Automated Theorem Proving in Geometry
Course Notes of 236714
Spring 2003

J.A. Makowsky and students

March 15, 2004

Students

Name	e-mail	Faculty	Status	Scribe of Lecture
Alex Glikson	aglik@@cs	CS	M.Sc	
Avi Magid	magid@@tx	Inter	M.Sc.	
Yonit Magid	yonitm@@tx	CS	M.Sc	
Daniel Zeitlin	zeitlin@@tx	CS	external	
Mark Kozdoba	marik@@tx	Math+CS	M.Sc.	
Eran Talmor	teran@@tx	CS	external	4

Prerequisites

We assume our students are familiar with basic logic and computability as tought in our courses Logic for CS 1 (234292) or Logic and Sets for CS (234293) and Theory of Computation (236343).

We shall also quote results from Logic 2 (236304) but the course is not a prerequisite. We also assume that the students remember some basic algebra (Algebra A and possibly Algebra B) but we shall state explicitly what is needed. There is some (little) overlap with the course Computability and Definability (236331).

Course assignments

Students have to do homework as assigned during the lectures. Furthermore, they have to work out ONE session in the style of the following notes. Finally, they have to do a final project, which consists of preparing the results of research papers into teachable form (slides or text).

1 Overview on Theorem Proving

Lecture 1, March 10, 2003, 3 hours
Notes by J. Makowsky

Automated Theorem Proving comprises two very different topics.

- General Theorem Proving: The Theorem Prover (program) receives two inputs:

  (i) A theory T in some formalism, say Propositional Calculus (PC), First Order Logic (FOL), Temporal Logic, Modal Logic, Second Order Logic

  (ii) A formula (sentence) ϕ in the formalism.

  The program then should decide whether ϕ follows logically from T.

- Special Theorem Proving: The Theorem Prover is specially tuned to a specific theory T, say Elementary Geometry, Group Theory, or any mathematical theory axiomatizable in First Order or Second Order Logic.

  The program then receives as input a sentence (candidate theorem) ϕ and is supposed to check whether ϕ is a theorem of the theory T.

The goal of the course is to study both cases to some extent. In this lecture we give a survey of these aspects. We leave it to the audience, at the end of this lecture, to decide on which aspect to put the emphasis.

1.1 Propositional Logic

Theorem proving in PC is usually reduced to SAT, satisfiability checking. For a set T of PC-formulas and ϕ a PC-formula instead of $T \models \phi$ one checks whether $T \cup \{\phi\}$ is satisfiable. The general problem is known to be **NP**-complete.

A very popular method to solve SAT is the RESOLUTION method. It is known to have exponential time worst case complexity. But it performs well in many practical problems.

This can be explained theoretically, as its average time complexity is polynomial for many probability distributions which seem to model real situations. However, the average case complexity of RESOLUTION is exponential for some (equally realistic) probability distributions.

RESOLUTION works fast for special classes of formulas, the $HORN$-formulas. Horn formulas are formulas in CNF (Conjunctive normal form) where each disjunct has at most one non-negated variable. Other easy classes of formulas (for SAT) are formulas of bounded tree width or bounded clique width. There is a vast literature on various heuristics for special formulas. An excellent survey is

- Dingzhu Du, Jun Gu and Panos M. Pardalos (eds), Satisfiability Problem: Theory and Applications, DIMACS Series, vol. 35, American mathematical Society, 1997

Thesis Topic 1 *Classify these heuristics.*

1.2 First Order Logic

The general Theorem Proving Problem (historically called the Decision Problem) is undecidable. In modern language this reads (as tought in the course Logic 2):

Theorem 1 (Gödel 1929, Church, Turing 1936) *For a relational vocabulary τ which contains at least one binary relation symbol, the set of valid (provable) $FOL(\tau)$-sentences is semi-computable but not computable.*

The theorem depends on the choice of a vocabulary. There is no underlying theory T, only the logical axioms are assumed.

In the early literature, 1920ff, people tried to prove computability for special classes of formulas, hoping that finally an induction proof would emerge. A common classification of FOL-sentences is by their quantifier prefix. Here we use that every sentence is equivalent to a sentence in prenex normal form, i.e. a sentence of the form

$$Q_1 x_1, Q_2 x_2, \ldots Q_m x_m B(X_1, \ldots x_m)$$

where $Q_i \in \{\forall, \exists\}$ and B is a quantifier free formula, or equivalently, a boolean combination of atomic formulas. A formula (sentence) is *universal (existential* if all the quantifiers Q_i above are $\forall$ ($\exists$).

For example we have

Theorem 2 (Bernays and Schönfinkel 1928, Ramsey 1931) *For every relational vocabulary τ with equality, the set of valid (provable) universal (existential) $FOL(\tau)$-sentences is computable.*

Theorem 3 (Lewis 1978) *For every relational vocabulary τ with equality, The set of satisfiable universal $FOL(\tau)$-sentences recognizable in non-deterministic exponential time. For large enough vocabularies, the problem is complete for non-deterministic exponential time.*

A survey of everything one knows for decidable cases of the Decision Problem may be found in

- E. Börger and E. Grädel and Y. Gurevich, The Classical Decision Problem, Springer-Verlag, 1997.

Many General Theorem Provers have been designed. They all produce correct results, but do not necessarely terminate. They work in practical situations of knowledge processing, where there are large amounts of data, but little Theorem Proving is required. The most popular method is based on a combination of RESOLUTION methods and UNIFICATION, due to M. Davis and H. Putnam (1960), and popularized by J.A. Robinson[1] in 1965.

[1] There are four Robinsons who are of importance for this course: Julia Robinson, Raphael Robinson, Abraham Robinson and John Alan Robinson.

A good survey is

- Dov M. Gabbay, C.J. Hogger and J.A. Robinson, Handbook of Logic in Artificial Intelligence and Logic Programming I: Logical Foundations, Oxford Science Publications, Oxford University Press, 1993.

The programming language PROLOG is based in General Theorem Provers of this type.

In attempts to identify computable cases, one looks at special mathematical theories, like various theories of arithmetic and geometry, or theories related to these, such as group theory, the theory of order.

1.3 Theories of a fixed structure

Let $\mathfrak{A}$ be a τ-structure. $FOL^0(\tau)$ is the set of sentences of $FOL)(\tau)$, i.e. the formulas without free variables.

We denote by

$$Th_\tau^{FOL}(\mathfrak{A}) = Th(\mathfrak{A}) = \{\phi \in FOL^0(\tau) : \mathfrak{A} \models \phi\}$$

the complete theory of $\mathfrak{A}$.

Definition 4 *A set $T \subseteq FOL^0(\tau)$ is complete, if T is satisfiable, and for every $\phi \in FOL^0(\tau)$ either $T \models \phi$ or $T \models \neg\phi$.*

Clearly, $Th(\mathfrak{A})$ is complete, even in the stronger sense that $\phi \in T$ or $\neg\phi \in T$.

Let

$$\mathfrak{N} = \langle \mathbb{N}, +_N, \times_N, \leq_N, 0_N, 1_N \rangle$$

$$\mathfrak{Z} = \langle \mathbb{N}, +_Z, \times_Z, \leq_Z, 0_Z, 1_Z \rangle$$

$$\mathfrak{Q} = \langle \mathbb{Q}, +_Q, \times_Q, \leq_Q, 0_Q, 1_Q \rangle$$

$$\mathfrak{R} = \langle \mathbb{R}, +_R, \times_R, \leq_R, 0_R, 1_R \rangle$$

$$\mathfrak{C} = \langle \mathbb{C}, +_C, \times_C, 0_C, 1_C \rangle$$

$$\mathfrak{Z}_+ = \langle \mathbb{N}, +_Z, \leq_Z, 0_Z, 1_Z \rangle$$

$$\mathfrak{R}_+ = \langle \mathbb{R}, +_R, \leq_R, 0_R, 1_R \rangle$$

$$\mathfrak{R}_{add} = \langle \mathbb{R}, +_R, 0_R, 1_R \rangle$$

$$\mathfrak{R}_< = \langle \mathbb{R}, \leq_R \rangle$$

be the FOL-theories of the natural numbers, integers, rational, reals and complex numbers with the indicated aritmetic operations and (except for the complex numbers) the order relation.

Theorem 5 (Goedel 1931, Julia Robinson 1949)
The theories $Th(\mathfrak{N})$, $Th(\mathfrak{Z})$ and $Th(\mathfrak{Q})$ are not even semi-computable.

For the quantifier free sentences of these theories we have algorithms (which we learn in primary school).

Homework 1 *Prove this.*

For the existential theory $Th_{\Sigma}(\mathfrak{N})$ and $Th_{\Sigma}(\mathfrak{Z})$ we have

Theorem 6 (Davis, Putnam, J. Robinson and Matijasevič 1949-1970) *The existential theories $Th_{\Sigma}(\mathfrak{N})$ and $Th_{\Sigma}(\mathfrak{Z})$ are not even semi-computable.*

In contrast to this we have

Theorem 7 (Presburger 1929, Cooper 1972) *The theory $Th(\mathfrak{Z}_{+})$ is computable in deterministic doubly exponential time.*

Theorem 8 (Langford 1926, Tarski 1931, 1948) *The theories $Th(\mathfrak{R}_{<})$, $Th(\mathfrak{R}_{add})$, $Th(\mathfrak{R}_{+})$, $Th(\mathfrak{R})$ and $Th(\mathfrak{C})$ are computable.*

Theorem 9 (Ferrante, Rackoff 1974, Collins 1975) *The theories $Th(\mathfrak{R}_{<})$, $Th(\mathfrak{R}_{add})$, $Th(\mathfrak{R}_{+})$, $Th(\mathfrak{R})$ and $Th(\mathfrak{C})$ are computable in deterministic doubly exponential time.*

The theory of the reals with its arithmetic is important because it represents the algebraization of GEOMETRY. The Tarski-Collins algorithm gives a THEOREM PROVER for EUCLIDEAN GEOMETRY.

1.4 Adding functions to the reals

It is natural to ask what happens if we add a function symbol to the vocabulary and fix its interpretation.

We denote by

$$\mathfrak{R}_{sin} = \langle \mathbb{R}, +_R, \times_R, sin(-)_R, \leq_R, 0_R, 1_R \rangle$$

$$\mathfrak{R}_{exp} = \langle \mathbb{R}, +_R, \times_R, exp(-)_R, \leq_R, 0_R, 1_R \rangle$$

the structure of the reals with the sinus function and the exponential function respectively.

It is easy to show, by reduction to $Th(\mathfrak{N})$, that

Proposition 10 *$Th(\mathfrak{R}_{sin})$ is not even semi-computable.*

The following is one of the great open problems:

Problem 11 (Tarski) *Is $Th(\mathfrak{R}_{exp})$ computable?*

Very recently a partial answer was given by MacIntyre and Wilkey. It says that under deep number theoretic conjecture (Shnirelman's conjecture), $Th(\mathfrak{R}_{exp})$ is computable.

1.5 Axiomatic theories

Sometimes we are not only interested in theories of specific structures, but in theories $Th(K)$ of classes of τ-structures K which are axiomatized (defined) by finite or computable sets of sentences (axioms) $\Sigma \subseteq FOL(\tau)$. We denote by

$$Th(\Sigma) = \{\phi \in FOL^0(\tau) : \Sigma \models \phi\}.$$

Examples are

(i) Infinite sets (with equality only)

(ii) Linear orders

(iii) Abelian groups

(iv) Groups

(v) First Order Peano arithmetic.

Homework 2 *Write down the axioms of these theories.*

In this list we have

Theorem 12 *(i) The theories of infinite sets, linear orders (Läuchli and Leonhard, 1966)), Abelian groups (Szmielev 1955) are computable.*

(ii) The theory of groups (Mal'cev 1961) and of Peano arithmetic (Gödel 1931, Turing 1936) are not computable.

Excellent surveys can be found in

- J. D. Monk, Mathematical Logic, (Part III), Springer 1976
- Y. Ershov, I. Lavrov, A. Taimanov and M. Taitslin, Elementary theories, Russian Mathematical Surveys, 20 (1965) 35-105.

1.6 Goal of the course

The following options were voted:

- Study *SAT* and General Theorem Provers for half of the course, and then Geometrical Theorem Provers.
- Concentrate on Geometry only.

The second option was chosen unanimously.

1.7 Outline of the course

In the next lecture we show

Theorem 13 (Langford 1926) *The theory $Th(\mathfrak{R}_<)$ is computable.*

There will be two proofs. The first is a pure existence proof. We show that $Th(\mathfrak{R}_<) = Th(DLO_{noextr}$, where DLO_{noextr} consists of the axioms which say

(i) The relation $<_R$ is a linear order.

(ii) The relation $<_R$ is dense order, i.e. between any two elements there is a third.

(iii) There are no first nor last elements.

In other words, DLO_{noextr} is complete. Then we use Gödel's Completeness Theorem, which says that the consequence relation is semi-computable. The algorithm now consists in using two Turing machines, one for $DLO_{noextr} \models \phi$ and one for $DLO_{noextr} \models \neg\phi$. As DLO_{noextr} is complete, this always terminates.

The second proof constructs an algorithm which uses ELIMINATION of QUANTIFIERS.

Our next goal is to show:

Theorem 14 (Fourier 1826, Dines 1918, Motzkin 1936, Ferrante, Rackoff 1974) *The theory $Th(\mathfrak{R}_+)$ is computable in doubly exponential time.*

We shall see three proofs, an existence proof for the algorithm and two specially taylored algorithms.

Then we shall have an interlude about real closed fields. Good references are:

- Serge Lang, Algebra (Chapters 11-12), Addison-Wesley 1965 (many editions)
- Nathan Jacobson, Lectures in Abstract Algebra, Volume III: Theory of fields and Galois theory (Chapter VI), Van Nostrand 1964.

Next we shall have an interlude on geometry. Our reference is

- Shang-Ching Chou, Mechanical Geometry Theorem Proving, Reidel, 1988

For the proof of Theorem 8 we shall provide explicit notes

- J.A. Makowsky and K. Meer, Real Number Complexity Theory (Chapter 3), Draft of a book available at

  `www.cs.technion.ac.il/~janos/COURSES/THPR/tarskiproof.ps`

2 Decidable Theories I: Vaught's Test

Lecture 2, March 17, 2003, 1 hour
Notes by J. Makowsky and N.N.

We want to use the following:

Homework 3 *Let $\mathfrak{A}$ and $\mathfrak{B}$ two isomorphic τ-structures. Then $Th(\mathfrak{A}) = Th(\mathfrak{B})$*

Theorem 15 (Cantor, ca. 1870) *Let $\mathfrak{A}$ and $\mathfrak{B}$ be two countable dense linear orderings such that they have corresponding first and last elements. Then $\mathfrak{A} \simeq \mathfrak{B}$.*

The proof will be given in Lecture 3.

Theorem 16 (Löwenheim, Skolem, Tarski, ca. 1930) *Let T be a countable satisfiable set of sentences of $FOL^0(\tau)$. If T has an infinite model then there are models of T of every infinite cardinality.*

This is proved in the Course Logic 2.

We use these two Theorems to show

Theorem 17 *The theory $DLO_{noextr} \subseteq FOL^0(R_<)$ is complete.*

Proof:
Assume not. Then there is $\phi \in FOL^0(R_<)$ with neither $DOL_{noextr} \models \phi$ nor $DOL_{noextr} \models \neg\phi$.

Hence both $DOL_{noextr} \cup \{\phi\}$ and $DOL_{noextr} \cup \{\neg\phi\}$ are satisfiable, and have only infinite models which satisfy DOL_{noextr}.

Using Theorem 16 they have both countable models $\mathfrak{A} \models DOL_{noextr} \cup \{\phi\}$ and $\mathfrak{B} \models DOL_{noextr} \cup \{\neg\phi\}$.

By Theorem 15, they are isomorphic. By Homework 3 $Th(\mathfrak{A}) = Th(\mathfrak{B})$. But $\phi \in Th(\mathfrak{A})$ and $\neg\phi \in Th(\mathfrak{B})$. So both $\phi, \neg\phi \in Th(\mathfrak{A})$. But this contradicts the satisfiability of $Th(\mathfrak{A})$. □

Homework 4 *Write down the sentences for the theories $DLO + firstandlastelements$, $DLO + firstbutnolastelement$, $DLO + nofirstbutlastelement$ and show that they are also complete.*

An almost identical proof like the one of Theorem 17 gives

Theorem 18 (Vaught 1954) *Let $T \subseteq FOL^0(\tau)$ be a countable satsifiable theory such that for some cardinality κ, all models of T of cardinality κ are isomorphic. Then T is complete.*

Homework 5 *Prove Theorem 18.*

Proposition 19 *Let $T \subseteq FOL^0(\tau)$ be a computable theory (i.e., T is a computable set). If T is complete then $Th(T)$ is also computable.*

Homework 6 *Prove Proposition 19*

Putting all this together we get:

Theorem 20 *$Th(DLO)$ is computable (but not complete).*

Homework 7 *Prove Theorem 20 in detail.*

Homework 8 *Let INF be the set of formulas with equality only which contains all the formulas*

$$\exists x_1 \exists x_2 \ldots \exists x_k \bigwedge_{i,j \leq k, i \neq j} \neg x_i \approx x_j$$

(i) Show that INF is complete and $Th(INF)$ is computable.

(ii) Show that for $\phi \in FOL^0(\emptyset)$ we have $DLO \models \phi$ iff $INF \models \phi$.

3 Langford's Theorem

Lecture 3, March 24, 2003, 3 hours
Notes by J. Makowsky and N.N.

Project 1 *Edit and complete the notes of this lecture.*

3.1 Proof of Cantor's Theorem

Proof:
[Proof of Theorem 15] The proof used the back and forth construction of the isomorphism. It uses the countability of the structures to make sure every element is both in the domain and range of the isomorphism. It uses the properties of the dense ordering with prescribed extremal elements to ensure that the construction can be continued after finitely many steps. □

Homework 9 *Complete the details of the proof.*

3.2 Elimination of Quantifiers

Definition 21 *Let $T \subseteq FOL(\tau)$ be a theory and $\Delta \subseteq FOL(\tau)$ a set of formulas closed under boolean combinations and which contains* **True** *and* **False***.*

(i) T admits Δ-Elimination *if for every formula $\phi(\bar{x}) \in FOL(\tau)$ with free variable $\bar{x} = (x_1, \ldots, x_m)$, there is a formula $\psi(\bar{x}) \in \Delta$ with the same free variables, such that*

$$T \models \forall \bar{x}(\phi(\bar{x}) \leftrightarrow \psi(\bar{x}))$$

(ii) T admits QE (Quantifier Elimination) *if Δ consists of all quantifier free formulas of $FOL(\tau) \cup \{\mathbf{True}, \mathbf{False}\}$ and T admits Δ-elimination.*

(iii) T admits effective QE*, if the quantifier free formula ψ is computable from ϕ.*

(iv) T admits fast QE*, if the quantifier free formula ψ is computable from ϕ in polynomial time (in some reasonable model of computation).*

(v) A formula ϕ is simple if ϕ is of the form

$$\exists x B(x, \bar{y})$$

where B is quantifier free. and of the form $\bigwedge_i^n A_i$ and each A_i is either an atomic formula or the negation of an atomic formula.

Proposition 22 *Let $T \subseteq FOL(\tau)$ be a theory which admits effective QE. Assume further that the set of variable free sentences which are consequences of T is computable. Then $Th(T)$ is computable.*

□

Lemma 23 *Let $T \subseteq FOL(\tau)$ be a theory. Assume that for every simple formula $\exists x B(x, \bar{y})$ there is a quantifier free formula $B'(\bar{y})$ such that*

$$T \models \forall \bar{y}(\exists x B(x, \bar{y}) \leftrightarrow B'(\bar{x})).$$

Then T admits QE.

Proof:
Use the following normal forms from the Course Logic 1; Conjunctive Normal Form (CNF), Disjunctive Normal Form (DNF), Negational Normal Form (NNF), Prenex Normal Form (PNF) and the rules of manipulation of quantifiers. □

Lemma 24 *The following formulas are logically equivalent:*

$$\exists x(\phi(x) \wedge x = y) \text{ and } \phi(x) \mid_y^x$$

where $\phi(x) \mid_y^x$ is the result of substituting y for x in ϕ.

Proof:
Use the definition of the meaning function for $\exists$ and the definition of substitution. □

Homework 10 *Fill in the details in the proof of Lemmas 23 and 24.*

Theorem 25 *The theory INF admits effective QE.*

Proof:
By Lemma 23 we it suffices to prove it for simple formulas. For this we use Lemma 24. The proof we sketched in the lecture eliminated one variable at the time, and in each step performed a transformation into DNF. This resulted in an algorithm which used iterated exponential time. □

Homework 11 *Design an algorithm for QE for INF and estimate its running time. Can you find an algorithm which runs in doubly exponential time? in exponential time?*

Theorem 26 (Langford 1926) *The theory DLO_{noextr} admits effective QE.*

Proof:
Similar to the proof of Theorem 25. But here we have to look at all the order configurations of the free variables. Again our proof sketch eliminated one variable at the time and used iterated exponential time. □

Homework 12 *Design an algorithm for QE for DLO_{noextr} and estimate its running time. Can you find an algorithm which runs in doubly exponential time? in exponential time?*

Next we stated Tarski's Theorem.

The theory of real closed fields, RCF, consists of the following axioms (which are all true in $\mathfrak{R}$).

(i) The field axioms.

(ii) The axioms of linear order.

(iii) The compatibility of the order with addition and multiplication: $0 < 1$ and The product and sum of positive elements are postive.

(iv) Every positive element has a square root.

(v) Every univariate polynomial of odd degree has a zero.

Homework 13 *Write down these axioms in FOL.*

Theorem 27 (Tarski 1931, 1948, A. Robinson 1955) *RCF is complete and admits effective QE. Hence $Th(RCF) = Th(\mathfrak{R})$ and $Th(RCF)$ and is computable.*

The proof will be given later. To get a feeling for the strength of this theorem we compute some examples.

Homework 14 *Find a quantifier free formula for the following formulas*

$$\exists x(a_1 x + a_0 \approx 0)$$

$$\exists x(a_2 x^2 + a_1 x + a_0 \approx 0)$$

$$\exists x(y_2 x^2 + y_1 x + y_0 \approx 0)$$

$$\exists x(a_3 x^3 + a_2 x^2 + a_1 x + a_0 \approx 0)$$

$$\exists x(a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0 \approx 0)$$

where x and y_i are free variables.

In the next lecture we look at $\mathfrak{R}_+$.

4 The reals as ordered Abelian group, I

Lecture 4, March 31, 2003, 3 hours
Notes by J. Makowsky and E. Talmor

Frege has formally defined quantifiers in 1870. Before that, quantifiers were used inexplicitly. For example, the following problem was considered, where a solution is to be found for a simultaneous system of polynomial equations:

$$\left.\begin{array}{l} p_1(\bar{x}) = 0 \\ \vdots \\ p_n(\bar{x}) = 0 \end{array}\right\} \in \mathbb{R}[\bar{x}] \text{ (i.e. the ring of polynomials over } \mathbb{R})$$

with coefficients in $\mathbb{Q}$ or in $\mathbb{Z}$. Asking "is there a solution?" in FOL is simply a matter of satisfying the following existential formula:

$$\exists \bar{x} \Big(\bigwedge_{i=1}^{k} p_i(\bar{x}) \overset{<}{\geqq} 0 \Big)$$

If the polynomials are linear equations it is the case of linear programming. Generally, it is the classical problem of existential / optimal formulas. At the end of this lecture we shall learn significance of this rather natural problem.

We now look at $\mathfrak{R}_{add}$ and $\mathfrak{R}_{+}$.
The following properties hold for $\mathfrak{R}_{add}$.

(i) The group is non-trivial, i.e., there is some a such that $a \neq 0$. In FOL:

$$\exists a (a \neq 0)$$

(ii) Addition makes it into an Abelian (commutative) group:

$$\begin{array}{rl} \forall a, b & (a + b = b + a) \\ \forall a, b, c & (a + (b + c) = (a + b) + c) \\ \forall a & (0 + a = a + 0 = 0) \\ \forall a, b \exists x & (a + x = b) \\ \forall a & (a + (-a) = 0) \end{array}$$

(iii) The group is *torsion free*, i.e., for all $a \neq 0$ and for all $n \in \mathbb{N}$

$$\underbrace{a + a + \ldots + a}_{n} \neq 0$$

In FOL, this gives us a formula for each $n \in \mathbb{N}$:

$$\forall a (\underbrace{a + a + \ldots + a}_{n} \neq 0)$$

(iv) The group is *divisible*, i.e., for every a, and every $n \in \mathbb{N}$ there is some b such that

$$\underbrace{b+b+\ldots+b}_{n}=a$$

In FOL, this gives us a formula for each $n \in \mathbb{N}$:

$$\forall a \exists b(\underbrace{b+b+\ldots+b}_{n}=a)$$

(v) For $\mathfrak{R}_+$, additionally, it is an ordered Abelian group, i.e. for every three elements a, b, c, if $a \leq b$ then $a+c \leq b+c$. In FOL:

$$\forall a \forall b \forall c(a \leq b \Rightarrow a+c \leq b+c)$$

We say that $\mathfrak{R}_{add}$ is a divisible torsion free Abelian group ($DTFAG$) and that $\mathfrak{R}_+$ is an ordered divisible torsion free Abelian group ($ODTFAG$).

There are many structures which satisfy $DTFAG$: The additive structure of $\mathbb{Q}$, of $\mathbb{R}$ and of $\mathbb{C}$. Also the additive structure of the complex rationals $\mathbb{CQ}$, i.e. complex numbers with rational real and complex part, satisfy $DTFAG$. Both $\mathbb{Q}$ and $\mathbb{CQ}$ are countable, but they are not isomorphic as abelian groups. In $\mathbb{Q}$, take any $a \neq 0, b \neq 0$, at least one of the formulas

$$(\underbrace{a+a+\ldots+a}_{u}+\underbrace{b+b+\ldots+b}_{v}=0) \vee$$
$$(\underbrace{a+a+\ldots+a}_{u}+\underbrace{(-b)+(-b)+\ldots+(-b)}_{v}=0)$$

must be satisfied, for some $u, v \in \mathbb{N}$. This is true because of the linear dependency of a and b, and the fact that the formula $q_1 a + q_2 b = 0$, where $q_1, q_2 \in \mathbb{Q}$ can be transformed to either $ua + vb = 0$ or $ua - vb = 0$. On the other hand, take $1, i \in \mathbb{CQ}$. There is no function f and no $u, v \in \mathbb{N}$ such that

$$(\underbrace{f(1)+f(1)+\ldots+f(1)}_{u}+\underbrace{f(i)+f(i)+\ldots+f(i)}_{v}=0) \vee$$
$$(\underbrace{f(1)+f(1)+\ldots+f(1)}_{u}+\underbrace{(-f(i))+(-f(i))+\ldots+(-f(i))}_{v}=0)$$

is satisfied. A good book on the subject is ”Infinite Abelian Groups” by Kaplansky.

The structure of $\mathbb{Q}$ is minimal in some manner, by the following

Theorem 28 *If a structure G satisfies $DTFAG$, then G has a subgroup $G' \in G$ such that $G' \cong \mathbb{Q}$.*

Moreover, it follows from Linear Algebra, that every $DTFAG$ can be viewed as a vector space over $\mathfrak{Q}$, and therefore we have

Theorem 29 *If a structure G satisfies $DTFAG$, then there is a set I such that $G \cong \bigoplus_{i\in I} \mathbb{Q}$.*

and also

Theorem 30 *Let $\mathfrak{A}$ and $\mathfrak{B}$ be two models of $DTFAG$ which are of the some uncountable cardinality κ. Then $\mathfrak{A}$ and $\mathfrak{B}$ are isomorphic as Abelian groups.*

We first show:

Theorem 31 (Tarski 1931, 1948, Robinson 1954)
$Th(\mathfrak{R}_{add}) = Th(DTFAG)$.
In particular, the theory $DTFAG$ is complete and computable.

Proof:
We apply Vaught's test:
Given dictionary $FOL(\tau)$ and $T \in FOL(\tau)$ such that

(i) T has models (i.e., T is satisfiable).

(ii) T has no finite models.

(iii) there is $\kappa \in Card$ such that all models of size κ are isomorphic.

then T is complete.

And indeed $DTFAG$ is FOL, and

(i) $\mathbb{R}$ is a model of $DTFAG$.

(ii) $DTFAG$ has no finite models. Otherwise for some finite model, some $a \neq 0$, and some $n, m \in \mathbb{N}$, $n \neq m$, the following must hold: $\underbrace{a + a + \ldots + a}_{n} = \underbrace{a + a + \ldots + a}_{m}$. Without loss of generality $n < m$. Therefore we must have $\underbrace{a + a + \ldots + a}_{m-n} = 0$, in contradiction to the torsion free property.

(iii) Follows from theorem 30.

Thus $DTFAG$ is complete. Since $Th(\mathfrak{R}_{add}) \models Th(DTFAG)$, it follows that $Th(\mathfrak{R}_{add}) = Th(DTFAG)$ $\Box$

Corollary 32 *There is no theorem in abelian groups that distinguishes $\mathbb{Q}$ from $\mathbb{R}$.*

Next we have

Theorem 33 (Tarski 1931, 1948, Robinson 1954)
$Th(\mathfrak{R}_{+}) = Th(ODTFAG)$.
In particular, the theory ODTFAG is complete and computable.

However, here an abstract proof needs some more model theoretic work. You can find such a proof in the original work by A. Robinson:

- A. Robinson, Complete Theories, Studies in Logic, North Holland, 1956

We shall give a proof of using effective quantifier elimination. In 1826, Fourier solved the problem of the existence of a solution for a simultaneous system of linear equations. By that he has proven QE. However, that work had never been published, but was followed by separate works by Dines and Motzkin, who had actually proved the same, giving us the following theorem.

Theorem 34 (Fourier 1826, Dines 1918, Motzkin 1936) *The theory* $Th(\mathfrak{R}_+)$ *admits effective* QE *and hence is complete.*

Proof:
Given a formula $f(\bar{y})$, we first bring it to prenex normal form, and then the QE is applied to the biggest sub formula of f having only one quantifier: $\exists x g(x,\bar{y})$ (without loss of generality). Moreover we can bring g to DNF. The following QE will be applied to a formula g having a single clause. However, it is easily seen that the QE is local, and can be applied to DNF as well. For readability, we use the single clause form. Another issue to point out, is that the atomic sub-formulas within g take the form of $(ux\Delta g'(\bar{y}))$, where $g'(\bar{y})$ doesn't contain x, $u \in \mathbb{N}$, and $Delta \in \{\leq, <, =, >, \geq\}$. This is true since the only operator is $+$. Thus, $g(\bar{y})$ takes the form:

$$\exists x \left(\bigwedge_i t_i(\bar{y})\Delta_i u_i x \wedge \bigwedge_j u_j x \Delta_j t'_j(\bar{y}) \wedge \bigwedge_k s_k(\bar{y})\Delta_k 0 \right) \tag{1}$$

Where $\Delta_i, \Delta_j \in \{\leq, <\}$, and $u_i, u_j \in \mathbb{N}$. But this is equivalent to

$$\exists x \left(\bigwedge_i t_i(\bar{y})\Delta_i u_i x \wedge \bigwedge_j u_j x \Delta_j t'_j(\bar{y}) \right) \wedge \left(\bigwedge_j s_j(\bar{y})\Delta_j 0 \right)$$

But

$$\exists x \left(\bigwedge_i t_i(\bar{y})\Delta_i u_i x \wedge \bigwedge_j u_j x \Delta_j t'_j(\bar{y}) \right)$$

is equivalent to

$$\bigwedge_{i,j} u_j t_i(\bar{y}) \Delta_{i,j} u_i t'_j(\bar{y})$$

where

$$\Delta_{i,j} = \begin{cases} \leq & \text{if both } \Delta_i = \Delta_j = \leq \\ < & \text{if } \Delta_i =< \text{ or } \Delta_j =< \end{cases}$$

Here we eliminated one quantifier $(\exists x)$, and can return to the form in (1). Thus we apply this elimination inductively, until all quantifiers are eliminated. At that point, only comparisons between rational numbers are left - these comparisons are obviously computable $\Box$

The last equivalence in the proof is Fourier's. As seen before, iterations of quantifier eliminations cause an exponential blow-up. However, the existence of the algorithm proves completeness of $Th(\mathfrak{R}_+)$.

5 The reals as an ordered Abelian group, II

Lecture 5, April 7, 2003, 3 hours
Notes by J. Makowsky and A. Magid and Y. Magid

In the last lecture we proved

Theorem 35 *The theory $Th(\mathfrak{R}_+)$*

(i) has QE

(ii) is axiomatized ($= Ded(ODTFAG)$)

(iii) $Th(ODTFAG)$ is complete and decidable

(iv) $Th(\mathfrak{R}_+) = Th(\mathfrak{Q}_+)$

In this lecture we shall look at:

$$\mathbb{Z}_+ = \langle \mathbb{Z}, +, -, <, 0\rangle$$

Theorem 36 (Presburger 1926) *$Th(\mathfrak{Z}_+)$ is decidable*

Theorem 37 (Skolem) *The same (different proof)*

Note: In this case there is no QE. Another example is that $Th(\langle \mathbb{R}, +, -, \cdot, <, 0, 1\rangle)$ has QE, but without the $<$ there is no QE.
$x \geq 0$ iff $\exists y(y^2 \approx x)$
However, we can observe that every formula has an equivalent formula which is a boolean combination of atomic formulas or formulas of the form $\exists y(y^2 \approx t)$.

In order to prove lack of QE we use the following lemma:

Lemma 38 Diagram Lemma: (A. Robinson): *If $Th(\mathfrak{A})$ has QE then $Th(\mathfrak{A}) \cup D(\mathfrak{A})$ is complete, where*

$$D(\mathfrak{A}) = \{B(\bar{a}) : \mathfrak{A} \models B(\bar{a})\}$$

and $B(\bar{a})$ is a basic atomic or negated atomic formula and each a_i is a constant symbol with interpretation i.

Proof:
Assume for contradiction that $T = Th(\mathfrak{A}) \cup D(\mathfrak{A})$ is not complete.
Take $\varphi(\bar{a})$ ($\bar{a}$ constants of diagram) and assume for contradiction that both $T \cup \{\varphi(\bar{a})\}$ and $T \cup \{\neg\varphi(\bar{a})\}$ are satisfiable.
Without loss of generality we can assume that φ is quantifier free (since $Th(\mathfrak{A})$ has QE), and of the form:

$$\bigwedge \bigvee B_i(\bar{a})$$

But for every $B_i(\bar{a})$ we can derive from $D(\mathfrak{A})$ whether it is true or false in contradiction. □

We shall use the above lemma to show that $Th(\langle\mathbb{R}, +, -, \cdot, 0, 1\rangle)$ doesn't have QE. Define

$$T = Th(\langle\mathbb{R}, +, -, \cdot, 0, 1\rangle) \cup D(\langle\mathbb{R}, +, -, \cdot, 0, 1\rangle)$$

Take $\sqrt{2}$ for example. Over the language of fileds, there exists an automorphism which swaps between $\sqrt{2}$ and $-\sqrt{2}$. Therefore T cannot be complete (for example a formula such as

$$\sqrt{2} > 0 : \exists y(y^2 \approx \sqrt{2})$$

cannot be derived from T since otherwise, for the automorphism it would have to hold for $-\sqrt{2}$.

Back to Presburger's theorem. We shall find an axiomatization for $\mathbb{Z}_+$

(a) Abelian group

(b) Ordered group

$$\forall x \forall y((x > 0 \wedge y > 0) \to x + y > 0)$$

$$\forall x \neg((x > 0) \wedge (-x > 0))$$

$$\forall x((x > 0) \vee (x = 0) \vee (-x > 0))$$

(c) The order is discrete

$$\forall x((x > 0) \leftrightarrow (x = 1 \vee (x - 1 > 0)))$$

The above axiomatization will be referred to as *Discrete Ordered Abelian Group (or Disc.OAG).*

Theorem 39 Disc.OAG *(over the language of $\mathbb{Z}_+$) is complete but has no QE.*

Homework 15 *Define*

$$G = (\mathbb{Z} \oplus \mathbb{Z}, +, -, 0, <_G)$$

where $(a, b) >_G (0, 0)$ iff $a > 0 \vee (a = 0 \wedge b > 0)$
Show that G satisfies Disc.OAG

Add $D_n(x)$ "n divides x"

(d_n)

$$\forall x(D_n(x) \leftrightarrow \exists y(x = \underbrace{y + \ldots + y}_{n}))$$

(e_n)

$$\forall x(D_n(x) \vee D_n(x+1) \vee \ldots \vee D_n(x + \underbrace{1 + \ldots + 1}_{n-1}))$$

Theorem 40 *(a) - (e_n) has QE.*

Theorem 41 (Skolem's Theorem) *$Th(\mathfrak{Z}, <, +, 0, 1, q \cdot \bullet, \lceil\bullet\rceil)$ has QE.*

Theorem 42 (Presburger's Theorem) *$Th(\mathfrak{Z}, <, +, 0, 1, \bullet \equiv_n \bullet)$ has QE.*

Project Proposals

- Presburger + Skolem comparison
- Cooper's algorithm for Presburger
- Lower bounds (Fisher Rabin)
- Ferrante - Rackoff algorithm for Presburger
- Lower bounds Fisher - Rabin
- Wu's Geometry
- Simple exponential QE for $\exists \bar{x} B(\bar{x})$ over $\mathfrak{R}$

Improvement for QE Complexity

In the simple method for QE, before each elimination step we have to bring the formula to DNF (since the simple method handles $\exists x(B(x)$ where $B(x)$ is in DNF so that the existential quantifier can be "pushed" inward), which causes an exponential explosion in the formula's size.

New approach: Manipulate only atomic formulas while preserving the formula's boolean structure (up to a small boolean "noise" at the innermost level of the formula), so no repetetive DNF rearrangement is necessary.

For handling $\exists x(D(x, \bar{y})$: Atomic formulas of D are of the following form:

$$\sum \frac{a_i}{b_i} y_i \Delta x, \Delta \in \{<, =, >\}$$

For the 3 types of atomic formulas, we calculate $D_{-\infty}$ and D_{∞} in the following way:

- $x < t$ replace by $true$ for $D_{-\infty}$ and by $false$ for D_{∞}
- $t < x$ replace by $false$ for $D_{-\infty}$ and by $true$ for D_{∞}
- $t = x$ replace by $false$ for both $D_{-\infty}$ and D_{∞}

Now the formula $\exists x(D(x,\bar{y})$ will be replaced by:

$$D_{-\infty} \vee D_{\infty} \bigvee_{t,v \in U} D(\frac{t+v}{2}, \bar{y})$$

which is equivalent (if D is satisfiable then it is satisfiable by either a large enough value of x (∞) or a small enough value of x ($-\infty$), or by a value which is between 2 relevant terms).

The new formula's size:

$$|D_{-\infty}|, |D_{\infty}| = O(|D|)$$

$$|\bigvee_{t,v \in U} D(\frac{t+v}{2}, \bar{y})| = n^2 O(|D|)$$

Therefore the growth in each step is polynomial. For handling universal quantifiers, $\forall x$ is replaced by $\neg \exists x \neg$.

Complexity:
$t_n = (t_{n-1})^2 = (n)^{2^n} \Longrightarrow$ double exponential time.

Homework Solution

- G is an abelian group - immediate
- G is an ordered group:

$$((x_1, x_2) >_G 0 \wedge (y_1, y_2) >_G 0) \Rightarrow$$
$$(x_1 > 0 \vee (x_1 = 0 \wedge x_2 > 0)) \wedge (y_1 > 0 \vee (y_1 = 0 \wedge y_2 > 0))$$
$$\Rightarrow (x_1 + y_1 > 0) \vee (x_1 + y_1 = 0 \wedge x_2 + y_2 > 0) \Rightarrow$$
$$(x_1 + y_1, x_2 + y_2) >_G 0 \Rightarrow$$
$$\forall (x_1, x_2) \forall (y_1, y_2)(((x_1, x_2) >_G 0 \wedge (y_1, y_2) >_G 0)$$
$$\rightarrow (x_1, x_2) + (y_1, y_2) >_G 0)$$

$$((x_1, x_2) >_G 0 \wedge (-x_1, -x_2) >_G 0) \Rightarrow$$
$$(x_1 > 0 \vee (x_1 = 0 \wedge x_2 > 0)) \wedge (-x_1 > 0 \vee (-x_1 = 0 \wedge -x_2 > 0))$$
$$\Rightarrow false \Rightarrow \forall \neg ((x_1, x_2) >_G 0 \wedge (-x_1, -x_2) >_G 0)$$

$\forall (x_1, x_2)((x_1, x_2) >_G 0 \vee (x_1, x_2) = 0 \vee (-x_1, -x_2) >_G 0)$ - immediate

- $<_G$ is a discrete order:

$$\forall (x_1, x_2)((x_1, x_2) >_G 0 \leftrightarrow (x_1 > 0 \vee (x_1 = 0 \wedge x_2 > 0))$$
$$\leftrightarrow ((x_1, x_2) = (1, 0) \vee (x_1, x_2) - (1, 0) >_G 0))$$

6 $\mathbb{R}^2$ and Euclidean Geometry

Lecture 6, April 28, 2003, 2 hours
Notes by J. Makowsky and A. Magid and Y. Magid

How can we justify the connection between $\mathbb{R}^2$ and Euclidean Geometry?
In Geometry the basic objects are:
points A,B,C,...
lines e,f,g,h,...

In $\mathbb{R}^2$ these objects can be interpreted as:
points $\{(x, y)\}$
lines $\{(x, y) : ax + b = y\}$

In Geometry:
$A \in l$ (A is incident to l)
The distance between A and B "dist(A,B) is a number"

We would like to take the model of Euclidean Geometry and find (interpret) it in fields.

Dist in $\mathbb{R}^2$:

$$dist((x_1, y_1), (x_2, y_2)) = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$$

We would like to show that every axiom in Euclidean Geometry , when interpreted into $\mathbb{R}^2$, will be provable in $\mathbb{R}^2$ i.e -

Theorem 43 *Every translation of a Euclidean Geometry axiom is provable from RCF.*

Note: $\sqrt{}$ is not a part of the language but it can be eliminated by using the square function (writing formulas concerning $dist^2$ instead of dist). Also , it is definable by a quantified formula for which the quantifier can be eliminated by using QE (since RCF has QE).

Example 1:

Let g , g' be lines and O , E , A , B be points such that $O \in g$, $E \in g$, $A \in g$, $B \in g$ as drawn in figure 1. We would like to find the point $A + B$ using a Geometrical method:
Choose E' on g'.
Draw h such that h is a line and $E' \in h$ and h is parallel to g.
Draw the line $E'A$
Draw the line AC such that $c \in h$ and AC is parallel to g'.
Draw the line CR such that $R \in g$ and CR is parallel to $E'A$.
The point R is the required point which its distance is $A + B$.

Note: The location of the point R should not depend on the choice of E'.

Example 2:

This time we would like to use a Geometrical method in order to calculate the point $A \cdot B$:
Draw the line EE' such that $E' \in g'$.

Draw the line $E'A$.
Draw the line BC such that $C \in g'$ and BC is parallel to EE'.
Draw the line CR such that $R \in g$ and CR is parallel to $E'A$.
The point R is the required point which its distance is $A \cdot B$.

Geometrical Axioms:

$I_1 I_2$ $A \neq B \rightarrow \exists! a(A \in a \wedge B \in a)$
There exists only one line between two different points (and the other way around).

I_3 $\forall a \exists A \exists B(A \neq B \wedge A \in a \wedge B \in A)$
$\wedge \exists A \exists B \exists C \neg \exists a(A \in a \wedge B \in a \wedge C \in A)$
For each line there exists at least 2 points which are on it, and there exist 3 points which are not on any common line.

The definition of $a || b$:

$$\exists A(A \in a \wedge A \in b) \rightarrow a = b$$

I_4 $\forall a \forall A(\neg(A \in a) \rightarrow \exists! b(A \in b \wedge a || b))$
For each line and a point which is not on it, there exists exactly one line parallel to the first which goes through the point.

Let's define a relation: ABC := "B lies between A and C", $B \neq A$, $B \neq C$.
Now we will define another group of axioms:

II_1 $ABC \rightarrow CBA \wedge \exists a(A \in a \wedge B \in a \wedge Cina) \wedge A \neq B \wedge B \neq C \wedge A \neq C$

II_2 $A \neq B \rightarrow \exists C(ABC)$

II_3 $ABC \rightarrow \neg ACB \wedge \neg BAC$

II_4 (Pasch)

$$[\neg \exists x(A \in x \wedge B \in x \wedge C \in x) \wedge \neg(A \in a) \wedge \neg(B \in a) \wedge \neg(C \in a) \wedge D \in a \wedge ADB]$$
$$\rightarrow \exists E(E \in a \wedge AEC) \vee \exists F(F \in a \wedge BFC)$$

7 Geometry and Algebra, II

Lecture 7, May 5, 2003, 3 hours
Notes by J. Makowsky and D. Zeitlin.

In this lecture we follow

Hart Robin Hartshorne, Geometry: Euclid and Beyond, Springer, 2000

Chou Shang-Ching Chou, Mechanical Geometry Theorem Proving, Reidel, 1988

Wu Wen-tsün Wu, Mechanical Theorem Proving in Geometries, Springer 1994

We continue the discussion on how Geometry is related to Algebra.

7.1 Atomic relations

Unary predicates Lines L, and points P.

Incidence $A \in l$ stands for "the point A is on the line l", for $l \in L$ and $A \in P$.

Betweenness $B(A, B, C)$ stands for "A, B, C are on the same line and B lies between A and C".

Equidistance $E_1(A, B, C, D)$ stand for "the distance between A and B equals the distance between C and D".

Equiangularity $E_2(A, B, C, D, E, F)$ stand for "the angle between A, B, C and D, E, Foare the same".

Orthogonality $E_3(l_1, l_2)$ stands for " the lines l_1 and l_2 are orthogonal".

In Hilbert's Geometry we have besides incidence $\in$ the relations betweenness B, and E_1 and E_2. This vocabulary is denoted by $\tau_{Hilbert}$.

In Wu's Geometry we have besides incidence $\in$ the relations E_1 and E_3. This vocabulary is denoted by τ_{Wu}.

The vocabulary consisting of incidence and E_1 alone is denoted by τ_0.

7.2 List of Axioms

Incidence Axioms

(I1)
(I2)
(I3)

Parallel Axiom

(P)

Betweenness Axioms

(B1)
(B2)
(B3)
(B4)

Congruence Axioms, segments

(C1)
(C2)
(C3)
(Desargues)
(Pappus)

Congruence Axioms, angles

(C4)
(C5)
(C6)

Circle Intersection Axiom Stated in [Hart], page 108.

(E) Given two circles Δ and Γ such that Δ has both points inside Γ and outside Γ, then $\Delta \cap \Gamma \neq \emptyset$.

Orthogonality Axioms These are stated in [Wu], pages 71-72.

(O1)
(O2)
(O3)
(O4)
(O5)

Midpoint Axioms These are stated in [Wu], pages 91-95. Axiom (T) is called there (δ').

(S): Axiom of symmetric axis.
(T): Axiom of transposition.

Infinity

(Inf) Axiom of infinity
(D) Dedekind's Axiom:

$$\exists z \forall xy\, (x \in X \wedge y \in Y \rightarrow B(z, x, y)) \rightarrow \exists z \forall xy\, (x \in X \wedge y \in Y \rightarrow B(x, z, y))$$

(FOL-D) Dedekind's Axiom for FOL-definable sets:
For every $\tau_{Hilbert}$-formulas ϕ, ψ

$$\exists z \forall xy\, (\phi(x) \wedge \psi(y) \rightarrow B(z, x, y)) \rightarrow \exists z \forall xy\, (\phi(x) \wedge \psi(y) \rightarrow B(x, z, y))$$

(A) Archimedian Axiom

Definition 44

(i) *A* Hilbert plane *is $\tau_{Hilbert}$-structure which satisfies (I1-I3), (B1-B4) and (C1-C6).*

(ii) *A* Euclidean plane *is Hilbert plane which satisfies additionally (P) and (E).*

(iii) *A* Pappus plane *is τ_0-structure which satisfies (I1-I3), (P), (Pappus), (Inf). This is also called a model of affine geometry.*

(iv) *A* orthogonal Wu plane *is τ_{Wu}-structure which satisfies (I1-I3), (P), (Desargues), (O1-O5), (Inf).*

(v) *A* metric Wu plane *is τ_{Wu}-structure which satisfies (I1-I3), (P), (Desargues), (O1-O5), (Inf), (S) and (T).*

7.3 Geometry and fields

Given a field F we define the standard geometry over F, or the Cartesian Plane Π_F, where points are in F^2 and lines are defined by linear equations $ax + by + c = 0$.

Proposition 45
If F is any field, then Π_F satisfies (I1-I3) and (P).

Given a model of geometry, we choose a points O and 1, we can define addition and multiplcation using segment arithmetic, which gives us a standard number system.

In [Hart] propositions 15.4, 19.2 and 19.3 we have

Theorem 46

(i) *In any Hilbert plane with (P) the standard number system is a field of characteristic 0 which can be unquely ordered such that it is an ordered field.*

(ii) *The ordered field is archimedian iff the geometry satisfies additionally the Archimedian axiom.*

(iii) *The ordered field is Dedekind complete iff the geometry satisfies additionally Dedekind's axiom (D).*

Theorem 47 (Tarski)
In any Hilbert plane with (P) the standard number system is a real closed (ordered) field iff the geometry satisfies (FOL-D).

Theorem 48 (Schur 1903)
In an orthogonal Wu plane the standard number system is a (commutative) field.

Theorem 49
In a Pappus plane the standard number system is a a commutative field of characteristic 0*. Conversely, in every commutative field of characteristic* 0 *the standard geometry is a Pappus plane.*

In [Chou], page 39, we have:

Theorem 50 (Wu, Chou)
In a metric Wu plane the standard number system is a pythagorean[2] *field , i.e. a fileds which satisfies the Pythagorean axiom*

$$\forall x, y \exists z (x_2 + y + 2 = z_2).$$

Conversely, in every pythagorean field the standard geometry is a metric Wu plane.

[2] In [Wu] and [Chou] this is called a Hilbert field.

8 Decidability of Geometry, I

Lecture 8, May 12, 2003, 3 hours
Notes by J. Makowsky and A. Magid and Y. Magid

In this lecture we follow

- M. Ziegler, Einige unentscheidbare Körpertheorien, in Logic and Algorithmic, An international Symposium held in honour of E. Specker, E. Engeler, H. Läuchli, V. Strassen, eds. L'enseignement mathématique, 1982, pp. 381-392
- [Wu], [Chou], [Hart]
- Bhubaneswar Mishra, Algorithmic Algebra, Springer 1993

8.1 Reduction

From the previous lectures we can now get the following translations.

Given a $FOL(\tau_{Wu})$-formula ϕ we can define inductively a $FOL(\tau_{field})$-formula $tr_1(\phi)$.

(i) Equality between points $P = (p_1, p_2), Q = (q_1, q_2)$:

$$p_1 = q_1 \wedge p_2 = q_2$$

(ii) Equality between lines $l_1 = (a_1, b_1, c_1), l_2 = (a_2, b_2, c_2)$:

$$\exists d(da_1 = a_2 \wedge db_1 = b_2 \wedge dc_1 = c_2)$$

(iii) Incidence $P \in l_1$:

$$a_1p_1 + b_1p_2 + c_1 = 0$$

(iv) Equidistance $AB = CD$:

$$(a_1 - b_1)^2 + (a_2 - b_2)^2 = (c_1 - d_1)^2 + (c_2 - d_2)^2$$

(v) Orthoganility $l_1 \perp l_2$:

$$a_1a_2 + b_1b_2 = 0$$

(vi) Boolean operations and quantifiers:

$$tr_1((\phi_1 \wedge \phi_2)) = (tr_1(\phi_1) \wedge tr_1(\phi_2))$$
$$tr_1((\phi_1 \vee \phi_2)) = (tr_1(\phi_1) \vee tr_1(\phi_2))$$
$$tr_1(\neg\phi_1) = \neg tr_1(\phi_1)$$
$$tr_1(\exists x\phi_1) = \exists x tr_1(\phi_1)$$
$$tr_1(\forall x\phi_1) = \forall x tr_1(\phi_1)$$

Conversely, Given a $FOL(\tau_{field})$-formula ϕ we can define inductively a $FOL(\tau_{Wu} \cup \{0,1\})$-formula $tr_2(\phi)$. The elements of the field are equivalence classes of line segments of equal length.

(i) Equality:

$$E_1(A, B, C, D)$$

(ii) Addition: Use the construction discussed in the previous lectures in order to construct a line segment of length x+y.

(iii) Multiplication: Use the construction discussed in the previous lectures in order to construct a line segment of length xy.

(iv) Boolean operations as for tr_1.

Exercise 51
Formulate the corresponding translation between formulas for a Hilbert plane and formulas of ordered fields, tr_1^H, tr_2^H.

Theorem 52
Let ϕ be a $FOL(\tau_{field})$-formula and let ψ be a $FOL(\tau_{WU})$-formula. Denote by F_{pyth} the axioms of pythagorean fields of characteristic 0 and by G_{Wu} the axioms of the metric Wu plane.

(i) $F_{pyth} \vdash \phi$ iff $G_{Wu} \vdash tr_1(\phi)$.

(ii) $G_{Wu} \vdash \psi$ iff $F_{Pyth} \vdash tr_2(\psi)$.

Proof:
□

Theorem 53
Let ϕ be a $FOL(\tau_{ofield})$-formula and let ψ be a $FOL(\tau_{Hilbert})$-formula. Denote by RCF the axioms of real closed fields, and by G_{Euclid} the axioms of the Euclidean plane.

(i) $RCF \vdash \phi$ iff $G_{Euclid} + (FOL - D) \vdash tr_1(\phi)$.

(ii) $G_{Euclid} + (FOL - D) \vdash \psi$ iff $RCF \vdash tr_2(\psi)$.

Proof:
□

8.2 Decidability of the theory of fields

How can we now mechanize Geometry? By mechanizing the Algebra of various Fields. Is this possible? Not always.

Let Σ be a set of $FOL(\tau)$-sentences. We denote by

$$Ded(\Sigma) = \{\phi \in FOL(\tau) : \Sigma \vdash \phi\}$$

and

$$Conseq(\Sigma) = \{\phi \in FOL(\tau) : \Sigma \models \phi\}$$

$Ded(\Sigma) = Conseq(\Sigma)$ by the Completeness Theorem of First Order Logic. The Completeness Theorem also gives: If Σ is semi-computable or computable then $Ded(\Sigma) = Conseq(\Sigma)$ is semi-computable. But in general $Ded(\Sigma)$ need not be computable.

Definition 54
Σ is decidable *if $Ded(\Sigma)$ is computable. Otherwise, Σ is called* undecidable.

Theorem 55 (Julia Robinson, 1949)
The following are undecidable.

(i) The theory of fields.

(ii) The theory of fields of characteristic 0.

(iii) The theory of ordered fields.

Theorem 56 (Tarski, 1931, 1948)
The following are decidable.

(i) The theory of algebraic closed fields of characteristic 0.

(ii) For every prime p, the theory of algebraic closed fields of characteristic p.

(iii) The theory of real closed fields.

Theorem 57 (Ziegler, 1982)

(i) Let T be a finite set of τ_{field}-sentences which has an algebraic closed field as model. Then T is undecidable.

(ii) Let T be a finite set of τ_{ofield}-sentences which has a real closed field as model. Then T is undecidable.

Corollary 58
The following theories are undecidable;

(i) The theory of orthogonal Wu planes.

(ii) The theory of metric Wu planes.

(iii) The theory of Hilbert planes.

(iv) The theory of Euclidean planes.

8.3 The form of geometric theorems

However, geometric theorems have a rather simple structure.

We are given a construction of points $P_1, P_2, \ldots, P_n$ and lines $l_1, l_2, \ldots, l_m$ using ruler and compass. The theorem then asserts that a subset of points either meet, are colinear or cocircular, a subset of lines either meet, are parallel or perpendicular, or a subset of pairs of points are pairwise equidistant.

Translating this into the language of (ordered) fields we get a formula of the form

$$\forall \bar{x} \bigwedge_{i \in I} f_i(\bar{x}) = 0 \wedge \bigwedge_{j \in J} h_j(\bar{x}) \neq 0 \rightarrow g(\bar{x}) = 0$$

Here the f_i, h_j, g are polynomials of degree 2. In particular, the statement is of the form $\forall \bar{x} \Phi(\bar{x})$, with Φ quantifier free.

Problem 59
What happens when we allow marked ruler in the construction?

We denote by $\forall FOL(\tau)$ the set of universal $FOL(\tau)$-sentences, i.e., the set of formulas of the form $\forall \bar{x} \Phi(\bar{x})$, with Φ quantifier free. We denote by

$$\forall Ded(\Sigma) = \{\phi \in \forall FOL(\tau) : \Sigma \vdash \phi\}.$$

Denote by ACF_0 (ACF_p) the theory of algebaric closed fields of charactersitic 0 (p).

Theorem 60 (JAM)
Let T be a set of τ_{field}-sentences (τ_{ofield}-sentences) and let ϕ be a universal τ_{field}-sentence (τ_{ofield}-sentence).

(i) If T has an algebraic closed field as model, then

$$T \vdash \phi \text{ iff } ACF_0 \vdash \phi.$$

(ii) If T has a real closed field as model, then

$$T \vdash \phi \text{ iff } RCF \vdash \phi.$$

In particlar, in both cases $\forall Ded(T)$ is decidable.

Proof:
We first prove (i).

Let $T \vdash \phi$. As ACF_0 is complete, and there is a model $\mathfrak{A} \models T$ such that also $\mathfrak{A} \models ACF_0$, we have that $ACF_0 \vdash T$. So $ACF_0 \vdash \phi$.

Conversely, assume $T \not\vdash \phi$. Then there is a model $\mathfrak{A} \models T$ such that $\mathfrak{A} \models \neg\phi$. Let $\bar{\mathfrak{A}}$ be the algebraic closure of $\mathfrak{A}$. This exists by the classic result of Steinitz. $\bar{\mathfrak{A}} \models ACF_0$, and hence $\bar{\mathfrak{A}} \models T$ by the hypothesis.

Now we use that ϕ is universal, and hence $\neg\phi$ is existential. As $\mathfrak{A} \models \neg\phi$, and $\mathfrak{A} \subseteq \bar{\mathfrak{A}}$ we have also $\bar{\mathfrak{A}} \models \neg\phi$. By the completeness of ACF_0 we get So $ACF_0 \vdash \neg\phi$.

The proof of (ii) is similar. We just need that RCF is complete, and that every ordered field has a real closure. □

8.4 Complexity

Here we suppose that the reader is familiar with the course Computability over the Reals.

The Turing Model - A binary world. Too low level.
We would like to define what is an *Algorithm over* $\mathbb{R}, \mathbb{C}$. There are several variations. One of the problems is whether or not we can use equality between reals as a subroutine.

For defining an algorithm we use the *BSS Model.* There are two representations for a BSS Machine:

- A Flow Chart
- A sequence of Register Machine Instructions (with ∞ registers, each holding a real number, no indirect addressing).

Accordingly, $P_{\mathbb{R}}, NP_{\mathbb{R}}, P_{\mathbb{C}}, NP_{\mathbb{C}}$ were defined and the following problems discussed:

- $P_{Turing} = P_{\mathbb{Z}_2}$
- $NP_{Turing} = NP_{\mathbb{Z}_2} \subseteq EXPT_{Turing}$
- $NP_{\mathbb{R}} \overset{?}{\subseteq} EXPT_{\mathbb{R}}$
- $NP_{\mathbb{R}} \overset{?}{\subseteq} COMP_{\mathbb{R}}$

The last two problems turned out to be significant problems.

Theorem 61 (Tarski) *QE over* $\mathbb{R} \Rightarrow NP_{\mathbb{R}} \subseteq COMP_{\mathbb{R}}$

Theorem 62 (Gregoriev - Heintz - Ronegar) *QE over* $\mathbb{R} \Rightarrow NP_{\mathbb{R}} \subseteq EXPT_{\mathbb{R}}$

Uriel G. Rothblum and B. Curtis Eaves:
Linear Algorithm $\leftrightarrow$ Linear Problem

In a similar way we can try to define an *Elementary Geometrical Algorithm (Ruler + Compass Alg.)* and an *Elementary Geometrical Problem* and try to find an equivalence between them.
Instead of the Reals we would start with *Euclidean Geometry.*
For tests we will use the relations which were defined in the previous lectures.
Instructions would be line intersections, drawing of a circle, ... Instead of variables we have Points.

An algorithm can be represented as a flow chart, and we can inductively classify the formulas which can be derived from such programs.

We can also discuss complexity:
NP in Geometry: Assuming a set of Points, guess another set of points, such that a construction is formed. In some cases the resulting constructions will be invariant to the guesses.

Are there NP Complete problems? The assumption is that there are.

8.5 Homework Solution

Given a $FOL(\tau_{Hilbert})$-formula ϕ we can define inductively a $FOL(\tau_{field})$-formula $tr_1^H(\phi)$.

(i) Equality between points $P = (p_1, p_2), Q = (q_1, q_2)$:

$$p_1 = q_1 \wedge p_2 = q_2$$

(ii) Equality between lines $l_1 = (a_1, b_1, c_1), l_2 = (a_2, b_2, c_2)$:

$$\exists d(da_1 = a_2 \wedge db_1 = b_2 \wedge dc_1 = c_2)$$

(iii) Incidence $P \in l_1$:

$$a_1p_1 + b_1p_2 + c_1 = 0$$

(iv) Equidistance $AB = CD$:

$$(a_1 - b_1)^2 + (a_2 - b_2)^2 = (c_1 - d_1)^2 + (c_2 - d_2)^2$$

(v) Equiangular $ABC = DEF$:

$$\sin(ABC) = \sin(DEF) \wedge \cos(ABC) = \cos(DEF)$$

where the $\sin(ABC)$ and $\cos(ABC)$ will be calculated by finding the line $l = (x, y, z)$ such that $A \in l$ and $l \perp BC$ (defined as for the translation from $FOL(\tau_{Wu})$-formulas), finding the intersection point between l and BC, O_1 and then:

$$\sin(ABC) \overset{\text{def}}{=} \frac{AO_1}{AB}$$
$$\cos(ABC) \overset{\text{def}}{=} \frac{BO_1}{AB}$$

(vi) Betweeness $B(A, C, D)$:

$$(\exists l(A \in l \wedge C \in l \wedge D \in l) \wedge (a_1 < c_1) \wedge (c_1 < d_1))$$

where $P \in l$ is translated as shown above.

(vii) Boolean operations and quantifiers:

$$
\begin{aligned}
tr_1^H((\phi_1 \wedge \phi_2)) &= (tr_1^H(\phi_1) \wedge tr_1^H(\phi_2)) \\
tr_1^H((\phi_1 \vee \phi_2)) &= (tr_1^H(\phi_1) \vee tr_1^H(\phi_2)) \\
tr_1^H(\neg\phi_1) &= \neg tr_1^H(\phi_1) \\
tr_1^H(\exists x \phi_1) &= \exists x tr_1^H(\phi_1) \\
tr_1^H(\forall x \phi_1) &= \forall x tr_1^H(\phi_1)
\end{aligned}
$$

Conversely, Given a $FOL(\tau_{field})$-formula ϕ we can define inductively a $FOL(\tau_{Hilbert} \cup \{0,1\})$-formula $tr_2^H(\phi)$. The elements of the field are equivalence classes of line segments of equal length.

(i) Equality:

$$E_1(A, B, C, D)$$

(ii) Addition: Use the construction discussed in the previous lectures in order to construct a line segment of length x+y.

(iii) Multiplication: Use the construction discussed in the previous lectures in order to construct a line segment of length xy.

(iv) Boolean operations as for tr_1^H.

9 Proving Geometric Theorems

Lecture 9, April 19, 2003, 3 hours
Notes by J. Makowsky and E. Talmor.

9.1 Introduction

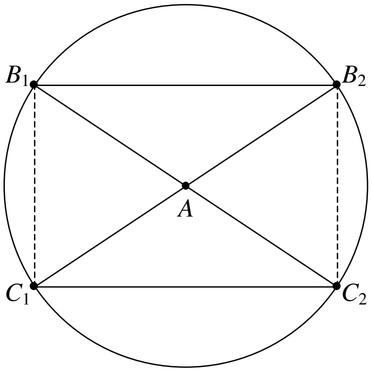
This lecture will deal with some notion of "common" geometry, i.e. proving geometric theorems having a very limited use of quantifiers. Such a theorem consists of:

(i) An independent set of points and lines. For example, an independent set of three points A, B, and C, (also known as a set in general position) admits that the points are not co-linear, and that there is no right angle formed between them. If we now add a line, it cannot be independent of the choice of A, B, and C, because it may or may not separate the points between the two half planes it forms.

(ii) All points where circles and lines intersect with other objects.

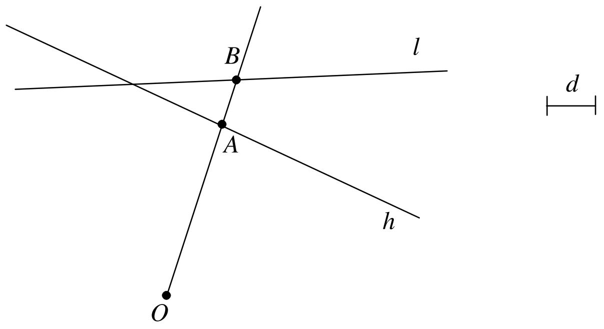
(iii) Objective: Prove that if for a configuration some equations hold, then some more equations hold.

For example:



Choose an independent point A as a circle center. Now B_1, B_2, C_1, C_2, are not independent. Prove that if $\overline{B_1B_2} = \overline{C_1C_2}$, then $\overline{B_1C_1} = \overline{B_2C_2}$

Another example, is the "marked ruler":



Given O, l, h, d find A, B such that $A \in h$, $B \in l$, $\overline{AB} = d$, $A \in \overline{OB}$.

Generally, these problems translated to coordinates have the following structure:

$$\forall \bar{x} \Bigg(\underbrace{\bigwedge_{i \in I} (f_i(\bar{x}) = 0) \wedge \bigwedge_{l \in L} (s_l(\bar{x}) \neq 0)}_{\text{configuration}} \Longrightarrow \Big(\bigwedge_{j \in J} (y_j(\bar{x}) = 0) \Rightarrow h(\bar{x}) = 0 \Big) \Bigg)$$

where f_i, s_l, y_j, h are all quadratic polynomials. Consider the following logical equalities:

$$\begin{array}{l} A \Rightarrow (B \Rightarrow C) = \neg A \vee (B \Rightarrow C) = \\ \neg A \vee (\neg B \vee C) = (\neg A \vee \neg B) \vee C = \\ \neg (A \wedge B) \vee C = (A \wedge B) \Rightarrow C \end{array}$$

Then we can rewrite the problem structure as

$$\forall \bar{x} \Bigg(\text{quadratic equalities and inequalities} \Longrightarrow \text{quadratic equality} \Bigg)$$

9.2 Restricted Decidability

In the previous lecture we have seen that TH(Euclidean Field) is undecidable. However, we have the following

Theorem 63 *$Ded_{\forall}$(Euclidean Field) is decidable.*

Where $Ded_{\forall}$(Euclidean Field) is the collection of all formulas of the form

$$\forall \bar{x} \Bigg(\text{polynomial equalities and inequalities} \Longrightarrow \text{polynomial equality / inequality} \Bigg)$$

but we shall prove the following stronger theorem.

Theorem 64 *For all formulas φ of the form described in theorem 63* *(i)* $ACF_0 \models \forall\bar{x}\varphi(\bar{x})$ *iff*

(ii) Pythagorean Field $\models \forall\bar{x}\varphi(\bar{x})$ *iff*

(iii) $T \models \forall\bar{x}\varphi(\bar{x})$, *where* $T \cup AFC_0$ *is satisfiable, and every model* $\mathfrak{A}$ *of* T *has an extension* $\mathfrak{B}$, $\mathfrak{A} \subseteq \mathfrak{B} \models ACF_0$.

We have shown previously, using Vaught's Test, and a theorem by Stienitz that ACF_0 is complete, and hence decidable. Therefore, given theorem 64, the automated theorem proving algorithm for ACF_0 can be used to prove (or disprove) anything in T.

Let us recall that in a pythagorean field, $\forall xy\exists z(x^2 + y^2 = z^2)$.

Observation 65 $ACF_0 \models$ *Pythagorean Field.*

Proof: It is obvious that $F \models$ field. So we have to show that $ACF_0 \models \forall xy\exists z(x^2+y^2-z^2 = 0)$. Take any specific x,y and expand the dictionary τ with a new constant c, where $c = x^2+y^2$. Let τ' be this expanded dictionary. So with τ', $ACF_0 \models \exists z(c - z^2 = 0)$, because the field is algebraically closed. Therefore, with τ, $ACF_0 \models \exists z(x^2+y^2-z^2 = 0)$, and thus $ACF_0 \models \forall xy\exists z(x^2+y^2-z^2 = 0)$ □

This gives us (i)⇒(ii) for theorem 64.

Observation 66 $T \models \forall\bar{x}\varphi(\bar{x}) \Rightarrow AFC_0 \models \forall\bar{x}\varphi(\bar{x})$.

Proof: We know that ACF_0 is decidable, and that $T \cup ACF_0$ is satisfiable. Therefore, $ACF_0 \models T$. Therefore $T \models \forall\bar{x}\varphi(\bar{x}) \Rightarrow AFC_0 \models \forall\bar{x}\varphi(\bar{x})$ □

This gives us (iii)⇒(i).

Now, for (i)⇒(iii), we assume that in ACF_0, $\forall\bar{x}\varphi(\bar{x})$ holds. We want to show that it holds in T as well. The following observation will aid us:

Observation 67 (Tarski) *Let* $\mathfrak{A} \subseteq \mathfrak{B}$, *be* τ *structures, i.e.* $\mathfrak{A}$ *is a substructure of* $\mathfrak{B}$ *(with the same relations, and function closure). Then*

$$\mathfrak{B} \models \forall\bar{x}\varphi(\bar{x}) \Rightarrow \mathfrak{A} \models \forall\bar{x}\varphi(\bar{x})$$

and

$$\mathfrak{A} \models \exists\bar{x}\psi(\bar{x}) \Rightarrow \mathfrak{B} \models \exists\bar{x}\psi(\bar{x})$$

where φ, ψ *are quantifier free, and* FOL.

Proof: This is simply because if there is an $\bar{x}$ in $\mathfrak{A}$ that satisfies ψ, then $\bar{x}$ is in $\mathfrak{B}$ as well. If all members in $\mathfrak{B}$ satisfy φ, then all members of $\mathfrak{A}$ satisfy φ as well, since they are included □

Lemma 68 *$ACF_0 \models \forall\bar{x}\varphi(\bar{x}) \Longrightarrow T \models \forall\bar{x}\varphi(\bar{x})$*

Proof: Now assume for contradiction that (i)$\not\Rightarrow$(iii). So we want to show: if $T \cup (\exists\bar{x}\neg\varphi(\bar{x}))$ is satisfiable, then $ACF_0 \cup (\exists\bar{x}\neg\varphi(\bar{x}))$ is satisfiable. This will contradict the assumption of (i) : $ACF_0 \models \forall\bar{x}\varphi(\bar{x})$. $T \cup (\exists\bar{x}\neg\varphi\bar{x})$ is satisfiable. Therefore, there is a model $\mathfrak{A} \models T \cup (\exists\bar{x}\neg\varphi(\bar{x}))$. by assumption (iii) of theorem 64 there is an extension $\mathfrak{B}$, $\mathfrak{A} \subseteq \mathfrak{B} \models ACF_0$. From observation 65, $\mathfrak{A} \models \exists\bar{x}\neg\varphi(\bar{x}) \Rightarrow \mathfrak{B} \models ACF_0 \cup (\exists\bar{x}\neg\varphi(\bar{x}))$. Therefore, $ACF_0 \cup (\exists\bar{x}\neg\varphi\bar{x})$ is satisfiable. □

It is left to show that (ii)$\Rightarrow$(i), i.e. that every pythagorean field has an extension $\mathfrak{B} \models ACF_0$. This follows from a more general theorem which we will not prove here:

Theorem 69 *Every field $\mathfrak{A}$ of characteristic 0, has an extension $\mathfrak{B} \models ACF_0$.*

This completes the proof of Theorem 64.
Next, we can prove a similar theorem to theorem 64

Theorem 70 *For all formulas φ of the form described in theorem 63*

(i) $RCF_0 \models \forall\bar{x}\varphi(\bar{x})$ iff

(ii) Euclidean Field $\models \forall\bar{x}\varphi(\bar{x})$ iff

(iii) $T \models \forall\bar{x}\varphi(\bar{x})$, where $T \cup RFC_0$ is satisfiable, and every model $\mathfrak{A}$ of T has an extension $\mathfrak{B}$, $\mathfrak{A} \subseteq \mathfrak{B} \models RCF_0$.

Similar to Observation 65, we first prove the $RCF \models$ Euclidean Field. The proof goes along the same lines: $F \models$ Field trivially. Then we show that $RCF \models \forall x > 0 \exists y(x = y^2)$, by the same technique of adding a constant $c = x$ to the dictionary τ and then showing that $\exists y(c - y^2 = 0)$ due to the RCF etc... We would also use a similar theorem to theorem 69: every ordered field has an extension $\mathfrak{B} \models RCF$. We use Wu field to prove the ACF_0 version of the theorem, and Hilbert for the RCF version.

It would have been more straight forward to work on the real field, instead of RCF, and indeed Hilbert tried to define the axioms for a field being exactly $\mathbb{R}$. However, Tarski has shown that it was impossible in FOL, and therefore settled with the definition of RCF, using Dedekind's Axiom (field version given here):

$$\begin{aligned}\forall XY \quad \big((\forall x \in X \forall y \in Y(x < y)) \wedge (\forall x \in X \exists x' \in X(x < x')) \wedge \\ (\forall y \in Y \exists y' \in Y(y' < y)) \\ \Longrightarrow \exists z(\forall x \in X(x < z) \wedge \forall y \in Y(z < y))\big)\end{aligned}$$

This definition is clearly second order logic. The FOL alternative, is to define a (infinite) set of axioms, for any two sets X Y, with functions $\varphi(x)$, and $\psi(y)$ replacing $x \in X$, and $y \in Y$ respectively. Using such a definition, we have $Ded_{\varphi,\psi}$ in FOL.

9.3 Quadratic is Good Enough

Now we shall justify the restriction of our geometric problems to quatratic polynomials. Again, the general form is:

$$\forall x\Big(\bigwedge_{i,j}((f_i(\bar{x})=0)\wedge(g_j(\bar{x})\neq 0))\Rightarrow h(\bar{x})\Big)$$

Now, take for example the polynomial equality $x^3 f(\bar{z}) = 0$. By adding quantified variables, we can reduce the degree of x:

$$\begin{aligned} x^3 f(\bar{z}) = 0 \quad &\Leftrightarrow \quad \exists u(x^2 = u \wedge uxf(\bar{z}) = 0) \\ &\Leftrightarrow \quad \exists uu'(x^2 = u \wedge u' = ux \wedge uf(\bar{z}) = 0) \end{aligned}$$

For an inequation $g(\bar{x}) \neq 0$, we replace it with $\exists u''(g(\bar{x})u'' = 1)$. Thus, if there is a good algorithm for quadratic polynomials, there is a good algorithm for higher degree polynomials as well.

For Wu geometry

$$\begin{aligned} &\neg\forall\bar{x}\big(\bigwedge f_i(\bar{x}) = 0 \Rightarrow h(\bar{x}) = 0\big) \\ &\Leftrightarrow \exists\bar{x}\neg\big(\neg\bigwedge f_i(\bar{x}) = 0 \vee h(\bar{x}) = 0\big) \\ &\Leftrightarrow \exists\bar{x}\big(\neg\neg\bigwedge f_i(\bar{x}) = 0 \wedge h(\bar{x}) \neq 0\big) \\ &\Leftrightarrow \exists\bar{x}, u\big(\bigwedge f_i(\bar{x}) = 0 \wedge uh(\bar{x}) - 1 = 0\big) \end{aligned}$$

9.4 Evaluating the Quadratic Equations

Finally we want to know how to actually determine whether a solution to a set of quadratic equations exists. For instance, we would like to know whether $\exists xy(x^2 + xy + y = 0 \wedge 2x^2 + 3y^2 = 0)$. If y is constant, we have a quadratic equation in one variable (x), thus we can solve it. If we have a linear set of equations, i.e. $\bigwedge_{j\in J}\sum_i a_{ij}x_i = b_j$, we can rewrite it as $A\bar{x} = \bar{b}$ where A is an $n \times n$ matrix, without loss of generality. A set of equations is solvable if the resolvent suffices certain conditions. The resolvent of a set of linear equations relates to the determinant. Thus a non constructive method for determining solvability is defined by $\exists\bar{x}A\bar{x} = \bar{b}$ iff $\det(A) \neq 0$. Gauss gave a constructive method in the 19th century - Gauss Elimination - by triangulating the matrix A.

For non linear equations, Hilbert's Nullstellensatz provides a non constructive method. Later on, G. Hermans offered a constructive method (based on works of Nöthe and Hilbert as well). Solutions for ACF_0: Grother Basis (1970), Wu-Riff method. RCF poses a harder problem, and two important works should be mentioned here: Collins - Cylindric Algebraic Decomposition, and Strum - Sequences (1860).