Representation Change in the Formalization of Geometry in Coq

Gabriel Braun Jérémie Koenig Julien Narboux Pascal Schreck

University of Strasbourg - LSIIT - ICube - CNRS

Strasbourg, July 2012

Automatic Deduction in Geometry

Algebraic methods

- Gröbner bases [Kap86]
- Wu's method [Wu78, Cho85, Cho88, Wan01, Wan04]
- Geometric Algebra [LW00]

Synthetic

- Gelernter [Gel59]
- Deductive database [cCsGzZ00]
- The area method [CGZ94]
- Full angle method [CGZ96]

Automatic Deduction in Geometry

Algebraic methods

- Gröbner bases [Kap86][Pot08, GPT10][CW07]
- Wu's method [Wu78, Cho85, Cho88, Wan01, Wan04]
- Geometric Algebra [LW00][FT11]

Synthetic

- Gelernter [Gel59]
- Deductive database [cCsGzZ00]
- The area method [CGZ94][Nar04, JNQ10]
- Full angle method [CGZ96]

Automatic Deduction in Geometry

Algebraic methods

- Gröbner bases [Kap86][Pot08, GPT10][CW07]
- Wu's method [Wu78, Cho85, Cho88, Wan01, Wan04]
- Geometric Algebra [LW00][FT11]

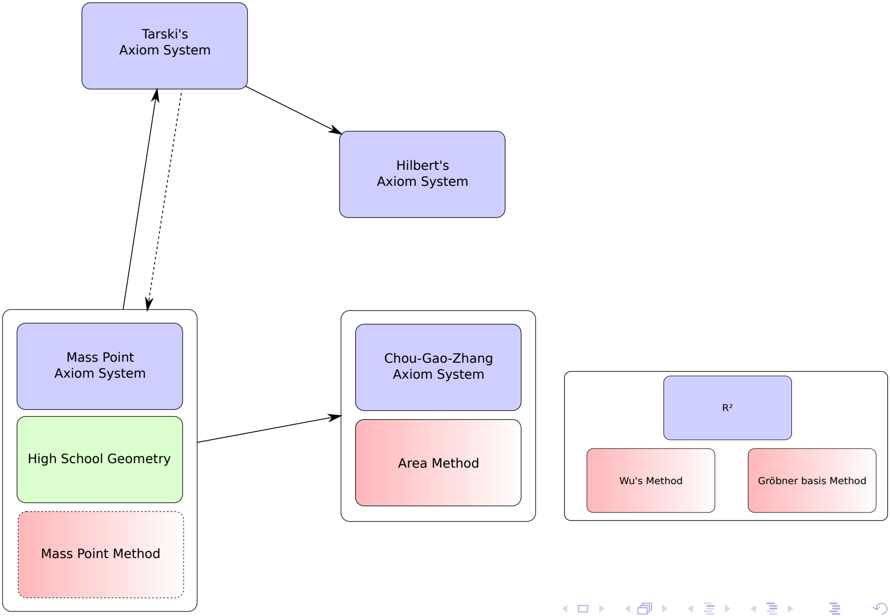
Synthetic

- Gelernter [Gel59]
- Deductive database [cCsGzZ00]
- The area method [CGZ94][Nar04, JNQ10]
- Full angle method [CGZ96]

Formalization of Geometry in Coq

- Projective Geometry [MNS09]
- High-school Geometry [Gui04, PBN11]
- Hilbert's Geometry [DDS00]
- Tarski's Geometry [Nar08, BN12]

Formalization of Geometry in Coq



Outline

Example of change of representation

Hilbert style world	Tarski's or algebraïc world
Point	Point
Line	Pair of distinct points
Circle	Pair of distinct points
$\parallel$:: $Line \rightarrow Line \rightarrow Prop$	$\parallel$: $Point^4 \rightarrow Prop$
$\perp$:: $Line \rightarrow Line \rightarrow Prop$	$\perp$: $Point^4 \rightarrow Prop$

How to translate a statement from one language to the other one ?

Definition of the defining points of circles and lines

GeoProof Construction	**Defining points**
l passing through A and B	$\mathcal{P}_1(l) = A$ $\mathcal{P}_2(l) = B$
l parallel line to m passing through A	$\mathcal{P}_1(l) = A$ $\mathcal{P}_2(l) = P2_l$
l perpendicular line to m passing through A	$\mathcal{P}_1(l) = A$ $\mathcal{P}_2(l) = P2_l$
l perpendicular bisector of A and B	$\mathcal{P}_1(l) = P1_l$ $\mathcal{P}_2(l) = P2_l$
l bisector of the angle formed by A, B and C	$\mathcal{P}_1(l) = B$ $\mathcal{P}_2(l) = P2_l$
c circle of center O passing through A	$\mathcal{O}(c) = O$ $\mathcal{P}(c) = A$
c circle whose diameter is AB	$\mathcal{O}(c) = O_c$ $\mathcal{P}(c) = A$

GeoProof Construction	Predicate form
Free point	*true*
Point P on line l	$collinear(P, \mathcal{P}_1(l), \mathcal{P}_2(l))$
Point P on circle c	$\mathcal{O}(c)\mathcal{P}(c) = P\mathcal{O}(c)$
I midpoint of A and B	$IA = IB \wedge collinear(I, A, B)$
I intersection of l_1 and l_2	$collinear(I, \mathcal{P}_1(l_1), \mathcal{P}_2(l_1)) \wedge$ $collinear(I, \mathcal{P}_1(l_2), \mathcal{P}_2(l_2)) \wedge$ $\neg parallel(\mathcal{P}_1(l_1), \mathcal{P}_2(l_1), \mathcal{P}_1(l_2), \mathcal{P}_2(l_2))$
I an intersection of c_1 and c_2	$I\mathcal{O}(c_1) = \mathcal{O}(c_1)\mathcal{P}(c_1) \wedge$ $I\mathcal{O}(c_2) = \mathcal{O}(c_2)\mathcal{P}(c_2) \wedge$ $\neg isotropic(\mathcal{O}(c_1), \mathcal{O}(c_2))$
I an intersection of c and l	$I\mathcal{O}(c) = \mathcal{O}(c)\mathcal{P}(c) \wedge$ $collinear(I, \mathcal{P}_1(l), \mathcal{P}_2(l)) \wedge$ $\neg isotropic(\mathcal{P}_1(l), \mathcal{P}_2(l))$
l passing through A and B	$A \neq B$
l parallel to m passing through A	$parallel(A, \mathcal{P}_2(l), \mathcal{P}_1(m), \mathcal{P}_2(m)) \wedge$ $A \neq \mathcal{P}_2(l)$
l perpendicular to m passing through A	$perpendicular(A, \mathcal{P}_2(l), \mathcal{P}_1(m), \mathcal{P}_2(m)) \wedge$ $A \neq \mathcal{P}_2(l)$
l perpendicular bisector of A and B	$\mathcal{P}_1(l)A = \mathcal{P}_1(l)B \wedge \mathcal{P}_2(l)A = \mathcal{P}_2(l)B \wedge$ $\mathcal{P}_1(l) \neq \mathcal{P}_2(l) \wedge A \neq B$
l bisector of the angle A,B,C	$eq\_angle(A, B, \mathcal{P}_2(l), \mathcal{P}_2(l), B, C) \wedge$ $B \neq \mathcal{P}_2(l) \wedge A \neq B \wedge B \neq C$
c circle of center O passing through A	*true*
c circle whose diameter is A B	$collinear(\mathcal{O}(c), A, B) \wedge$ $\mathcal{O}(c)A = \mathcal{O}(c)B$

Questions

- How to be convinced that this transformation is correct ?
- How to build a tactic which performs this transformation ?
    - using an *adhoc* tactic written in Ltac
    - using a correct by construction approach

Type classes

A way to formalize algebraic structures/ axiom systems/ generic interfaces.

Example: Monoid

Definition

A monoid is a mathematical structure composed of :

- A carrier A
- A binary, associative operation . on A
- A neutral element $1 \in A$ for .

Type class definition

```
Class Monoid {A:Type}(dot : A -> A -> A)(unit : A)
: Type := {
dot_assoc : forall x y z:A,
dot x (dot y z)= dot (dot x y) z;
unit_left : forall x, dot unit x = x;
unit_right : forall x, dot x unit = x }.
```

Remark

Behind the scene classes are implemented using records.

Power

A general definition of power

```
Fixpoint power `{M :Monoid A dot one}(a:A)(n:nat) :=
match n with 0%nat => one
| S p => dot a (power a p)
end.
```

Formalization of signature/logic (Jérémie Koenig)

```
Class Contextes := context : Type.

Class Formulas `{Ctx : Contexts} := formula:context → Type

Class ExtendFormula `{F : Formulas} `{Cle : Le context} :=
  extend_formula :
    ∀ (Γ Γ' : context) {HΓ : PropHolds (Γ ≤ Γ')},
                                    formula Γ → formula Γ'.

Notation "φ ↑ Γ" := (extend_formula _ Γ φ) (at level 40).
```

Valuations

```
Class Sat ‘{F : !Formulas} :=
  sat :> ∀ {Γ} I {HI : PropHolds (well_formed Γ I)},
    Denotation (formula Γ) Prop.
```

Sortes, Termes, . . .

```
Class Sorts :=
  sort : Set.
Class Terms `{Contexts} `{Sorts} :=
  term : context → sort → Type.
```

Interpretation

```
Class Carriers `{S : Sorts} :=
  carrier :> Denotation sort Type.
Class Interpretation `{S : Sorts}
                     `{T : !Terms}
                     `{E : !Carriers} :=
  value :> ∀ {Γ} I {HI : PropHolds (well_formed Γ I)},
    ∀ {s : sort}, Denotation (term Γ s) [[s]].
```

In the future

- Define the two signatures.
- Define the translation.
- Show that the translation preserves satisfiability.

Tarski's axiom system

- 11 axioms
- dimension of the space can be changed easily
- many proofs do not use Euclidean axiom
- most axioms have been shown to be independent from the others [Gup65]

Motivations

- for education we need the concept of lines, half-lines, angle,. . .
- Hilbert's axioms are higher level.

Tarski's axiom system

Identity	$\beta\ A\ B\ A \Rightarrow (A = B)$
Pseudo-Transitivity	$AB \equiv CD \land AB \equiv EF \Rightarrow CD \equiv EF$
Symmetry	$AB \equiv BA$
Identity	$AB \equiv CC \Rightarrow A = B$
Pasch	$\beta\ A\ P\ C \land \beta\ B\ Q\ C \Rightarrow \exists X, \beta\ P\ X\ B \land \beta\ Q\ X\ A$
Euclid	$\exists XY, \beta\ A\ D\ T \land \beta\ B\ D\ C \land A \neq D \Rightarrow$ $\beta\ A\ B\ X \land \beta\ A\ C\ Y \land \beta\ X\ T\ Y$
5 segments	$AB \equiv A'B' \land BC \equiv B'C' \land$ $AD \equiv A'D' \land BD \equiv B'D' \land$ $\beta\ A\ B\ C \land \beta\ A'\ B'\ C' \land A \neq B \Rightarrow CD \equiv C'D'$
Construction	$\exists E, \beta\ A\ B\ E \land BE \equiv CD$
Lower Dimension	$\exists ABC, \neg\beta\ A\ B\ C \land \neg\beta\ B\ C\ A \land \neg\beta\ C\ A\ B$
Upper Dimension	$AP \equiv AQ \land BP \equiv BQ \land CP \equiv CQ \land P \neq Q$ $\Rightarrow \beta\ A\ B\ C \lor \beta\ B\ C\ A \lor \beta\ C\ A\ B$
Continuity	$\forall XY, (\exists A, (\forall xy, x \in X \land y \in Y \Rightarrow \beta\ A\ x\ y)) \Rightarrow$ $\exists B, (\forall xy, x \in X \Rightarrow y \in Y \Rightarrow \beta\ x\ B\ y)$.

Tarski's axiom system in Coq

```
Class Tarski := {
 Tpoint : Type;
 Bet   : Tpoint -> Tpoint -> Tpoint -> Prop;
 Cong : Tpoint -> Tpoint -> Tpoint -> Tpoint -> Prop;
 between_identity : forall A B, Bet A B A -> A=B;
 cong_pseudo_reflexivity : forall A B : Tpoint, Cong A B B A;
 cong_identity : forall A B C : Tpoint, Cong A B C C -> A = B;
 cong_inner_transitivity : forall A B C D E F : Tpoint,
   Cong A B C D -> Cong A B E F -> Cong C D E F;
 inner_pasch : forall A B C P Q : Tpoint,
   Bet A P C -> Bet B Q C -> exists x, Bet P x B /\ Bet Q x A;
 euclid : forall A B C D T : Tpoint,
   Bet A D T -> Bet B D C -> A<>D ->
   exists x, exists y, Bet A B x /\ Bet A C y /\ Bet x T y;
 five_segments : forall A A' B B' C C' D D' : Tpoint,
   Cong A B A' B' -> Cong B C B' C' -> Cong A D A' D' -> Cong B D B' D' ->
   Bet A B C -> Bet A' B' C' -> A <> B -> Cong C D C' D';
 segment_construction : forall A B C D : Tpoint,
   exists E : Tpoint, Bet A B E /\ Cong B E C D;
 lower_dim : exists A, exists B, exists C, ~ (Bet A B C \/ Bet B C A \/ Bet C A B);
 upper_dim : forall A B C P Q : Tpoint,
   P <> Q -> Cong A P A Q -> Cong B P B Q -> Cong C P C Q ->
   (Bet A B C \/ Bet B C A \/ Bet C A B)
}
```

Hilbert's axiom system

Hilbert axiom system is based on two abstract types: points and lines

```
Point : Type
Line  : Type
```

We assume that the type `Line` is equipped with an equivalence relation `EqL` which denotes equality between lines:

```
EqL     : Line -> Line -> Prop
EqL_Equiv : Equivalence EqL
```

We do not use Leibniz equality (the built-in equality of Coq), because when we will define the notion of line inside Tarski's system, the equality will be a defined notion.

Incidence Axioms I

Axiom (I 1)

For every two distinct points A, B there exist a line l such that A and B are incident to l.

```
line_existence : forall A B, A<>B ->
                 exists l, Incid A l /\ Incid B l;
```

Axiom (I 2)

For every two distinct points A, B there exist at most one line l such that A and B are incident to l.

```
line_unicity : forall A B l m, A <> B ->
Incid A l -> Incid B l -> Incid A m -> Incid B m -> EqL l m;
```

Incidence Axioms II

Axiom (I 3)

There exist at least two points on a line. There exist at least three points that do not lie on a line.

```
two_points_on_line : forall l, exists A, exists B,
                     Incid B l /\ Incid A l /\ A <> B

ColH A B C := exists l, Incid A l /\ Incid B l /\ Incid C l

plan : exists A, exists B, exists C, ~ ColH A B C
```

Order Axioms I

```
BetH : Point -> Point -> Point -> Prop
```

Axiom (II 1)

If a point B lies between a point A and a point C then the point A,B,C are three distinct points through of a line, and B also lies between C and A.

```
between_col : forall A B C:Point, BetH A B C -> ColH A B C
between_comm: forall A B C:Point, BetH A B C -> BetH C B A
```

Axiom (II 2)

For two distinct points A and B, there always exists at least one point C on line AB such that B lies between A and C.

```
between_out :  forall A B   : Point,
                  A <> B -> exists C : Point, BetH A B C
```

Order Axioms II

Axiom (II 3)

Of any three distinct points situated on a straight line, there is always one and only one which lies between the other two.

```
between_only_one : forall A B C : Point,
              BetH A B C -> ~ BetH B C A /\ ~ BetH B A C

between_one : forall A B C, A<>B -> A<>C -> B<>C ->
  ColH A B C -> BetH A B C \/ BetH B C A \/ BetH B A C
```

Order Axioms III

Axiom (II 4 - Pasch)

Let A, B and C be three points that do not lie in a line and let a be a line (in the plane ABC) which does not meet any of the points A, B, C. If the line a passes through a point of the segment AB, it also passes through a point of the segment AC or through a point of the segment BC.

To give a formal definition for this axiom we need an extra definition:

```
cut l A B := ~Incid A l /\ ~Incid B l /\
                      exists I, Incid I l /\ BetH A I B
```

```
pasch : forall A B C l, ~ColH A B C -> ~Incid C l ->
       cut l A B -> cut l A C \/ cut l B C
```

Parallels

```
Para l m := ~ exists X, Incid X l /\ Incid X m;
euclid_existence : forall l P, ~ Incid P l ->
                             exists m, Para l m;
euclid_unicity :  forall l P m1 m2, ~ Incid P l ->
                        Para l m1 -> Incid P m1 ->
                        Para l m2 -> Incid P m2 ->
                                      EqL m1 m2;
```

Congruence Axioms I

Axiom (IV 1)

If A, B are two points on a straight line a, and if A' is a point upon the same or another straight line a', then, upon a given side of A' on the straight line a', we can always find one and only one point B' so that the segment AB is congruent to the segment $A'B'$. We indicate this relation by writing $AB \equiv A'B'$.

```
cong_existence : forall A B l M, A <> B -> Incid M l ->
   exists A', exists B', Incid A' l /\ Incid B' l /\
          BetH A' M B' /\  CongH M A' A B /\ CongH M B' A B

cong_unicity : forall A B l M A' B' A'' B'',A<>B -> Incid M l
   Incid A'  l     -> Incid B'  l ->
   BetH A'  M B'  -> CongH M A'  A B -> CongH M B'  A B ->
   Incid A'' l     -> Incid B'' l ->
   BetH A'' M B'' -> CongH M A'' A B -> CongH M B'' A B ->
   (A' = A'' /\ B' = B'') \/ (A' = B'' /\ B' = A'')
```

Congruence Axioms II

Axiom (IV 2)

If a segment AB is congruent to the segment $A'B'$ and also to the segment $A''B''$, then the segment $A'B'$ is congruent to the segment $A''B''$.

```
cong_pseudo_transitivity : forall A B A' B' A'' B'',
 CongH A B A' B' -> CongH A B A'' B'' -> CongH A' B' A'' B''
```

Congruence Axioms III

Axiom (IV 3)

Let AB and BC be two segments of a straight line a which have no points in common aside from the point B, and, furthermore, let $A'B'$ and $B'C'$ be two segments of the same or of another straight line a' having, likewise, no point other than B' in common. Then, if $AB \equiv A'B'$ and $BC \equiv B'C'$, we have $AC \equiv A'C'$.

```
Definition disjoint A B C D :=
         ~ exists P, Between_H A P B /\ Between_H C P D.

 addition: forall A B C A' B' C',
     ColH A B C -> ColH A' B' C' ->
     disjoint A B B C -> disjoint A' B' B' C' ->
     CongH A B A' B' -> CongH B C B' C' -> CongH A C A' C'
```

Congruence Axioms III

Axiom (IV-4)

Given an angle α, an half-line h emanating from a point O and given a point P, not on the line generated by h, there is a unique half-line h' emanating from O, such as the angle α' defined by (h, O, h') is congruent with α and such every point inside α' and P are on the same side relatively to the line generated by h.

Axiom (IV 5)

If the following congruences hold $AB \equiv A'B'$, $AC \equiv A'C'$, $\measuredangle BAC \equiv \measuredangle B'A'C'$ then $\measuredangle ABC \equiv \measuredangle A'B'C'$

Hilbert follows from Tarski

We need to define the concept of line:

```
Record Couple {A:Type} : Type :=
       build_couple {P1: A ; P2 : A ; Cond: P1 <> P2}.

Definition Line := @Couple Tpoint.

Definition Eq : relation Line :=
       fun l m => forall X, Incident X l <-> Incident X m.
```

Main result

```
Section Hilbert_to_Tarski.

Context `{T:Tarski}.

Instance Hilbert_follow_from_Tarski : Hilbert.
Proof.
 ... (* omitted here *)
Qed.

End Hilbert_to_Tarski.
```

Overview

Chapter 2: betweness properties

Chapter 3: congruence properties

Chapter 4: properties of betweeness and congruence

Chapter 5: order relation over pair of points

Chapter 6: the ternary relation out

Chapter 7: property of the midpoint

Chapter 8: orthogonality lemmas

Chapter 9: position of two points relatively to a line

Chapter 10: orthogonal symmetry

Chapter 11: properties about angles

Chapter 12: parallelism

Statistics

Chapter	lemmas	lines of specification	lines of proof
Betweeness properties	16	69	111
Congruence properties	16	54	116
Properties of betweeness and congruence	19	151	183
Order relation over pair of points	17	88	340
The ternary relation out	22	103	426
Property of the midpoint	21	101	758
Orthogonality lemmas	77	191	2412
Position of two points relatively to a line	37	145	2333
Orthogonal symmetry	44	173	2712
Properties about angles	187	433	10612
Parallelism	68	163	3560

Conclusion

- Clear foundations for geometry
- Next step: define analytic geometry inside Tarski.
- Proof of correctness for ADG

Questions ?

Bibliography I

Gabriel Braun and Julien Narboux.
From tarski to hilbert, 2012.
submitted to ADG 2012.

Shang ching Chou, Xiao shan Gao, and Jing zhong Zhang.
A deductive database approach to automated geometry theorem proving and discovering.
Journal of Automated Reasoning, 25:219–246, 2000.

Shang-Ching Chou, Xiao-Shan Gao, and Jing-Zhong Zhang.
Machine Proofs in Geometry.
World Scientific, Singapore, 1994.

Shang-Ching Chou, Xiao-Shan Gao, and Jing-Zhong Zhang.
Automated generation of readable proofs with geometric invariants, theorem proving with full angle.
Journal of Automated Reasoning, 17:325–347, 1996.

Bibliography II

Shang-Ching Chou.
Proving and discovering geometry theorems using Wu's method.
PhD thesis, The University of Texas, Austin, December 1985.

Shang-Ching Chou.
Mechanical Geometry Theorem Proving.
D. Reidel Publishing Company, 1988.

Amine Chaieb and Makarius Wenzel.
Context aware Calculation and Deduction — Ring Equalities via Gröbner Bases in Isabelle.
In M. Kauers, M. Kerber, R. Miner, and W. Windsteiger, editors, *CALCULEMUS 2007*, volume 4573 of *Lecture Notes in Computer Science*, pages 27–39. Springer, 2007.

Bibliography III

Christophe Dehlinger, Jean-François Dufourd, and Pascal Schreck.
Higher-order intuitionistic formalization and proofs in Hilbert's elementary geometry.
In *Automated Deduction in Geometry*, pages 306–324, 2000.

Laurent Fuchs and Laurent Théry.
A Formalisation of Grassmann-Cayley Algebra in Coq.
In *Post-proceedings of Automated Deduction in Geometry (ADG 2010)*, 2011.

H. Gelernter.
Realization of a geometry theorem machine.
In *Proc. Int. Conf. in Info. Process*, pages 273–282, Paris, 1959.

Bibliography IV

Benjamin Grégoire, Loïc Pottier, and Laurent Théry.
Proof certificates for algebra and their application to automatic geometry theorem proving.
In *Post-Proceedings of ADG 2008*, volume 6301 of *LNAI*, 2010.

Frédérique Guilhot.
Formalisation en coq d'un cours de géométrie pour le lycée.
In *Journées Francophones des Langages Applicatifs*, Janvier 2004.

Haragauri Narayan Gupta.
Contributions to the axiomatic foundations of geometry.
PhD thesis, University of California, Berkley, 1965.

Predrag Janičić, Julien Narboux, and Pedro Quaresma.
The Area Method: a Recapitulation.
Journal of Automated Reasoning, 2010.
online first.

Bibliography V

Deepak Kapur.
Geometry Theorem Proving using Hilbert's Nullstellensatz.
In *SYMSAC '86: Proceedings of the fifth ACM symposium on Symbolic and algebraic computation*, pages 202–208, New York, NY, USA, 1986. ACM Press.

Hongbo Li and Yihong Wu.
Mechanical theorem proving in projective geometry with bracket algebra.
Computer Mathematics, pages 120–129, Singapore, 2000. World Scientific.

Nicolas Magaud, Julien Narboux, and Pascal Schreck.
Formalizing Desargues' Theorem in Coq using Ranks.
In *SAC*, pages 1110–1115, 2009.

Bibliography VI

Julien Narboux.
A Decision Procedure for Geometry in Coq.
In Slind Konrad, Bunker Annett, and Gopalakrishnan Ganesh, editors, *Proceedings of TPHOLs'2004*, volume 3223 of *Lecture Notes in Computer Science*. Springer-Verlag, 2004.

Julien Narboux.
Mechanical theorem proving in Tarski's geometry.
In *Post-proceedings of Automatic Deduction in Geometry 06*, volume 4869 of *Lecture Notes in Computer Science*, pages 139–156. Springer, 2008.

Bibliography VII

Tuan Minh Pham, Yves Bertot, and Julien Narboux.
A Coq-based Library for Interactive and Automated Theorem Proving in Plane Geometry.
In *Proceedings of the 11th International Conference on Computational Science and Its Applications (ICCSA 2011)*, Lecture Notes in Computer Science. Springer-Verlag, 2011.

Loïc Pottier.
Connecting Gröbner Bases Programs with Coq to do Proofs in Algebra, Geometry and Arithmetics.
In G. Sutcliffe, P. Rudnicki, R. Schmidt, B. Konev, and S. Schulz, editors, *Knowledge Exchange: Automated Provers and Proof Assistants*, CEUR Workshop Proceedings, page 418, Doha, Qatar, 2008.

Bibliography VIII

Dongming Wang.
Elimination Method.
Springer-Verlag, 2001.

Dongming Wang.
Elimination Practice.
Springer-Verlag, 2004.

Wen-Tsün Wu.
On the Decision Problem and the Mechanization of Theorem Proving in Elementary Geometry.
In *Scientia Sinica*, volume 21, pages 157–179. 1978.