DIPLOMARBEIT

Sketch-as-proof

A proof-theoretic analysis of axiomatic projective geometry

ausgeführt am
Institut für Algebra und Diskrete Mathematik
der Technischen Universität Wien

unter Anleitung von
Univ.-Doz. Dr. phil. Matthias Baaz

durch
Norbert Preining
1160 Wien, Starkenburggasse 62

Ich möchte Dr. Matthias Baaz für seine intensive Betreuung im Rahmen dieser Diplomarbeit, meiner Mutter dafür, daß sie mir dieses Studium ermöglicht hat und meiner Freundin Brigitte für die sorgfältige und mühevolle Durchsicht des Manuskripts danken.

Contents

List of Figures

Chapter 1

Introduction

This thesis results from the wish to connect two interesting parts of mathematics, proof theory and projective geometry. We applied theoretic methods of proof theory to projective geometry. This should be another try to span the gap between theoretical and applied mathematics. The gap arises from the fact, that "applied mathematicians" don't want to use the methods of proof theory, because these are highly formal and syntactical, and logicians don't think that it is necessary to apply their theoretical framework.

Besides the natural numbers in form of the Peano arithmetic, which are subject to various forms of analysis before and after Gödels historic work [5] on the incompleteness of Peano arithmetic, the geometry was used for logical analysis for many years. For instance Hilbert put up an axiom system for Euclidean geometry (cf. [6]), and many analyses followed. But most logicians stayed to these classical fields (c.f. [12]) and to my knowledge there is no analysis of projective geometry, although the projective geometry happens to be in an already axiomatized form (see 2.2 for details). There are analyses on mechanical proving in special geometries (c.f. [17]), but these analyses restrict themselves to the case of geometries which can be coordinatized. This yields a decision procedure, since the real closed fields can be decided (c.f. [16]), while "pure" projective geometry cannot be coordinatized.[1]

By the following thesis we hope to open up a new field of research for logicians and mathematicians to better understand the properties of projective geometry.

[1]But there where some other interesting approaches to applied mathematics by logical means. One of these approaches is Gaisi Takeutis "A Conservative Extension of Peano Arithmetic"[14]. Other applications of logic can be found in fuzzy logic, knowledge based systems and various other fields.

Chapter 2

Projective Geometry

In this chapter we will first make a tour through the history of geometry and its foundation in logic (cf. 2.1), next we will give a definition of projective geometry (cf. 2.2), then we will present examples of projective planes (cf. 2.3), furthermore we will discuss the connection between the "reality" of projective planes and the axiomatic theory (cf. 2.4) and finally we will present some consequences of the axioms for projective geometry (cf. 2.5). For a good textbook on projective geometry see [3].

2.1 Historical Background

The earliest systematic method used in the study of geometry was the deductive axiomatic method introduced by the Greeks. Thales (640-546 B.C.) is generally considered to be the first to treat geometry as a logical structure. In the next 300 years much geometric knowledge was developed. Then Euclid (*c.* 300 B.C.) collected and systematized all the geometry previously created. He did this by starting out with a set of axioms, statements to be accepted as "true", from which all theorems were deduced as logical consequences (cf. app. A).

Though the Greek realized the need for axioms, they did not seem to find a logical need for undefined terms. Euclid therefore attempted to define everything (cf. A.1). The assumptions which Euclid used in his proofs were not all stated explicitly. For example, there is nothing in Euclid's axioms from which we can deduce that an angle bisector of a triangle will intersect the opposite side. Further, where constructions demand the intersection of two circles, or of a line and a circle, Euclid simply assumed the existence of the needed points of intersection. Though there were attempts to improve on Euclid's definitions and axioms, nevertheless, Euclid reigned supreme until the 19th century. Then came the discovery of non-Euclidean geometry and with it a re-examination of the foundations of Euclidean geometry.

2.1.1 The Euclidean Axiom of Parallelism

The first four of Euclid's axioms (cf. A.2) were accepted as simple and "obvious". The fifth, however, was not. Euclid proved his 28 propositions without using the fifth axiom. For 2000 years mathematicians tried to prove this axiom; i.e., tried to deduce it from the other axioms and the first 28 propositions. But they only succeeded in replacing it by various equivalent assumptions.

In the 19th century the conclusion was reached that not only could the parallel postulate not be proved, but that a logical system of geometry could be constructed without its use. Up to this point no one thought of arguing against the "truth" of Euclid's parallel postulate. But in the 19th century the founders of non-Euclidean geometry—Carl Friedrich Gauss (1777–1855), Nicolai Ivanovitch Lobachevsky (1793–1856), and Johann Bolyai (1802–1860)—concluded independently that a consistent geometry denying Euclid's parallel postulate could be set up.

Gauss, from 1792 to 1813, tried to prove Euclid's parallel postulate, but after 1813 his letters show that he had overcome the usual prejudice and developed a non-Euclidean geometry. But, fearing ridicule and controversy, he kept these revolutionary ideas to himself, except for letters to his friends. Lobachevsky and Bolyai were the first to publish expositions of the new geometry, Lobachevsky in 1829 and Bolyai in 1832. This geometry is known today as Hyperbolic Geometry. In 1854 Bernhard Riemann (1826–1866) developed another non-Euclidean geometry, known as Elliptic Geometry.

2.1.2 Hilbert and the new approach to Geometry

The next great step in the development of the logic of geometry was the break with the long hold tradition of defining everything mathematics or geometry speak about. It's not easy to see the great step, but the fact of treating Points and Lines as primitives dispenses you of the awful duty to define Points as "impartable objects", "the entity in space" and all the other interesting definitions Greek philosophers invented. Only a few undefined objects and relations are assumed as primitives and the axioms determine the "behavior" of them.

Though defects in Euclid's logical structure were pointed out earlier, it was not until after the discovery of non-Euclidean geometry that mathematicians began carefully scrutinizing the foundations of Euclidean geometry and formulating precise sets of axioms for it. The problem was to erect the entire structure of Euclidean geometry upon the simplest foundation possible; i.e., to choose a minimum number of undefined elements and relations and a set of axioms concerning them, with the property that all of Euclidean geometry can be logically deduced from these without any further appeal to intuition. There were many such axiom sets formulated at the end of the 19th century beginning with the work of Pasch (1882), known for the Pasch Axiom, Peano (1889), primary known for his axiomatization of the natural numbers—the Peano Arithmetic—and Pieri (1899) and culminating with the famous set by David Hilbert (1899, cf. app. B and [6]).

The roots of projective geometry can be traced back to ancient Greeks who knew some of the theorems as part of Euclidean geometry. Its formal development probably started in the 15th century by artists who were looking for a theory of perspective drawing; i.e., the laws of constructing the projections of three-dimensional objects on a two-dimensional plane. The theory was extended by Desargues (1593–1662), an engineer and architect who, in 1639, published a treatise on conic sections using the concept of projection. It was here that Desargues used the idea of adding one point "at infinity" to each line with the locus of these "ideal points" forming an "ideal line", added to the Euclidean plane, where parallel lines were to intersect. However, it was not until Monge (1746–1818), with his co-workers at the Ecole Polytechnique in Paris, developed his descriptive geometry—the analysis and representation of three-dimensional objects by means of their projections on different planes—that the study of projective geometry began to flourish.

Mathematicians classified geometric properties into two categories: *metric* properties, which are those concerned with measurements of distances, angles, and areas, and *descriptive* properties, which are those concerned with the positional relations of geometric figures to one another. For example, the length of a line segment and the congruence of three lines are metric properties, but the collinearity of three points and the concurrence of three lines are descriptive properties. In the case of plane figures, descriptive properties are preserved when a figure is projected from one plane onto another (provided we consider parallel lines as intersecting at an "ideal point"), while metric properties may not be preserved. Thus the property of a given curve being a circle is a metric property but that of its being a conic is a descriptive or projective property.

The beginning of the modern period of the development of projective geometry is usually placed at 1822 when Poncelet (1788–1867), a pupil of Monge, published his great treatise on the projective properties of figures, written while he was a prisoner in Russia. Throughout the 19th century, the subject was developed rapidly by Gergonne, Brianchon, Plücker, Steiner, Von Staudt and others.

For the most part, however, projective geometry was developed as an extension of Euclidean geometry (cf. 2.3.1); e.g., the parallel postulate was still used and a line was added to the Euclidean plane to contain the "ideal points" mentioned above. It was only at the end of the 19th century and the beginning of the 20th century, through the work of Felix Klein (1849–1925), Oswald Veblen (1880–1960), David Hilbert, and others, that projective geometry was seen to be independent of the theory of parallels. Projective geometry was then developed as an abstract science based on its own set of axioms.

In the next section we will discuss the properties of projective geometry in greater detail and we will also see an axiomatization in the sense of Hilbert for the projective geometry.

2.2 What is Projective Geometry

We will now give an axiomatization of projective geometry in the sense of the previous sections. The projective geometry deals, like the Euclidian geometry, with points and lines. These two elements are primitives, which aren't further defined. Only the axioms tell us about their properties. The axioms for the projective geometry are very simple, the reason why I chose this geometry for a proof-theoretic analysis.

Now let me begin with the definition of the projective geometry: There are two classes of objects, called *Points* and *Lines*[1], and one predicate, that puts up a relation between Points and Lines, called *Incidence*.

Furthermore we must give some axioms to express certain properties of Points and Lines and to specify the behavior of the incidence on Points and Lines:

(PG1) For every two distinct Points there is one and only one Line, so that these two Points incide with this Line.

(PG2) For every two distinct Lines there is one and only one Point, so that this Point incides with the two Lines[2].

(PG3) There are four Points, which never incide with a Line defined by any of the three other Points.

The next chapter will present some examples of Projective Planes.

2.3 Examples for Projective Planes

2.3.1 The projective closed Euclidean plane Π_{EP}

The easiest approach to projective geometry is via the Euclidean plane. If we add one Point "at infinity" to each line and one "ideal Line", consisting of all these "ideal Points", it follows that two Points determine exactly one Line and two distinct Lines determine exactly one Point[3] (cf. 2.1). So the axioms are satisfied.

This projective plane is called Π_{EP} and has a lot of other interesting properties, especially that it is a classical projective plane.

[1]We will use the expression "Point" (note the capital P) for the objects of projective geometry and "points" as usual for e.g. a point in a plane. The same applies to "Line" and "line".

[2]"one and only one" can be replaced by "one", because the fact that there is not more than one Point can be proven from axiom (PE1).

[3]More precise: The "ideal Points" are the congruence classes with respect to the parallel relation and the "ideal Line" is the class of these congruence classes.

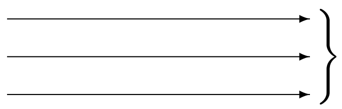

Figure 2.1: “Ideal Points” in Π_{EP}

2.3.2 The projective Desargues-Plane

A very well known property of Π_{EP} is the Desargues’ Theorem. To understand it, some definitions (cf. fig. 2.2):

DEFINITION 2.1 *Two triangles are said to be* perspective from a Point O *if there is a one-to-one correspondence between the vertices so that Lines joining corresponding vertices all go through* O*. Dually, two triangles are said to be* perspective from a Line o *if there is a one-to-one correspondence between the sides of the triangles such that the Points of intersection of corresponding sides all lie on* o*.*

THEOREM 2.1 (DESARGUES’ THEOREM) *If two triangles are perspective from a Point, then they are perspective from a Line.*

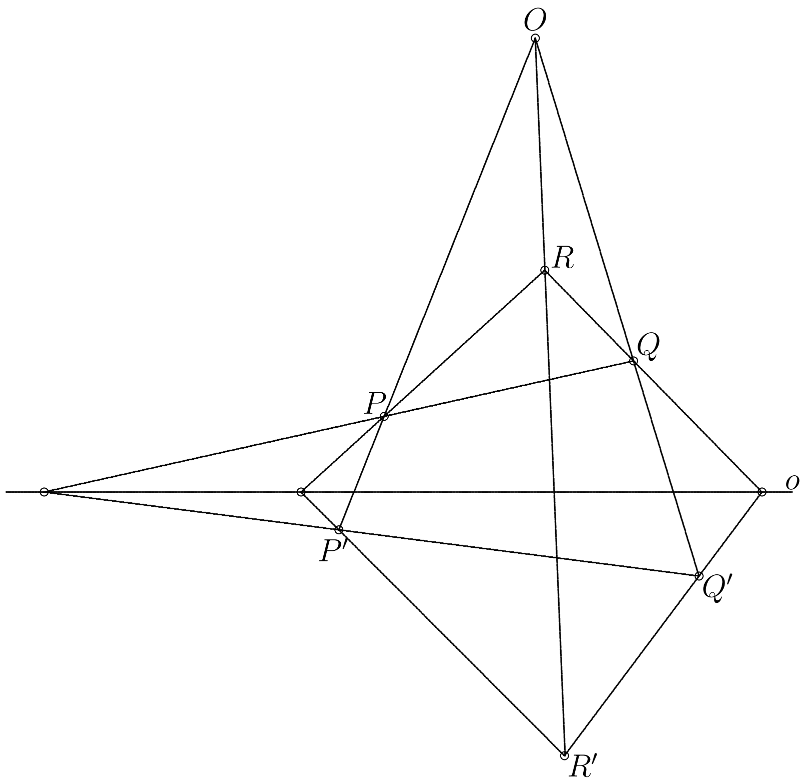

Figure 2.2: Desargues’ Theorem

Finally an example for a finite Projective Plane:

2.3.3 The minimal Projective Plane

One of the basic properties of projective planes is the fact, that there are seven distinct Points. Four Points satisfying axiom (PG3) and the three diagonal Points $([A_0B_0][C_0D_0]) =: D_1$, $([A_0C_0][B_0D_0]) =: D_2$ and $([A_0D_0][B_0C_0]) =: D_3$. If we can set up a relation of incidence on these Points such as that the axioms (PG1) and (PG2) are satisfied, then we have a minimal projective plane. Fig. 2.3 defines such an incidence-table. In this table not only the usual lines are Lines for the projective geometry, but also the circle.

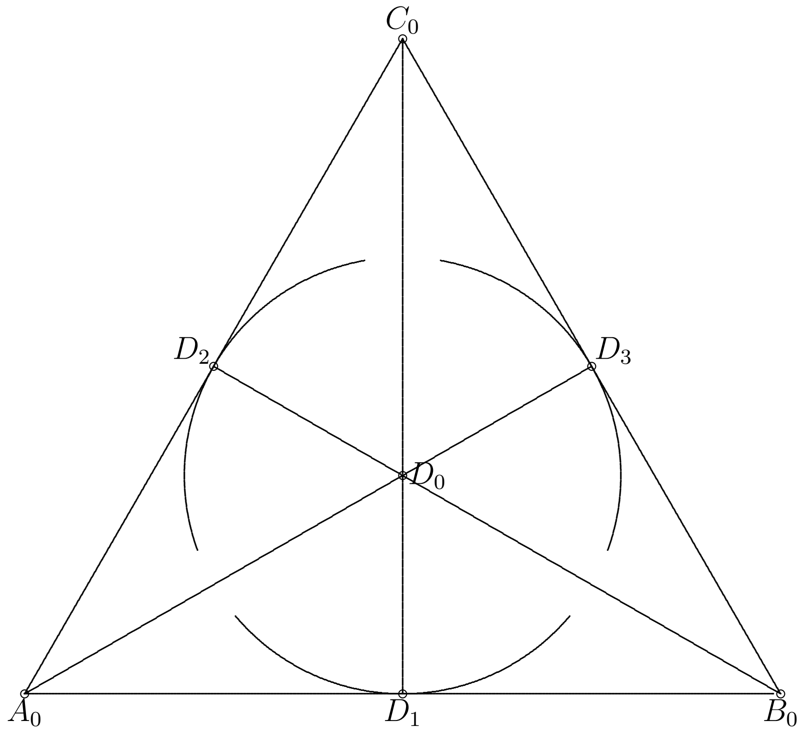

Figure 2.3: Incidence Table for the minimal Projective Plane

We could attribute a number called "order", which is the number of Points on a Line minus one, to every finite projective plane. Then there is the question for which number n there is a projective plane with order n. One partial solution for this problem depends on the existence of finite fields. If we have a finite field, we can construct a finite projective plane with the same order. Since there are finite fields for every power of a prime[4], for any such number there is also a projective plane.

Principally these questions can be answered simply by trying all possible relation tables with n Points and n Lines and look, whether there is one satisfying the axioms. But this method is much too difficult to do, because the number of

[4]The so called Galois Field GF(n).

such tables rises exponentially.

2.4 The Connection between "Reality" and the Axiomatic Method

The idea behind an axiomatic approach to a mathematical problem is the same as developing a general formula for the roots of quadratic equations. The generalities are searched between all the different equations and one solution is given for all different instances of the one general equation.

The axiomatic (or logic) approach tries to formulate the basic principles of an idea. Then all the logical conclusions are valid in all instances of the given set of axioms, in the language of the logician, valid in all models of this set of axioms.

So we can define a projective plane as every structure, such as that the constants, function constants and predicate constants can be interpreted in this structure and via this interpretation the axioms are true in this structure.

There is one restriction to the facts which can be proven from the axioms: All facts must be valid in all the models of the three axioms, i.e. also in all the finite projective planes. Simple consequence from this is that you cannot prove such as "There are n different objects which satisfy …"[5].

If some certain properties are needed, than they are added as axioms. The most important ones are the Theorem of Desargues (cf. 2.3.2), the Theorem of Pappos and a few more. They are important to proof properties of Π_{AE} (cf. 2.3.1), e.g. certain properties on conics.

2.5 Some Consequences of the Axioms

- There are seven distinct Points in a projective plane, namely the four constants $A_0, \ldots, D_0$ and the three diagonal Points $D_1 = ([A_0B_0][C_0D_0])$, $D_1 = ([A_0C_0][B_0D_0])$, $D_3 = ([A_0D_0][B_0C_0])$.
- For each Line there are three distinct Points which incide with this Line.
- For distinct Lines g and h there is a Point P such that $P \not{I} g$ and $P \not{I} h$.
- There is a one-to-one mapping from the set of Points to the set of Lines in a projective plane.
- If there are exactly $n+1$ distinct Points on a Line, then on every Line there are $n+1$ distinct Points, for each Point there are exactly $n+1$ different Lines passing through it and there are exactly n^2+n+1 Points and exactly that much Lines.

[5]For the geometers: If $n > 7$, because in every projective plane there are 7 distinct points.

Chapter 3

Proof Theory

3.1 Introduction to Proof Theory

Logic is the study of reasoning; and mathematical logic is the study of the type of reasoning done by mathematicians. To discover the proper approach to mathematical logic, we must therefore examine the methods of the mathematician.

The conspicuous feature of mathematics, as opposed to other sciences, is the use of proofs instead of observations. A physicist may prove physical laws from other physical laws; but he usually regards agreement with observations. A mathematician may, on occasions, use observations; for example, he may measure the angles of many triangles and conclude that the sum of the angles is always 180°. However, he will accept this as a law of mathematics only when it has been proved.

Nevertheless, it is clearly impossible to prove all mathematical laws out of nothing. Euclid himself overcame the problem of the initial laws in defining everything, but this is essentially the same. The first laws which one accepts cannot be proved, since there are no earlier laws from which they can be proved. Hence we have certain first laws, called *axioms*, which we accept without proof; the remaining laws, called *theorems*, are proved from the axioms. Axioms, theorems and certain concepts of derivation build up an *axiom system* (see [13] or [7] for a good introduction[1] to mathematical logic).

The study of axioms and theorems as sentences, sequences of glyphs, is called the *syntactical* study of axiom systems; the study of the meaning of these sentences is called the *semantic* study of axiom systems. There are two subfields of mathematical logic each dedicated to one of this approaches. *Model theory* discusses the meaning of axioms and theorems. It is concerned with the semantic aspect of axiom systems (see [9] for a good introduction to model theory).

On the other hand there is *proof theory*, which investigates the syntactical properties of sentences and proofs. Since the proof is the basic derivation concept

[1]maybe the best

of a mathematician, it is interesting to learn what the meaning of a proof is (see [15] and [4] for good introductions to proof theory).

In a sense, mathematics is a collection of proofs. Therefore, in investigating "mathematics", a fruitful method is to formalize proofs of mathematics and investigate the structure of these proofs. This is what proof theory is concerned with. So proof theory is mainly concerned with formal syntax: proofs, formulas and their various generalizations.

From a more abstract point of view proof theory is concerned with the relation between finite and infinite objects, more precisely, the very nature of what we are doing:

– when denoting (infinite) mathematical objects by means of (finite) syntactical constructions;

– when proving facts concerning (infinitary) objects by means of (finite) proofs.

That's the proof theory in D. Hilbert's sense. This approach was later developed by the work of G. Gentzen and followers, the so-called Gentzen-like proof theory.

There are some other approaches to proof theory. One of these has been developed by Brouwer, which considers the proofs as the semantic of mathematics, not the syntax. I.e. a proof of $A \supset B$ is considered as an instruction how to construct a proof of B from a proof of A.

We will not give detailed exposition of classical logic, for this see [13],[1],[7] or [10]. Since we are interested in the relations between proofs and properties of the proven object, we will follow Gentzen-like proof theory, so ...

3.2 What is Gentzen-like Proof Theory?

The proof theory according to Gentzen is based on the sequent calculus, Gentzen's formulation of the first order predicate calculus **LK** ("logistischer klassischer Kalkül").

I will skip the usual formalization of statements, terms, (atomic) formulas, substitution since they will come at a later stage (see sec. 4) and only mention, that in this thesis the following logical symbols are used:

$\neg$ for "not"
$\wedge$ for "and"
$\vee$ for "or"
$\supset$ for "implies"
$\forall$ for "for all"
$\exists$ for "there exists"

and that parentheses are used freely for better readability. A detailed exposition of the formalization can be found in various books on proof theory (e.g. [15], [4]).

In the following, let Greek capital letters Γ, Δ, Π, Λ, Γ_0, $\ldots$ denote finite (possibly empty) sequences of formulas separated by commas.

DEFINITION 3.1 *For arbitrary* Γ *and* Δ, $\Gamma \rightarrow \Delta$ *is called a* sequent. Γ *and* Δ *are called the* antecedent *and* succedent, *respectively, of the sequent.*

Intuitively, a sequent $A_1, \ldots, A_m \rightarrow B_1, \ldots, B_n$ (where $m, n \geq 1$) means: if $A_1 \wedge \ldots \wedge A_m$, then $B_1 \vee \ldots \vee B_n$. For $m \geq 1$, $A_1, \ldots, A_m \rightarrow$ means that $A_1 \wedge \ldots \wedge A_m$ yields a contradiction. For $n \geq 1$, $\rightarrow B_1, \ldots, B_n$ means, that $B_1 \vee \ldots \vee B_n$ holds. The empty sequent $\rightarrow$ means there is a contradiction. Sequents will be denoted by the letter S, with or without subscripts.

DEFINITION 3.2 *An* inference *is an expression of the form*

$$\frac{S_1 \quad \ldots \quad S_n}{S} \qquad \textit{where } n = 1, 2 \textit{ (ev. } 3\textit{)}$$

where the S_i *and* S *are sequents. The* S_i *are called the* upper sequents *and* S *is called the* lower sequent *of the inference.*

Intuitively this means that when S_i are asserted, we can infer S from them. We restrict ourselves to inferences obtained from the following rules of inferences, in which A, B, C, D, $F(a)$ denote formulas.

1. Structural rules:

   (a) *Weakening:*

   $$\frac{\Gamma \rightarrow \Delta}{D, \Gamma \rightarrow \Delta} \text{ (W:left)} \qquad \frac{\Gamma \rightarrow \Delta}{\Gamma \rightarrow \Delta, D} \text{ (W:right)}$$

   D is called the *weakening formula.*

   (b) *Contraction:*

   $$\frac{D, D, \Gamma \rightarrow \Delta}{D, \Gamma \rightarrow \Delta} \text{ (C:left)} \qquad \frac{\Gamma \rightarrow \Delta, D, D}{\Gamma \rightarrow \Delta, D} \text{ (C:right)}$$

   (c) *Exchange:*

   $$\frac{\Gamma, C, D, \Pi \rightarrow \Delta}{\Gamma, D, C, \Pi \rightarrow \Delta} \text{ (E:left)} \qquad \frac{\Gamma \rightarrow \Delta, C, D, \Lambda}{\Gamma \rightarrow \Delta, D, C, \Lambda} \text{ (E:right)}$$

   We will refer to these three kinds of inferences as “weak inferences”, while all others will be called “strong inferences”.

2. Logical rules:

(a)

$$\frac{\Delta \to \Gamma, D}{\neg D, \Gamma \to \Delta}\ (\neg\text{:left}) \qquad \frac{D, \Gamma \to \Delta}{\Gamma \to \Delta, \neg D}\ (\neg\text{:right})$$

(b)

$$\frac{C, \Gamma \to \Delta}{C \wedge D, \Gamma \to \Delta}\ (\wedge\text{:left}) \quad \text{and} \quad \frac{D, \Gamma \to \Delta}{C \wedge D, \Gamma \to \Delta}\ (\wedge\text{:left})$$

$$\frac{\Gamma \to \Delta, C \quad \Gamma \to \Delta, D}{\Gamma \to \Delta, C \wedge D}\ (\wedge\text{:right})$$

(c)

$$\frac{C, \Gamma \to \Delta \quad D, \Gamma \to \Delta}{C \vee D, \Gamma \to \Delta}\ (\vee\text{:left})$$

$$\frac{\Gamma \to \Delta, C}{\Gamma \to \Delta, C \vee D}\ (\vee\text{:right}) \quad \text{and} \quad \frac{\Gamma \to \Delta, D}{\Gamma \to \Delta, C \wedge D}\ (\vee\text{:right})$$

(d)

$$\frac{\Gamma \to \Delta, C \quad D, \Pi \to \Lambda}{C \supset D, \Gamma, \Pi \to \Delta, \Lambda}\ (\supset\text{:left})$$

$$\frac{C, \Gamma \to \Delta, D}{\Gamma \to \Delta, C \supset D}\ (\supset\text{:right})$$

(e)

$$\frac{F(t), \Gamma \to \Delta}{\forall x F(x), \Gamma \to \Delta}\ (\forall\text{:left}) \qquad \frac{\Gamma \to \Delta, F(a)}{\Gamma \to \Delta, \forall x F(x)}\ (\forall\text{:right})$$

where t is an arbitrary term, and a does not occur in the lower sequent. The a in ($\forall$:right) is called the *eigenvariable* of this inference.

(f)

$$\frac{F(a), \Gamma \to \Delta}{\exists x F(x), \Gamma \to \Delta}\ (\exists\text{:left}) \qquad \frac{\Gamma \to \Delta, F(t)}{\Gamma \to \Delta, \exists x F(x)}\ (\exists\text{:right})$$

where a does not occur in the lower sequent, and t is an arbitrary term. The a in ($\exists$:left) is called the *eigenvariable* of this inference.

3. Cut:

$$\frac{\Gamma \to \Delta, D \quad D, \Pi \to \Lambda}{\Gamma, \Pi \to \Delta, \Lambda}\ (D)$$

D is called the *cut formula* of this inference.

DEFINITION 3.3 *A sequent of the form* $A \to A$ *is called an* initial sequent. *A* proof P *(in* ***LK****) is a tree of sequents satisfying the following conditions:*

1. *The topmost sequents of* P *are initial sequents.*

2. *Every sequent in P except the lowest one is an upper sequent of an inference whose lower sequent is also in P.*

Although the formula A in an initial sequent $A \to A$ can be highly complex, we can restrict ourselves to atomic formulas in initial sequents.

We now have a formal concept of a proof and can analyze proofs carried out in this calculus. The investigation of properties of this calculus and the structure of proofs in it is the Gentzen-like proof theory.

3.3 Example Proofs in LK

$$
\begin{array}{cl}
A \to A & \\ \hline
\to A, \neg A & (\neg\text{:right}) \\ \hline
\to A, A \vee \wedge A & (\vee\text{:right}) \\ \hline
\to A \vee \neg A, A & (\text{E:right}) \\ \hline
\to A \vee \neg A, A \vee \neg A & (\vee\text{:right}) \\ \hline
\to A \vee \neg A & (\text{C:right})
\end{array}
$$

Suppose that a is fully indicated in $F(a)$.

$$
\begin{array}{cl}
F(a) \to F(a) & \\ \hline
F(a) \to \exists x F(x) & (\exists\text{:left}) \\ \hline
\to \exists x F(x), \neg F(a) & (\neg\text{:right}) \\ \hline
\to \exists x F(x), \forall y \neg F(y) & (\forall\text{:right}) \\ \hline
\neg \forall y \neg F(y) \to \exists x F(x) & (\neg\text{:left}) \\ \hline
\to \neg \forall y \neg F(y) \supset \exists x F(x) & (\supset\text{:right})
\end{array}
$$

3.4 Results on LK

Proof theory investigates the structure of proofs, so the main objects we are talking about in proof theory is the calculus **LK** and proofs carried out in this calculus. We will now present a few theorems without a proof. The proofs for all the stated theorems can be found in [15].

THEOREM 3.1 (COMPLETENESS AND SOUNDNESS OF **LK**)
*A formula is provable in **LK** if and only if it is valid.*

This theorem states nothing else than that **LK** doesn't deduce something stupid (soundness) and that every "true" formula can be deduced (completeness).

The most important fact about **LK** is the cut-elimination theorem, also known as Gentzen's Hauptsatz:

Theorem 3.2 (Cut Elimination Theorem)
*If a sequent is **LK**-provable, then it is **LK**-provable without a cut.*

This means that any theorem in the predicate calculus can be proved without detours. That's the meaning of the following corollary:

Corollary 3.1 (Subformula Property)
*In a cut-free proof in **LK** all the formulas which occur in it are subformulas of the formulas in the end-sequent.*[2]

The cut-elimination is one of the most interesting features. When a typical mathematician proves a new theorem, he uses a lot of other lemmas, theorems. These lemmas are specialized for the given fact and used in the proof to formulate a contradiction or to derive a certain property. In a formal proof this is equivalent to a cut. We know that a fact is true, so we can assume it and cut the assumption out of the proof at a later stage. So using the (Cut)-rule seems to be a natural[3] procedure. Why try to eliminate the cuts in a proof?

The reason lies in the fact that a proof should represent something that can be constructed, maybe like a program that tells you what to do and when. It is the constructivity which makes the cut-elimination so interesting. On of the important corollaries to the cut-elimination theorem is the midsequent theorem (see below), which is nothing else than the good old Herbrand's theorem.

Another difference is the following: What is interesting for a mathematician in a proof is, besides that it proves a theorem, the esthetic component. A proof is honored for its elegance[4]. A logician and especially a proof theoretician is interested in what is necessary to prove a theorem and tries to pull out as much information from the proof as possible, maybe discussing more than one proof for the same theorem.

Corollary 3.2 (Gentzen's Midsequent Theorem)
*Let S be a sequent which consists of prenex formulas only and is provable in **LK**. Then there is a cut-free proof of S which contains a sequent (called a midsequent), say S', which satisfies the following:*

1. *S' is quantifier-free.*

2. *Every inference above S' is either structural or propositional.*

3. *Every inference below S' is either structural or a quantifier inference.*

---

[2]I skipped the definition of *subformula*. It can be found in many books and is somehow "self-describing"

[3]or whatever a mathematician means by "natural"

[4]Today elegance is the ability to use methods from a part of mathematics as far as possible away from ones' one.

Thus a midsequent splits the proof into an upper part, which contains the propositional inferences, and a lower part, which contains the quantifier inferences.

Another important consequence of the cut-elimination theorem is the Maehara's lemma and the interpolation theorem as a consequence of it: For technical reason we introduce the predicate symbol T, with 0 argument places, and admit $\rightarrow T$ as an additional initial sequent. (T stands for "true".) The system which is obtained from **LK** thus extended is denoted by **LK** #.

Corollary 3.3 (Maehara's Lemma)
Let $\Gamma \rightarrow \Delta$ *be* ***LK****-provable, and let* (Γ_1, Γ_2) *and* (Δ_1, Δ_2) *be arbitrary partitions of* Γ *and* Δ*, respectively (including the cases that one or more of* $\Gamma_1, \Gamma_2, \Delta_1, \Delta_2$ *are empty). We denote such a partition by* $[\{\Gamma_1; \Delta_1\}, \{\Gamma_2; \Delta_2\}]$ *and call it a partition of the sequent* $\Gamma \rightarrow \Delta$*. Then there exists a formula* C *of* ***LK*** *# (called an interpolant of* $[\{\Gamma_1; \Delta_1\}, \{\Gamma_2; \Delta_2\}]$*) such that:*

(i) $\Gamma_1 \rightarrow \Delta_1, C$ *and* $C, \Gamma_2 \rightarrow \Delta_2$ *are both* ***LK*** *#-provable;*

(ii) All free variables and individual and predicate constants in C *(apart from* T*) occur in* $\Gamma_1 \cup \Delta_1$ *and* $\Gamma_2 \cup \Delta_2$*.*

As a consequence of this Lemma we will present

Corollary 3.4 (Craig's Interpolation Theorem for **LK**)
Let A *and* B *be two formulas such that* $A \supset B$ *is* ***LK****-provable. If* A *and* B *have at least one predicate constant in common, then there exists a formula* C*, called an interpolant of* $A \supset B$*, such that* C *contains only those individual constants predicate constants and free variables that occur in both* A *and* B*, and such that* $A \supset C$ *and* $C \supset B$ *are* ***LK****-provable. If* A *and* B *contain no predicate constant in common, then either* $A \rightarrow$ *or* $\rightarrow B$ *is* ***LK****-provable.*

The significance of the proof for Maehara's lemma lies in the fact, that an interpolant of $A \supset B$ can be constructively formed from a proof of $A \supset B$.

Corollary 3.5 (Beth's Definability Theorem for **LK**)
If a predicate constant R *is defined implicitly in terms of* $R_1, \ldots, R_n$ *by* $A(R, R_1, \ldots, R_n)$*, then* R *can be defined explicitly in terms of* $A_1, \ldots, A_n$ *and the individual constants in* $A(R, R_1, \ldots, R_n)$*.*

Chapter 4

The Calculus $\mathbf{L_{PG}K}$

In this chapter the calculus $\mathbf{L_{PG}K}$ will be presented. It's based on Gentzen's **LK** (cf. 3.2) and extends it by certain means.

Each of the following sections deals with a certain topic of the calculus. These topics are the definition of the language (4.1), the formalization of terms, atomic formulas and formulas (4.2) and the laying down of the initial sequents and the rules of inference (4.3).

Finally we will give some examples for proofs in $\mathbf{L_{PG}K}$ (cf. 4.4).

4.1 The Language $\mathbf{L_{PG}}$ for $\mathbf{L_{PG}K}$

The language for $\mathbf{L_{PG}K}$ is a type language with two types, Points and Lines. These two types will be denoted with $\tau_{\mathcal{P}}$ and $\tau_{\mathcal{L}}$, respectively.

So the language $\mathbf{L_{PG}}$ for $\mathbf{L_{PG}K}$ consists of the following parts:

1. *Constants:*
   (a) Individual constants of type $\tau_{\mathcal{P}}$: A_0, B_0, C_0, D_0.
   (b) Function constants (the type is given in parenthesis): con:$[\tau_{\mathcal{P}}, \tau_{\mathcal{P}} \to \tau_{\mathcal{L}}]$, intsec:$[\tau_{\mathcal{L}}, \tau_{\mathcal{L}} \to \tau_{\mathcal{P}}]$.
   (c) Predicate constants (the type is given in parenthesis): $\mathcal{I}$:$[\tau_{\mathcal{P}}, \tau_{\mathcal{P}}]$, $=$.
2. *Variables:*
   (a) Free variables of type $\tau_{\mathcal{P}}$: P_0, P_1, ..., P_j $(j = 0, 1, 2, \ldots)$.
   (b) Bound variables of type $\tau_{\mathcal{P}}$: X_0, X_1, ..., X_j $(j = 0, 1, 2, \ldots)$.
   (c) Free variables of type $\tau_{\mathcal{L}}$: g_0, g_1, ..., g_j $(j = 0, 1, 2, \ldots)$.
   (d) Bound variables of type $\tau_{\mathcal{L}}$: x_0, x_1, ..., x_j $(j = 0, 1, 2, \ldots)$.

3. *Logical symbols:*
   $\neg$ (not), $\wedge$ (and), $\vee$ (or), $\supset$ (implies), $\forall_{\tau_{\mathcal{P}}}$ (for all Points), $\forall_{\tau_{\mathcal{L}}}$ (for all Lines), $\exists_{\tau_{\mathcal{P}}}$ (there exists a Point), $\exists_{\tau_{\mathcal{L}}}$ (there exists a Line). The first four are called propositional connectives and the last four are called quantifiers.

4. *Auxiliary symbols:* (,), and , (comma).

The constants $A_0,\ldots,D_0$ are used to denote the four Points obeying (PG3). We will use further capital letters, with or without sub– and superscripts, for Points[1] and lowercase letters, with or without sub– and superscripts, for Lines. Furthermore we will use the notation $[PQ]$ for the connection $\mathrm{con}(P,Q)$ of two Points and the notation (gh) for the intersection $\mathrm{intsec}(g,h)$ of two Lines to agree with the classical notation in projective geometry. Finally $\mathcal{I}(P,g)$ will be written $P\mathcal{I}g$.

We also lose the subscript $_{\tau_{\mathcal{P}}}$ and $_{\tau_{\mathcal{L}}}$ in $\forall_{\tau_{\mathcal{P}}}$, ..., since the right quantifier is easy to deduce from the bound variable.

We have discussed also other languages, e.g. not typed languages with special predicates identifying Points and Lines, but considered this formalization easier to handle. For extensions of the language to higher types, see 9.1.

4.2 Formalization of Terms, Atomic Formulas and Formulas

In the following we assume that the language $\mathbf{L_{PG}}$ is fixed. Any finite sequence of symbols (from the language $\mathbf{L_{PG}}$) is called an expression (of $\mathbf{L_{PG}}$).

Definition 4.1 *Terms of type are defined inductively as follows:*

1. *Every individual constant is a term of the respective type.*
2. *Every free variable is a term of the respective type.*
3. *If R and S are terms of type $\tau_{\mathcal{P}}$, then $[RS]$ is a term of type $\tau_{\mathcal{L}}$.*
4. *If g and h are terms of type $\tau_{\mathcal{L}}$, then (gh) is a term of type $\tau_{\mathcal{P}}$.*
5. *Terms are only those expressions obtained by 1–4.*

Definition 4.2 *If P is of type $\tau_{\mathcal{P}}$ and g is of type $\tau_{\mathcal{L}}$, then $P\mathcal{I}g$ is an* atomic formula*. If t and u are terms of the same type, then $x = y$ is an atomic formula.* Formulas *and their* outermost logical symbols *are defined inductively as follows:*

[1]Capital letters are also used for formulas, but this shouldn't confuse the reader, since the context in each case is totally different.

1. *Every atomic formula is a formula. It has no outermost logical symbol.*

2. *If* A *and* B *are formulas, then* $(\neg A)$, $(A \wedge B)$, $(A \vee B)$, $A \supset B$ *are formulas. Their outermost symbols are* $\neg$, $\wedge$, $\vee$, $\supset$, *respectively.*

3. *If* A *is a formula,* P *is a free variable of type* $\tau_{\mathcal{P}}$ *and* X *is a bound variable of type* $\tau_{\mathcal{P}}$ *not occurring in* A*, then* $(\forall X)A'$ *and* $(\exists X)A'$ *are formulas, where* A' *is the expression obtained from* A *by writing* X *in place of* P *at each occurrence of* P *in* A*. Their outermost symbols are* $\forall$ *and* $\exists$*, respectively.*

4. *If* A *is a formula,* g *is a free variable of type* $\tau_{\mathcal{L}}$ *and* x *is a bound variable of type* $\tau_{\mathcal{L}}$ *not occurring in* A*, then* $(\forall x)A'$ *and* $(\exists x)A'$ *are formulas, where* A' *is the expression obtained from* A *by writing* x *in place of* g *at each occurrence of* P *in* A*. Their outermost symbols are* $\forall$ *and* $\exists$*, respectively.*

A formula without free variables is called a closed formula *. A formula which is defined without the use of the last two clauses is called* quantifier-free*.*

4.3 The Rules and Initial Sequents of $\mathbf{L_{PG}K}$

This section will give the rules and initial sequents of $\mathbf{L_{PG}K}$. So it completes the definition of $\mathbf{L_{PG}K}$.

DEFINITION 4.3 *A* logical initial sequent *is a sequent of the form* $A \to A$*, where* A *is atomic.*
The mathematical initial sequents *are formulas of one of the following forms:*

1. $\to P\mathcal{I}[PQ]$ *and* $\to Q\mathcal{I}[PQ]$*.*

2. $\to (gh)\mathcal{I}g$ *and* $\to (gh)\mathcal{I}h$*.*

3. $X = Y \to$ *where* $X, Y \in \{A_0, B_0, C_0, D_0\}$ *and* $X \neq Y$*.*

4. $\to x = x$ *where* x *is a free variable.*

The initial sequents for $\mathbf{L_{PG}K}$ *are the logical initial sequents and the mathematical initial sequents.*

The first two clauses are nothing else then (PG1) and (PG2). (PG3) is realized by a rule.

DEFINITION 4.4 *The* rules for $\mathbf{L_{PG}K}$ *are (cf. 3.2)*

1. *Structural rules (cf. p. 11)*

2. *Logical rules (cf. p. 11)*

3. *Cut rule (cf. p. 12)*

4. *Equality rules*

$$\frac{\Gamma \to \Delta, s = t \quad s = u, \Gamma \to \Delta}{t = u, \Gamma \to \Delta} \text{ (trans:left)}$$

$$\frac{\Gamma \to \Delta, s = t \quad \Gamma \to \Delta, s = u}{\Gamma \to \Delta, t = u} \text{ (trans:right)}$$

$$\frac{s = t, \Gamma \to \Delta}{t = s, \Gamma \to \Delta} \text{ (symm:left)} \qquad \frac{\Gamma \to \Delta, s = t}{\Gamma \to \Delta, t = s} \text{ (symm:right)}$$

$$\frac{\Gamma \to \Delta, s = t \quad s\mathcal{I}u, \Gamma \to \Delta}{t\mathcal{I}u, \Gamma \to \Delta} \text{ (id-}\mathcal{I}_{\tau_\mathcal{P}}\text{:left)}$$

$$\frac{\Gamma \to \Delta, s = t \quad \Gamma \to \Delta, s\mathcal{I}u}{\Gamma \to \Delta, t\mathcal{I}u} \text{ (id-}\mathcal{I}_{\tau_\mathcal{P}}\text{:right)}$$

$$\frac{\Gamma \to \Delta, u = v \quad s\mathcal{I}u, \Gamma \to \Delta}{s\mathcal{I}v, \Gamma \to \Delta} \text{ (id-}\mathcal{I}_{\tau_\mathcal{L}}\text{:left)}$$

$$\frac{\Gamma \to \Delta, u = v \quad \Gamma \to \Delta, s\mathcal{I}u}{\Gamma \to \Delta, s\mathcal{I}v} \text{ (id-}\mathcal{I}_{\tau_\mathcal{L}}\text{:left)}$$

$$\frac{\Gamma \to \Delta, s = t}{\Gamma \to \Delta, [su] = [tu]} \text{ (id-con:1)} \qquad \frac{\Gamma \to \Delta, u = v}{\Gamma \to \Delta, [su] = [sv]} \text{ (id-con:2)}$$

$$\frac{\Gamma \to \Delta, g = h}{\Gamma \to \Delta, (tg) = (th)} \text{ (id-int:1)} \qquad \frac{\Gamma \to \Delta, g = h}{\Gamma \to \Delta, (gt) = (ht)} \text{ (id-int:2)}$$

5. *Mathematical rules: (PG1-ID) and (Erase)*

$$\frac{\Gamma \to \Delta, P\mathcal{I}g \quad \Gamma \to \Delta, Q\mathcal{I}g \quad P = Q, \Gamma \to \Delta}{\Gamma \to \Delta, [PQ] = g} \text{ (PG1-ID)}$$

$$\frac{\Gamma \to \Delta, X\mathcal{I}[YZ]}{\Gamma \to \Delta} \text{ (Erase)}$$

where $\neq(X, Y, Z)$ *and* $X, Y, Z \in \{A_0, B_0, C_0, D_0\}$

We now have all the essentials for the calculus $\mathbf{L_{PG}K}$ and can define the notion of a proof:

DEFINITION 4.5 *A* proof P in $\mathbf{L_{PG}K}$ *is a tree of sequents satisfying the following conditions:*

1. *The topmost sequents of* P *are initial sequents for* $\mathbf{L_{PG}K}$.

2. *Every sequent in* P *except the lowest one is an upper sequent of an inference for* $\mathbf{L_{PG}K}$ *whose lower sequent is also in* P.

4.4 Sample Proofs in $\mathbf{L_{PG}K}$

We will now give some example proofs in $\mathbf{L_{PG}K}$.

4.4.1 The Diagonal-points

We will proof that the diagonal-points D_1, D_2, D_3 (cf. 2.3.3) are distinct from one another and from $A_0, \ldots, D_0$.

$$\dfrac{\begin{matrix}\vdots & \vdots & \vdots & \vdots \\ \to A_0 \neq D_1 & \to B_0 \neq D_1 & \to C_0 \neq D_1 & \to D_0 \neq D_1\end{matrix}}{\to \neq (A_0, B_0, C_0, D_0, D_1)}$$

Each of the proof-parts is similar to the following for $\to A_0 \neq D_1$

$$\dfrac{\dfrac{\dfrac{A_0 = ([A_0B_0][C_0D_0]) \to A_0 = ([A_0B_0][C_0D_0]) \quad \to ([A_0B_0][C_0D_0])\mathcal{I}[C_0D_0]}{A_0 = ([A_0B_0][C_0D_0]) \to A_0\mathcal{I}[C_0D_0]}\text{(atom)}}{A_0 = ([A_0B_0][C_0D_0]) \to}\text{(Erase)}}{\to A_0 \neq ([A_0B_0][C_0D_0])}(\neg\text{:right})$$

4.4.2 Identity of the Intersection-point

We will proof the fact, that there is only one intersection-point of g and h, i.e, the dual fact of (PG1-ID).

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{P\mathcal{I}g \to P\mathcal{I}g \quad \to (gh)\mathcal{I}g \quad P = (gh) \to P = (gh)}{P\mathcal{I}g \to P = (gh), [P(gh)] = g}\text{(atom)} \quad \dfrac{P\mathcal{I}h \to P\mathcal{I}h \quad \to (gh)\mathcal{I}h \quad P = (gh) \to P = (gh)}{P\mathcal{I}h \to P = (gh), [P(gh)] = h}\text{(atom)}}{P\mathcal{I}g, P\mathcal{I}h \to P = (gh), g = h}\text{(atom)}}{g \neq h, P\mathcal{I}g, P\mathcal{I}h \to P = (gh)}(\neg\text{:left})}{P\mathcal{I}g \wedge P\mathcal{I}h \wedge g \neq h \to P = (gh)}(\wedge\text{:left})}{\to P\mathcal{I}g \wedge P\mathcal{I}h \wedge g \neq h \supset P = (gh)}(\supset\text{:right})}{\to (\forall X)(\forall u)(\forall v)(X\mathcal{I}u \wedge X\mathcal{I}v \wedge u \neq v \supset X = (uv))}(\forall\text{:right})$$

Chapter 5

On the Structure of Proofs in $\mathbf{L_{PG}K}$

In this chapter we will analyze the structure of a proof in the calculus $\mathbf{L_{PG}K}$. After discussing the proofs we will give a cut-elimination theorem for $\mathbf{L_{PG}K}$. Finally we will discuss certain consequences of the cut-elimination theorem, especially the structure of terms and minimal proofs. This will lead us to some interesting results about proofs and sketches in the next chapters.

5.1 The Cut Elimination Theorem for $\mathbf{L_{PG}K}$

We will now study the structure of proofs carried out in the calculus $\mathbf{L_{PG}K}$. Starting with a general proof we will first analyze the underlying combination of geometric and logical structures and bring them into a context with the proof. Then we will discuss the cuts and show that they can be eliminated due to the special structure of the rules of the calculus.

We will refer to the equality rules (cf. p. 19), (PG1-ID) and (Erase) as (atom)-rules, because they only operate on atomic formulas and therefore they can be shifted above any logical rule (see Step 1 below). We will now transform any given proof in $\mathbf{L_{PG}K}$ step by step into another satisfying some special conditions, especially that the new one contains no (Cut).

Definition 5.1 (normalized proof) *A proof $\mathcal{P}$ is in* normalized *if there is no application of a logical rule above any application of a (atom)-rule.*

A normalized proof is split into two parts $\mathcal{P}_1$ and $\mathcal{P}_2$

$$\begin{array}{c} \vdots\, \mathcal{P}_1 \\ \vdots\, \mathcal{P}_2 \\ \Pi \rightarrow \Gamma \end{array}$$

where $\mathcal{P}_1$ is an (atom)-part with (atom)- and structural rules only and $\mathcal{P}_2$ is a logical part with logical and structural rules only.

The semantic content of these parts is easy to understand: In the first part geometry is practiced in the sense that in this part the knowledge about projective planes is used. The second part is a logical part connecting the statements from the geometric part to more complex statements with logical connectives.

LEMMA 5.1 *For every proof of a sequent* $\Gamma \to \Delta$ *there is a proof in normal form for the same sequent.*

PROOF: (atom)-rules only operate on atomic formulas and therefore they cannot interfere with any of the logical rules. So every application of a logical rule above a given (atom)-rule must operate on a formula which cannot be an ancestor of the formula the (atom)-rule operates on. Therefore the (atom)-rule can be shifted above the logical rule. □

We now come to the essential lemma for proving the cut-elimination theorem. We will show that from a proof with only one application of the (Cut)-rule the cut can be eliminated. The cut-elimination theorem then follows with induction on the number of cuts in a proof.

LEMMA 5.2 *For every proof in normal form with only one cut there is a normalized proof of the same endsequent without a cut.*

PROOF: STEP 1: We will start with the cut-elimination procedure as usual in **LK**. We will now give only the idea behind this step, the detailed proof can be found in many textbooks on mathematical logic, e.g. [15]. The proof is a double induction on the grade and the rank of a proof (these are measurements of the complexity of the proof and the formula).

This procedure shifts a cut higher and higher till the cut is at an axiom where it can be eliminated trivially. Since in our case above all the logical rules there is the (atom)-part, the given procedure will only shift the cut in front of this part. We will now give some typical parts when shifting over rules. In this proof not the (Cut)-rule itself is used, but the equivalent (Mix)-rule, which is

$$\frac{\Gamma \to \Delta \quad \Pi \to \Lambda}{\Gamma, \Pi^{\#} \to \Delta^{\#}, \Lambda}\ (\text{Mix})$$

where both Δ and Π contain the formula A, and $\Delta^{\#}$ and $\Pi^{\#}$ are obtained from Δ and Π respectively by deleting all the occurrences of A in them.

If the outermost logical symbol of the mix-formula is $\wedge$ then a proof

$$\frac{\dfrac{\Gamma \to \Delta_1, B \quad \Gamma \to \Delta_1, C}{\Gamma \to \Delta_1, B \wedge C} \qquad \dfrac{B, \Gamma_1 \to \Lambda}{B \wedge C, \Pi_1 \to \Lambda}}{\Gamma, \Pi_1 \to \Delta_1, \Lambda}\ (\text{Mix})$$

where none of the proofs ending with $\Gamma \rightarrow \Delta_1, B$; $\Gamma \rightarrow \Delta_1, C$ or $B, \Pi_1 \rightarrow \Lambda$ contains a mix. Then the mix is reduced in its complexity by:

$$\frac{\Gamma \rightarrow \Delta_1, B \quad B, \Pi_1 \rightarrow \Lambda}{\Gamma, \Pi_1^{\#} \rightarrow \Delta_1^{\#}, \Lambda}$$

where $\Pi_1^{\#}$ and $\Delta_1^{\#}$ are obtained from Π_1 and Δ_1 by omitting all occurrences of B. This proof contains only one mix, furthermore the grade of the mix formula B is less than the grade of $A = B \wedge C$. So by induction hypothesis we can obtain a proof which contains no mixes and whose end-sequent is $\Gamma, \Pi_1^{\#} \rightarrow \Delta_1^{\#}, \Lambda$. From this we can obtain a proof without a mix with end-sequent $\Gamma, \Pi_1 \rightarrow \Delta_1, \Lambda$.

Step 2: Now the cut is already in front of the (atom)-part:

$$\frac{\begin{matrix} \vdots\, \mathcal{P}_1 \\ \Pi_1 \rightarrow \Gamma_1, P(t,u) \end{matrix} \quad \begin{matrix} \vdots\, \mathcal{P}_2 \\ P(t,u), \Pi_2 \rightarrow \Gamma_2 \end{matrix}}{\Pi \rightarrow \Gamma}\ (\mathrm{Cut})$$

- First we shift all the applications of rules in $\mathcal{P}_2$ not necessary, i.e. all applications of rules not operating on the formula $P(t,u)$ or one of his predecessors in the antecedent of $\mathcal{P}_2$, under the cut-rule. I.e., if we have ((atom) in this proof stands for any application of an (atom)-rule)

$$\frac{\begin{matrix} \vdots\, \mathcal{P}_1 \\ \Pi_1 \rightarrow \Gamma_1, P(t,u) \end{matrix} \quad \dfrac{\dfrac{\begin{matrix}\vdots \\ \Delta \rightarrow \Lambda\end{matrix} \quad \begin{matrix}\vdots \\ A', P(t,u), \Pi'' \rightarrow \Gamma''\end{matrix}}{A, P(t,u), \Pi' \rightarrow \Gamma'}\ (\mathrm{atom})}{P(t,u), A, \Pi' \rightarrow \Gamma'}\ (\mathrm{E{:}left})}{A, \Pi \rightarrow \Gamma}\ (\mathrm{Cut})$$

we can shift the cut above the (atom)-rule and get

$$\frac{\begin{matrix}\vdots \\ \Delta \rightarrow \Lambda\end{matrix} \quad \begin{matrix} \dfrac{\begin{matrix} \vdots\, \mathcal{P}_1 \\ \Pi_1 \rightarrow \Gamma_1 \end{matrix} \quad \dfrac{\begin{matrix}\vdots \\ A', P(t,u), \Pi'' \rightarrow \Gamma''\end{matrix}}{P(t,u), A', \Pi'' \rightarrow \Gamma''}\ (\mathrm{E{:}left})}{\Pi_1, A, \Pi'' \rightarrow \Gamma_1, \Gamma''}\ (\mathrm{Cut}) \\ \vdots\ (\mathrm{E{:}left}) \\ A', \Pi_1, \Pi'' \rightarrow \Gamma'' \end{matrix}}{A, \Pi \rightarrow \Gamma}\ (\mathrm{atom})$$

By iterating this procedure we finally get something like that for $\mathcal{P}_2$:

$$\begin{matrix} \dfrac{\begin{matrix}\vdots \\ \Delta' \rightarrow \Lambda', u_1 = u_2\end{matrix} \quad \dfrac{\Delta \rightarrow \Lambda, t_1 = t_2 \quad \begin{matrix}\vdots \\ P(t_1,u_1) \rightarrow P(t_1,u_1)\end{matrix}}{P(t_2,u_1), \Pi' \rightarrow \Gamma', P(t_1,u_1)}}{P(t_2,u_2), \Pi'' \rightarrow \Gamma'', P(t_1,u_1)} \\ \vdots \\ P(t,u), \Pi_2 \rightarrow \Gamma_2 \end{matrix}$$

(Note that the $P(t,u)$ need not to be present in the succedent when the axiom is a mathematical one, e.g $A_0 = B_0$.) In other words, $\mathcal{P}_2$ is a chain of applications of (atom)-rules on the predecessor of the cut-formula.

- Now we can apply the dual rules[1] in inverse order on the formula $P(t,u)$ in the endsequent of $\mathcal{P}_1$ and we get one of the following proofs, depending on whether the axiom in $\mathcal{P}_2$ is a logical or a mathematical one.

  Case 1. The axiom is a logical one. So the proof looks like this

$$\dfrac{\overset{\vdots\ \mathcal{P}'}{\Pi \to \Gamma, P(t,u)} \quad P(t,u) \to P(t,u)}{\Pi \to \Gamma, P(t,u)}\ \text{(Cut)}$$

  This case can easily be handled since the cut is unnecessary and this part of the proof can be substituted by $\mathcal{P}'$ only.

  Case 2. The axiom is a mathematical one. This is only possible if $P(t,u)$ is an instance of $x = y \to$ with x and y pairwise distinct in $\{A_0, B_0, C_0, D_0\}$. Let's assume it's $A_0 = B_0 \to$. The proof now looks like this:

$$\dfrac{\overset{\vdots\ \mathcal{P}_1}{\Pi \to \Gamma, A_0 = B_0} \quad A_0 = B_0 \to}{\Pi \to \Gamma}\ \text{(Cut)}$$

  We now turn our analysis to the $\mathcal{P}_1$ part of this proof: How can the formula $A_0 = B_0$ in the succedent of the end-sequent of $\mathcal{P}_1$ emerge from the axioms? First note that a formula of the form $X = Y$ with X and Y Points can only originate from a logical axiom $t = u \to t = u$ or $\to x = x$ via a set of equality-rules operating on the right side, i.e. the set {(symm:right), (trans:right), (id-$\mathcal{I}_{\tau_\mathcal{P}}$:right), (id-$\mathcal{I}_{\tau_\mathcal{L}}$:right), (id-con:1), (id-con:2), (id-int:1), (id-int:2) } (without (PG1-ID), because this rule generates a formula $x = y$ where x and y are Lines) or from a weakening at the right side (W:right). We will only discuss the first case and the third one in detail, since the second one is analog to the first one. Assume the proof looks like this:

$$\dfrac{\dfrac{\overset{\vdots}{\Delta \to \Lambda, u = u'} \quad \dfrac{\overset{\vdots}{\Pi' \to \Gamma', t = t'} \quad t = u \to t = u}{t = u, \Pi' \to \Gamma', t' = u}}{\overset{\displaystyle t = u, \Pi'' \to \Gamma'', t' = u'}{\vdots}} \qquad}{}$$

$$\dfrac{t = u, \Pi \to \Gamma, A_0 = B_0 \qquad A_0 = B_0 \to}{t = u, \Pi \to \Gamma}\ \text{(Cut)}$$

[1] E.g. (trans:left) and (trans:right) are dual rules

If we now apply these equality-rules dually in reverse order on the mathematical axiom $A_0 = B_0 \rightarrow$, then the proof is transformed into a new one where the cut-rule is eliminated:

$$\dfrac{\begin{matrix}\vdots \\ \Delta \rightarrow \Lambda, u' = u\end{matrix} \qquad \dfrac{\begin{matrix} & A_0 = B_0 \rightarrow \\ \vdots & \vdots \\ \Pi' \rightarrow \Gamma', t = t' & t' = u', \Pi'' \rightarrow \Gamma''\end{matrix}}{t = u', \Pi' \rightarrow \Gamma'}}{t = u, \Pi \rightarrow \Gamma}$$

The procedure is the same if the axiom we are starting from is not $t = u \rightarrow t = u$ but $\rightarrow x = x$.

For the case of (W:right) we loose this application, loose all the (atom)-rules operating on the successors of the weakening formula and get the same endsequent of this part of the proof by some (W:left) to get the formulas which come into the antecedent via the now lost (atom)-rules.

That completes the proof of the lemma. □

Example: A trivial example should explain this method: The proof

$$\dfrac{\dfrac{x_2 = x_3 \rightarrow x_2 = x_3 \qquad \dfrac{x_1 = x_2 \rightarrow x_1 = x_2 \quad x_1 = u \rightarrow x_1 = u}{x_1 = x_2, x_1 = u \rightarrow x_2 = u}}{x_2 = x_3, x_1 = x_2, x_1 = u \rightarrow x_3 = u} \qquad x_3 = u \rightarrow}{x_2 = x_3, x_1 = x_2, x_1 = u \rightarrow} \text{(Cut)}$$

will be transformed to

$$\dfrac{x_1 = x_2 \rightarrow x_1 = x_2 \qquad \dfrac{x_2 = x_3 \rightarrow x_2 = x_3 \quad x_3 = u \rightarrow}{x_2 = x_3, x_2 = u \rightarrow}}{x_1 = x_2, x_2 = x_3, x_1 = u \rightarrow}$$

♡

As the final consequence from this part we state the cut-elimination theorem for $\mathbf{L_{PG}K}$:

Theorem 5.1 (Cut Elimination for $\mathbf{L_{PG}K}$) *If there is a proof of an end-sequent $\Pi \rightarrow \Gamma$ in $\mathbf{L_{PG}K}$, then there is also a proof without a cut.*

Proof: By the fact that everything above a given sequent is a proof of this sequent and by using Lemma 5.2 and induction on the number of cuts in a proof we could eliminate one cut after another and end up with a cut-free proof. □

The existence of this theorem primary depends on the existence of equality-rules like

$$\dfrac{\rightarrow x = y \quad P(x, w) \rightarrow}{P(y, w) \rightarrow}$$

and on the (Erase)-rules like

$$\frac{\Pi \to \Gamma, A_0\mathcal{I}[B_0C_0]}{\Pi \to \Gamma}\ \text{(Erase)}$$

For the first rules this is reasonable from the transformation of proofs given above. For the latter, the (Erase)-rules, this was an interesting discovery: In almost all of the many developed calculi there were no (Erase)-rules, but a set of left-axioms (e.g $A_0\mathcal{I}[B_0C_0] \to$). We first expected that all the left-axioms, i.e. all axioms concerning the four constant Points with the properties given in (PG3) would cause problems in the cut elimination process.

Further investigations showed, that axioms like $A_0 = B_0 \to$ cause no problems, but the axioms $A_0\mathcal{I}[B_0C_0] \to$ in conjunction with the positive mathematical axioms $\to X\mathcal{I}[XY]$. It can be proved, that if we take the calculus with the mathematical left-axioms $A_0\mathcal{I}[B_0C_0]$ and no (Erase)-rules, not all cuts can be eliminated, but cuts from such left-axioms with descendents of mathematical right-axioms (via a chain of equality-rules, see the description above) remain.

Example: We will now present an example proof and the corresponding proof without a cut. We want to prove that for every line there is a point not on that line, in formula: $(\forall g)(\exists X)(X\not\mathcal{I}g)$.

Before we give the proof in $\mathbf{L_{PG}K}$, a few words about the way something is really proved in any sequential calculus: When you want to prove a fact, it is good to start from the bottom, the root of the prooftree and work up the tree to the axioms, the leafs. This is a procedure which is a bit more according to the human reasoning and normal proving. This we will keep in mind when proving the mentioned fact.

We will first give the proof in words and then in $\mathbf{L_{PG}K}$.

Proof: (Words) When $A_0\not\mathcal{I}g$ then take A_0 for X. Otherwise $A_0\mathcal{I}g$. Next if $B_0\not\mathcal{I}g$ take B_0 for X. If also $B_0\mathcal{I}g$ then take C_0, since when A_0 and B_0 lie on g, then $g = [A_0B_0]$ and $C_0\not\mathcal{I}[A_0B_0] = g$ by (PG3). □

Proof: ($\mathbf{L_{PG}K}$) Now to the proof in $\mathbf{L_{PG}K}$ (Don't forget to read the proof the first time from bottom up!):

$$\dfrac{\dfrac{\dfrac{\dfrac{A_0\mathcal{I}g \to A_0\mathcal{I}g}{\to A_0\mathcal{I}g, A_0\not\mathcal{I}g}}{\to A_0\mathcal{I}g \vee A_0\not\mathcal{I}g} \qquad \dfrac{\dfrac{\dfrac{A_0\mathcal{I}g \to A_0\mathcal{I}g}{A_0\not\mathcal{I}g \to A_0\not\mathcal{I}g}}{A_0\not\mathcal{I}g \to (\exists X)(X\not\mathcal{I}g)} \qquad \dfrac{\dfrac{\dfrac{B_0\mathcal{I}g \to B_0\mathcal{I}g}{\to B_0\mathcal{I}g, B_0\not\mathcal{I}g}}{\to B_0\mathcal{I}g \vee B_0\not\mathcal{I}g} \qquad \dfrac{\dfrac{\dfrac{B_0\mathcal{I}g \to B_0\mathcal{I}g}{B_0\not\mathcal{I}g \to B_0\not\mathcal{I}g}}{B_0\not\mathcal{I}g \to (\exists X)(X\not\mathcal{I}g)} \qquad \begin{matrix}\vdots\ \Pi_1 \\ A_0\mathcal{I}g, B_0\mathcal{I}g \to (\exists X)(X\not\mathcal{I}g)\end{matrix}}{B_0\mathcal{I}g \vee B_0\not\mathcal{I}g, A_0\mathcal{I}g \to (\exists X)(X\not\mathcal{I}g)}}{A_0\mathcal{I}g \to (\exists X)(X\not\mathcal{I}g)}\ \text{(Cut)}}{A_0\mathcal{I}g \vee A_0\not\mathcal{I}g \to (\exists X)(X\not\mathcal{I}g)}}{\to (\exists X)(X\not\mathcal{I}g)}\ \text{(Cut)}}{\to (\forall g)(\exists X)(X\not\mathcal{I}g)}$$

Π_1 :

$$\dfrac{\dfrac{A_0\mathcal{I}g \to A_0\mathcal{I}g \quad B_0\mathcal{I}g \to B_0\mathcal{I}g \quad A_0 = B_0 \to}{A_0\mathcal{I}g, B_0\mathcal{I}g \to g = [A_0B_0]} \quad \dfrac{C_0\mathcal{I}[A_0B_0] \to C_0\mathcal{I}[A_0B_0]}{C_0\mathcal{I}[A_0B_0] \to}\,\text{(Erase)}}{\dfrac{A_0\mathcal{I}g, B_0\mathcal{I}g, C_0\mathcal{I}g \to}{A_0\mathcal{I}g, B_0\mathcal{I}g \to (\exists X)(X\not{\mathcal{I}}g)}}$$

□

The cut-elimination procedure[2] yields a cut-free proof of the same end-sequent:

$$\dfrac{\dfrac{A_0\mathcal{I}g \to B_0\mathcal{I}g \quad B_0\mathcal{I}g \to B_0\mathcal{I}g \quad A_0 = B_0 \to}{A_0\mathcal{I}g, B_0\mathcal{I}g \to g = [A_0B_0]} \quad \dfrac{C_0\mathcal{I}[A_0B_0] \to C_0\mathcal{I}[A_0B_0]}{C_0\mathcal{I}[A_0B_0] \to}\,\text{(Erase)}}{\dfrac{A_0\mathcal{I}g, B_0\mathcal{I}g, C_0\mathcal{I}g \to}{\dfrac{\to A_0\not{\mathcal{I}}g, B_0\not{\mathcal{I}}g, C_0\not{\mathcal{I}}g}{\dfrac{\to (\exists X)(X\not{\mathcal{I}}g), (\exists X)(X\not{\mathcal{I}}g), (\exists X)(X\not{\mathcal{I}}g)}{\dfrac{\to (\exists X)(X\not{\mathcal{I}}g)}{\to (\forall g)(\exists X)(X\not{\mathcal{I}}g)}}}}}$$

♡

5.2 Some Consequences of the Cut Elimination Theorem for $\mathbf{L_{PG}K}$

5.2.1 The Mid Sequent Theorem for $\mathbf{L_{PG}K}$

Corollary 5.1 (Midsequent Theorem for $\mathbf{L_{PG}K}$)
Let S be a sequent which consists of prenex formulas only and is provable in $\mathbf{L_{PG}K}$. *Then there is a cut-free proof of S which contains a sequent (called a midsequent), say S', which satisfies the following:*

1. *S' is quantifier-free.*

2. *Every inference above S' is either structural, propositional, mathematical or equality inference.*

3. *Every inference below S' is either structural or a quantifier inference.*

Thus a midsequent splits the proof into an upper part, which contains the propositional inferences, and a lower part, which contains the quantifier inferences.

[2]or a close look

PROOF: (Outline) Because of the cut-elimination theorem we may assume that there is a cut-free normalized proof of S, say P. All the initial sequents in P consist of atomic formulas (this is due to the special formalization of $\mathbf{L_{PG}K}$, but it can be achieved for every **LK**-calculus). Let I be a quantifier inference in P. The number of propositional inferences under I is called the order of I. The sum of the orders for all the quantifier inferences in P is called the order of P. The proof is carried out by induction on the order of P.

Case 1: The order of P is 0. If there is a propositional inference, take the lowermost such, and call its lower sequent S_0. Above this sequent there is no quantifier inference. Therefore, if there is a quantifier in or above S_0, then it is introduced by weakenings. Since the proof is cut-free, the weakening formula is a subformula of one of the formulas in the endsequent. Hence no propositional inferences apply to it. We can thus eliminate these weakenings and obtain a sequent S_0' corresponding to S_0. By adding some weakenings under S_0' (if necessary), we derive S, and S_0' serves as mid-sequent.

If there is no propositional inference in P, then take the uppermost quantifier inference. Its upper sequent serves as a midsequent.

Case 2: The order of P is not 0. Then there is at least one propositional inference which is below a quantifier inference. Moreover, there is a quantifier inference I with the following property: the uppermost logical inference under I is a propositional inference. Call it I'. We can lower the order by interchanging the positions of I and I'. Here we present just one example: say I is ($\forall$:right).

P:

$$\cfrac{\cfrac{\Gamma \to \Theta, F(a)}{\Gamma \to \Theta, (\forall x)F(x)}\ I}{\vdots\ (*) \\ \overline{\Delta \to \Lambda}\ I'}$$

where the (*)-part of P contains only structural inferences and Λ contains $(\forall x)F(x)$ as a sequent-formula. Transform P into the following proof P':

$$\begin{array}{c} \Gamma \to \Theta, F(a) \\ \hline \text{structural inferences} \\ \hline \Gamma \to F(a), \Theta, (\forall x)F(x) \\ \vdots \\ I' \\ \hline \Delta \to \Lambda, (\forall x)F(x) \quad I \\ \hline \Gamma \to \Delta \\ \vdots \end{array}$$

It is obvious that the order of P' is less than the order of P. □

Combining the description of proofs in 5.1 above and this corollary we get the following form of proofs in $\mathbf{L_{PG}K}$:

$$\begin{array}{c} \vdots\ \mathcal{P}_1 \\ \vdots\ \mathcal{P}_2 \\ \vdots\ \mathcal{P}_3 \\ \Pi \rightarrow \Gamma \end{array}$$

The first part $\mathcal{P}_1$ is the geometric part (see above), the second one $\mathcal{P}_2$ is the propositional part and the third one $\mathcal{P}_3$ is the quantifier part. In the example given at the end of the last section (c.f. p. 27) these three parts are easy to recognize: The first two inferences represent the geometry, the next one (actually the next three) the propositional part and the last the quantifier part.

As a corollary from this theorem the classical theorem of Herbrand can be derived. This theorem states that for any formula A there is a disjunction of instances of A which is equivalent to A. In other words, the right instances for the bound variables can be found in the Herbrand universe of this formula. This formula actually is the midsequent.

5.2.2 The Structure of Terms and minimal Proofs

There are two basic ways of measuring the complexity (or length) of proofs:

(1) to count the number of proof lines,

(2) to count the total size of the proof (i.e to count each symbol). Trivially the size is an upper bound to the number of proof lines. It is much more difficult to bound the size using the number of proof lines. Since in $\mathbf{L_{PG}K}$ function symbols are allowed, formulas in the proof may contain large terms and it is difficult to find some bounds to the size of these terms using only the information about the number of proof lines.

In general proofs with few proof lines may contain large terms. In this section we shall show that in cut-free proofs, which can be found for every proof in $\mathbf{L_{PG}K}$ due to theorem 5.1, one can replace large terms by terms whose size is bounded where the bound depends only on the number of proof lines and the size of the sequent that we want to prove.

We recall that a proof is a rooted tree with the nodes labeled with sequents and the vertices labeled with the rules and that terms only contain free variables.

Definition 5.2 *A* semiterm *is a term that is allowed to contain bound variables.*

The size *of a formula or a semiterm is the number of symbols in it. The size of a sequent is the sum of the sizes of formulas in the sequent. The size of a proof is the sum of the sizes of the sequents in the proof. The* number of proof lines *of a proof is the number of vertices of the tree. The size of a semiterm or formula or sequent or proof* X *will be denoted by* $|X|$*.*

Definition 5.3 (Proof Skeleton) *A* proof skeleton *is a rooted tree whose vertices are labeled by the inference rules of* $\mathbf{L_{PG}K}$*. Further, it is marked on the tree which son of a given vertex is the left one, (which one is the middle one,) which one is the right one. For the exchange rules (∃:left) and (∃:right) the label contains also the number of the pair to which it should be applied. For the (Erase)-rule the label contains the formula which is erased.*

The information which the skeleton does not contain are the terms and variables used in quantifier and equality rules. Every proof determines uniquely its skeleton. A *cut-free skeleton* is a skeleton in which no vertex is labeled by the cut rule.

Definition 5.4 (Preproof for $\mathbf{L_{PG}K}$) *A* preproof *for* $\mathbf{L_{PG}K}$ *is a structure which has all the properties of a proof except for the logical initial sequents which are only required to be of one of the following forms:*

$$B(s_1, \ldots, s_n) \to B(t_1, \ldots, t_n) \qquad (*)$$

where $s_1, \ldots, s_n, t_1, \ldots, t_n$ *are terms.*

To construct a preproof from a given proof skeleton proceed as follows:

(1) assign $\Gamma \to \Delta$ on the root of S,

(2) if a sequent has been assigned to a vertex v of S and v is not a leave, assign sequents to its sons according to the rule assigned to v. In some cases certain actions have to be done:

In case of structural and propositional rules these sequents are uniquely determined.

In case of the quantifier rules choose always a new free variable and substitute it for the bounded variable

In case of the equality rules (trans:left), (trans:right), (id-$\mathcal{I}_{\tau_\mathcal{P}}$:left), (id-$\mathcal{I}_{\tau_\mathcal{P}}$:right), (id-$\mathcal{I}_{\tau_\mathcal{L}}$:left), (id-$\mathcal{I}_{\tau_\mathcal{L}}$:right) introduce a new free variable and substitute it for the "lost term" in application of this rule.

In case of (id-con:1), (id-con:2), (id-int:1), (id-int:2) this part of the partly filled proof skeleton looks for (id-con:1) like (the other 3 cases are similar)

$$\frac{}{\Gamma \to \Delta, t = u} \text{(id-con:1)}$$

If t is not already $[nm]$ for some terms n, m, then substitute in the whole proof $[xy]$ for t, where x, y are new free variables. The same happens for u. So we have

$$\frac{}{\Gamma \to \Delta, [xy] = [zw]} \text{(id-con:1)}$$

and can fill up the skeleton to

$$\frac{\Gamma \to \Delta, x = z}{\Gamma \to \Delta, [xy] = [zw]} \text{(id-con:1)}$$

This happens at each occurrence of one of the above mentioned rules.

In case of (PG1-ID) it is similar to the last one, but only the left term of the equality has to be substituted in certain circumstances.

It is clear that if there is a proof of $\Gamma \rightarrow \Delta$ with skeleton S, the procedure above constructs a preproof P_0 such that each regular proof P of $\Gamma \rightarrow \Delta$ with skeleton S can be obtained from P_0 by substituting suitable terms for the free variables introduced at the vertices labeled by ($\forall$:left) and ($\exists$:right) and by renaming the free variables. This method is due to Matthias Baaz and the estimation and formalization can be found in [8].

The preunification problem U is constructed from a preproof P_0 as follows:

(1) We treat bounded variables, eigenvariables and free variables of $\Gamma \rightarrow \Delta$ and $A_0, \ldots, D_0$ as constants i.e. they cannot be substituted for;

(2) $(t, s) \in U$ iff $t = t_i$, $s = s_i$, $i \leq n$, for some logical initial sequent of P_0 of the form $(*)$ above;

(3) for every free variable A introduced at some ($\forall$:left) or ($\exists$:right) vertex require that any term $\sigma(a)$ substituted for a must not contain a bound variable, an eigenvariable of the proof of a free variable of $\Gamma \rightarrow \Delta$

The final set unification problem consists of unification problems, which are obtained from the preunification problem by adding for each initial sequent in P_0 of the form $t = u \rightarrow$ two pairs, one of the $(t, x), x \in \{A_0, B_0, C_0, D_0\}$ and one of the $(u, y), y \in \{A_0, B_0, C_0, D_0\}$, in any combination. Since there is only a finite number of initial sequents of the above form, there is only a finite number of unification problems.

A solution for the set of unification problems is a mapping $\sigma : A \rightarrow T$, where A is the set of free variables introduced at ($\forall$:left) and ($\exists$:right) vertices, and T the set of all terms, which is a solution for one of the unification problems in the set.

Because of (1), the restrictions in (3) are of a special type and under this circumstances the following claim can be proved:

Claim: For every $\sigma : A \rightarrow T$, σ is a solution for the set of unification problems with the restrictions iff σ produces a regular proof from P_0. $\square$

Since there is a solution to this problem there is a most general unifier which minimizes the term depth in P. For such a minimal proof the depth of the terms can be bound.

Chapter 6

The Sketch in Projective Geometry

Most of the proofs in projective geometry are illustrated by a sketch. But this method of a graphical representation of the maybe abstract facts is not only used in areas like projective geometry, but also in other fields like algebra, analysis and I have even seen sketches to support understanding in a lecture about large ordinals, which is highly abstract!

The difference between these sketches and the sketches used in projective geometry (and similar fields) is the fact, that the proofs in projective geometry deal with geometric objects like Points and Lines, which are indeed objects we can imagine and draw on a piece of paper (which is not necessary true for large ordinals).

So the sketch in projective geometry has a more concrete task than only illustrating the facts, since it exhibits the incidences, which is the only predicate constant besides equality really needed in the formulization of projective geometry. It is a sort of proof by itself and so potentially interesting for a proof-theoretic analysis.

As a first example I want to demonstrate a proof of projective geometry, which is supported by a sketch. It deals with a special sort of mappings, the so called "collineation". This is a bijective mapping from the set of Points to the set of Points, which preserves collinearity. In a formula:

$$\mathrm{coll}(R, S, T) \supset \mathrm{coll}(R\kappa, S\kappa, T\kappa)$$

(Don't forget, in projective geometry functions are written behind the variables, see chap. 2) The fact we want to proof is

$$\neg\mathrm{coll}(R, S, T) \supset \neg\mathrm{coll}(R\kappa, S\kappa, T\kappa)$$

That means, that not only collinearity but non-collinearity is preserved under a collineation.

The proof is relatively easy and is depicted in fig. 6.1: If $R\kappa$, $S\kappa$ and $T\kappa$ are collinear, then there exists a Point X' not incident with the Line defined by $R\kappa$, $S\kappa$, $T\kappa$. There exists a Point X, such that $X\kappa = X'$. This Point X doesn't lie on any of the Lines defined by R, S, T. Let $Q = ([RT][XS])$ then $Q\kappa\mathcal{I}[R\kappa S\kappa]$ and $Q\kappa\mathcal{I}[S\kappa X\kappa]$, that is $Q\kappa\mathcal{I}[S\kappa X']$ (since collinearity is preserved). So $Q\kappa = S\kappa$ (since $Q\kappa = ([R\kappa S\kappa][S\kappa X']) = S\kappa$), which is together with $Q \neq S$ a contradiction to the injectivity of κ.

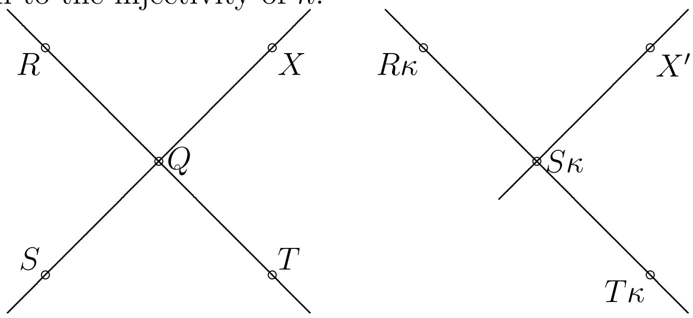

Figure 6.1: Sketch of the proof $\neg\text{coll}(R, S, T) \supset \neg\text{coll}(R\kappa, S\kappa, T\kappa)$

This sketch helps you to understand the relation of the geometric objects and you can follow the single steps of the verbal proof.

If we are interested in the concept of the sketch in mathematics in general and in projective geometry in special then we must set up a formal description of what we mean by a sketch. This is necessary if we want to be more concrete on facts on sketches. So we come to ...

6.1 A Formalization of Sketches in Projective Geometry

In this part we want to give a formalization of the sketch in projective geometry and want to explain our motivation behind some of these concepts.

All Points and Lines are combined in the sets called $\tau_{\mathcal{P}}$ and $\tau_{\mathcal{L}}$, respectively. So if we say, that $x \in \tau_{\mathcal{P}}$, than we mean that x is from type Point, means it's any term which describes a Point.

Sketches speak about geometric objects, that are Points and Lines. So the first logical objects necessary for the formalization are constants or variables for Points and Lines. From these constants we could build more and more complex objects by connecting and intersection. This step is described in

Definition 6.1 (Set of Terms over $\mathcal{C}$) *Let $\mathcal{C}$ be a set of constants of type $\tau_{\mathcal{P}}$ or $\tau_{\mathcal{L}}$, than $\mathcal{T}_n$ is inductively defined*

- $\mathcal{T}_0(\mathcal{C}) = \mathcal{C}$
- $\mathcal{T}_{n+1}(\mathcal{C}) = \mathcal{T}_n(\mathcal{C}) \cup \{[tu] : t, u \in \mathcal{T}_n(\mathcal{C}); t, u \in \tau_{\mathcal{P}}\}$

$$\cup\{(tu) : t, u \in \mathcal{T}_n(\mathcal{C}); t, u \in \tau_{\mathcal{L}}\}$$

DEFINITION 6.2 (DEPTH) *The* depth *of a term t is defined as the number n, at which t is added (or constructed) in the process given above.*

The expression "depth" describes nothing else than it says, namely how deep a term is nested.

To ensure consistency inside a set of starting objects, they must obey one rule, namely that if a compound term is in the set, than also the subterms are. That's the reason for the next definition.

DEFINITION 6.3 (ADMISSIBLE SET OF TERMS) *Let $\mathcal{M}$ be a subset of $\mathcal{T}(\mathcal{C})$, $\mathcal{C}$ a set of constants, then $\mathcal{M}$ is called admissible if it obeys the following rules:*

- $(\forall[XY] \in \mathcal{M})(X, Y \in \mathcal{M})$
- $(\forall(gh) \in \mathcal{M})(g, h \in \mathcal{M})$

The idea is to define a set of Points, Lines and certain combinations of them (the intersection points and connection lines) and let the sketch be a subset of all possible atomic formulas over these terms.

DEFINITION 6.4 (UNIVERSE OF FORMULAS) *Let $\mathcal{M}$ be an admissible termset and $\mathcal{P}$ a set of predicates, then the* universe of formulas *over $\mathcal{M}$ with regard to $\mathcal{P}$ is defined as*

$$\mathcal{FU}_{\mathcal{P}}(\mathcal{M}) = \{P(t_1, t_2) : P \in \mathcal{P}; t_i \textit{ of the right types}\}$$

$\mathcal{P}$ will only be $\{\mathcal{I}, =\}$ or $\{\mathcal{I}\}$. The set $\mathcal{FU}$ contains all the possible positive statements which can be made over the termset $\mathcal{M}$.

If we bear in mind that we want to do something proof-theoretic with the formalization of the sketch, we must ensure that nothing evil happens when a simple procedure without any knowledge about geometry is working with it. And one of the evils that could happen is a

DEFINITION 6.5 (CRITICAL CONSTELLATION) *Let P and Q be terms in $\tau_{\mathcal{P}}$ and g and h terms in $\tau_{\mathcal{L}}$. Than we call the appearance of the following four formulas a* critical constellation*:*

$$\begin{array}{c|c} P\mathcal{I}g & P\mathcal{I}h \\ \hline Q\mathcal{I}g & Q\mathcal{I}h \end{array}$$

We will denote such critical constellations by $(P, Q; g, h)$.

Such a constellation is called critical, because from these four formulas it follows that either $P = Q$ or $g = h$ (or both), but we cannot determine which one without supplementary information (see fig. 6.2).

When constructing any sketch we start from some assumptions over a set of constants and then construct new objects and deduce new relations. From

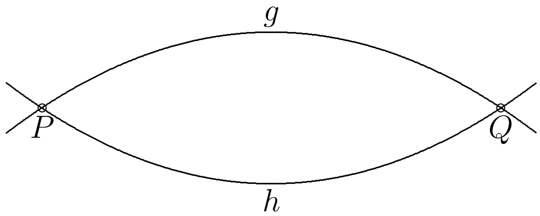

Figure 6.2: The two solutions for a critical constellation

a proof-theoretic point of view these first assumptions are the left side of the deduced sequent, i.e. the assumptions from which you deduce the fact. In the proof given at the beginning of this section the assumptions are that R, S, T are not collinear and that $R\kappa, S\kappa, T\kappa$ are collinear. Then we tried to deduce a contradiction to show, that one of the assumptions is wrong, i.e. that from $\neg\text{coll}(R, S, T)$ $\neg\text{coll}(R\kappa, S\kappa, T\kappa)$ can be deduced.

We now come to the final definition of the sketch. We want that a sketch is a set describing all the incidences in the sketch[1]. But we want also that this subset is closed under trivial incidences, which means that if we talk about a Line which is the connection of Points, then we want that the trivial formulas expressing that these two Points lie on the correspondending Line.

Further we don't want to have a critical constellation in a sketch. That arises from the fact that we want that every geometric object is described only by one logical object, i.e. one term. Since a critical constellation implies the equality of two logical objects, which we cannot determine automatically, we want to exclude such cases.

Definition 6.6 (Sketch) *Let $\mathcal{M}$ be a admissible termset over a set of constants $\mathcal{C}$, $\{A_0, B_0, C_0, D_0, [A_0B_0], \ldots, [C_0D_0]\} \subset \mathcal{M}$,*
let $\mathcal{E}_+$ be a subset of $\mathcal{FU}_{\{\mathcal{I}\}}(\mathcal{M})$
and $\mathcal{E}_-$ a subset of $\overline{\mathcal{FU}_{\{\mathcal{I},=\}}(\mathcal{M})}$ with $A_0 \neq B_0$, $\ldots$, $C_0 \neq D_0$, $A_0 \not\mathcal{I} [B_0C_0]$, $\ldots$, $D_0 \not\mathcal{I} [A_0B_0] \in \mathcal{E}_-$,
let Q be a set of equalities and let the quadruple $(\mathcal{M}, \mathcal{E}_+, \mathcal{E}_-, Q)$ obey the following requirements:

$$(\forall X, Y \in \mathcal{M}, \tau_{\mathcal{P}})([XY] \in \mathcal{M} \supset (X\mathcal{I}[XY]) \in \mathcal{E}_+ \wedge (Y\mathcal{I}[XY]) \in \mathcal{E}_+)$$

$$(\forall g, h \in \mathcal{M}, \tau_{\mathcal{L}})((gh) \in \mathcal{M} \supset ((gh)\mathcal{I}g) \in \mathcal{E}_+ \wedge ((gh)\mathcal{I}h) \in \mathcal{E}_+) \quad \text{(S.1)}$$

$$(\neg\exists x, y \in \mathcal{M})(P(x, y) \in \mathcal{E}_+ \wedge \neg P(x, y) \in \mathcal{E}_-)$$

$$(\neg\exists x \in \mathcal{M})((x \neq x) \in \mathcal{E}_-) \quad \text{(S.2)}$$

there are no critical constellations in $\mathcal{E}_+$ (S.3)

$$(\forall x \in \mathcal{M})((x = x) \in Q) \quad \text{(S.4)}$$

Then we call the quadruple $\mathcal{S} = (\mathcal{M}, \mathcal{E}_+, \mathcal{E}_-, Q)$ a sketch.

[1]This one is on the paper!

We will call the violation of S.2 also a direct contradiction.

A small example should help to understand the concepts:

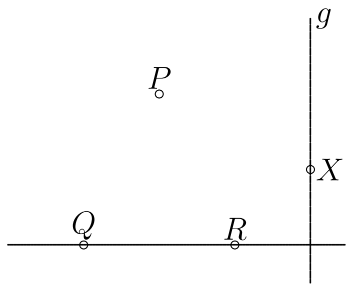

Figure 6.3: A sample sketch

In the sketch depicted in fig. 6.3 the different sets are (where the incidences of the constants are lost!):

$$\begin{aligned}
&\mathcal{C} = \{P, Q, R, X, g\} \\
&\mathcal{M} = \{P, Q, R, X, g, [RQ]\} \\
&\mathcal{FU}_{\{\mathcal{I},=\}} = \{P\mathcal{I}g, Q\mathcal{I}g, R\mathcal{I}g, X\mathcal{I}g \\
&\qquad P\mathcal{I}[RQ], Q\mathcal{I}[RQ], R\mathcal{I}[RQ], X\mathcal{I}[RQ] \\
&\qquad P = Q, P = R, P = X, Q = R, Q = X, R = X, g = [RQ]\} \\
&\mathcal{E}_+ = \{Q\mathcal{I}[RQ], R\mathcal{I}[RQ], X\mathcal{I}g\} \\
&\mathcal{E}_- = \{P\not{\mathcal{I}}g, Q\not{\mathcal{I}}g, R\not{\mathcal{I}}g, P\not{\mathcal{I}}[QR], X\not{\mathcal{I}}[QR]\}
\end{aligned}$$

A few words to the habit of writing: If we are writing expressions like $P \in \mathcal{S}, (P\mathcal{I}g) \in \mathcal{S}, (P\not{\mathcal{I}}h) \in \mathcal{S} \ldots$, then $P \in \mathcal{M}, (P\mathcal{I}g) \in \mathcal{E}_+, (P\not{\mathcal{I}}h) \in \mathcal{E}_-$, respectively is meant. Any other similar expression has to be interpreted accordingly.

Why should the set $\mathcal{E}_+$ only be a subset of $\mathcal{FU}_{\{\mathcal{I}\}}(\mathcal{M})$ and not of $\mathcal{FU}_{\{\mathcal{I},=\}}(\mathcal{M})$? The reason is, that in a sketch every geometric object should have one and only one name and should also be described by one logical object. The same idea lies behind the introduction of the concept of the critical constellation.

Note that one sketch is only one stage in the process of a construction, which starting from some initial assumptions forming a sketch deduces more and more facts and so constructs more and more complex sketches.

The set Q in the definition of the sketch initially was absent, but investigations in the equality of proofs and constructions showed, that this set is important for the proof, although it is not used in the sketch. This depends on the usage of the equality: in the sketch it is a strict one, i.e., there is only one name for an object allowed, while in a proof you can use one time one name, the other another name. In the sketch, as we will later see, there is not a local substitution of a term, but a global, therefore only one name is "actual" at a time for an object. But if we want to translate a proof into a construction, which is one of the aims of this work, we need informations on all the name-changes that are possible.

6.2 Actions on Sketches

Till now a sketch is only a static concept, nothing could happen, you cannot "construct". So we want to give some actions on a sketch, which construct a new sketch with more information. This new sketch must not obey the requirements S.1–S.3, but it will be a ...

DEFINITION 6.7 (SEMISKETCH) *A* semisketch *is a sketch that need not obey to S.2 and S.3.*

These actions should correspond to similar actions in the real constructing. After these actions are defined we can explain what we mean by a construction in this calculus for construction.

The actions primarily operate on the set $\mathcal{E}_+$, since the positive facts are those which are really constructed in a sketch. But on the other hand there are some actions to add negative facts to a sketch. This is necessary for formalizing the elementary way of proving a theorem by an indirect approach.

The following list defines the allowed actions and what controls has to be executed. The following list describes the changes that have to be done on the quadruple of a sketch when we want to carry out the corresponding action.

In the following listing we will use the function closure(Q) on a set of equalities Q. This function deduces all equalities which are consequences of the set Q. This is a relatively easy computation. If we have $Q = \{x = x, y = y, z = z, x = y, y = z\}$, then the procedure returns $Q \cup \{x = z\}$. This function is used to update the set Q of a sketch after a substitution.

Connection of two Points X, Y; Symbol: $[XY]$

- $\mathcal{M}' = \mathcal{M} + [XY]$
- $\mathcal{E}'_+ = \mathcal{E}_+ + \{X\mathcal{I}[XY], Y\mathcal{I}[XY]\}$
- $\mathcal{E}'_- = \mathcal{E}_-$
- $Q' = Q + ([XY] = [XY])$

The requirement (S.1) and (S.4) is fulfilled since the necessary formulas are added to $\mathcal{E}_+$ and Q. This action can produce a semisketch from a sketch.

Intersection of two Lines g, h; Symbol (gh)
Dual to the connection of two points.

Assuming a new Object C in general position, Symbol $\{C\}$

- $\mathcal{M}' = \mathcal{M} + C$
- $\mathcal{E}'_+ = \mathcal{E}_+$
- $\mathcal{E}'_- = \mathcal{E}_-$

- $Q' = Q + (C = C)$

That $\mathcal{S}'$ is a sketch is trivial, since C is a completely new constant. C must be a constant of type $\tau_{\mathcal{P}}$ or $\tau_{\mathcal{L}}$.

Giving the Line $[XY]$ a name $g := [XY]$; Symbol $g := [XY]$

- $\mathcal{M}' = \mathcal{M}[[XY]/g]$
- $\mathcal{E}'_+ = \mathcal{E}_+[[XY]/g]$
- $\mathcal{E}'_- = \mathcal{E}_-[[XY]/g]$
- $Q' = Q[[XY]/g]$

$\mathcal{S}'$ is a sketch since this operation is only a name-change.

Giving the Point (gh) a name $P := (gh)$; Symbol $P := (gh)$
Dual to giving an intersection-point a name.

Identifying two Points u and t; Symbol $u = t$

- $\mathcal{M}' = \mathcal{M} \setminus \{u\}$
- $\mathcal{E}'_+ = \mathcal{E}_+[u/t]$
- $\mathcal{E}'_- = \mathcal{E}_-[u/t]$
- $Q' = \text{closure}(Q \cup \{u = t\})$

Note that the set Q' can contain terms t not in $\mathcal{M}'$. This action can produce a semisketch from a sketch. For an example c.f. fig. 6.4.

Identifying two Lines l and m; Symbol $l = m$
Dual to identifying two Points.

Using a "Lemma": Adding $t\mathcal{I}u$; Symbol $t\mathcal{I}u$

- $\mathcal{M}' = \mathcal{M}$
- $\mathcal{E}'_+ = \mathcal{E}_+ + (t\mathcal{I}u)$
- $\mathcal{E}'_- = \mathcal{E}_-$
- $Q' = Q$

This action can produce a semisketch from a sketch.

Adding a negative literal $t\not{\mathcal{I}}u$; Symbol $t\not{\mathcal{I}}u$

- $\mathcal{M}' = \mathcal{M}$
- $\mathcal{E}'_+ = \mathcal{E}_+$
- $\mathcal{E}'_- = \mathcal{E}_- + (t\not{\mathcal{I}}u)$

- $Q' = Q$

Adding a negative literal $t \neq u$**; Symbol** $t \neq u$

- $\mathcal{M}' = \mathcal{M}$
- $\mathcal{E}'_+ = \mathcal{E}_+$
- $\mathcal{E}'_- = \mathcal{E}_- + (t \neq u)$
- $Q' = Q$

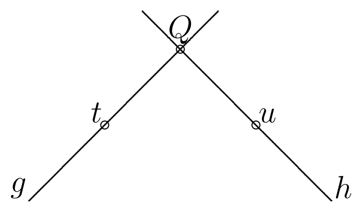

Figure 6.4: Identifying two objects t and u

To deduce a fact with sketches we connect the concept of the sketch and the concept of the actions into a new concept called construction. This construction will deduce the facts.

Definition 6.8 (Construction) *A* construction *is a rooted and directed tree with a semisketch attached to each node and an action attached to each vertex and satisfying the following conditions: If a vertex with action A leads from node N_1 to node N_2, then N_2 is obtained from N_1 by carrying out the action on N_1. If from a node N there is a vertex labeled with $[XY]$, (gh), $\{C\}$, $g := [XY]$, $P := (gh)$, then there is no other vertex from N. Furthermore if the pair $(\mathcal{E}_+, \mathcal{E}_-)$ attached to a node ...*

- *yields a direct contradiction, then it has no successor,*
- *is a semisketch but not a sketch, i.e. that there are critical constellations, let $(P, Q; g, h)$ be one of them, then there are exactly two successors, one labeled with the action $P = Q$ and one labeled with the action $g = h$.*

What is deduced by a construction: A formula is true when it is true in all the models of the given calculus. The distinct models in a construction are achieved by case-distinctions. So if a formula should be deduced by a construction, it must be in all the leafs of the tree. But since some leafs end with contradictions and from the logical principle "ex falso quodlibet" we only require that a formula, which should be deduced, has to be in all leafs which are not contradictious.

We also have to pay attention to the way a construction handles identities. Since in a construction an identity is carried out in the way that all occurrences of one term are substituted for the other, we not only prove an atomic formula, but also all the formulas which are variants with respect to the corresponding set Q. This notion will now be defined.

DEFINITION 6.9 *Two atomic formulas* $P(t_1, u_1)$ *and* $P(t_2, u_2)$ *are said to be* equivalent with respect to Q, *where* Q *is a set of equalities, in symbols* $P(t_1, u_1) \equiv_{Q_N} P(t_2, u_2)$, *when* $(t_1 = t_2), (u_1 = u_2) \in Q_N$ *(or the symmetric one).*

Now we can define the notion of what a construction deduces:

DEFINITION 6.10 *A construction deduces a set of atomic formulas* Δ *iff for all* $A \in \Delta$ *there is a not contradictious leaf, where either* $A \in Q_N$ *or* $(\exists B \in \mathcal{E}_+(N) \cup \mathcal{E}_-(N))A \equiv_{Q(N)} B$.

For an example see section 7.

In the approach to formalize the sketch in projective geometry, one of the early approaches was influenced by the idea of a closed world assumption: In a sketch everything what is drawn unequal should be unequal and only those incidences drawn are valid, all the others are wrong. It is similar to someone at the airport asking for a connection from A to B, not finding such a connection, deducing that there is none. But the negation of all not explicitly stated atomic formulas led to serious problems, since projective geometry is not complete, i.e., there are theorems which are true in one model and false in another. Take for an example the formula $D_1\mathcal{I}[D_2D_3]$, where the D_i are the diagonal-points of the points $A_0, \ldots, D_0$. As shown in sec. 2.3 there is projective geometry, e.g. the minimal projective geometry, where this incidence is true, and other ones, e.g. Π_{EP}, where this incidence is wrong. So if we negate this axiom we would leave the generality of models and restrict ourselves to special models. But this is possible, if we assume this incidence in the initial sketch. For a detailed discussion on different closed world assumptions compare to [2] and [11].

Chapter 7

An Example of a Construction

In this section we want to give an example proved on the one hand within $\mathbf{L_{PG}K}$ and on the other hand within the calculus of construction given in the last section.

We want to prove the fact that the diagonal-point $D_1 := ([A_0B_0][C_0D_0])$ and the diagonal-point $D_2 := ([A_0C_0][B_0D_0])$ are distinct. See fig. 7.1 for the final sketch, i.e. we have already constructed all the necessary objects from the given Points A_0, B_0, C_0, D_0. This step is relatively easy and there are no problems with any of the controls.

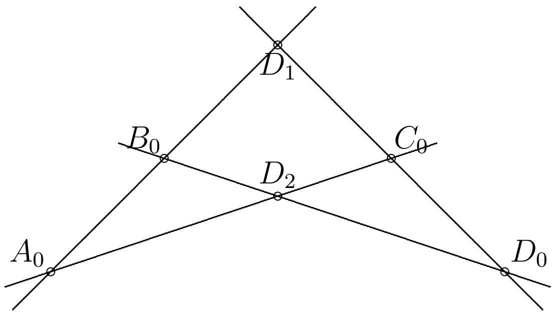

Figure 7.1: A sample construction

We will first give the construction tree and will then explain the single steps:

The respective labels can be found on p. 42

Note the bold formulas in $\mathcal{E}_+^5, \mathcal{E}_-^5$ and in $\mathcal{E}_+^6, \mathcal{E}_-^6$, which yield the contradiction.

In the following lists and in the figure not all formulas are mentioned, especially such formulas unnecessary for the construction are not listed. For the construction tree compare with fig. 7.2. We can see, that the case-distinction after $D_1 = D_2$ yields a contradiction in any branch, therefore we could deduce with the construction that $D_1 \neq D_2$, since this formula is in all leafs, which are not contradictious.

We will now give also a short description of what is happening in this tree:

$$\mathcal{M}^0 = \{A_0, B_0, C_0, D_0, [A_0B_0], \dots\}$$
$$\mathcal{E}^0_+ = \{A_0\mathcal{I}[A_0B_0], \dots\}$$
$$\mathcal{E}^0_- = \{A_0 \neq B_0, \dots, A_0\not\mathcal{I}[C_0D_0]\}$$
$$Q^0 = \{A_0 = A_0, \dots, [A_0B_0] = [A_0B_0], \dots\}$$
$$a1 = \quad ([A_0B_0][C_0D_0])$$
$$\mathcal{M}^1 = \{A_0, B_0, C_0, D_0, [A_0B_0], \dots, ([A_0B_0][C_0D_0])\}$$
$$\mathcal{E}^1_+ = \{A_0\mathcal{I}[A_0B_0], \dots, ([A_0B_0][C_0D_0])\mathcal{I}[A_0B_0], \dots\}$$
$$\mathcal{E}^1_- = \{A_0 \neq B_0, \dots, A_0\not\mathcal{I}[C_0D_0]\}$$
$$Q^1 = Q^0 \cup \{([A_0B_0][C_0D_0])\}$$
$$a2 = \quad ([A_0C_0][B_0D_0])$$
$$\mathcal{M}^2 = \{A_0, B_0, C_0, D_0, [A_0B_0], \dots, ([A_0B_0][C_0D_0]), ([A_0C_0][B_0D_0])\}$$
$$\mathcal{E}^2_+ = \{A_0\mathcal{I}[A_0B_0], \dots, ([A_0B_0][C_0D_0])\mathcal{I}[A_0B_0], ([A_0C_0][B_0D_0])\mathcal{I}[A_0C_0], \dots\}$$
$$\mathcal{E}^2_- = \{A_0 \neq B_0, \dots, A_0\not\mathcal{I}[C_0D_0]\}$$
$$Q^2 = Q^1 \cup \{([A_0C_0][B_0D_0])\}$$
$$a3 = \quad g := [A_0B_0], h := [C_0D_0], l := [A_0C_0], m := [B_0D_0], D_1 := (gh), D_2 := (lm)$$
$$\mathcal{M}^3 = \{A_0, B_0, C_0, D_0, g, h, l, m, D_1, D_2\}$$
$$\mathcal{E}^3_+ = \{A_0\mathcal{I}g, B_0\mathcal{I}g, C_0\mathcal{I}h, D_0\mathcal{I}h, A_0\mathcal{I}l, C_0\mathcal{I}l, B_0\mathcal{I}m, D_0\mathcal{I}m, D_1\mathcal{I}g, D_1\mathcal{I}h, D_2\mathcal{I}l, D_2\mathcal{I}m\}$$
$$\mathcal{E}^3_- = \{C_0\not\mathcal{I}g, D_0\not\mathcal{I}g, A_0\not\mathcal{I}h, B_0\not\mathcal{I}h, B_0\not\mathcal{I}l, D_0\not\mathcal{I}l, A_0\not\mathcal{I}m, C_0\not\mathcal{I}m, A_0 \neq B_0, \dots\}$$
$$Q^3 = \{A_0 = A_0, \dots, g = g, h = h, l = l, m = m, D_1 = D_1, D_2 = D_2\}$$
$$a4 = \quad D_1 = D_2$$
$$\mathcal{E}^4_+ = \{A_0\mathcal{I}g, B_0\mathcal{I}g, C_0\mathcal{I}h, D_0\mathcal{I}h, A_0\mathcal{I}l, C_0\mathcal{I}l, B_0\mathcal{I}m, D_0\mathcal{I}m, D_1\mathcal{I}g, D_1\mathcal{I}h, D_1\mathcal{I}l, D_1\mathcal{I}m\}$$
$$\mathcal{E}^4_- = \{C_0\not\mathcal{I}g, D_0\not\mathcal{I}g, A_0\not\mathcal{I}h, B_0\not\mathcal{I}h, B_0\not\mathcal{I}l, D_0\not\mathcal{I}l, A_0\not\mathcal{I}m, C_0\not\mathcal{I}m, A_0 \neq B_0, \dots\}$$
$$Q^4 = \{A_0 = A_0, \dots, g = g, h = h, l = l, m = m, D_1 = D_1, D_2 = D_2, D_1 = D_2\}$$
$$a5 = \quad g = l$$
$$\mathcal{E}^5_+ = \{A_0\mathcal{I}g, B_0\mathcal{I}g, C_0\mathcal{I}h, D_0\mathcal{I}h, \mathbf{C_0}\mathcal{I}\mathbf{g}, B_0\mathcal{I}m, D_0\mathcal{I}m, D_1\mathcal{I}g, D_1\mathcal{I}h, D_1\mathcal{I}m\}$$
$$\mathcal{E}^5_- = \{\mathbf{C_0}\not\mathcal{I}\mathbf{g}, D_0\not\mathcal{I}g, A_0\not\mathcal{I}h, B_0\not\mathcal{I}h, B_0\not\mathcal{I}g, D_0\not\mathcal{I}g, A_0\not\mathcal{I}m, C_0\not\mathcal{I}m, A_0 \neq B_0, \dots\}$$
$$Q^5 = \{A_0 = A_0, \dots, g = g, h = h, l = l, m = m, D_1 = D_1, D_2 = D_2, D_1 = D_2, g = l\}$$
$$a6 = \quad A_0 = D_1$$
$$\mathcal{E}^6_+ = \{A_0\mathcal{I}g, B_0\mathcal{I}g, C_0\mathcal{I}h, D_0\mathcal{I}h, A_0\mathcal{I}l, C_0\mathcal{I}l, B_0\mathcal{I}m, D_0\mathcal{I}m, A_0\mathcal{I}h, \mathbf{A_0}\mathcal{I}\mathbf{m}\}$$
$$\mathcal{E}^6_- = \{C_0\not\mathcal{I}g, D_0\not\mathcal{I}g, A_0\not\mathcal{I}h, B_0\not\mathcal{I}h, B_0\not\mathcal{I}l, D_0\not\mathcal{I}l, \mathbf{A_0}\not\mathcal{I}\mathbf{m}, C_0\not\mathcal{I}m, A_0 \neq B_0, \dots\}$$
$$Q^6 = \{A_0 = A_0, \dots, g = g, h = h, l = l, m = m, D_1 = D_1, D_2 = D_2, D_1 = D_2, A_0 = D_1, A_0 = D_2\}$$
$$a7 = \quad D_1 \neq D_2$$
$$\mathcal{E}^7_+ = \{A_0\mathcal{I}g, B_0\mathcal{I}g, C_0\mathcal{I}h, D_0\mathcal{I}h, A_0\mathcal{I}l, C_0\mathcal{I}l, B_0\mathcal{I}m, D_0\mathcal{I}m, D_1\mathcal{I}g, D_1\mathcal{I}h, D_2\mathcal{I}l, D_2\mathcal{I}m\}$$
$$\mathcal{E}^7_- = \{C_0\not\mathcal{I}g, D_0\not\mathcal{I}g, A_0\not\mathcal{I}h, B_0\not\mathcal{I}h, B_0\not\mathcal{I}l, D_0\not\mathcal{I}l, A_0\not\mathcal{I}m, C_0\not\mathcal{I}m, A_0 \neq B_0, \dots, D_1 \neq D_2\}$$
$$Q^7 = \{A_0 = A_0, \dots, g = g, h = h, l = l, m = m, D_1 = D_1, D_2 = D_2\}$$

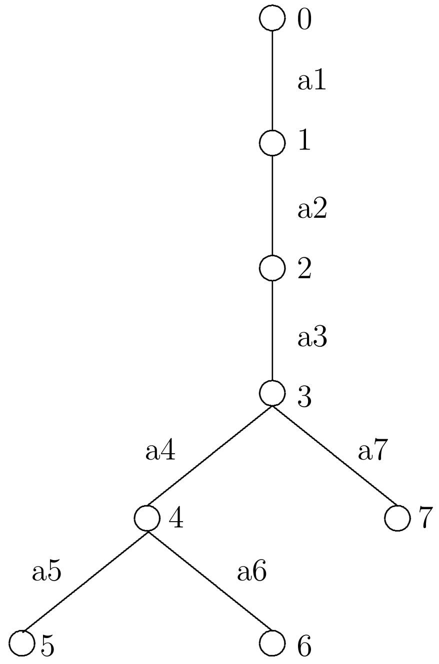

Figure 7.2: Construction Tree

The initial sketch is

$$\begin{aligned}\mathcal{M} &= \{A_0, B_0, C_0, D_0, [A_0B_0], \dots\}\\ \mathcal{E}_+ &= \{A_0\mathcal{I}[A_0B_0], \dots, D_0\mathcal{I}[C_0D_0]\}\\ \mathcal{E}_- &= \{A_0\not{\mathcal{I}}[B_0C_0], \dots, D_0\not{\mathcal{I}}[A_0B_0]\}\end{aligned}$$

After constructing the points D_1 and D_2 and with the shortcuts $[A_0B_0] = g$, $[C_0D_0] = h$, $[A_0C_0] = l$, $[B_0D_0] = m$ we obtain

$$\begin{aligned}\mathcal{M} &= \{A_0, B_0, C_0, D_0, g, h, l, m, D_1, D_2, \dots\}\\ \mathcal{E}_+ &= \{A_0\mathcal{I}g, B_0\mathcal{I}g, C_0\mathcal{I}h, D_0\mathcal{I}h,\\ &\qquad A_0\mathcal{I}l, C_0\mathcal{I}l, B_0\mathcal{I}m, D_0\mathcal{I}m,\\ &\qquad D_1\mathcal{I}g, D_1\mathcal{I}h, D_2\mathcal{I}l, D_2\mathcal{I}m\}\\ \mathcal{E}_- &= \{C_0\not{\mathcal{I}}g, D_0\not{\mathcal{I}}g, A_0\not{\mathcal{I}}h, B_0\not{\mathcal{I}}h,\\ &\qquad B_0\not{\mathcal{I}}l, D_0\not{\mathcal{I}}l, A_0\not{\mathcal{I}}m, C_0\not{\mathcal{I}}m,\\ &\qquad A_0 \neq B_0, \dots\}\end{aligned}$$

We now want to add $D_1 \neq D_2$. For this purpose we identify D_1 and D_2 and put the new sets through the contradiction procedure. We will now follow the single steps:

$$D_2 \leftarrow D_1 \tag{1}$$

and as a consequence

$$D_2\mathcal{I}l \Rightarrow D_1\mathcal{I}l \tag{1a}$$
$$D_2\mathcal{I}m \Rightarrow D_1\mathcal{I}m \tag{1b}$$

and so we get the critical constellation $(A_0, D_1; g, l)$

$$A_0\mathcal{I}g, A_0\mathcal{I}l, D_1\mathcal{I}g, D_1\mathcal{I}l \tag{C}$$

Inquiring the first solution $g = l$ yields

$$l \leftarrow g \tag{1.1}$$

and as a consequence

$$C_0\mathcal{I}l \Rightarrow C_0\mathcal{I}g \tag{1.1a}$$

which is a contradiction to

$$C_0\not{\mathcal{I}}g \in \mathcal{E}_- \tag{1.1b}$$

Inquiring the second solution $D_1 = A_0$ yields

$$D_1 \leftarrow A_0 \tag{1.2}$$

and as a consequence

$$D_1\mathcal{I}m \Rightarrow A_0\mathcal{I}m \tag{1.2a}$$

which is a contradiction to

$$A_0\not{\mathcal{I}}m \in \mathcal{E}_- \tag{1.2b}$$

Since these are all the critical constellations and a contradiction is derived for each branch, the assumption that $D_1 = D_2$ is wrong and $D_1 \neq D_2$ can be added to $\mathcal{E}_-$.

We will now give a proof in $\mathbf{L_{PG}K}$ which corresponds to the above construction. The labels in this proof will not be the rules of $\mathbf{L_{PG}K}$, but references to the above lines.

Π_1 :

$$\cfrac{\cfrac{\overset{(1.1)}{g = l \rightarrow g = l} \quad \rightarrow C_0\mathcal{I}l}{g = l \rightarrow C_0\mathcal{I}g}\,(1.1a)}{g = l \rightarrow}\,(1.1b)$$

Π_2 :

$$\dfrac{\dfrac{\overset{(1.2)}{A_0 = D_1 \to A_0 = D_1} \qquad \dfrac{\overset{(1)}{D_1 = D_2 \to D_1 = D_2} \quad \to D_2 \mathcal{I} m}{D_1 = D_2 \to D_1 \mathcal{I} m}\,(1\text{b})}{A_0 = D_1, D_1 = D_2 \to A_0 \mathcal{I} m}\,(1.2\text{a})}{A_0 = D_1, D_1 = D_2 \to}\,(1.2\text{b})$$

Π_3 :

$$\dfrac{\dfrac{\dfrac{\to A_0 \mathcal{I} g \quad \to A_0 \mathcal{I} l \quad \overset{(1.1)}{g = l \to g = l}}{\to g = l, A_0 = (gl)} \qquad \dfrac{\to D_1 \mathcal{I} g \quad \dfrac{\overset{(1)}{D_1 = D_2 \to D_1 = D_2} \quad \to D_2 \mathcal{I} l}{D_1 = D_2 \to D_1 \mathcal{I} l}\,(1\text{a}) \quad \overset{(1.1)}{g = l \to g = l}}{D_1 = D_2 \to g = l, D_1 = (gl)}}{D_1 = D_2 \to g = l, A_0 = D_1}}{D_1 = D_2 \to g = l \lor A_0 = D_1}$$

Π_1 examines the branch when $g = l$, Π_2 examines the branch when $A_0 = D_1$, and Π_3 deduces that either $g = l$ or $D_1 = A_0$ under the assumption that $D_1 = D_2$ has to be true. The final proof is

$$\dfrac{\overset{\vdots\, \Pi_3}{D_1 = D_2 \to g = l \lor A_0 = D_1} \qquad \dfrac{\overset{\vdots\, \Pi_1}{g = l \to} \quad \overset{\vdots\, \Pi_2}{A_0 = D_1, D_1 = D_2 \to}}{g = l \lor A_0 = D_1, D_1 = D_2 \to}}{D_1 = D_2 \to}\,(\text{Cut})$$

From this example we can see that construction and proof are very similar in this case. In the next section we want to prove the general result that any construction can be transformed into a proof and vice versa.

Chapter 8

The Relation between Sketches and Proofs

The aim of this chapter is the equivalence theorem, which states that proofs and sketches are equivalent, i.e. that a proof can be translated into a sketch and otherwise.

8.1 Translation from Construction to Proof

We will now start with a construction tree defined in sec. 6 and translate it into a proof in $\mathbf{L_{PG}K}$. For this purpose we will define some notions used in this translation: We will use $\mathcal{E}^0_+, \mathcal{E}^0_-, N^0, \ldots$ for the root node of a tree.

Definition 8.1 *The* set of assumptions *of a construction tree $\mathcal{T}$ is a set $As(\mathcal{T})$ of formulas with*

- *All formulas in $\mathcal{E}^0_+$ which are not instances of mathematical axioms are contained in $As(\mathcal{T})$.*
- *All formulas in $\mathcal{E}^0_-$ which are not instances of mathematical axioms are contained in $As(\mathcal{T})$.*
- *for any action $u = t$ in $\mathcal{T}$, $(u = t) \in As$*
- *for any action $u\mathcal{I}t$ in $\mathcal{T}$, $(u\mathcal{I}t) \in As$*
- *for any action $u \neq t$ in $\mathcal{T}$, $(u \neq t) \in As$*
- *for any action $u\not{\mathcal{I}}t$ in $\mathcal{T}$, $(u\not{\mathcal{I}}t) \in As$*

The set of assumptions for a node N, denoted with $As(N)$ is the set of all assumptions from the root and all assumptions from actions $u = t$ and $u\mathcal{I}t$ above the node N.

For the following lemma we start with a rather trivial claim about the necessity of name-changes.

CLAIM: If a construction deduces a fact, then there is also a construction without the use of the actions $P := (gh)$ and $g := [PQ]$, i.e. without a name-change, deducing the same facts, when trivial substitutions are ignored. □

The following lemma is the essential translation from construction trees to $\mathbf{L_{PG}K}$-proofs:

LEMMA 8.1 (TRANSLATION LEMMA) *For any nonempty subset Δ of formulas of a node N in a construction without a name-change there is a proof in $\mathbf{L_{PG}K}$ of the sequent $As(N) \to \Delta$.*

PROOF: The proof is an induction on the number n of vertices in the construction above the node N.

Case $n = 0$: Take a formula $A \in \Delta$. Either A is an instance of a mathematical axiom, then $\mathrm{As}(N) \to \Delta$ is a weakening of this axiom or A is in $\mathrm{As}(N) = \mathrm{As}(\mathcal{T})$ and then $\mathrm{As}(N) \to \Delta$ is a weakening of $A \to A$.

Case $n > 0$: In the following discussion we will denote the last node with N, its ancestor with N' and the action leading from N' to N with α. We will now discuss the different possibilities of α:

$\alpha =$"$[XY]$": If $\Delta \subset N'$, then there is a proof of $\mathrm{As}(N') \to \Delta$ and since $\mathrm{As}(N') = \mathrm{As}(N)$ also a proof for $\mathrm{As}(N) \to \Delta$. If $\Delta \not\subset N'$ it must be $X\mathcal{I}[XY]$ or $Y\mathcal{I}[XY]$ contained in Δ and therefore $\mathrm{As}(N) \to \Delta$ is a weakening of the mathematical axiom $\to X\mathcal{I}[XY]$ or $\to Y\mathcal{I}[XY]$.

$\alpha =$"(gh)": This case is similar to "$[XY]$".

$\alpha =$"$\{C\}$": Since there are no new formulas this is trivial.

$\alpha =$"$t = u$": We will denote the set of formulas in N', from which the formulas in Δ are generated by the substitution process with Δ'.

If $\Delta' \subset N'$ then there is a proof of $\mathrm{As}(N') \to \Delta'$. Since the substitution in the sketch is carried out on all levels of the term depth we have to construct all these terms. By first applying the rules (id-con:1), (id-con:2), (id-int:1), (id-int:2) we can proof equalities for all the terms in which u is substituted for t. With this equalities we can proof $t = u, \mathrm{As}(N') \to \Delta$, which is $\mathrm{As}(N) \to \Delta$.

EXAMPLE: As an example take the tree starting with no additional assumptions to that one about $A_0, \ldots, D_0$, followed by the action of constructing the intersection point $([A_0B_0]g)$, then the action of assumption that this point incides with s, i.e., $([A_0B_0]g)\mathcal{I}s$ and finally substituting h for $[A_0B_0]$. In the leaf we get the formula $(hg)\mathcal{I}s$. $\mathrm{As}(N') = \{([A_0B_0]g)\mathcal{I}s\}$, $\mathrm{As}(N) = \{([A_0B_0]g)\mathcal{I}s, [A_0B_0] = h\}$.

Take the following proof:

$$\dfrac{\dfrac{[A_0B_0] = h \to [A_0B_0] = h}{[A_0B_0] = h \to ([A_0B_0]g) = (hg)} \quad ([A_0B_0]g)\mathcal{I}s \to ([A_0B_0]g)\mathcal{I}s}{\mathrm{As}(N) \to (hg)\mathcal{I}s}$$

♡

If $\Delta' \not\subset N'$, then $t = u$ must be in Δ. Then $\mathrm{As}(N) \to \Delta$ is a weakening of the logical axiom $t = u \to t = u$.

$\alpha =$"$t\mathcal{I}u$": If $\Delta \subset N'$, then there is a proof of $\mathrm{As}(N') \to \Delta$ and by weakening with $t\mathcal{I}u$ we get a proof of $\mathrm{As}(N) \to \Delta$. If $\Delta \not\subset N'$, then $t\mathcal{I}u$ must be in Δ and therefore $\mathrm{As}(N) \to t\mathcal{I}u$ is a weakening of the logical axiom $t\mathcal{I}u \to t\mathcal{I}u$, since $(t\mathcal{I}u) \in \mathrm{As}(N)$.

$\alpha =$"$t \neq u$": If $\Delta \subset N'$, then there is a proof of $\mathrm{As}(N') \to \Delta$ and by weakening with $t \neq u$ we get a proof of $\mathrm{As}(N) \to \Delta$. If $\Delta \not\subset N'$, then $t \neq u$ must be in Δ and therefore $\mathrm{As}(N) \to t \neq u$ is a weakening of $t \neq u \to t \neq u$, which is easily deduced from $t = u \to t = u$.

$\alpha =$"$t\not{\mathcal{I}}u$": If $\Delta \subset N'$, then there is a proof of $\mathrm{As}(N') \to \Delta$ and by weakening with $t\not{\mathcal{I}}u$ we get a proof of $\mathrm{As}(N) \to \Delta$. If $\Delta \not\subset N'$, then $t\not{\mathcal{I}}u$ must be in Δ and therefore $\mathrm{As}(N) \to t\not{\mathcal{I}}u$ is a weakening of $t\not{\mathcal{I}}u \to t\not{\mathcal{I}}u$, which is easily deduced from $t\mathcal{I}u \to t\mathcal{I}u$.
This completes the proof. □

We now want to show that for all the formulas a construction deduces there is a proof of certain assumptions → formula. The certain assumptions are not all the formulas in $\mathrm{As}(\mathcal{T})$, since in this set there are usually a lot of case-distinctions and solutions for critical constellations. So we will define a set of essential assumptions, which should contain the assumptions really made, and a set of case-assumptions which contain only those assumptions, which are used for case-distinction.

Definition 8.2 *The set $eAs(\mathcal{T})$ of the essential assumptions contains the following formulas:*

- *All formulas in $\mathcal{E}^0_+$ which are not instances of mathematical axioms are contained in $eAs(\mathcal{T})$.*
- *All formulas in $\mathcal{E}^0_-$ which are not instances of mathematical axioms are contained in $As(\mathcal{T})$.*
- *If there is a node N and a vertex labeled with $P(t,u)$ and this is the only vertex from N, then $P(t,u) \in eAs$. (Note that $P(t,u)$ can be $t = u, t \neq u, t\mathcal{I}u, t\not{\mathcal{I}}u$)*

The set $cAs(\mathcal{T})$ of case-assumptions contains all formulas which are labeled to vertices leading from a node with critical constellations and all those formulas $P(t,u)$ such that there is a node N with two vertices, one labeled with $P(t,u)$ and the other labeled with $\neg P(t,u)$ ($P \in \{\mathcal{I}, =\}$).

We will denote with $cAs(N)$ for a node N all the formulas from $cAs(\mathcal{T})$ which are above N.

EXAMPLE: (continued from sec. 7) For the given construction $\mathrm{As}(\mathcal{T}) = \{D_1 = D_2, D_1 \neq D_2, g = l, A_0 = D_1, \dots\}$ where the dots stand for the assumptions of the initial sketch, which are nothing else than the axiom (PG3).

The set $\mathrm{eAs}(\mathcal{T})$ consists only of the formulas in N_0, the assumptions of the initial sketch. The set $\mathrm{cAs}(\mathcal{T})$ consists of the formulas $D_1 = D_2, D_1 \neq D_2, g = l, A_0 = D_1$. The set of case-assumptions for the node N_4 consists only of $D_1 = D_2$. The set of case-assumptions of node N_5 consists of $D_1 = D_2, g = l$. ♡

We will now give the essential lemma for translating a construction into a proof:

LEMMA 8.2 *For any given construction $\mathcal{T}$ and any node N in it, we can give a proof of*

$$eAs(\mathcal{T}), cAs(N) \to$$

if all branches below N end with a contradiction and

$$eAs(\mathcal{T}), cAs(N) \to \Delta$$

for any set Δ of formulas, such that for each $A \in \Delta$ there is a not contradictious leaf under N, such that $A \in N$.

This lemma essentially erases all the assumptions in the proof generated from the translation lemma, which come from case distinctions and distinctions after critical constellations, which are below the node N. This is intuitively easy to understand, since for such a distinction either the one case or the other case must happen and therefore both the subtrees below N realizing this distinction prove the corresponding facts without this distinction.

PROOF: We will prove this lemma by induction on the number N of vertices below N. We will denote a vertex leading from N with α and the node it leads to with N'.

Case $n = 0$: If the node N is contradictious, then there is either a formula $P(t,u)$, such that $P(t,u)$ and $\neg P(t,u)$ are in N. From lemma 8.1 we get proofs P_1 of $\mathrm{As}(N) \to P(t,u)$ and P_2 of $\mathrm{As}(N) \to \neg P(t,u)$. An easy transformation of P_1 gives us a proof P_1' of $P(t,u), \mathrm{As}(N) \to$ and with the cut rule a proof of $\mathrm{As}(N) \to$. By weakening and exchange we get $\mathrm{eAs}(\mathcal{T}), \mathrm{cAs}(N) \to$.

If the node is contradictious and there is no such formula, then there is a formula $t \neq t$ in N. Again from the translation lemma we get a proof

P of $\mathrm{As}(N) \to t \neq t$. An easy transformation of P gives us a proof P' of $t = t, \mathrm{As}(N) \to$ and by cutting with the axiom $\to t = t$ we get a proof of $\mathrm{As}(N) \to$. By weakening and exchange we get $\mathrm{eAs}(\mathcal{T}), \mathrm{cAs}(N) \to$.

If the node N is not contradictious we get, again by the translation lemma, a proof of $\mathrm{As}(N) \to \Delta$ and by weakening and exchange a proof of

$$\mathrm{eAs}(\mathcal{T}), \mathrm{cAs}(N) \to A$$

Case $n > 0$*:* The proof is relatively simple. If there is only one successor of the node N, say N', and the action is not a substitution, then there is no distinction. By induction hypothesis we get a proof of $\mathrm{eAs}(\mathcal{T}), \mathrm{cAs}(N') \to \Delta$ which is nothing else then $\mathrm{eAs}(\mathcal{T}), \mathrm{cAs}(N) \to \Delta$, maybe weakened by a formula.

The other cases, i.e. if there is more than one successor or the substitution, we will now discuss. We will denote the successors of N with N' (and N'' if necessary).

$\alpha =$"$t = u$": We will denote the set of formulas which arise from Δ by carrying out the substitution $[t/u]$ with Δ'.

- There is no other vertex leaving from N: By induction hypothesis we get a proof of $\mathrm{eAs}(\mathcal{T}), \mathrm{cAs}(N') \to \Delta'$. By applying the same construction as described in the proof of the translation lemma, but in the opposite direction (not substituting t for u, but u for t) we get a proof of $\mathrm{eAs}(\mathcal{T}), \mathrm{cAs}(N) \to \Delta$, since $t = u \in \mathrm{eAs}(\mathcal{T})$.

- There is another vertex from N to N'' labeled with $t \neq u$: Then by induction hypothesis there are proofs P_1' of $\mathrm{eAs}(\mathcal{T}), \mathrm{cAs}(N') \to \Delta'$ and P_2 of $\mathrm{eAs}(\mathcal{T}), \mathrm{cAs}(N'') \to \Delta$. From the construction given above we get a proof of P_1 of $t = u, \mathrm{eAs}(\mathcal{T}), \mathrm{cAs}(N) \to \Delta$.Take the following proof:

$$\dfrac{\dfrac{\dfrac{t = u \to t = u}{\to t \neq u, t = u}}{\to t \neq u \vee t = u} \qquad \dfrac{\dfrac{\vdots\, P_2}{\mathrm{eAs}(\mathcal{T}), \mathrm{cAs}(N'') \to \Delta}}{t \neq u, \mathrm{eAs}(\mathcal{T}), \mathrm{cAs}(N) \to \Delta} \quad \dfrac{\vdots\, P_1}{t = u, \mathrm{eAs}(\mathcal{T}), \mathrm{cAs}(N) \to \Delta}}{\dfrac{t \neq u \vee t = u, \mathrm{eAs}(\mathcal{T}), \mathrm{cAs}(N) \to \Delta}{\mathrm{eAs}(\mathcal{T}), \mathrm{cAs}(N) \to \Delta}\ (\mathrm{Cut})}$$

This is possible since $t \neq u \in \mathrm{cAs}(N'')$.

- There is another vertex from N to N'' labeled with $g = h$. Then there is a critical constellation $(t, u; g, h)$ or $(g, h; t, u)$ in N. Let $t =: P$, $U =: Q$ for convenient reading. From induction hypothesis and the above construction there are proofs P_1 of $P = Q, \mathrm{eAs}(T), \mathrm{cAs}(N) \to \Delta$ and a proof P_2 of $g = h, \mathrm{eAs}(\mathcal{T}), \mathrm{cAs}(N) \to \Delta$. Since in N there is a critical constellation from the translation lemma we get proofs S_1, S_2, T_1, T_2 for $\mathrm{As}(N) \to P\mathcal{I}g$,

$\mathrm{As}(N) \to P\mathcal{I}h$, $\mathrm{As}(N) \to Q\mathcal{I}g$, $\mathrm{As}(N) \to Q\mathcal{I}h$, respectively. Take the following proof:

$$\dfrac{\begin{array}{c}\vdots\ \Pi_1\\ \mathrm{eAs}(\mathcal{T}),\mathrm{cAs}(N) \to g=h \vee P=Q\end{array} \quad \begin{array}{c}\vdots\ \Pi_2\\ P=Q \vee g=h, \mathrm{eAs}(\mathcal{T}),\mathrm{cAs}(N) \to \Delta\end{array}}{\mathrm{eAs}(\mathcal{T}),\mathrm{cAs}(N) \to \Delta}\ (\mathrm{Cut})$$

where Π_1 :

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\begin{array}{c}\vdots\ S_1\\ \mathrm{As}(N)\to t\mathcal{I}g\end{array} \quad \begin{array}{c}\vdots\ S_2\\ \mathrm{As}(N)\to t\mathcal{I}h\end{array} \quad g=h\to g=h}{\mathrm{As}(N)\to g=h, t=(gh)} \quad \dfrac{\begin{array}{c}\vdots\ T_1\\ \mathrm{As}(N)\to Q\mathcal{I}g\end{array} \quad \begin{array}{c}\vdots\ T_2\\ \mathrm{As}(N)\to Q\mathcal{I}h\end{array} \quad g=h\to g=h}{\mathrm{As}(N)\to g=h, Q=(gh)}}{\mathrm{As}(N)\to g=h, t=Q}}{\mathrm{As}(N)\to g=h\vee P=Q}}{\mathrm{eAs}(\mathcal{T}),\mathrm{cAs}(N)\to g=h\vee P=Q}}{}$$

and Π_2 :

$$\dfrac{\begin{array}{c}\vdots\ P_1\\ P=Q, \mathrm{eAs}(\mathcal{T}),\mathrm{cAs}(N)\to\Delta\end{array} \quad \begin{array}{c}\vdots\ P_2\\ g=h, \mathrm{eAs}(\mathcal{T}),\mathrm{cAs}(N)\to\Delta\end{array}}{P=Q\vee g=h, \mathrm{eAs}(\mathcal{T}),\mathrm{cAs}(N)\to\Delta}$$

$\alpha =$"$t \neq u$": This case is dual to the case $t = u$, part 2.
$\alpha =$"$t\mathcal{I}u$": This case is similar to the case $t = u$, part 2.
$\alpha =$"$t\not\mathcal{I}u$": This case is dual to $t\mathcal{I}u$.

This completes the proof. □

The final theorem is only an application of the above lemma:

THEOREM 8.1 *If a construction $\mathcal{T}$ deduces a set Δ, then there is a proof in* $\mathbf{L_{PG}K}$ *of the sequent*

$$eAs(\mathcal{T}) \to \Delta$$

PROOF: Take as node N for the lemma the root of the construction $\mathcal{T}$ and we get a proof of

$$\mathrm{eAs}(\mathcal{T}),\mathrm{cAs}(N) \to \Delta$$

but since $\mathrm{cAs}(N) = \emptyset$ this is a proof of

$$\mathrm{eAs}(\mathcal{T}) \to \Delta$$

□

8.2 Translation from Proof to Construction

In this section we want to show that any proof can be translated into a construction. But since a construction and a proof handle identities differently, we will take care of consequences of identities.

The first lemmas will operate only on the (atom)-part of a proof, as described in sec. 5 and will show that all such parts can be coded in a construction (sec. 8.2.1). The reducing from a general formula to this part will be done in 8.2.2.

8.2.1 Translation for the (atom)-part of a proof

LEMMA 8.3 *For any cut-free proof* Π *in* $\mathbf{L_{PG}K}$ *of a sequent* $\Gamma \to \Delta$*, where* Γ *and* Δ *consist only of atomic formulas, there is a construction, which deduces a subset of* $\overline{\Gamma} \cup \Delta$*.*

Furthermore we can say that any leaf, which is not contradictious, will yield only one formula of the subset.

Note that if a subset can be deduced, the whole sequent is a direct consequence of the subset by weakening.

PROOF: The proof is an induction on the number n of prooflines in the proof Π. We will first give some general remarks on the transformation.

(i) We will start with a sketch with no assumptions, i.e. only with the formulas expressing the axiom (PG3). As constants we will take beside the given $A_0, \ldots, D_0$ all the constants occurring in the proof which has to be transformed.

(ii) Then we will build up a tree, which is a construction cum grosso modo, but will not be consistent in substitutions, in other words, by carrying the action of identifying t and u, we will not cut t from the set $\mathcal{M}$, as given in the description of the actions. So we can use t later again. Furthermore there will be nodes in the new tree, which are contradictious but do have successors. We will refer to this kind of tree as the term preconstruction.

(iii) Any of the given trees, say $\mathcal{T}$, will start with a part, where all the terms necessary in the proof are constructed. In this part no case distinction can arise, but a splitting into a distinction by a critical constellation is possible anyway, if a term used in the proof describes the same object as any other term. For an example take the term $([A_0B_0][A_0C_0])$ and A_0 itself. To avoid such situations, we will in a first step substitute inherent equal terms with their minimal form, i.e. we will substitute x for $([xy][xz])$ or $[(xy)(xz)]$ (where $[xy]$ can be $[yx]$ and similar) in the whole proof. This yields a set of terms which do not inherently describe the same objects. We will assume that, when we append one construction onto another, then the new construction starts with a part constructing the terms necessary for both constructions, followed by the other actions of the first tree and followed by the other actions of the second tree.

(iv) The principle of the transformation is that we start with no assumptions and for every logical axiom we make a case distinction. Since the rules of the calculus don't generate more formulas from the axioms we get one and only one formula in the endsequent as consequence for any combination of positive/negative parts of the logical axioms. This will happen in the proof, too. In each node, which is not contradictious there will be only one formula, which will be equivalent to a formula in the sequent.

(v) Finally we will give a transformation making a real construction from a preconstruction described in (ii) which proves the same sequent.

So let us start with a proof, in which the transformation given in (ii) about inherent equal terms are already carried out. For such a proof we will show the lemma.

Case $n = 1$: The proof is an axiom. We start with constructing the necessary terms. If the axiom is mathematical, then the sequent consists only of one formula and this formula is in the last $\mathcal{E}_+$ which has been constructed. If the axiom is a logical one, then we will make a case distinction. On the one side there will be $\neg P(t, u)$ in $\mathcal{E}_-$ and in $\overline{\Gamma}$, on the other side there will be $P(t, u)$ either in $\mathcal{E}_+$ and $\Delta_{\mathcal{I}}$ or in Q and $\Delta_=$.

Case $n > 1$: We must now scrutinize all the rules of $\mathbf{L_{PG}K}$, which can be used to construct a (atom)-part. That are the weakening-rules, the exchange-rules, the contraction-rules, the equality-rules and the mathematical rules (Erase) and (PG1-ID). For the first three of them the proof is easy: By induction hypothesis there is a construction for the above sequent. Take the same construction for the lower one. What remains are the equality and the mathematical rules. In the following we will refer to the lower sequent as S, to the left upper as S_1 and to the right upper as S_2. By induction hypothesis there are preconstructions $\mathcal{T}_1$ and $\mathcal{T}_2$ for S_1 and S_2, respectively.

If $\mathcal{T}_i$ also prove the sequent without the main formula, i.e. the formulas which are identified in the listing of the rules in sec. 4.3, then $\mathcal{T}_i$ can be used as preconstruction for the lower sequent, too. So in the following we will assume that in the preconstructions of S_1 and S_2 the main formulas are essential, i.e., they are contained in a leaf, which is not contradictious. We can also assume that there is only one such leaf, as this is proved by the induction, too. This nodes we will refer to as N_1 and N_2.

For the rules (id-$\mathcal{I}_{\tau_\mathcal{P}}$:left), (id-$\mathcal{I}_{\tau_\mathcal{P}}$:right), (id-$\mathcal{I}_{\tau_\mathcal{L}}$:left), (id-$\mathcal{I}_{\tau_\mathcal{L}}$:right) the procedures are the same: There is exactly one node for the main formula in the sequent S_2, onto this node we hang on the tree $\mathcal{T}_1$ for the left upper sequent. In the node N_2 there is the main formula of S_2, say $P(s, u)$. In the node N_1 of the composed tree, which is a leaf, there is the main formula for S_1, say $s = t$. This substitution is carried out anywhere in the tree and in the node N_1 of the composed tree the set Q_{N_1} contains $s = t$. If the formula $P(s, u)$ from N_2 becomes $P(s', u')$ in N_1 by some substitutions, there is $s = s'$ and $u = u'$ in Q_{N_1}, and combined with

$s = t$ there is, since the sets Q are closed under equality rules, $t = s'$ in Q_{N_1}, and therefore $P(s', u') \equiv_{Q_{N_1}} P(t, u)$, which is necessary that the combined tree proves $P(t, u)$.

For the rules (trans:left) and (trans:right) the system is the same like above, but this time the set Q_{N_1} gives the necessary formulas.

For the rules (symm:left) and (symm:right) the preconstruction from the upper sequent is taken.

For the rules (id-con:1), (id-con:2), (id-int:1), (id-int:2) the preconstructions from the upper sequent are taken. Since this terms are already constructed at the top of the tree (c.f. (iii) above) the identity is already in Q_{N_1}.

Finally we must discuss the mathematical rules (Erase) and (PG1-ID). The construction for the upper sequent of (Erase) surely doesn't prove e.g. $A_0\mathcal{I}[B_0C_0]$, because if this formula is in $\mathcal{E}_+$, this leaf is contradictious and therefore isn't discussed further on. For (PG1-ID) there are preconstructions $\mathcal{T}_1$, $\mathcal{T}_2$ and $\mathcal{T}_3$ for the sequents $\Gamma \to \Delta, P\mathcal{I}g$, $\Gamma \to \Delta, Q\mathcal{I}g$ and $P = Q, \Gamma \to \Delta$, respectively. The corresponding last nodes are N_i. First we make the term-part, where all the terms are constructed and add to this one the construction of $[PQ]$. Then we put $\mathcal{T}_1$ after the node N_2 of $\mathcal{T}_2$ and this tree again after the node N_3 of $\mathcal{T}_3$. Since the last action above N_1 must generate the formula $P\mathcal{I}g$, in this node there will be a critical constellation $(P, Q; [PQ], g)$ (or any other term, which is already substituted for $[PQ]$). This is the case because in the first part of the construction all the terms are already built. The distinction into cases for this critical constellation is $P = Q$ and $[PQ] = g$. But in the node N_3, and therefore also in all subsequent nodes, there is a variant of $P \neq Q$ in $\mathcal{E}_-$. Therefore the vertex leading from N_1 labeled with $P = Q$ yields a contradiction. So the only new leaf contains the formula $[PQ] = g$ in its Q-part and therefore proves the lower sequent.

To complete the proof of the lemma we must give a transformation of a preconstruction into a construction preserving the property of what it deduces. We read the preconstruction from the root. When we come to a substitution, we carry it out in the whole subtree below this vertex and updating all the sets Q in this subtree. After this pass we read the whole construction from the root again and if we come to a node which is contradictious, then we delete the whole subtree under this node. After this parse we obtain a construction. Why does this construction preserve the property of what it deduces?

First note that there are less or equal leafs which are not contradictious. So no essential new formulas are derived which have to be in the sequent proved. Further note that if a formula A was in a leaf N and equivalent w.r. to Q_N to B and B in $\Gamma \to \Delta$, and the formula has changed by some substitutions, the respective equalities are contained in the set Q_N and therefore also the new formula A' is equivalent w.r. to Q_N to B. This yields a construction for a subset of $\overline{\Gamma} \cup \Delta$. So we have a construction which deduces the sequent $\Gamma \to \Delta$. □

8.2.2 Reduction of a general formula to sequents with atomic components

We start from a sequent containing only one formula to the right which is in prenex normal form and the matrix in conjunctive normal form

$$\rightarrow (Q_1 x_1)\dots(Q_n x_n)A(t_1,\dots,t_n)$$

This is no loss of generality, since any sequent can be transformed in such a formula.

From Herbrand's theorem[1] we get a disjunction of instances of the matrix of this formula, which is, with some knowledge on the sequence of instantiations, equivalent to the original formula.

$$\rightarrow \bigvee_{i=1}^{k} A(t_1^i,\dots,t_n^i)$$

This formula can be brought into conjunctive normal form:

$$\bigwedge_{i=1}^{n} L_1^i \vee \dots \vee L_{n_i}^i$$

The next step backward in the proof is the solving of the conjunction into several sequents with disjunction formulas, i.e. we get n sequents of the form

$$\rightarrow L_1^i \vee \dots \vee L_{n_i}^i$$

This sequents can easily be reduced to sequents without the connective $\vee$ and further by bringing all the negative literals to the left side, we get a sequent

$$\Gamma \rightarrow \Delta$$

where all the formulas in Γ and Δ are atomic. So a construction of $\Gamma \rightarrow \Delta$ yields a construction for

$$\rightarrow L_1^i \vee \dots \vee L_{n_i}^i$$

and n such constructions yield a proof by construction for the sequent

$$\bigwedge_{i=1}^{n} L_1^i \vee \dots \vee L_{n_i}^i$$

which is equivalent to the sequent

$$\rightarrow \bigvee_{i=1}^{k} A(t_1^i,\dots,t_n^i)$$

[1] or the midsequent theorem

The construction for this sequent together with the knowledge on the sequence of instantiations yield a proof for the original sequent

$$\rightarrow (Q_1 x_1) \ldots (Q_n x_n) A(t_1, \ldots, t_n)$$

So we can state the final theorem

THEOREM 8.2 *For any proof in* $\mathbf{L_{PG}K}$ *there is a set of constructions such that the constructions deduce this sequent.*

Chapter 9

Closing Comments

We hope that this first analysis of projective geometry from a proof-theoretic point of view opens up a new interesting way to discuss features of projective geometry, which is widely used in a lot of applied techniques. Especially the fact, that the sketches drawn by geometers have actually the same strength as the proofs given in a formal calculus, puts these constructions in a new light. Till now they were considered as nothing more then hints to understand the formal proof by exhibiting you the incidences. But they can be used as proves by themselves.

There are some ways to extend the calculus $\mathbf{L_{PG}K}$ to deduce more complex facts, i.e. expressions dealing with functions and predicates. For this purpose we will consider higher order logic systems. We will now present some of them already developed.

9.1 Other Calculi

During this thesis we considered some other calculi for projective geometry. One of the first attempts was a calculus with restricted second order properties. The reason was that we want to speak about functions and theorems on them since lot of the theorems in projective geometry are really theorems in meta-projective geometry, i.e. theorems about the structure of the objects in the projective geometry.

This calculus had quantors for the types constructed only from the primitive types, i.e. quantors for the type $[\tau_1, \ldots, \tau_n \to \tau]$ with $\tau_i, \tau \in \{\tau_{\mathcal{P}}, \tau_{\mathcal{L}}\}$. It was also necessary to introduce an operator on functions which realizes the composition of the functions, in other words, it was necessary to introduce a case-distinction as a special term:

$$T(f(x), g(x), a) = \begin{cases} f(x) & \text{if } x = a, \\ g(x) & \text{if } x \neq a. \end{cases}$$

This calculus has the property that already a lot of real life projective geometry, i.e., also theorems about projective geometry, can be carried out in it.

Another calculus considered for first order logic is a variant of the presented and differs only in the fact, that there are no types. To identify points and lines there are special predicates $\mathcal{P}(x)$ and $\mathcal{L}(x)$ which are true when x is a point or a line. Furthermore there are certain axioms on these predicates stating that the corresponding sets build a partition of the universe. With this predicates there is in any proven theorem a prefix identifying the variables.

$$(\forall_{\tau_{\mathcal{L}}} x)(\exists_{\tau_{\mathcal{P}}} Y)(Y \not{I} x)$$

becomes

$$(\forall x)(\mathcal{L}(x) \supset (\exists y)(\mathcal{P}(y) \wedge y \not{I} x))$$

Although this calculus has the advantage of having only one type, the sentences are more complex and error-prone.

9.2 What to do?

There are a lot of interesting directions further investigations can explore.

The discussion of the various calculi is one of them. Then we can extend the formulization of the construction to the using of more complex lemmas. Furthermore it is interesting to discuss the fact that the axioms imply a one-to-one function between the points and the lines and so that any given model has exactly the same number of points and lines. This is something like categoricity, but in another sense than the usual one.

The various interpolation theorems, which can be also applied to the calculus $\mathbf{L_{PG}K}$, and the discussion of Beth's definability theorem will yield interesting consequences on projective geometry and the way new concepts are defined in projective geometry.

Finally it will be fascinating to set up an automatic theorem proving facility based on the calculus $\mathbf{L_{PG}K}$.

Appendix A

The Euclidean Axioms for Affine Geometry

A.1 Definitions

1. A point is that which has no part.
2. A line is breadthless length.
3. The extremities of a line are points.
4. A straight line is a line which lies evenly with the points on itself.
5. A surface is that which has length and breadth only.
6. The extremities of a surface are lines.
7. A plane surface is a surface which lies evenly with straight lines on itself.
8. A plane angle is the inclination to one another of two lines in a plane which meet one another and do not lie in a straight line.
9. And when the lines containing the angle are straight, the angle is called rectilinear.
10. When a straight line set up on a straight line makes the adjacent angles equal to one another, each of the equal angles is right, and the straight line standing on the other is called perpendicular to that on which it stands.
11. An obtuse angle is an angle greater than a right angle.
12. An acute angle is an angle less than a right angle.
13. A boundary is that which is an extremity of anything.

14. A figure is that which is contained by any boundary or boundaries.

15. A circle is a plane figure contained by one line such that all the straight lines falling upon it from one point among those lying within the figure are equal to one another.

16. And the point is called the centre of the circle.

17. A diameter of the circle is any straight line drawn through the centre and terminated in both directions by the circumference of the circle, and such a straight line also bisects the circle.

18. A semicircle is a figure contained by the diameter and the circumference cut off by it. And the centre of the semicircle is the same as that of the circle.

19. Rectilinear figures are those which are contained by straight lines, trilateral figures being those contained by three, quadrilateral those contained by four, and multilateral those contained by more than four straight lines.

20. Of trilateral figures, an equilateral triangle is that which has three sides equal, an isosceles triangle that which has two of its sides alone equal, and a scalene triangle that which has its three sides unequal.

21. Further, of trilateral figures, a right-angled triangle is that which has a right angle, an obtuse-angled triangle that which has an obtuse angle, and an acute-angled triangle that which has its three angles acute.

22. Of quadrilateral figures, a square is that which is both equilateral and right-angled; an oblong that which is right-angled but not equilateral; a rhombus that which is equilateral but not right-angled; and a rhomboid that which has its opposite sides and angles equal to one another but is neither equilateral nor right-angled. And let quadrilaterals other than these be called trapezia.

23. Parallel straight lines are straight lines, which, being in the same plane and being produced indefinitely in both directions, do not meet one another in either direction

A.2 The Postulates

1. To draw a straight line from any point to any point.

2. To produce a finite straight line continuously in a straight line.

3. To describe a circle with any centre and distance.

4. That all right angles are equal to one another.

5. That, if a straight line falling on two straight lines make the interior angles on the same side less than two right angles, the two straight lines, if produced indefinitely, meet on that side on which are the angles less than the two right angles.

A.3 The Common Notions

1. Things which are equal to the same thing are also equal to one another.

2. If equals be added to equals, the wholes are equal.

3. If equals be subtracted from equals, the remainders are equal.

4. Things which coincide with one another are equal to one another.

5. The whole is greater than the part.

Appendix B

Hilbert's Axioms for Euclidean Plane Geometry

B.1 Group I — *Axioms of Connection*

1. Through any two distinct points A, B, there is always a line m.

2. Through any two distinct points A, B, there is not more than one line m.

3. On every line there exists at least two distinct points. There exists at least three points which are not on the same line.

4. Through any three points, not on the same line, there is one and only one plane.

B.2 Group II — *Axioms of Order*

1. If point B is between points A and C, then A, B, C are distinct points on the same line, and B is between C and A.

2. For any two distinct points A and C, there is at least one point B on the line AC such that C is between A and B.

3. If A, B, C are three distinct points on the same line, then only one of the points is between the other two.

   DEFINITION B.1 *By the* segment AB *is meant the set of all points which are between A and B. Points A and B are called the* end points *of the segment. The segment* AB *is the same as segment* BA*.*

4. (Pasch's Axiom) Let A, B, C be three points not on the same line and let m be a line in the plane A, B, C, which does not pass through any of the

points A, B, C. Then if m passes through a point of the segment AB, it will also pass through a point of segment AC or a point of segment BC.

B.3 Group III — *Axioms of Congruence*

Definition B.2 *By the* ray AB *is meant the set of points consisting of those which are between* A *and* B*, the point* B *itself, and all points* C *such that* B *is between* A *and* C*. The ray* AB *is said to* emanate from *point* A*.*

A point A, on a given line m, divides m into two rays such that two points are on the same ray if and only if A is not between them.

Definition B.3 *If* A*,* B*,* C *are three points not on the same line, then the system of three segments* AB*,* BC*,* CA *and their endpoints is called the* triangle ABC*. The three segments are called the* sides *of the triangle, and the three points are called the* vertices*.*

1. If A and B are distinct points on line m, and if A' is a point on line m' (not necessarily distinct from m), then there is one and only one point B' on each ray of m' emanating from A' such that the segment $A'B'$ is congruent to the segment AB.

2. If two segments are each congruent to a third, then they are congruent to each other.
(from this it can be shown that congruence of segments is an equivalence relation; i.e, $AB \cong AB$; if $AB \cong A'B'$, then $A'B' \cong AB$; and if $AB \cong CD$ and $CD \cong EF$, then $AB \cong EF$.)

3. If point C is between A and B, and point C' is between A' and B', and if the segment $AC \cong$ segment $A'C'$, and the segment $CB \cong$ segment $C'B'$, then segment $AB \cong$ segment $A'B'$.

Definition B.4 *By an* angle *is meant a point (called the* vertex *of the angle) and two rays (called the* sides *of the angle) emanating from the point.*

If the vertex of the angle is point A and if B and C are any two points other than A on the two sides of the angle, we speak of the angle BAC or CAB or simply of angle A.

4. If BAC is an angle whose sides do not lie on the same line and if in a given plane, $A'B'$ is a ray emanating from A', then there is one and only one ray $A'C'$ on a given side of line $A'B'$, such that $\angle B'A'C' \cong \angle BAC$. In short, a given angle in a given plane can laid off on a given ray in one and only one way. Every angle is congruent to itself.

Definition B.5 *If ABC is a triangle then the three angles BAC, CBA, and ACB are called the angles of the triangle. Angle BAC is said to be* included *by the sides AB and AC of the triangle.*

5. If two sides and the included angle of one triangle are congruent respectively to two sides and the included angle of another triangle, then each of the remaining angles of the first triangle is congruent to the corresponding angle of the second triangle.

B.4 Group IV — *Axiom of Parallels (for a plane)*

1. (Playfair's postulate) Through a given point A not on a given line m there passes at most one line, which does not intersect m.

B.5 Group V — *Axioms of Continuity*

1. (Axiom of measure or the Archimedean axiom) If AB and CD are arbitrary segments, then there exists a number n such that if segment CD is laid off n times on the ray AB starting from A, then a point E is reached, where $n \cdot CD = AE$, and where B is between A and E.
2. (Axiom of linear completeness) The system of points on a line with its order and congruence relations cannot be extended in such a way that relations existing among its elements as well as the basic properties of linear order and congruence resulting from Axioms I–III, and V-1 remain valid.

Bibliography

[1] Georg Boolos and Richard Jeffrey. *Computability and Logic*. Cambridge University Press, 1973.

[2] Marco Cadoli and Maurizio Lenzerini. The complexity of closed world reasoning and circumscription. 1989.

[3] H. S. M. Coxeter. *Projective Geometry*. Springer-Verlag, 1994.

[4] Jean-Yves Girard. *Proof Theory and Logical Complexity*. Bibliopolis, 1987.

[5] Kurt Gödel. Über formal unentscheidbare Sätze der Principia Mathematica und Verwandter Systeme i. *Monatshefte für Mathematik und Physik*, 38:173–198, 1931.

[6] David Hilbert. *Grundlagen der Geometrie*. B. G. Teubner, 1899.

[7] Stephan Cole Kleene. *Introduction to metamathematics*, volume I. North-Holland, bibliotheca mathematica edition, 1952.

[8] J. Krajíček and P. Pudlák. The number of proof lines and the size of proofs in first order logic. *Arch. Math. Logic*, pages 69–84, 1988.

[9] G. Kreisel and J.-L. Krivine. *Modelltheorie*. Springer-Verlag, 1972.

[10] Werner Kuich. Mathematische Logik. Skriptum zur Vorlesung an der TU Wien.

[11] J. Minker. On indefinite databases and the closed world assumption. In *Proceedings of the 6th CADE Conference*, 1982.

[12] Wolfram Schwabhäuser, Wanda Szmielew, and Alfred Tarski. *Metamathematische Methoden in der Geometrie*. Springer Verlag, 1983.

[13] Joseph R. Shoenfield. *Mathematical Logic*. Addison-Wesley, 1967.

[14] Gaisi Takeuti. A conservative extension of Peano arithmetic.

[15] Gaisi Takeuti. *Proof Theory*. North Holland, 1987.

[16] Alfred Tarski. *A decision method for elementary algebra and geometry*. University of California Press, Berkeley, 1951.

[17] Wen-tsün Wu. *Mechanical Theorem Proving in Geometries*. Springer-Verlag, 1994.