From Tarski to Hilbert

Gabriel Braun Julien Narboux

University of Strasbourg - LSIIT - ICube - CNRS

ADG 2012, Edinburgh

Motivations I

- Can we trust automatic provers ?

Motivations I

- Can we trust automatic provers ?

Test file	Auto		Recio		Botana		PureSymbolic		OpenGeoProver	
	Result	Speed	Result	Speed	Result	Speed	Result	Speed	Result	Speed
foot-exists.ggb	true	404	undefined	6	undefined	17	undefined	15	true	386
lines-parallel.ggb	false	7	false	10	false	36	false	7	false	128
points-collinear.ggb	false	11	false	6	false	32	false	6	false	230
points-equal.ggb	false	21	false	22	false	102	false	22	false	142
bisector-midpoint.ggb	true	6	true	8	true	112	true	23	true	178
centroid-median-ratio.ggb	true	47	undefined	4	true	45	undefined	5	true	787
circumcenter1.ggb	true	13	true	15	true	46	true	45	true	298
circumcenter2.ggb	true	14	true	16	true	42	true	43	true	208
circumcenter3.ggb	true	7	true	14	true	35	true	37	true	238
circumcenter4.ggb	true	14	true	13	true	44	true	33	true	219
circumcenter5.ggb	true	60	undefined	3	true	55	undefined	3	true	188
def-line-perpline-perpline.ggb	true	11	true	9	true	40	true	13	true	148
def-points-on-a-circle1.ggb	true	67	undefined	6	true	66	undefined	8	true	358
def-points-on-a-circle2.ggb	true	70	undefined	7	true	63	undefined	7	true	215
def-points-on-a-line.ggb	true	6	true	11	true	37	true	13	true	127
Desargues.ggb	true	2744	true	2516	false	123	true	59421	true	1035
EulerLine.ggb	true	25	true	27	true	58	true	709	true	990
line-circle-intersection.ggb	true	42	undefined	6	true	42	undefined	4	true	285
nine-points-circle.ggb	true	51	true	30	true	77	true	160776	true	721
orthocenter1.ggb	true	15	true	16	true	43	true	134	true	334
orthocenter2.ggb	true	7	true	12	true	41	true	14	true	177
orthocenter3.ggb	true	8	true	15	true	42	true	34	true	198
orthocenter4.ggb	true	13	true	11	true	30	true	38	true	190
orthocenter5.ggb	true	21	true	18	true	129	true	84	true	192
orthocenter6.ggb	true	22	true	18	true	47	true	42	true	172
orthocenter7.ggb	true	13	true	13	true	119	true	97	true	205
Pappus.ggb	true	809	true	808	true	58	true	127735	true	1037
parallelogram-diagonals.ggb	true	33	true	33	true	119	true	101	true	471
point-equal.ggb	true	23	true	28	true	84	true	24	true	124
powerline-perpendicular.ggb	true	58	undefined	8	true	54	undefined	7	undefined	205
regular-triangle.ggb	true	43	undefined	4	true	32	undefined	5	true	248
Simson1.ggb	false	19414	undefined	7	false	11308	undefined	9	true	421
Simson2.ggb	false	8291	undefined	6	false	9824	undefined	9	true	442
Thales1.ggb	true	67	undefined	7	true	58	undefined	4	true	315
Thales2.ggb	false	30	undefined	3	false	25	undefined	2	undefined	174
Thales3.ggb	true	45	undefined	7	true	48	undefined	4	undefined	192

Motivations II

The choice of a coordinate system hides an assumption about the points !

Formalization of Geometry

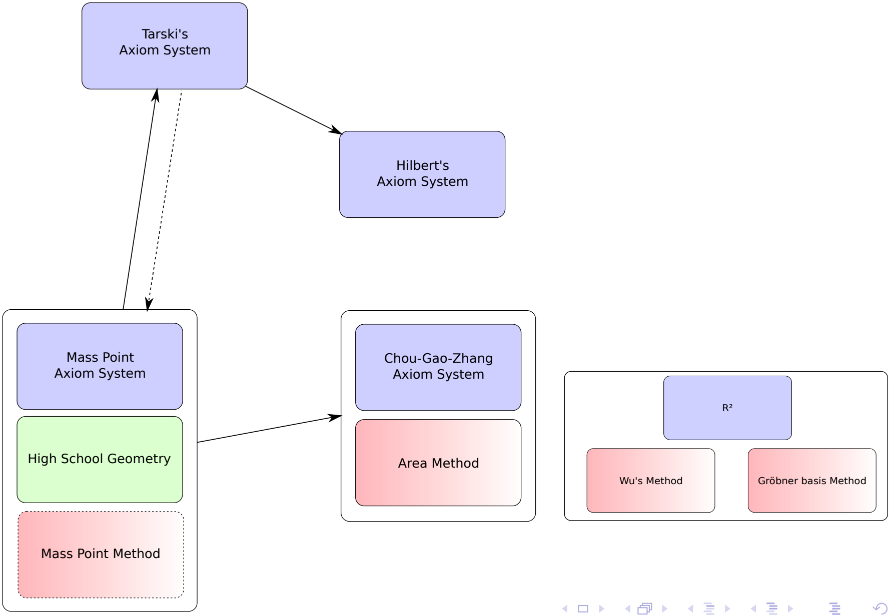
In Coq

- Projective Geometry [MNS09]
- High-school Geometry [Gui04, PBN11]
- Hilbert's Geometry [DDS00]
- Tarski's Geometry [Nar07]
- The area method [JNQ09]
- Wu's method [GNS11]
- Geometric Algebras [FT10]
- ...

In Isabelle

- Hilbert's Geometry [MF03, SF11]
- ...

Formalization of Geometry in Coq



Motivations

Why Tarski's geometry ?

- Axioms are *simple*: we do not need definitions to state the axioms.
- Dimension of the space can be changed easily.
- Many proofs do not use Euclidean axiom/dimension axioms.
- Most axioms have been shown to be independent from the others [Gup65].

Why Hilbert's geometry ?

- For education we need the concept of lines, half-lines, angle,. . .
- Hilbert's axioms are higher level.
- A good test for our formalization.
- An open question in [MF03].

Tarski's axiom system

- One type : points
- Two predicates:
  1. congruence $AB \equiv CD$
  2. betweenness $\beta\ A\ B\ C$ (non strict)
- 11 axioms

Our setting

- We use Szmielew version's [SST83].
- We focus on 2D results.
- We do not use the continuity axioms.

Logical framework

- Tarski's geometry is defined in a first order setting.
- We use the calculus of constructions + classical logic.
- The meta-theoretical results of Tarski may not apply to our formalization.

Tarski's axiom system

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

Formalization

- We use Coq type classes of Sozeau and Oury [SO08].
- Type classes are first class citizens.

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 $\measuredangle ABC \equiv \measuredangle A'B'C'$

```
hcong_4_existence: forall a h P, ~Incid P (line_of_hline h)->
 ~ BetH (V1 a)(V a)(V2 a) -> exists h1, (P1 h) = (P1 h1) /\
(forall CondAux : P2 h1 <> P1 h,
         CongaH a (angle (P2 h) (P1 h) (P2 h1)
(conj (sym_not_equal (Cond h)) CondAux)) /\
 (forall M, ~ Incid M (line_of_hline h) /\
InAngleH (angle (P2 h) (P1 h) (P2 h1)
  (conj (sym_not_equal (Cond h)) CondAux)) M ->
same_side P M (line_of_hline h)));
```

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.

DefinitionBetween_HABC := BetABC/\A<>B/\B<>C/\A<>C.
```

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

Lessons learned

- Many degenerated cases are overlooked in the original proofs.
- We had to introduce many lemmas.
  For example, the fact that **given a line l, two points not on l, are either on the same side of l or on both sides** is used implicitly, but there is no explicit proof of this fact.

Automation

- We use just a few tactics implemented using Ltac (the tactic language of Coq)
- Proof are *ugly*, but can be understood by replaying them (cf Bill Richter's messages on mailing lists).
- Work in progress by Predrag Janicic et al. about using a prover based on coherent logic to automate some proofs.
- Automation could/should be improved (cf Michael Beeson's invited talk).
- Automatic proof simplification would be also interesting.

Statistics I

- Statements: 60pages,
- Statements + proofs script: 657 pages.
- De Bruijn factor: 5

Statistics II

Chapter	lemmas	lines of spec	lines of proof	lines per lemma
Betweeness properties	16	69	111	6.93
Congruence properties	16	54	116	7,25
Properties of betweeness and congruence	19	151	183	9.63
Order relation over pair of points	17	88	340	20
The ternary relation out	22	103	426	19,36
Property of the midpoint	21	101	758	36,09
Orthogonality lemmas	77	191	2412	141,88 (560)
Position of two points relatively to a line	37	145	2333	63,05
Orthogonal symmetry	44	173	2712	61,63
Properties about angles	187	433	10612	56,74
Parallelism	68	163	3560	52,35
Total	**524**	**1671**	**23563**	**45**

Conclusion

- Clear foundations for geometry.
- Hilbert's axioms can be proved using Tarski's axioms (without continuity and in a higher order logic).

Perspectives

Define analytic geometry inside Tarski's

- Prove Pappus and Desargues.
- Define coordinates, and prove field properties.
- Show characterization of geometry predicates using coordinates.
- Connect with algebraic methods in geometry.

Prove Tarski's axioms within some/the models

- Danijela Petrovic and Filip Maric's work.

Questions ?

Bibliography I

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.

Jean-David Genevaux, Julien Narboux, and Pascal Schreck.
Formalization of Wu's simple method in Coq.
In Jean-Pierre Jouannaud and Zhong Shao, editors, *CPP 2011 First International Conference on Certified Programs and Proofs*, volume 7086 of *LNCS*, pages 71–86, Kenting, Taiwan, Province Of China, December 2011. Springer-Verlag.

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

Bibliography II

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.
submitted, october 2009.

Laura Meikle and Jacques Fleuriot.
Formalizing Hilbert's Grundlagen in Isabelle/Isar.
In *TPHOLs'03*, volume 2758 of *LNCS*, pages 319–334, 2003.

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

Bibliography III

Julien Narboux.
Mechanical theorem proving in Tarski's geometry.
In *ADG'06*, volume 4869 of *LNAI*, pages 139–156. Springer-Verlag, 2007.

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.

Bibliography IV

Phil Scott and Jacques Fleuriot.
An Investigation of Hilbert's Implicit Reasoning through Proof Discovery in Idle-Time.
In Pascal Schreck, Julien Narboux, and Jürgen Richter-Gebert, editors, *Automated Deduction in Geometry*, volume 6877 of *Lecture Notes in Computer Science*, page 182–200. Springer Berlin / Heidelberg, 2011. 10.1007/978-3-642-25070-5_11.

Matthieu Sozeau and Nicolas Oury.
First-Class Type Classes.
In *TPHOLs 08*, LNCS. Springer, 2008.
to appear.

Bibliography V

Wolfram Schwabhäuser, Wanda Szmielew, and Alfred Tarski.
Metamathematische Methoden in der Geometrie.
Springer-Verlag, 1983.
In german.