# Mechanical Theorem Proving in Tarski's Geometry

Julien Narboux

Équipe LogiCal, LIX
École Polytechnique, 91128 Palaiseau Cedex, France
Julien.Narboux@inria.fr
http://www.lix.polytechnique.fr/Labo/Julien.Narboux/

**Abstract.** This paper describes the mechanization of the proofs of the first height chapters of Schwabäuser, Szmielew and Tarski's book: *Metamathematische Methoden in der Geometrie*. The proofs are checked formally using the Coq proof assistant. The goal of this development is to provide foundations for other formalizations of geometry and implementations of decision procedures. We compare the mechanized proofs with the informal proofs. We also compare this piece of formalization with the previous work done about Hilbert's *Grundlagen der Geometrie*. We analyze the differences between the two axiom systems from the formalization point of view.

## 1 Introduction

Euclid is considered as the pioneer of the axiomatic method, in the *Elements*, starting from a small number of self-evident truths, called postulates or common notions, he derives by purely logical rules most of the geometrical facts that were discovered in the two or three centuries before him. But upon a closer reading of Euclid's *Elements*, we find that he does not adhere as strictly as he should to the axiomatic method. Indeed, at some steps in certain proofs he uses a method of "superposition of triangles". This kind of justifications can not be derived from his set of postulates.

In 1899, in *der Grundlagen der Geometrie*, Hilbert described a more formal approach and proposed a new axiom system to fill the gaps in Euclid's system.

Recently, the task consisting in mechanizing Hilbert's *Grundlagen der Geometrie* has been partially achieved. A first formalization using the Coq proof assistant [1] was proposed by Christophe Dehlinger, Jean-François Dufourd and Pascal Schreck [2]. This first approach was realized in an intuitionist setting, and concluded that the decidability of point equality and collinearity is necessary to check Hilbert's proofs. Another formalization using the Isabelle/Isar proof assistant [3] was performed by Jacques Fleuriot and Laura Meikle [4]. Both formalizations have concluded that, even if Hilbert has done some pioneering work about formal systems, his proofs are in fact not fully formal, in particular degenerated cases are often implicit in the presentation of Hilbert. The proofs can be made more rigorous by machine assistance. Indeed, in the different editions

F. Botana and T. Recio (Eds.): ADG 2006, LNAI 4869, pp. 139–156, 2007.

of *die Grundlagen der Geometrie* the axioms were changed, but the proofs were note always changed accordingly, this obviously resulted in some inconsistencies. The use of a proof assistant solves this problem: when an axiom is changed it is easy to check if the proofs are still valid.

In the early 60s, Wanda Szmielew and Alfred Tarski started the project of a treaty about the foundations of geometry based on another axiom system for geometry designed by Tarski in the 20s[1]. A systematic development of euclidean geometry was supposed to constitute the first part but the early death of Wanda Szmielew put an end to this project. Finally, Wolfram Schwabhäuser continued the project of Wanda Szmielew and Alfred Tarski. He published the treaty in 1983 in German: *Metamathematische Methoden in der Geometrie* [6]. In [7], Art Quaife used a general purpose theorem prover to automate the proof of some lemmas in Tarski's geometry.

In this paper we describe our formalization of the first eight chapters of the book of Wolfram Schwabhäuser, Wanda Szmielew and Alfred Tarski in the Coq proof assistant.

We will first describe the different axioms of Tarski's geometry and give an history of the different versions of this axiom system. Then after a shot introduction to the system Coq, we present our formalization of the axiom system and the mechanization of one example theorem. Finally, we compare our formalization with existing ones and compare Tarski's axiomatic system with Hilbert's system from the mechanization point of view.

## 2 Motivations

We aim at two applications: the first one is the use of a proof assistant in the education to teach geometry [8,9], the second one is the proof of programs in the field computational geometry.

These two themes have already been partially addressed by the community. Frédérique Guilhot has realized a large Coq development about euclidean geometry following a presentation suitable for use in french high-school [10]. Concerning the proof of programs in the field of computational geometry we can cite the formalization of convex hulls algorithms by David Pichardie and Yves Bertot in Coq [11] and by Laura Meikle and Jacques Fleuriot in Isabelle [12] and the formalization of an image segmentation algorithm by Jean-François Dufourd [13]. In [14,15], we have presented the formalization and implementation in the Coq proof assistant of the area decision procedure of Chou, Gao and Zhang [16].

Formalizing geometry in a proof assistant has not only the advantage of providing a very high level of confidence in the proof generated, it also permits to insert purely geometric arguments within other kind of proofs such as for instance proof of correctness of programs or proofs by induction. For the time being all the formal developments we have cited are distinct and as they do not use the same axiomatic system, they can not be combined.

[1] These historical pieces of information are taken from the introduction of the publication by Givant in 1999 [5] of a letter from Tarski to Schwabhäuser (1978).

The goal of our mechanization is to do a first step in the direction of the merging of these developments. We aim at providing very clear foundations for other formalizations of geometry and implementations of decision procedures.

## 3 Tarski's Axiom System

Alfred Tarski worked on the axiomatization and meta-mathematics of euclidean geometry from 1926 until his death in 1983. Several axiom systems were produced by Tarski and his students. In this section, we first give an informal description of the propositions which appeared in the different versions of Tarski's axiom system, then we provide an history of these versions and finally we present the version we have formalized.

The axioms are based on first order logic and two predicates:

***betweenness.*** The ternary *betweenness* predicate $\beta\ A\,B\,C$ informally states that $B$ lies on the line $AC$ between $A$ and $C$.

***equidistance.*** The quaternary *equidistance* predicate $AB \equiv CD$ informally means that the distance from $A$ to $B$ is equal to the distance from $C$ to $D$.

Note that in Tarski's geometry, only a set of points is assumed, in particular, lines are *defined* by two distinct points whereas in Hilbert's axiom system lines and planes are *assumed*.

### 3.1 Axioms

We reproduce here the list of propositions which appear in the different versions of Tarski's axiom system. We adopt the same numbering as in [5]. Free variables are considered to be implicitly quantified universally.

1 Symmetry for equidistance

$$AB \equiv BA$$

2 Pseudo-transitivity for equidistance[2]

$$AB \equiv PQ \wedge AB \equiv RS \Rightarrow PQ \equiv RS$$

3 Identity for equidistance

$$AB \equiv CC \Rightarrow A = B$$

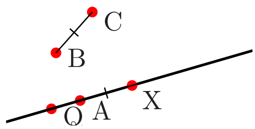
4 Segment construction

$$\exists X, \beta\ Q\,A\,X \wedge AX \equiv BC$$

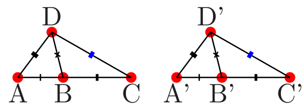
[2] Note that we call this property *pseudo*-transitivity because the transitivity property for equidistance should be:

$$AB \equiv PQ \wedge PQ \equiv RS \Rightarrow AB \equiv RS.$$

The segment construction axiom states that one can build a point on a ray at a given distance.




Segment construction




Five segments

5 Five segments

$$\begin{array}{l} A \neq B \wedge \beta\ A\, B\, C \wedge \beta\ A'\, B'\, C' \wedge \\ AB \equiv A'B' \wedge BC \equiv B'C' \wedge AD \equiv A'D' \wedge BD \equiv B'D' \end{array} \Rightarrow CD \equiv C'D'$$

$5_1$ Five segments (variant)

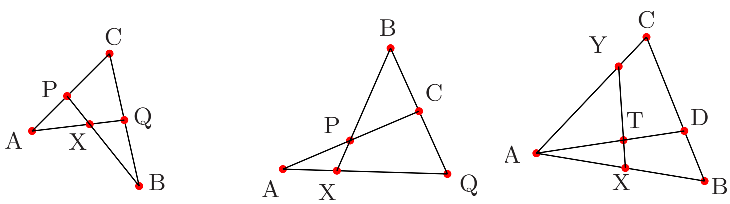
$$\begin{array}{l} A \neq B \wedge B \neq C \wedge \beta\ A\, B\, C \wedge \beta\ A'\, B'\, C' \wedge \\ AB \equiv A'B' \wedge BC \equiv B'C' \wedge AD \equiv A'D' \wedge BD \equiv B'D' \end{array} \Rightarrow CD \equiv C'D'$$

This second version differs from the first one only by the condition $B \neq C$.

6 Identity for betweenness

$$\beta\ A\, B\, A \Rightarrow A = B$$

The original Pasch axiom states that if a line intersects one side of a triangle and misses the three vertexes, then it must intersect one of the other two sides.




Inner form Outer form Weak form

**Fig. 1.** Axioms of Pasch

7 Pasch (inner form)

$$\beta\ A\, P\, C \wedge \beta\ B\, Q\, C \Rightarrow \exists X, \beta\ P\, X\, B \wedge \beta\ Q\, X\, A$$

$7_1$ Pasch (outer form)

$$\beta\ A\, P\, C \wedge \beta\ Q\, C\, B \Rightarrow \exists X, \beta\ A\, X\, Q \wedge \beta\ B\, P\, X$$

$7_2$ Pasch (outer form) (variant)

$$\beta\ A\, P\, C \wedge \beta\ Q\, C\, B \Rightarrow \exists X, \beta\ A\, X\, Q \wedge \beta\ X\, P\, B$$

$7_3$ weak Pasch

$$\beta\ A\,T\,D \wedge \beta\ B\,D\,C \Rightarrow \exists X, Y, \beta\ A\,X\,B \wedge \beta\ A\,Y\,C \wedge \beta\ Y\,T\,X$$

Dimension axioms provide upper and lower bound for the dimension of the space. Note that lower bound axioms for dimension $n$ are the negation of upper bound axioms for the dimension $n-1$.

8(2) Dimension, lower bound 2

$$\exists ABC, \neg\beta\ A\,B\,C \wedge \neg\beta\ B\,C\,A \wedge \neg\beta\ C\,A\,B$$

There are three non collinear points.

$8(n)$ Dimension, upper bound $n$

$$\exists ABCP_1P_2\ldots P_{n-1},\ \begin{array}{l} \bigwedge_{1\leq i<j<n} P_i \neq P_j \wedge \\ \bigwedge_{i=2}^{n-1} AP_1 \equiv AP_i \wedge BP_1 \equiv BP_i \wedge CP_1 \equiv CP_i \wedge \\ \neg\beta\ A\,B\,C \wedge \neg\beta\ B\,C\,A \wedge \neg\beta\ C\,A\,B \end{array}$$

9(1) Dimension, upper bound 1

$$\beta\ A\,B\,C \vee \beta\ B\,C\,A \vee \beta\ C\,A\,B$$

Three points are always on the same line.

$9(n)$ Dimension, upper bound n

$$\begin{array}{l} \bigwedge_{1\leq i<j\leq n} P_i \neq P_j \wedge \\ \bigwedge_{i=2}^{n} AP_1 \equiv AP_i \wedge BP_1 \equiv BP_i \wedge CP_1 \equiv CP_i \end{array} \Rightarrow \beta\ A\,B\,C \vee \beta\ B\,C\,A \vee \beta\ C\,A\,B$$

$9_1(2)$ Dimension, upper bound 2 (variant)[3]

$$\exists Y, (ColXYA \wedge \beta\ B\,Y\,C) \vee (ColXYB \wedge \beta\ C\,Y\,A) \vee (ColXYC \wedge \beta\ A\,Y\,B)$$

10 Euclid's axiom

$$\beta\ A\,D\,T \wedge \beta\ B\,D\,C \wedge A \neq D \Rightarrow \exists X, Y\ \beta\ A\,B\,X \wedge \beta\ A\,C\,Y \wedge \beta\ X\,T\,Y$$

$10_1$ Euclid's axiom (variant)

$$\beta\ A\,D\,T \wedge \beta\ B\,D\,C \wedge A \neq D \Rightarrow \exists X, Y\ \beta\ A\,B\,X \wedge \beta\ A\,C\,Y \wedge \beta\ Y\,T\,X$$

11 Continuity

$$\exists a, \forall xy, (x \in X \wedge y \in Y \Rightarrow \beta\ a\,x\,y) \Rightarrow \exists b, \forall xy, x \in X \wedge y \in Y \Rightarrow \beta\ x\,b\,y$$

*Schema* 11 Elementary Continuity (schema)

$$\exists a, \forall xy, (\alpha \wedge \beta \Rightarrow \beta\ a\,x\,y) \Rightarrow \exists b, \forall xy, \alpha \wedge \beta \Rightarrow \beta\ x\,b\,y$$

where $\alpha$ and $\beta$ are first order formulas, such that $a$, $b$ and $y$ do not appear free in $\alpha$; $a$, $b$ and $x$ do not appear free in $\beta$.

[3] $ColABC$ is a shorthand for $\beta\ A\,B\,C \vee \beta\ B\,C\,A \vee \beta\ C\,A\,B$ to simplify the presentation. The $Col$ predicate does not belong to the language of the theory of Tarski.

A geometry defined by the elementary continuity axiom schema instead of the higher order continuity axiom is called elementary.

12 Reflexivity of $\beta$

$$\beta\ A\,B\,B$$

$B$ is always between $A$ and $B$.

14 Symmetry of $\beta$

$$\beta\ A\,B\,C \Rightarrow \beta\ C\,B\,A$$

If $B$ is between $A$ and $C$ then $B$ is between $C$ and $A$.

13 Compatibility of equality with $\beta$

$$A = B \Rightarrow \beta\ A\,B\,A$$

19 Compatibility of equality with $\equiv$

$$A = B \Rightarrow AC \equiv BC$$

15 Transitivity (inner) of $\beta$

$$\beta\ A\,B\,D \wedge \beta\ B\,C\,D \Rightarrow \beta\ A\,B\,C$$

16 Transitivity (outer) of $\beta$

$$\beta\ A\,B\,C \wedge \beta\ B\,C\,D \wedge B \neq C \Rightarrow \beta\ A\,B\,D$$

17 Connectivity (inner) of $\beta$

$$\beta\ A\,B\,D \wedge \beta\ A\,C\,D \Rightarrow \beta\ A\,B\,C \vee \beta\ A\,C\,B$$

18 Connectivity (outer) of $\beta$

$$\beta\ A\,B\,C \wedge \beta\ A\,B\,D \wedge A \neq B \Rightarrow \beta\ A\,C\,D \vee \beta\ A\,D\,C$$

20 Triangle construction unicity

$$\begin{array}{l} AC \equiv AC' \wedge BC \equiv BC' \wedge \\ \beta\ A\,D\,B \wedge \beta\ A\,D'\,B \wedge \beta\ C\,D\,X \wedge \\ \beta\ C'\,D'\,X \wedge D \neq X \wedge D' \neq X \end{array} \Rightarrow C = C'$$

$20_1$ Triangle construction unicity (variant)

$$\begin{array}{l} A \neq B \wedge \\ AC \equiv AC' \wedge BC \equiv BC' \wedge \\ \beta\ B\,D\,C' \wedge (\beta\ A\,D\,C \vee \beta\ A\,C\,D) \end{array} \Rightarrow C = C'$$

21 Triangle construction existence

$$AB \equiv A'B' \Rightarrow \exists C X, \begin{array}{l} AC \equiv A'C' \wedge BC \equiv B'C' \wedge \\ \beta\ C\,X\,P \wedge (\beta\ A\,B\,X \vee \beta\ B\,X\,A \vee \beta\ X\,A\,B) \end{array}$$

| Year : | 1940 | 1951 | 1959 | 1965 | 1983 |
|---|---|---|---|---|---|
| Reference : | [18] | [17] | [19] | [20] | [6] |
| Axioms : | 1 | 1 | 1 | 1 | 1 |
| | 2 | 2 | 2 | 2 | 2 |
| | 3 | 3 | 3 | 3 | 3 |
| | 4 | 4 | 4 | 4 | 4 |
| | $5_1$ | $5_1$ | 5 | 5 | 5 |
| | 6 | 6 | 6 | | 6 |
| | $7_2$ | $7_2$ | $7_1$ | $7_1$ | 7 |
| | 8(2) | 8(2) | 8(2) | 8(2) | 8(2) |
| | $9_1(2)$ | $9_1(2)$ | 9(2) | 9(2) | 9(2) |
| | 10 | 10 | $10_1$ | $10_1$ | 10 |
| | 11 | 11 | 11 | 11 | 11 |
| | 12 | 12 | | | |
| | 13 | | | | |
| | 14 | 14 | | | |
| | 15 | 15 | 15 | 15 | |
| | 16 | 16 | | | |
| | 17 | 17 | | | |
| | 18 | 18 | 18 | | |
| | 19 | | | | |
| | 20 | $\rightarrow 20_1$ | | | |
| | 21 | 21 | | | |
| Nb of axioms : | 20 | 18 | 12 | 10 | 10 |
| | + | + | + | + | + |
| | 1 schema | 1 schema | 1 schema | 1 schema | 1 schema |

**Fig. 2.** History of Tarski's axiom systems

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

**Fig. 3.** Tarski's axiom system (Formalized version - 11 axioms)

### 3.2 History

Tarski began to work on his axiom system in 1926 and presented it during his lectures at Warsaw university[4]. He submitted it for publication in 1940 and was published in his first form in 1967 [18]. This version contains 20 axioms and one schema. A second version, slightly simpler was published in [17]. This first simplification consists only in considering a logic with built-in equality, axioms 13 and 19 are then useless. This second version was further simplified by Eva Kallin, Scott Taylor and Tarski into a system of twelve axioms [19]. The last simplification was obtained by Gupta in its PhD thesis [20], where he gives the proof that two more axioms can be derived from the remaining ones.

Figure 2 gives the list of axioms contained in each of these axiom systems. Figure 3 provides the final list of axioms that we used in our formalization.

## 4 A Short Introduction to the Coq Proof Assistant

The Coq system [1,21,22] is a proving tool based on a logical formalism called the calculus of inductive constructions [23]. Even if the Coq system has some automatic theorem proving features, it is *not* an automatic theorem prover. The proofs are mainly built by the user *interactively*. The system checks whether the proof is correct. In [14], we have described the formalization of decision procedure for geometry. This formalization, allows to use the area method to generate automatically proofs which are double checked by the Coq system. In this development, we do not want to make use of this procedure. Otherwise we would have a circularity problem because our goal is to provide solid foundations for different formal developments about geometry including this one.

The underlying logic of the Coq system is an intuitionist logic. This means that the proposition $A \vee \neg A$ is not taken for granted and, if it is needed, the user has to assume it explicitly. This allows to clarify the distinction between classical and constructive proofs.

The user interacts with the system using commands which modify the current state of the proof. The language used to interact with the system is called a tactic language[5].

## 5 Formalization in Coq

The mechanization of the proof we have realized prove formally that the simplifications of the first version of Tarski's axiom system are correct. The unnecessary axioms are derived from the remaining ones.

Now, we provide a quick overview of the content of each chapter. We will only detail an example proof in the next section.

[4] We use [5] and the footnotes in [17] to give a quick history of the different versions of Tarski's axiom system.

[5] Note that in the latest version of Coq (8.1) another proof language is available, this new language allows to write proofs which are more readable, unfortunately it was not available when have started this work.

**The first chapter** contains the declaration of all the axioms and the definition of the collinearity predicate (noted `Col`).

**The second chapter** contains some basic properties of the equidistance predicate (noted `Cong`). It contains also the proof of the unicity of the point constructed thanks to the segment construction axiom.

**The third chapter** contains some properties of the betweenness predicate (noted `Bet`). It contains in particular the proof of the axioms 12, 14 and 16.

**The fourth chapter** contains the proof of several properties of `Cong`, `Col` and `Bet`.

**The fifth chapter** contains some pseudo-transitivity properties of betweenness and the definition of the length comparison predicate (noted `le`) with some associated properties. It includes in particular the proofs of the axioms 17 and 18.

**The sixth chapter** defines the `out` predicate which means that a point lies on a line out of a segment. This predicate is used to prove some other properties of `Cong`, `Col` and `Bet` such as transitivity properties for `Col`.

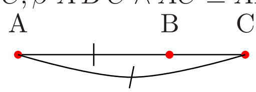
**The seventh chapter** defines the midpoint of a segment and the symmetric points. It has to be noted that at this step the existence of the midpoint is not derived yet.

**The eighth chapter** contains the definition of the predicate 'perpendicular' (`Perp`), and the proof of some related properties such as the existence of the foot of the perpendicular. Finally, the existence of the midpoint of a segment is derived.

### 5.1 Two Crucial Lemmas

Our formalization follows strictly the lines of the book by Schwabhäuser, Szmielew and Tarski except in the fifth chapter where we introduce two crucial lemmas which do not appear in the original text, and which are necessary to fill some gaps in the informal proofs. These two lemmas allows to deduce the equality of two points which lie on a segment under an hypotheses involving distances.

$$\forall ABC, \beta\ A\,B\,C \wedge AC \equiv AB \Rightarrow C = B$$




*Proof.* We use the lemma 4.6 of [6]:

$$\forall ABCA'B'C',\ \beta\ A\,B\,C \wedge Cong_3 ABCA'B'C' \Rightarrow \beta\ A'\,B'\,C'.$$

As we know by assumption that $\beta\ A\,B\,C$, we apply the lemma with $A := A$, $B := B$, $C := C$, $A' := A$ ,$B' := C$ and $C' := B$, to obtain that:

$$Cong_3 ABCACB \Rightarrow \beta\ A\,C\,B$$

The predicate $Cong_3 A_1A_2A_3B_1B_2B_3$ expresses that:

$$A_1A_2 \equiv B_1B_2 \wedge A_1A_3 \equiv B_1B_3 \wedge A_2A_3 \equiv B_2B_3$$

So here, we need to show that:

$$AB \equiv AC \wedge AC \equiv AB \wedge BC \equiv CB.$$

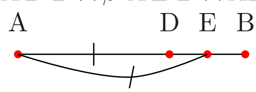
The first conjunct is shown by commutativity of $\equiv$ , the second one by hypothesis and the third one using the pseudo-commutativity property of the oriented distance.
As $\beta\ A\,B\,C$ and $\beta\ A\,C\,B$, we can conclude that $C = B$ using the lemma `between_equality`:

$$\forall ABC : Point, \beta\ A\,B\,C \wedge \beta\ B\,A\,C \Rightarrow A = B$$

and the symmetry property of $\beta$ .

The second lemma is the following, we omit the proof.

$$\forall ABDE, \beta\ A\,D\,B \wedge \beta\ A\,E\,B \wedge AD \equiv AE \Rightarrow D = E.$$




### 5.2 A Comparison Between the Formal and Informal Proofs

We first describe in detail the formal proof of a simple example: the first crucial lemma. Then, we reproduce here one of the non trivial proofs: the proof due to Gupta [20] that axiom 18 can be derived from the remaining ones. We translate the proof from [6] and provide in parallel the mechanized proof as a Coq script. For the conciseness of the presentation we provide only the beginning of the formal proof[6]. For the reader not familiar with the Coq proof assistant, we provide a quick informal explanation of the role of the main tactics we use in these proofs.

`intro` is used to introduced hypothesis in the context. It is the equivalent of the informal sentence: "Suppose that we have $A$"
`assert` is used to state what we want to prove. When it is followed by "..." this means that this assertion can be proved automatically.
`DecompExAnd` given an existential hypotheses, introduces the witness of the existential and decompose the knowledge about it.
`split` splits a conjunction into its components. This used the fact fact that to show $A \wedge B$, one can show first $A$ then $B$.
`apply` is used to apply an assumption, a lemma or theorem.
`Tarski,sTarski,Between,...` are automatic tactics which try to prove the current goal. Informally this can be read as "by simple properties of betweenness" or "by direct application of one of the axioms".
`unfold` replaces something by its definition.
`cases_equality` perform a reasoning by cases on the equality of two points.

[6] The full proofs are available at the address given at the end of this paper.

**A First Example.** First we input the statement of the lemma in Coq's syntax. $\beta\, A\,B\,C$ is noted `Bet A B C` and $AC \equiv AB$ is noted `Conq A C A B`. The text displayed after `Coq <` represents the input, the other pieces of text represent the output by the system.

```
Coq < Lemma between_cong : forall A B C,
Coq <  Bet A C B -> Cong A C A B -> C=B.
Coq < 1 subgoal

============================
thesis := forall A B C : Point, Bet A C B -> Cong A C A B -> C = B
```

The Coq system confirms that we have one statement to prove. The statements appearing above the horizontal line are the hypotheses and the one appearing under the horizontal line are the fact to be proved. Here we do not have any hypothesis yet. We can now start the proof.

```
Coq < Proof.
```

The first tactic we apply is the `intro` tactic. This introduces in the context the left hand side of the implications.

```
  Coq < intros.
1 subgoal

A : Point
B : Point
C : Point
H : Bet A C B
H0 : Cong A C A B
============================
thesis := C = B
```

Now, we have five hypotheses. We know that $A$, $B$ and $C$ are points, that $\beta\, A\,C\,B$ and that $AC \equiv AB$. We need to show that $C = B$.

Let's first prove that $\beta\, A\,B\,C$.

```
  Coq < assert (Bet A B C).
2 subgoals

A : Point
B : Point
C : Point
H : Bet A C B
H0 : Cong A C A B
============================
thesis := Bet A B C
subgoal 2 is: C = B
```

We have two statements two prove. The first one is $\beta\ A\,B\,C$ and the second one is $C = B$. Now, we apply the lemma 4.6. This changes our first subgoal into two subgoals which are the assumptions of the lemma 4.6.

```
Coq < eapply l4_6.
3 subgoals

A : Point
B : Point
C : Point
H : Bet A C B
H0 : Cong A C A B
============================
thesis := Bet ?X ?Y ?Z
subgoal 2 is: Cong_3 ?X ?Y ?Z A B C
subgoal 3 is: C = B
```

The first subgoal means that we have to prove $\beta\ ?X\,?Y\,?Z$ for some $?X$, $?Y$ and $?Z$. We choose to apply our assumption $H$. This instantiate $?X$, $?Y$ and $?Z$ with $A$, $C$ and $B$ respectively.

```
  Coq < apply H.
2 subgoals

A : Point
B : Point
C : Point
H : Bet A C B
H0 : Cong A C A B
============================
thesis := Cong_3 A C B A B C
subgoal 2 is: C = B
```

Now, we need to show that `Cong_3 A C B A B C`. This can be done by unfolding the definition of `Conq_3`, spliting the conjunction we get and solving the resulting subgoals using an automatic tactic.

```
  Coq < unfold Cong_3;repeat split;sTarski.
1 subgoal

A : Point
B : Point
C : Point
H : Bet A C B
H0 : Cong A C A B
H1 : Bet A B C
============================
thesis := C = B
```

Again, we need to show $C = B$, but this time we have the hypothesis `H1`.

```
  Coq < esTarski.
Proof completed.
```

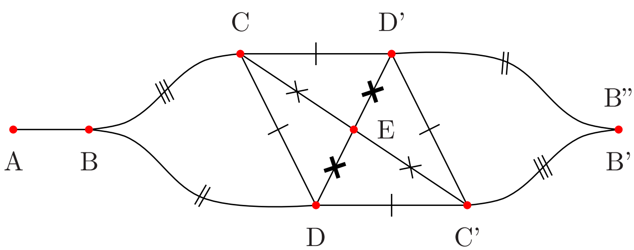
From `H` and `H1` it is possible to conclude using an automatic tactic. Finally, Coq checks again the proof and add it to its database.

```
  Coq < Qed.
between_cong is defined
```

Note that during the proof the system checks that the commands we give are correct but in this last step the proof is checked again by a small part of the Coq system called the kernel. Only the kernel of the system needs to be bug free to ensure the correctness of the proof. Bugs which are outside the kernel can not lead to a proof of a false statement.

**Axiom 18**

**Theorem 1 (Gupta).** $A \neq B \wedge \beta\ A\,B\,C \wedge \beta\ A\,B\,D \Rightarrow \beta\ A\,C\,D \vee \beta\ A\,D\,C$




Proof: Let $C'$ and $D'$ be points such that :

$$\beta\ A\,D\,C' \wedge DC' \equiv CD \text{ and } \beta\ A\,C\,D' \wedge CD' \equiv CD$$

```
assert (exists C', Bet A D C' /\ Cong D C' C D)...
DecompExAnd H2 C'.
assert (exists D', Bet A C D' /\ Cong C D' C D)...
DecompExAnd H2 D'.
```

We have to show that $C = C'$ or $D = D'$.
Let $B$ and $B''$ points such that :

$$\beta\ A\,C'\,B' \wedge C'B' \equiv CB \text{ and } \beta\ A\,D'\,B'' \wedge D'B'' \equiv DB$$

```
assert (exists B', Bet A C' B' /\ Cong C' B' C B)...
DecompExAnd H2 B'.
assert (exists B'', Bet A D' B'' /\ Cong D' B'' D B)...
DecompExAnd H2 B''.
```

Using the lemma 2.11[7] we can deduce that $BC' \equiv B''C$ and that $BB' \equiv B''B$.

```
assert (Cong B C' B'' C).
eapply l2_11.
3:apply cong_commutativity.
3:apply cong_symmetry.
3:apply H11.
Between.
Between.
esTarski.
assert (Cong B B' B'' B).
eapply l2_11;try apply H2;Between.
```

By unicity of the segment construction, we know that $B'' = B'$.

```
assert (B''=B').
apply construction_unicity with
(Q:=A) (A:=B) (B:=B'') (C:=B) (x:=B'') (y:=B');Between...
smart_subst B''.
```

We know that $FSC\begin{pmatrix} BCD'C' \\ B'C'DC \end{pmatrix}$ (The points form a five segments configuration).

```
assert (FSC B C D' C' B' C' D C).
unfold FSC;repeat split;unfold Col;Between;sTarski.
2:eapply cong_transitivity.
2:apply H7.
2:sTarski.
apply l2_11 with (A:=B) (B:=C) (C:=D') (A':=B') (B':=C') (C':=D);
Between;sTarski;esTarski.
```

Hence $C'D' \equiv CD$ (because if $B \neq C$ the five segments axiom gives the conclusion and if $B = C$ we can use the hypotheses).

```
assert (Cong C' D' C D).
cases_equality B C.
(* First case *)
treat_equalities.
eapply cong_transitivity.
apply cong_commutativity.
apply H11.
Tarski.
(* Second case *)
apply cong_commutativity.
eapply l4_16;try apply H3...
```

[7] The lemma 2.11 states that $\beta\ A\,B\,C \wedge \beta\ A'\,B'\,C' \wedge AB \equiv A'B' \wedge BC \equiv B'C' \Rightarrow AC \equiv A'C'$.

Using the axiom of Pasch, there is a point $E$ such that :

$$\beta\, C\, E\, C' \wedge \beta\, D\, E\, D'$$

```
assert (exists E, Bet C E C' /\ Bet D E D').
eapply inner_pash;Between.
DecompExAnd H13 E.
```

We omit the rest of the formal proof.

We can deduce that $IFS\begin{pmatrix} ded'c \\ ded'c' \end{pmatrix}$ and $IFS\begin{pmatrix} cec'd \\ cec'd' \end{pmatrix}$. Hence $EC \equiv EC'$ and $ED \equiv ED'$. Suppose that $C \neq C'$. We have to show that $D = D'$[8]. From the hypotheses, we can infer that $C \neq D'$. Using the segment construction axiom, we know that there are points $P$, $Q$ and $R$ such that :

$$\beta\, C'\, C\, P \wedge CP \equiv CD' \text{ and } \beta\, D'\, C\, R \wedge CR \equiv CE \text{ and } \beta\, P\, R\, Q \wedge RQ \equiv RP$$

Hence $FSC\begin{pmatrix} D'CRP \\ PCED' \end{pmatrix}$, so $RP \equiv ED'$ and $RQ \equiv ED$. We can infer that $FSC\begin{pmatrix} D'EDC \\ PRQC \end{pmatrix}$, so using lemma 2.11 we can conclude that $D'D \equiv PQ$ and $CQ \equiv CD$ (because the case $D' \neq E$ is solved using the five segments axiom, and in the other case we can deduce that $D' = D$ and $P = Q$). Using the theorem 4.17[9], as $R \neq C$ and $R$, $C$ and $D'$ are collinear we can conclude that $D'P \equiv D'Q$. As $C \neq D'$, $Col\, CD'B$ and $Col\, CD'B'$, we can also deduce that $BP \equiv BQ$ and $B'P \equiv B'Q$. As $C \neq D'$, we have $B \neq B'$ and as $Col\, BC'B'$ we have $C'P \equiv C'Q$. As $C \neq C'$ and $Col\, C'CP$ we have $PP \equiv PQ$. Using the identity axiom for equidistance, we can deduce that $P = Q$. As $PQ \equiv D'D$, we also have $D = D'$. □

### 5.3 About Degenerated Cases

Every paper about the formalization of geometry, in particular those about Hilbert's foundations of geometry [2,4] emphasizes the problem of the degenerated cases. In geometry, the degenerated cases are limit cases such as when two points are equals, three points are collinear or two lines are parallel. The formal proof of the theorems in the degenerated cases is often tedious and even sometimes difficult. These cases often do not even appear in the informal proof[10]. In order to limit the size of the proofs, we tried to automate some tasks. These pieces of automation should not be compared with the highly successful decision procedures for geometry, the goal is just to automate some easy but very tedious proofs

[8] Note that this step uses the decidability of equality between two points.

[9] The theorem 4.17 states that $A \neq B \wedge ColABC \wedge AP \equiv AQ \wedge BP \equiv BQ \Rightarrow CP \equiv CQ$.

[10] It seems that degenerated cases play the same role in geometry as $\alpha$-conversion in lambda calculus: they are a great source of difficulties in the context of a mechanization.

and, as stated before, as our goal is to build foundations for the implementation of decision procedures we can not use these more powerful procedures.

The main tactic to deal with degenerated cases is called `treat_equalities`. The basic idea is to propagate information about degenerated cases. For instance, if we know that $A = B$ and $AB \equiv CD$ we can deduce that $C = D$. This is very simple but it shortens the proofs of the degenerated cases quite effectively.

Moreover, we think that a source of degenerated cases come from the axiom system. In our personal experience the formalization of geometry using Hilbert axioms lead to far more degenerated cases because the axioms are not always stated in the most general and uniform way. We think that Tarski's geometry is a good candidate to mechanization because it is very simple, it has good meta-mathematical properties (cf [17]) and it produces few degenerated cases.

### 5.4 Comparison with Other Formalizations

Compared to Frédérique Guilhot formalization [10], our development should be considered low level. Our formalization has the advantage of being based on the axiom system of Tarski which is of an extreme simplicity: two predicates and eleven axioms. But this simplicity has a price, our formalization is not adapted to the context of education. Indeed, some intuitively simple properties are hard to prove in this context. For instance, the proof of the existence of the midpoint of segment is obtained only at the end of the eighth chapter after about 150 lemmas and 4000 lines of proof. Moreover, the small number of axioms imposes a scheduling of the lemmas which is not always intuitive. Indeed, some simple intuitive properties can only be proved late in the development. For instance the transitivity properties for collinearity are only proved in the chapter 6, this means that in the first fifth chapters we have to live in a world where we do not assume that collinearity has some transitivity properties.

Compared with formalizations using Hilbert's axiom system, we think that, as stated in the previous section, the use of Tarski's axiom system leads to more uniform proofs with less degenerated cases. Note that there are degenerated cases which are inherent to a statement: the statement is false otherwise. There are also degenerated cases which are inherent to the formulation of a statement, if one starts with an axiom system which contains numerous degenerated cases then the proofs of the first lemmas have to deal with these cases to obtain more uniform statements. The use of Tarski's axiom system has also the advantage that, as it is based only on points, it can be easily generalized to other dimensions by just changing the dimension axiom. In practice, in the context of a formal proof, this allows to prove the lemmas which do not use the dimension axiom only once. On the other end using Hilbert's axiom system, to change the dimension of the space, the language and axioms have to be changed and the proofs as well, for dimension 3 for instance, it is necessary to assume the existence of planes.

### 5.5 Classical vs. Intuitionist Logic

Our formalization of Tarski's geometry is performed in the system Coq. As the logic behind Coq is constructive, we need to tell Coq explicitly when we need classical logic. This is the case in this development. It appears quite often in the proofs that we need to distinguish between two cases such that $A = B$ and $A \neq B$ or $Col ABC$ and $\neg Col ABC$. This kind of reasoning relies on the decidability of point equality and collinearity. We proved these two facts using the excluded middle rule.

## 6 Future Work and Conclusion

A natural extension of our work consist in mechanizing the remaining chapters of [6] and proving the axioms of Hilbert. This work is under progress. We also plan to enrich our formalization to use it as a foundation for other formal Coq developments about geometry such as Frédérique Guilhot formalization of geometry as it is presented in the french curriculum [10] and our implementation in Coq of the area method of Chou, Gao and Zhang [14]. A longer-term challenge would be to perform a systematic development of geometry similar to the book of Schwabhäuser, Szmielew and Tarski but in the context of a constructive axiom system such as the axiom system of von Plato [24] which has already been formalized in the Coq proof assistant by Gilles Khan [25].

We have presented the mechanization of the proofs of over 150 lemmas in the context of Tarski's geometry. This includes the formal proof that the simplifications of the first version of Tarski's axiom system are corrects. Our main conclusion is that Tarski axiom system lead to more uniform proofs than Hilbert's axiom system and so it is better suited for a formalization.

## Availability

The full Coq development with the formal *proofs* and hypertext links to ease navigation can be found at the following url:

`http://www.lix.polytechnique.fr/Labo/Julien.Narboux/tarski.html`

## References


1. Coq development team, The: The Coq proof assistant reference manual, Version 8.0. LogiCal Project (2004)
2. Dehlinger, C., Dufourd, J.F., Schreck, P.: Higher-order intuitionistic formalization and proofs in Hilbert's elementary geometry. In: Richter-Gebert, J., Wang, D. (eds.) ADG 2000. LNCS (LNAI), vol. 2061, pp. 306–324. Springer, Heidelberg (2001), `http://www.springerlink.com/content/p2mh1ad6ede09g6x/`
3. Paulson, L.C.: The Isabelle reference manual (2006)
4. Meikle, L., Fleuriot, J.: Formalizing Hilbert's Grundlagen in Isabelle/Isar. In: Basin, D., Wolff, B. (eds.) TPHOLs 2003. LNCS, vol. 2758, pp. 319–334. Springer, Heidelberg (2003), `http://springerlink.metapress.com/content/6ngakhj9k7qj71th/?p=e4d2c272843b41148f0550f9c5ad8a2a&pi=20`
5. Tarski, A., Givant, S.: Tarski's system of geometry. The bulletin of Symbolic Logic 5(2) (1999)

6. Schwabhäuser, W., Szmielew, W., Tarski, A.: Metamathematische Methoden in der Geometrie. Springer, Berlin (1983)
7. Quaife, A.: Automated development of Tarski's geometry. Journal of Automated Reasoning 5(1), 97–118 (1989)
8. Narboux, J.: Toward the use of a proof assistant to teach mathematics. In (ICTMT7). Proceedings of the 7th International Conference on Technology in Mathematics Teaching (2005)
9. Narboux, J.: A graphical user interface for formal proofs in geometry. The Journal of Automated Reasoning special issue on User Interface for Theorem Proving 39(2) (2007), http://www.informatik.uni-bremen.de%7Ecxl/uitp-jar/, http://springerlink.metapress.com/content/b60418176x313vx6/?p=aa2ae37923ab455291ee15f6c9c39b9b&pi=3
10. Guilhot, F.: Formalisation en coq et visualisation d'un cours de géométrie pour le lycée. Revue des Sciences et Technologies de l'Information, Technique et Science Informatiques, Langages applicatifs 24, 1113–1138 (2005)
11. Pichardie, D., Bertot, Y.: Formalizing convex hulls algorithms. In: Boulton, R.J., Jackson, P.B. (eds.) TPHOLs 2001. LNCS, vol. 2152, pp. 346–361. Springer, Heidelberg (2001)
12. Meikle, L., Fleuriot, J.: Mechanical theorem proving in computation geometry. In: Hong, H., Wang, D. (eds.) ADG 2004. LNCS (LNAI), vol. 3763, pp. 1–18. Springer, Heidelberg (2006)
13. Dufourd, J.F.: Design and formal proof of a new optimal image segmentation program with hypermaps. In: Pattern Recognition, vol. 40(11), Elsevier, Amsterdam (2007), http://portal.acm.org/citation.cfm?id=1274191.1274325&coll=GUIDE&dl=%23url.coll
14. Narboux, J.: A decision procedure for geometry in Coq. In: Slind, K., Bunker, A., Gopalakrishnan, G.C. (eds.) TPHOLs 2004. LNCS, vol. 3223, Springer, Heidelberg (2004)
15. Narboux, J.: Formalisation et automatisation du raisonnement géométrique en Coq. PhD thesis, Université Paris Sud (September 2006)
16. Chou, S.C., Gao, X.S., Zhang, J.Z.: Machine Proofs in Geometry. World Scientific, Singapore (1994)
17. Tarski, A.: A decision method for elementary algebra and geometry. University of California Press (1951)
18. Tarski, A.: The completeness of elementary algebra and geometry (1967)
19. Tarski, A.: What is elementary geometry? In: Henkin, L., Tarski, P.S. (eds.) The axiomatic Method, with special reference to Geometry and Physics, Amsterdam, North-Holland, pp. 16–29 (1959)
20. Gupta, H.N.: Contributions to the axiomatic foundations of geometry. PhD thesis, University of California, Berkley (1965)
21. Huet, G., Kahn, G., Paulin-Mohring, C.: The Coq Proof Assistant - A tutorial - Version 8.0 (April 2004)
22. Bertot, Y., Castéran, P.: Interactive Theorem Proving and Program Development, Coq'Art: The Calculus of Inductive Constructions. In: Texts in Theoretical Computer Science. An EATCS Series, Springer, Heidelberg (2004)
23. Coquand, T., Paulin-Mohring, C.: Inductively defined types. In: Martin-Löf, P., Mints, G. (eds.) COLOG-88. LNCS, vol. 417, Springer, Heidelberg (1990)
24. von Plato, J.: The axioms of constructive geometry. Annals of Pure and Applied Logic 76, 169–200 (1995)
25. Kahn, G.: Constructive geometry according to Jan von Plato. Coq contribution, Coq V5.10 (1995)