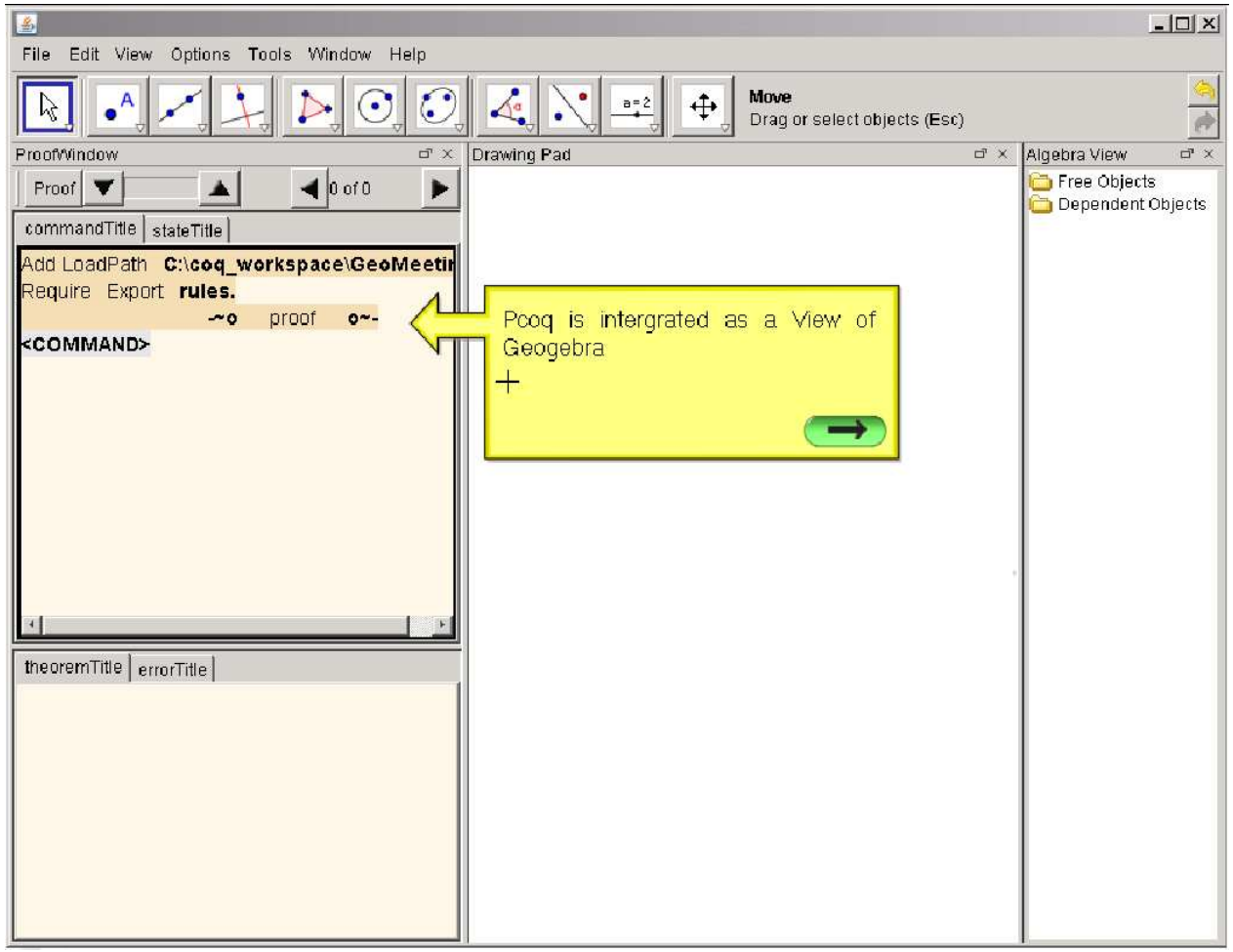
```
(* Theoreme de Morley : utilisation de la symetrie de la formule pour conclure.*)
Theorem Morley:
 forall (a b c : R) (A B C P Q T : PO),
 0 < a ->
 0 < b ->
 0 < c ->
 (a + b) + c = pisurtrois ->
 A <> B ->
 A <> C ->
 B <> C ->
 B <> P ->
 B <> Q ->
 A <> T ->
 C <> T ->
 image_angle b = cons_AV (vec B C) (vec B P) ->
 image_angle b = cons_AV (vec B P) (vec B Q) ->
 image_angle b = cons_AV (vec B Q) (vec B A) ->
 image_angle c = cons_AV (vec C P) (vec C B) ->
 image_angle c = cons_AV (vec C T) (vec C P) ->
 image_angle a = cons_AV (vec A B) (vec A Q) ->
 image_angle a = cons_AV (vec A Q) (vec A T) ->
 image_angle a = cons_AV (vec A T) (vec A C) ->  equilateral P Q T.
intros.
assert (triangle B C P).
apply (pisurtrois_triangle_utile2 (a:=a) (b:=b) (c:=c) (B:=B) (C:=C) (P:=P));
 auto.
deroule_triangle B C P.
assert (triangle B Q A).
apply (pisurtrois_triangle_utile2 (a:=a) (b:=b) (c:=c) (B:=B) (C:=Q) (P:=A));
 auto.
deroule_triangle B Q A.
assert (image_angle (3 * a) = cons_AV (vec A B) (vec A C)).
RReplace (3 * a) (a + (a + a)).
replace (cons_AV (vec A B) (vec A C))
    with (plus (cons_AV (vec A B) (vec A Q)) (cons_AV (vec A Q) (vec A C))).
```

```
image_angle c =
cons_AV
  (vec C P)
  (vec C B) ->
image_angle c =
cons_AV
  (vec C T)
  (vec C P) ->
image_angle a =
cons_AV
  (vec A B)
  (vec A Q) ->
image_angle a =
cons_AV
  (vec A Q)
  (vec A T) ->
image_angle a =
cons_AV
  (vec A T)
  (vec A C) ->
equilateral P Q
  T
```

Messages Errors Jobs

Ready, proving Morley Line: 751 Char: 40 Coq is ready 0 / 0

User Interface



Gröbner Basis

Geometry Theorem Proving Using Hilbert's Nullstellensatz

– Preliminary Version –

Deepak Kapur
Computer Science Branch
Corporate Research and Development
General Electric Company
Schenectady, NY

1. Introduction

The theory of elementary algebra and elementary geometry was shown to be decidable by Tarski using a quantifier elimination technique in the 1930's [26]. Subsquently, Tarski's decision algorithm was improved

Nullstellensatz

$$\forall X_1, \ldots, X_n \in R,$$
$$P_1(X_1, \ldots, X_n) = 0 \wedge \ldots \wedge P_s(X_1, \ldots, X_n) = 0$$
$$\Rightarrow P(X_1, \ldots, X_n) = 0$$

$$cP^r = \sum_{i=1}^{s} Q_i P_i, \quad (c \neq 0, \quad r > 0)$$

Polynomial Division

$$
\begin{array}{rr|l}
 & x^4y + x^2 - 1 & x^2 - z \\ \cline{3-3}
- & x^4y - x^2yz & x^2y + yz + 1 \\ \cline{2-2}
 & x^2yz + x^2 - 1 & \\
- & x^2yz - yz^2 & \\ \cline{2-2}
 & x^2 + yz^2 - 1 & \\
- & x^2 - z & \\ \cline{2-2}
 & yz^2 + z - 1 &
\end{array}
$$

Gröbner Basis

Dividing $x^2y^2 - y^4$ by $\{x^2 + 1, xy - 1\}$

$$x^2y^2 - y^4 \quad / \quad x^2 + 1 \qquad \rightsquigarrow \qquad -y^4 - y^2$$

$$x^2y^2 - y^4 \quad / \quad xy - 1 \qquad \rightsquigarrow \qquad -y^4 + 1$$

Gröbner Basis

$$\{x^2+1, xy-1\}$$

$$x^2y \quad / \quad x^2+1 \qquad \rightsquigarrow \qquad -y$$

$$x^2y \quad / \quad xy-1 \qquad \rightsquigarrow \qquad x$$

$$\{x^2+1, xy-1, x+y\}$$

Gröbner Basis

$$\{x^2+1, xy-1, x+y\}$$

$$x^2 \quad / \quad x^2+1 \qquad \rightsquigarrow \qquad -1$$

$$x^2 \quad / \quad x+y \qquad \rightsquigarrow \qquad -xy$$

$$\{x^2+1, xy-1, x+y\}$$

Gröbner Basis

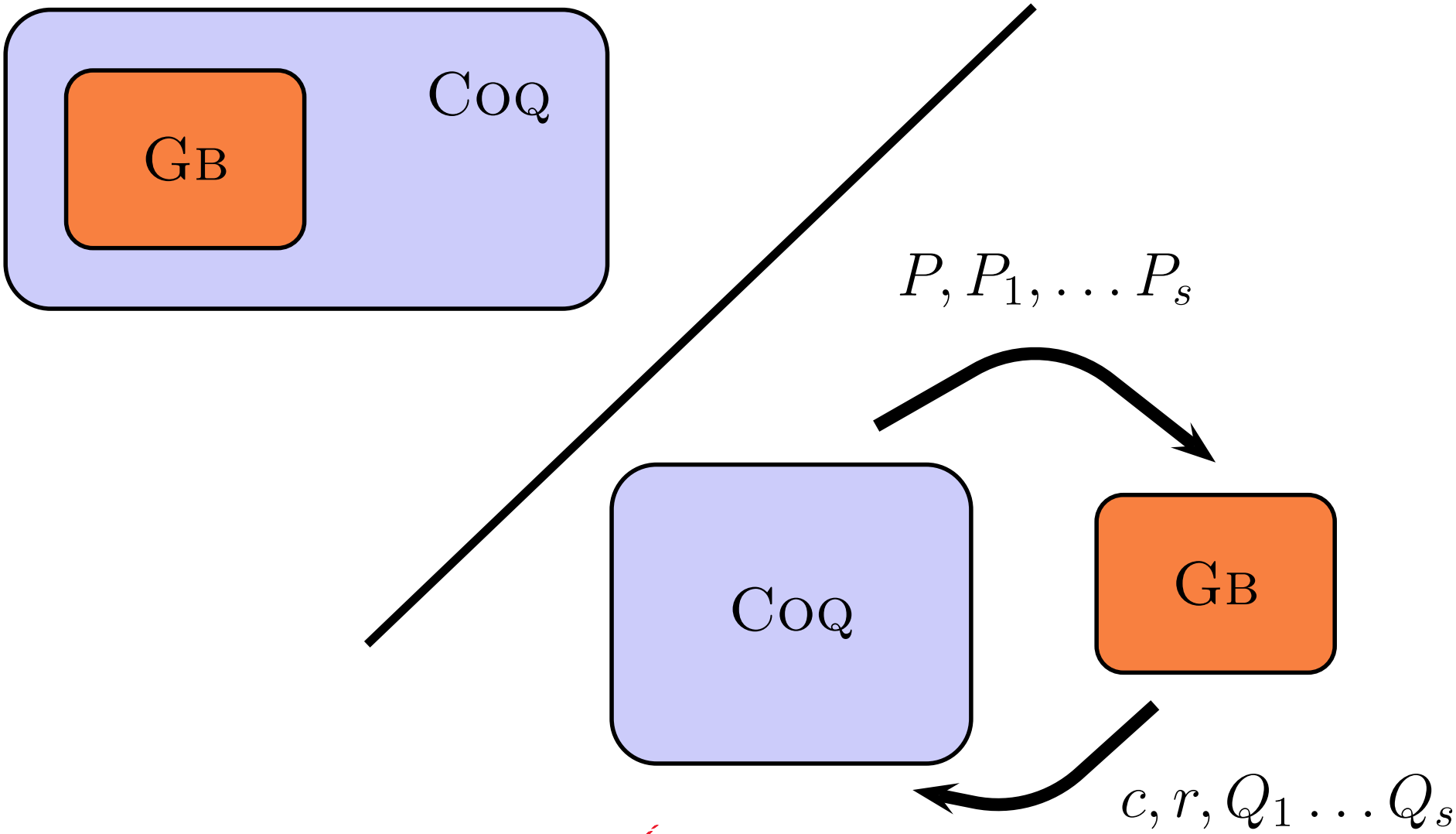
$$\{x^2+1, xy-1, x+y\}$$

$$xy \quad / \quad xy-1 \qquad \rightsquigarrow \qquad 1$$

$$xy \quad / \quad x+y \qquad \rightsquigarrow \qquad -y^2$$

$$\{x^2+1, xy-1, x+y, y^2-1\}$$

Integrating



Generating Certificate

$$P_1 = x^2 + 1, \qquad P_2 = xy - 1 \qquad P = x^3 - y$$

$$P_1 = 0 \wedge P_2 = 0 \Rightarrow P = 0$$

① Reduce P by the familly

$$R_1 = P - xP_1 = -x - y$$
$$R_2 = R_1 + P_3 = 0$$

② If it reduces to 0, terminate

$$0 = R_2 = R_1 + P_3 = (P - xP_1) + (yP_1 - xP_2)$$

$$P = (x - y)P_1 + xP_2$$

③ Adds a new spolynomial, goto ①

$$P_3 = yP_1 - xP_2 = x + y$$

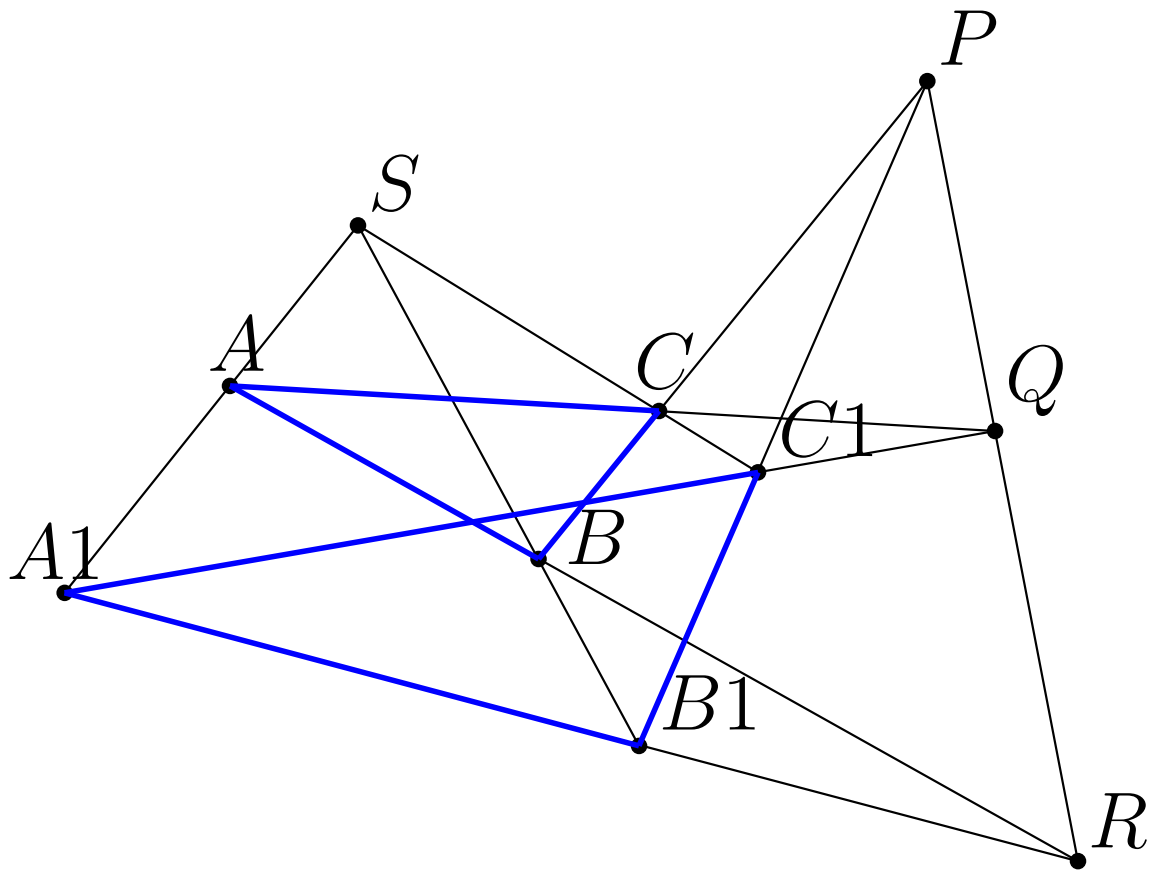
Certificate Format

$$
\begin{aligned}
CR = & \ [c_1, \ldots, c_{s+p}] \\
C = & \ [[a_{1\ s+1}, \ldots, a_{s\ s+1}], \\
& \ \ldots \\
& \ [a_{1\ s+p}, \ldots, a_{s\ s+p}, \ldots, a_{s+p-1\ s+p}]]
\end{aligned}
$$

$$
\begin{aligned}
CR = & \ [-x, 0, 1] \\
C = & \ [[y, -x]]
\end{aligned}
$$

Geometry Proving

Desargues



Encoding

`point` := $\{x : \mathbb{R},\ y : \mathbb{R}\}$.

`Definition` collinear $p_1\ p_2\ p_3$:=

$$(p_1.x - p_2.x)(p_3.y - p_2.y) - (p_1.y - p_2.y)(p_3.x - p_2.x) = 0.$$

`Definition` parallel $p_1\ p_2\ p_3\ p_4$:=

$$(p_1.x - p_2.x)(p_3.y - p_4.y) - (p_1.y - p_2.y)(p_3.x - p_4.x) = 0.$$

Coq Theorem

```
Lemma Desargues:  ∀ A B C A1 B1 C1 P Q R S : point,
    S.x = 0 ∧ S.y = 0
  ∧ A.y = 0
  ∧ collinear A S A1 ∧ collinear B S B1 ∧ collinear C S C1    ∧
collinear B1 C1 P ∧ collinear B C P
  ∧ collinear A1 C1 Q ∧ collinear A C Q
  ∧ collinear A1 B1 R ∧ collinear A B R
⇒
    collinear P Q R
  ∨ A, x = B.x
  ∨ A.x = C.x
  ∨ B.x = C.x
  ∨ A.x = 0
  ∨ collinear S B C
  ∨ parallel A C A1 C1

  ∨ parallel A B A1 B1.
```

Proving

```
Lemma Desargues: forall A B C A1 B1 C1 P Q R S:point,

  X S = 0 -> Y S = 0 -> Y A = 0 ->
  collinear A S A1 -> collinear B S B1 -> collinear C S C1 ->
  collinear B1 C1 P -> collinear B C P ->
  collinear A1 C1 Q -> collinear A C Q ->
  collinear A1 B1 R -> collinear A B R ->
  collinear P Q R
  \/ X A = X B \/ X A = X C \/ X B = X C  \/ X A = 0 \/ Y B = 0 \/
  \/ collinear S B C \/ parallel A C A1 C1 \/ parallel A B A1 B1.
Proof.
geo_begin.
idtac "Desargues".
Time
let lv := rev (X A
 :: X B
```

```
1 subgoal

(1/1)
forall A B C A1 B1 C1
P Q R S : point,
X S = 0 ->
Y S = 0 ->
Y A = 0 ->
collinear A S A1 ->
collinear B S B1 ->
collinear C S C1 ->
collinear B1 C1 P ->
```

Geometric Algebras

Implantation de l'Algèbre Géométrique en Objective Caml

S. Charneau, L. Fuchs & L. Aveneau

SIC, FRE CNRS 1731, Université de Poitiers
SP2MI, Bld Marie et Pierre Curie BP 30179
86962 Futuroscope Chasseneuil Cedex
`{charneau, fuchs, aveneau}@sic.univ-poitiers.fr`

Résumé

L'algèbre géométrique fournit un formalisme algébrique qui permet une description homogène des algorithmes géométriques. Cependant, la réalisation de bibliothèques logicielles utilisant ce formalisme reste assez délicate.

Dans cet article, nous présentons deux implantations de l'algèbre géométrique en Objective Caml. La première décrit l'algèbre géométrique d'un espace vectoriel prédéfini, tandis que la seconde présente un module générique de l'algèbre géométrique indépendant de tout espace (pseudo) euclidien. Ces implantations sont comparées à une autre écrite en C++, tant au niveau de leur programmation que de leur efficacité.

Geometric Algebras

On the Exterior Calculus of Invariant Theory

MARILENA BARNABEI*

Istituto Matematico, Università di Ferrara,
Via Machiavelli, 35, 44100 Ferrara, Italy

ANDREA BRINI*

Dipartimento di Matematica, Università di Bologna,
Piazza di Porta S. Donato, 5, 40127 Bologna, Italy

AND

GIAN-CARLO ROTA†

Department of Mathematics, Massachusetts Institute of Technology,
Cambridge, Massachusetts 02139

Communicated by David Buchsbaum

Received March 27, 1984

1. INTRODUCTION

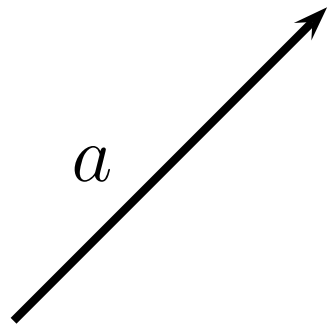
The full extent of the tragedy of Hermann Grassmann, which has been unfolding since his death, by a succession of misadventures and mis-

Geometric Algebras

$$\cdot \qquad + \qquad \vee \qquad \wedge \qquad \bullet \qquad \llcorner \qquad \lrcorner$$

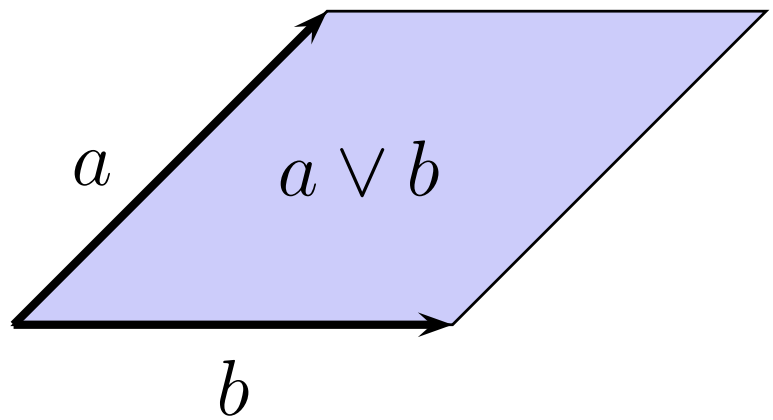
$$K^n \qquad G^n \qquad Cl^n$$

Grassmann-Cayley Algebra



vectors: $a, b, c, \ldots$
scalar: λa
sum: $a + b$

Join Product



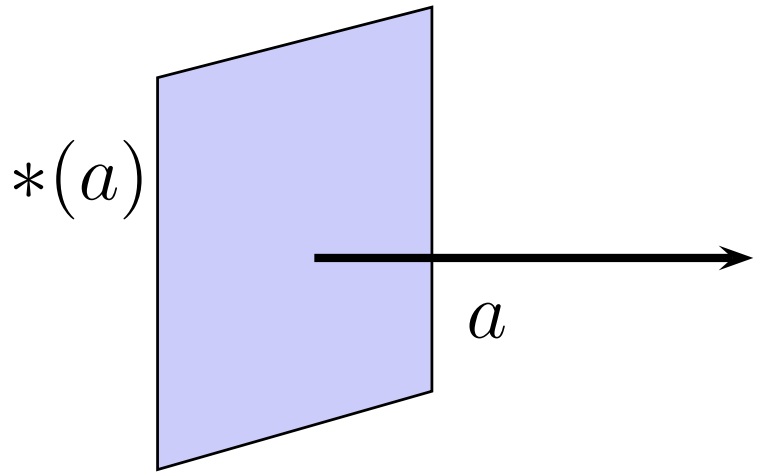
bi-vector: $a \vee b$

$$a \vee a = 0 \qquad a \vee b = -b \vee a$$

$$\lambda a \vee b = \lambda(a \vee b) \qquad (a + b) \vee c = (a \vee c) + (b \vee c)$$

Ex: $(\lambda a + \beta b) \vee (a \vee b) = 0$

Duality

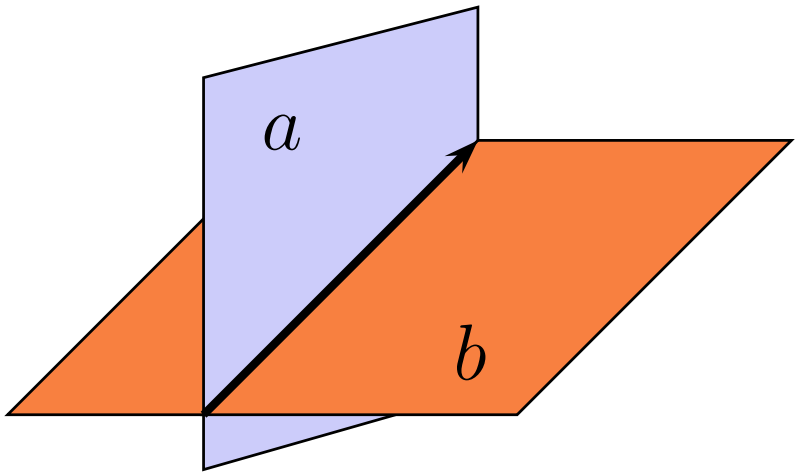


duality: $*(a)$

$$*(a+b) = *(a) + *(b) \qquad *(\lambda(a)) = \lambda *(a)$$

$$a \vee *(a) = \pm E \qquad *(*(a)) = (-1)^{k(n+1)} a$$

Meet



meet: $a \wedge b$

$$*(a \wedge b) = *(a) \vee *(b) \qquad *(a \vee b) = *(a) \wedge *(b)$$

G^3

Grade 0: 1

Grade 1: $e_1, \quad e_2, \quad e_3$

Grade 2: $e_1 \vee e_2, \quad e_1 \vee e_3, \quad e_2 \vee e_3$

Grade 3: $E = e_1 \vee e_2 \vee e_3$

Grassman Algebra

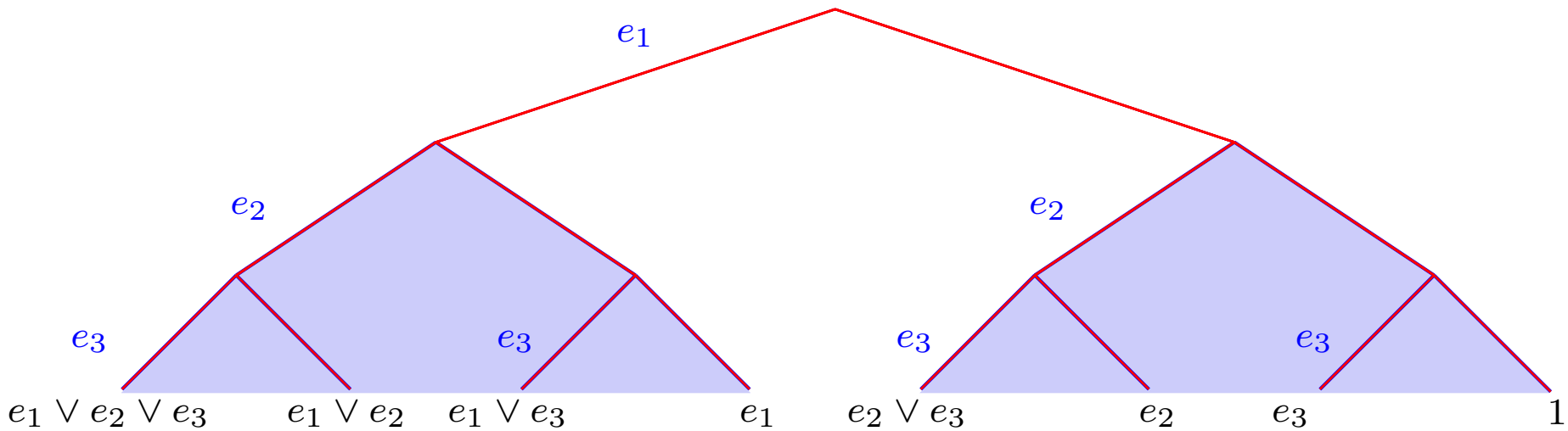
Binary Tree: $G^{n+1} = G^n \times G^n$

$$G^0 = K$$
$$G^1 = K \times K$$
$$G^2 = (K \times K) \times (K \times K)$$
$$G^3 = ((K \times K) \times (K \times K)) \times ((K \times K) \times (K \times K))$$

Interpretation w.r.t $(e_1, e_2, \ldots, e_n)$

$$[\![(x,\, y)_i]\!] = e_i \vee [\![x]\!] + [\![y]\!]$$

G^3



Base of G^3 :

$$\{\ 1,\ e_1, e_2, e_3,\ e_1 \vee e_2, e_1 \vee e_3, e_2 \vee e_3,\ e_1 \vee e_2 \vee e_3\ \}$$

Conjugate

$$X \vee a = a \vee \overline{X}$$

Ex: $(e_2 + e_2 \vee e_3) \vee e_1 = e_1 \vee (-e_2 + e_2 \vee e_3)$

Recursive definition

$$\begin{aligned} \overline{(X, Y)} &= (-\overline{X}, \overline{Y}) \\ \overline{\alpha} &= \alpha \end{aligned}$$

Join Product

$$
\begin{aligned}
&(e_i \vee X + Y) \vee (e_i \vee X' + Y') \\
&\quad = \quad e_i \vee X \vee Y' + Y \vee e_i \vee X' + Y \vee Y' \\
&\quad = \quad e_i \vee (X \vee Y' + \overline{Y} \vee X') + Y \vee Y'
\end{aligned}
$$

Recursive definition

$$
\begin{aligned}
(X, Y) \vee (X', Y') &= (X \vee Y' + \overline{Y} \vee X', Y \vee Y') \\
\alpha \vee \beta &= \alpha\beta
\end{aligned}
$$

Hodge Duality

Recursive definition

$$
\begin{aligned}
(X,Y) &= ((\overline{Y}), *(X)) \\
*(\alpha) &= \alpha
\end{aligned}
$$

Meet Product

Definition

$$X \wedge Y \quad = \quad *(*(X) \vee *(Y))$$

Geometry of Incidence

points p_i

elements of grade 1 (vector)

p_1 is a free point on line $[p_2, p_3]$

$p_1 \vee p_2 \vee p_3 = 0$ and $p_2 \vee p_3 \neq 0$

p_1 is the intersection of $[p_2, p_3]$ and $[p_4, p_5]$

$p_1 = (p_2 \vee p_3) \wedge (p_4 \vee p_5)$

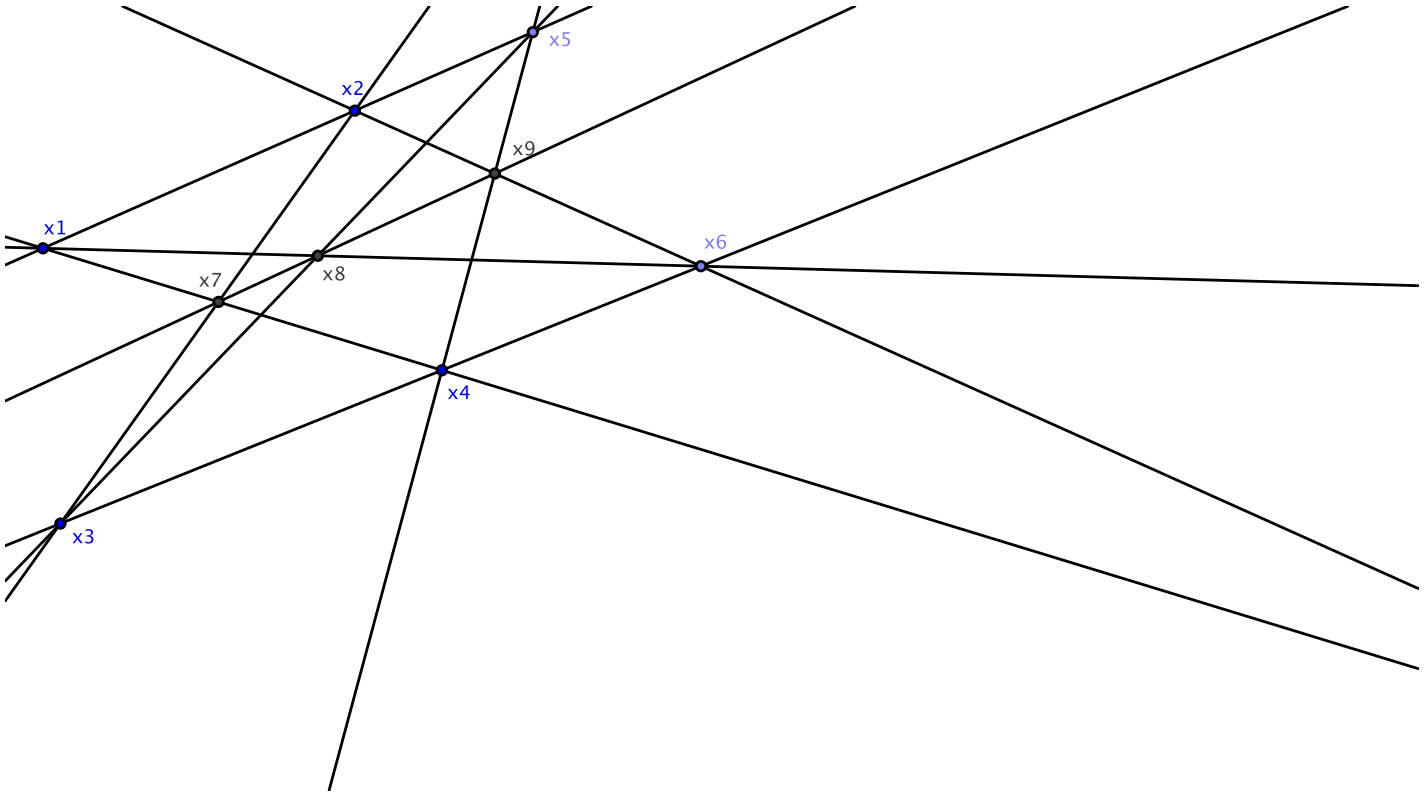
p_1 p_2 and p_3 are collinear

$p_1 \vee p_2 \vee p_3 = 0$

encoding in G^3

Geometry of Incidence

Pappus



Geometry of Incidence

```
∀ x1 x2 x3 x4 x5 x6 x7 x8 x9 :  point K,
if x5 :=:  free on [x1,x2]            and
   x6 :=:  free on [x3,x4]            and
   x7 :=:  [x2,x3] inter [x1,x4]      and
   x8 :=:  [x3,x5] inter [x1,x6]      and
   x9 :=:  [x4,x5] inter [x2,x6]
then collinear [x7, x8, x9]
```

Geometry of Incidence

$\forall\ x_1\ x_2\ x_3\ x_4\ x_5\ x_6\ x_7\ x_8\ x_9\ :\ \ K\hat{}3,$

$\text{if}\ x_1 \vee x_2 \neq 0\ \text{and}\ x_5 \vee x_1 \vee x_2 = 0\ \text{and}$

$\quad x_3 \vee x_4 \neq 0\ \text{and}\ x_6 \vee x_3 \vee x_4 = 0\ \text{and}$

$\quad x_7 = x_2 \vee x_3 \wedge x_1 \vee x_4\ \ \text{and}$

$\quad x_8 = x_3 \vee x_5 \wedge x_1 \vee x_6\ \ \text{and}$

$\quad x_9 = x_4 \vee x_5 \wedge x_2 \vee x_6$

$\text{then}\ x_7 \vee x_8 \vee x_9 = 0$

Proving

A geometric identity for Pappus' theorem

MICHAEL HAWRYLYCZ

Computer Research and Applications Group, Los Alamos National Laboratory, Los Alamos, NM 87544

Communicated by Gian-Carlo Rota, December 15, 1993

ABSTRACT **An expression in the exterior algebra of a Peano space yielding Pappus' theorem was originally given by Doubilet, Rota, and Stein [Doubilet, P., Rota, G.-C. & Stein, J. (1974) *Stud. Appl. Math.* 8, 185–216]. Motivated by an identity of Rota, I give an identity in a Grassmann–Cayley algebra of step 3, involving joins and meets alone, which expresses the theorem of Pappus.**

Proving

Automated Theorem Proving in Incidence Geometry – A Bracket Algebra Based Elimination Method

Hongbo Li and Yihong Wu

Academy of Mathematics and System Sciences
Chinese Academy of Sciences
Beijing 100080, P. R. China
{hli, yhwu}@mmrc.iss.ac.cn

Abstract. In this paper we propose a bracket algebra based elimination method for automated generation of readable proofs for theorems in incidence geometry. This method features three techniques, the first

Proving

CoqIde

File Edit View Navigation Try Tactics Templates Queries Tools Compile Windows Help

Tuple3.v

```
Section Pappus.

Lemma pappus :   forall x1 x2 x3 x4 x5 x6 x7 x8 x9: point K,
  x5 is_free_on [x1, x2] ->
  x6 is_free_on [x3, x4] ->
  x7 is_the_intersection_of [x2, x3] and [x1, x4] ->
  x8 is_the_intersection_of [x3, x5] and [x1, x6] ->
  x9 is_the_intersection_of [x4, x5] and [x2, x6] ->
  [x7, x9, x9] are_collinear.
Proof.
Time mTac.
Time Qed.
```

Messages

Ready in FF Line: 2226 Char: 12 Coq is ready 0 / 0

Conclusions

Plane Geometry : Nice Toy Example

Revisiting Standard Mathematics

Combining Proving and Computing

Certificate