# Topics in Automated Theorem Proving

## Course (236714, 2013/14)

Johann A. Makowsky*

* Faculty of Computer Science,
Technion - Israel Institute of Technology,
Haifa, Israel
janos@cs.technion.ac.il

Course homepage
http://www.cs.technion.ac.il/~janos/COURSES/THPR

# Lecture 8:

---

## The field of complex numbers $\langle \mathbb{C}, +, -, \times, ^{-1}, 0, 1 \rangle$ allows elimination of quantifiers

---

A. Tarski (1948); M. Chevalley (1955)
The proof here is after
G. Kreisel and J.-L. Krivine (1966)
and D. Delahaye and M. Mayero (2006)

# Fields $\mathcal{K} = \langle K, +, -, \times, 0, 1\rangle$ without $^{-1}$

$+$ and $\times$ are binary function symbols, $0, 1$ are constant symbols, and $-$ is a unary function symbol. We may include the unary function symbol $^{-1}$ with $\forall x(x = 0 \lor (x \times x^{-1} = 1))$.
We will later write $xy$ for $(x \times y)$

**Two elements:** $0 \neq 1$

**Associativity:**

$\forall x \forall y \forall z(x + (y + z) = (x + y) + z)$
$\forall x \forall y \forall z(x \times (y \times z) = (x \times y) \times z)$

**Commutativity:**

$\forall x \forall y(x + y = y + x)$
$\forall x \forall y(x \times y = y \times x)$

**Distributivity:**

$\forall x \forall y \forall z(x \times (y + z) = (x \times y) + (x \times z))$

**Inverses:**

$\forall x(x + 0 = x)$
$\forall x(x + (-x) = 0)$
$\forall x(x \times 0 = 0)$
$\forall x \exists y(x = 0 \lor x \times y = 1)$

# Terms in a field

Structures $\mathcal{K}$ satisfying these axioms are called fields.

We use the following for arbitrary fields $\mathcal{K}$:

- We write $p$ for the term $\underbrace{1+1+\ldots+1}_{p}$.
- We write $t^p$ for the term $\underbrace{t+t+\ldots+t}_{p}$.
- Constant terms are identified with integers $\mathbb{Z}$.
- Every term $t(x\bar{y})$ with free variables $x$ and $\bar{y} = (y_0, y_1, \ldots, y_\ell)$ can be written in polynomial normal form

$$t(x, \bar{y}) = \sum_{k=0}^{m} t_k(\bar{y}) x^k$$

where in the terms $t_k$ the variable $x$ does not occur.

# Algebraically closed fields of characteristic $p$

## The charactersitic $p$ is either 0 or a prime $p$.

---

**Characteristic $p$:** A field $\mathcal{K}$ has charactersitic $n$ for $n \in \mathbb{N}, n \neq 0$ if in $\mathcal{K}$ we have $\underbrace{1 + 1 + \ldots + 1}_{p} = 0$.

**Charactersitic 0:** A field $\mathcal{K}$ has charactersitic 0 if for no $n \in \mathbb{N}, n \neq 0$ it has charactersitic $n$.

**Algebraic closure:** A field $\mathcal{K}$ is alegebraically closed if in $\mathcal{K}$ the following holds for all $m \in \mathbb{N}$:

$$\forall y_0 \forall y_1 \ldots \forall y_{m-1} \exists x \left( \sum_{k+0}^{m-1} y_k x^k \right) + x^m = 0$$

# Ernst Steinitz (1871 – 1928);

## Algebraische Theorie der Körper, Crelle J. of Math. (1910) pp. 167–309

---

A field $\mathcal{K}$ is an algebraic extension of a field $\mathcal{K}_0$ if every element of $\mathcal{K}$ is the root of a univariate polynomial with coefficients in $\mathcal{K}_0$.

A field $\mathcal{C}$ is an algebraic closure of a field $\mathcal{K}$ if

- $\mathcal{C}$ is an algebraic extension of $\mathcal{K}$, and
- $\mathcal{C}$ is algebraically closed.

$\mathbb{C}$ is an algebraic closure of $\mathbb{R}$.
The algebraic numbers $\mathbb{A}$ are an algebraic closure of $\mathbb{Q}$.

**Theorem St-1:** Every field $\mathcal{K}$ has, up to isomorphism, a unique algebraic closure.

**Theorem St-2:** Any two uncountable algebraically closed fields of the same characteristic and cardinality are isomorphic.

## The axioms of algebraically closed fields of characteristic $p$.

We denote by $\mathrm{ACF}_p$ the axioms consisting of the field axioms, stating that the characteristic is $p$ or 0, and stating that every univariate polynomial has a root.

- $\mathrm{ACF}_p$ is an infinite set. No finite subset of $\mathrm{ACF}_p$ logically implies it.
- $\mathrm{ACF}_p$ is a complete theory, i.e., for every sentence in the language of fields $\phi$ we have
$$\mathrm{ACF}_p \models \phi \text{ or } \mathrm{ACF}_p \models \neg\phi$$

To prove completeness we use Thoerem St-2 and the Löwenheim-Skolem Theorem.

This type of proof is called Vaught's test.

## QE: The crucial step (in characteristic 0)

Let $P_i(x, \bar{y}) : i = 1, \ldots, n$ and $Q_i(x, \bar{y}) : i = 1, \ldots, m$ be polynomials in a polynomial ring $\mathcal{K}[x, \bar{y}]$ over a field $\mathcal{K}$.

We look at the formula

$$\Phi(\bar{y}) = \exists x \left( \bigwedge_{i=1}^{n} P_i(x, \bar{y}) = 0 \wedge \bigwedge_{j=1}^{m} Q_j(x, \bar{y}) \neq 0 \right)$$

We want to find a finite set of polynomials $E_i(\bar{y}), i \in I$ without the indeterminate $x$ and a boolean formula $B(b_i), i \in I$ such that for the assignement

$$b_i(\bar{y}) := (E_i(\bar{y}) = 0)$$

we have:

For all fields $\mathcal{K} \models \mathrm{ACF}_0$ and for all elements $\bar{a} \in \mathcal{K}$

$$\mathcal{K} \models \Phi(\bar{a}) \text{ iff } \mathcal{K} \models B(E_i(\bar{a}))$$

**We need some algebra!**

# Polynomial degree and division

Let $\mathcal{K}$ be a field.

- The degree of a polynomial $P(x) = \sum_{i=0}^{d} a_i x^i \in \mathcal{K}[x]$ with $a_d \neq 0$ is $d$. We denote the degree of $P$ by $\deg(P)$.

- Let $P, Q \in \mathcal{K}[x]$ be two polynomials. We say that $P$ divides $Q$ if there is $R \in \mathcal{K}[x]$ such that $P \cdot R = Q$ (in $\mathcal{K}[x]$).

- Let $P, Q \in \mathcal{K}[x]$ be two polynomials. Then there are unique polynomials $R, S \in \mathcal{K}[x]$ such that $Q = P \cdot R + S$

  $R$ and $S$ can be computed (in symbolic computation) by the Euclidean algorithm.

- We denote by $\gcd(P, Q)$ the unique polynomial of biggest possible degree $S$ such that $S$ divides both $P$ and $Q$.

  $\gcd(P, Q)$ can be computed by the Euclidean algorithm.

## Algorithmic Algebra

---

```
@book{waer:48,
author= {Waerden, B.L.~van der},
title= {Modern Algebra},
publisher= {Frederick Ungar Publishing Co., New York},
year= 1948
}

@book{gage:99,
author= {Gathen, J.~von zur  and J.~Gerhard},
title= {Modern Computer Algebra},
publisher= {Cambridge University Press},
year= 1999
}
```

# More algorithmic algebra

Let $\mathcal{K}$ be a field of characteristic 0.

**AA-1:** Let $P, Q \in \mathcal{K}[x]$ with $P \neq 0$ and $Q \neq 0$, and $G = \text{gcd}(P, Q)$.
Then $\exists x (P(x) = 0 \wedge Q(x) = 0)$ iff $\exists x G(x) = 0$.

**AA-2:** Let $Q \in \mathcal{K}[x]$ with $Q \neq 0$. Then $\exists x Q(x) \neq 0$.

**AA-3:** Let $P, Q \in \mathcal{K}[x]$ with $P \neq 0$ and $Q \neq 0$,
and $\text{gcd}(P, Q) = 1$ (relatively prime).
Then $\exists x P(x) = 0 \wedge Q(x) \neq 0$ iff $\exists x P(x) = 0$.

**AA-4:** Let $P, Q \in \mathcal{K}[x]$ with $P \neq 0$ and $Q \neq 0$, $G = \text{gcd}(P, Q)$,
and $P_1(x)$ with $P(x) = G(x) \cdot P_1(x)$.
Then $\exists x (P(x) = 0 \wedge Q(x) \neq 0)$ iff $\exists x (P_1(x) = 0 \wedge G(x) \neq 0)$.

**AA-5:** Let $P(x), Q(x), G(x)$ and $P_1(x)$ are as in AA-4.
If $G(x) \neq 1$ ($P, Q$ are not relatively prime), then $\text{deg}(P_1(x)) < \text{deg}(P(x))$.

# Constant polynomials and polynomials without roots

Let $P(x, \bar{y}) = \sum_{i=0}^{n} t_i(\bar{y}) x^i \in \mathcal{K}[\bar{y}][x]$ be a univariate polynomial over $\mathcal{K}[\bar{y}]$. Here, the indeterminates $\bar{y}$ are parameters.

- $P(x, \bar{y})$ is independent of $x$ if there is $a \in \mathcal{K}[\bar{y}]$ such that for all $x$ the equation $P(x, \bar{y}) = a$ holds. In other words

$$\mathrm{Const}(P, \bar{y}, a(\bar{y})) := \forall x P(x, \bar{y}) = a(\bar{y})$$

- $P(x, \bar{y})$ has no solution for $x$ if there is no $a \in \mathcal{K}[\bar{y}]$ such that for all $x$ the equation $P(x, \bar{y}) = a(\bar{y})$ holds. In other words

$$\mathrm{Nosol}(P, \bar{y}) := \forall x P(x, \bar{y}) \neq 0$$

## Constant polynomials and polynomials without roots (AA-0)

Here we use $\mathrm{ACF}_0$.

- Const$(P, \bar{y}, a)$ can be written quantifier-free:

$$\mathrm{Const}(P, \bar{y}, a) := \left( t_0(\bar{y}) = a \wedge \bigwedge_{i=1}^{n} t_i(\bar{y}) = 0 \right)$$

- Nosol$(P, \bar{y})$ can be written quantifier-free:

$$\mathrm{Nosol}(P, \bar{y}) := \left( t_0(\bar{y}) \neq 0 \wedge \bigwedge_{i=1}^{n} t_i(\bar{y}) = 0 \right)$$

- Const$(P, \bar{y}, a)$ and Nosol$(P, \bar{y})$ are equivalent to a conjunction of polynomial equations or inequalities.

- Their negations are equivalent to a disjunction of polynomial equations or inequalities.

**QE-I:** $\Phi(\bar{y}) = \exists x \left( \bigwedge_{i=1}^{n} P_i(x, \bar{y}) = 0 \wedge \bigwedge_{j=1}^{m} Q_j(x, \bar{y}) \neq 0 \right)$

---

We write it simpler by using
$P(x) = \text{gcd}(P_i, i = 1, \ldots, n)$ and $Q(x) = \prod_{j=1}^{m} Q_j(x)$.

$n = 0, m > 0$**:**

We use AA-0 and AA-2:

$\exists x Q(x) \neq 0$ is equivalent to $\neg \forall x Q(x) = 0$,
or equivalently, to $\neg\text{Const}(Q, \bar{y}, 0)$ with $Q(x) = \sum_{j=0}^{m} s_j(\bar{y}) x^j$. This can be written as

$$\left( s_0(\bar{y}) \neq 0 \vee \bigvee_{j=1} s_j(\bar{y}) \neq 0 \right)$$

(with the remaining free variables $\bar{y}$ free).

This is now a disjunction of inequalities.

## QE-II: $\Phi(\bar{y}) = \exists x \left( \bigwedge_{i=1}^{n} P_i(x, \bar{y}) = 0 \wedge \bigwedge_{j=1}^{m} Q_j(x, \bar{y}) \neq 0 \right)$

---

**$n > 0, m = 0$:**

We use AA-0, AA-1 and $\mathrm{ACF}_0$:

$\exists x P(x) = 0$ is equivalent to $\neg\mathrm{Nosol}(P, \bar{y})$.
For $P(x) = \sum_{j=0}^{n} t_i(\bar{y}) x^i$ this can be written as

$$\left( t_0(\bar{y}) = 0 \vee \bigvee_{i=1}^{n} t_i(\bar{y}) \neq 0 \right)$$

(with the remaining free variables $\bar{y}$ free).

This is now again a disjunction of equations and inequalities.

## QE-III: $\Phi(\bar{y}) = \exists x \left( \bigwedge_{i=1}^{n} P_i(x,\bar{y}) = 0 \wedge \bigwedge_{j=1}^{m} Q_j(x,\bar{y}) \neq 0 \right)$

---

$n > 0, m > 0$:

Let $G(x) = \text{gcd}(P, Q)$ and $P_1(x)$ such that $P(x) = G(x) \cdot P_1(x)$.

We use AA-0, AA-4 and AA-5:

$\Phi(\bar{y})$ is equivalent to

$$[(\text{Const}(P, x, 0) \wedge \neg\text{Const}(Q, x, 0)) \quad \vee$$
$$(\text{Const}(G, x, 1) \wedge \neg\text{Noso}(P, x)) \quad \vee$$
$$\exists x(P_1(x, \bar{y}) = 0 \wedge G(x, \bar{y}) \neq 0)]$$

For each of the disjuncts we know how to eliminate the quantifier, either by AA-0, AA-0, AA-1, AA-3 $\text{ACF}_0$, or, noting that $G$ and $P_1$ have lower degrees, by AA-4, AA-5.

# What do we need to prove AA-1 to AA-5?

Étienne Bézout (1730-1783)

**Bézout's identity**:

Let $P(x), Q(x) \in \mathcal{K}[x]$ with $G(x) = \text{gcd}(P(x), Q(x))$.
There exist $A(x), B(x) \in \mathcal{K}[x]$ such that

$$A(x) \cdot P(x) + B(x) \cdot Q(x) = G(x).$$

The proof uses again the Euclidean Algorithm.

It works in any ring which is a principal ideal domain, i.e., a ring in which for $a \neq 0, b \neq 0$ also $ab \neq 0$, and every ideal is generated by a single element.

# Eliminating inequalties

We can also first eliminate inequalities.

- We note that $Q_j(x, \bar{y}) \neq 0$ is equivalent to $\exists z_j (z_j \cdot Q_j(x, \bar{y}) - 1 = 0)$
- We apply this to $\Phi$: $\Phi(\bar{y}) = \exists x \left( \bigwedge_{i=1}^{n} P_i(x, \bar{y}) = 0 \wedge \bigwedge_{j=1}^{m} Q_j(x, \bar{y}) \neq 0 \right)$ and get $\exists x \left( \bigwedge_{i=1}^{n} P_i(x, \bar{y}) = 0 \wedge \bigwedge_{j=1}^{m} \exists z_j \left( z_j \cdot Q_j(x, \bar{y}) - 1 = 0 \right) \right)$.
  which is equivalent to
  $$\exists \bar{z}\ \exists x \left( \bigwedge_{i=1}^{n} P_i(x, \bar{y}) = 0 \wedge \bigwedge_{j=1}^{m} (z_j \cdot Q_j(x, \bar{y}) - 1 = 0) \right)$$
- However, this introduces new existential quantifiers!

# Handling the multiplicative inverse $^{-1}$

If we add the inverse function $^{-1}$ we can also eliminate it.

- Axiom for $^{-1}$:
$$\forall x(x \neq 0 \rightarrow (x \cdot x^{-1} = x^{-1} \cdot x = 1))$$
- To make it a function we postulate $0^{-1} = 0$.
- Constant terms are now rational numbers.
- To eliminate $^{-1}$ we observe:

  **Lemma:**
  Every atomic formula with rational coefficients is equivalent to an atomic formula with integer coefficients.

# Fields with QE

AA-0 – AA-5 hold in all fields.

The crucial elimination is in the formula $\exists x P(x, \bar{y}) = 0$.

- In the field of the reals $\mathbb{R}$ the formula $\exists x(x^2 = y)$ is only true for $y \geq 0$.
- In the field of the rational $\mathbb{Q}$ solvability of polynomial equations is very complicated.
- We have seen in the last lecture that for every field $\mathcal{K}$ in the language of fields the theory Th($\mathcal{K}$) is undecidable

## Characterizing fields $\mathcal{K}$ with QE

A. MacIntyre (1971), A. MacIntyre, K. McKenna and L. van den Dries (1983)

---

**Theorem:**

Let $\mathcal{K}$ be in the language of fields (without order)

such that $Th(\mathcal{K})$ admits QE.

Then $\mathcal{K}$ is either **finite** or **algebraically closed**.

# Complexity

We have two questions of complexity:

- Given $\phi$, how long does a Turing machine have to work to produce a quantifier free equivalent of $\phi$?
- Given $\phi$, how long is the shortest quantifier free equivalent of $\phi$?