Logic and Proof Hilary 2026

Algebraically Closed Fields

James Worrell

1 Fields

In this lecture we introduce the theory of algebraically closed fields and show that it has quantifier elimination. This gives, among other things, an algorithm that determines whether a system of polynomial equations has a solution in complex numbers.

Working in first-order logic with equality, consider a signature with binary function symbols $+$ and $\cdot$, together with constants 0 and 1. A *field* is a σ-structure $\mathcal{K} = (K, +^{\mathcal{K}}, \cdot^{\mathcal{K}}, 0^{\mathcal{K}}, 1^{\mathcal{K}})$ satisfying the following axioms:

$$\begin{aligned}
&\forall x \forall y \forall z\, ((x + y) + z = x + (y + z))\\
&\forall x \forall y\, (x + y = y + x)\\
&\forall x\, (x + 0 = x)\\
&\forall x \exists y\, (x + y = 0)\\
&\forall x \forall y \forall z\, ((x \cdot y) \cdot z = x \cdot (y \cdot z))\\
&\forall x \forall y\, (x \cdot y = y \cdot x)\\
&\forall x\, (x \cdot 1 = x)\\
&\forall x\, (x \neq 0 \rightarrow \exists y\, (x \cdot y = 1))\\
&1 \neq 0\\
&\forall x \forall y \forall z\, (x \cdot (y + z) = x \cdot y + x \cdot z)\,.
\end{aligned}$$

The axioms express that addition and multiplication are associative and commutative, with respective neutral elements 0 and 1; 0 is not equal to 1; every element has an additive inverse; every non-zero element has a multiplicative inverse; and multiplication distributes over addition.

Examples of fields are the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$ (with the usual addition and multiplication in all cases). For a prime number p, the set $\mathbb{F}_p$ of integers modulo p is a field. The ring of integers $\mathbb{Z}$ and the ring of polynomials $\mathbb{Q}[x]$ are not fields since not all non-zero elements have multiplicative inverses.

The *characteristic* of a field is the smallest natural number n such that $\underbrace{1 + \cdots + 1}_{n \text{ times}} = 0$, if such a number exists, and the characteristic is zero otherwise. It is easy to see that a non-zero characteristic must be prime. The field $\mathbb{F}_p$ has characteristic p, as does the field $\mathbb{F}_p(x)$ of rational functions (quotients of two polynomials in $\mathbb{F}_p[x]$) with coefficients in $\mathbb{F}_p$. The field $\mathbb{Q}$ has characteristic zero.

A field K is *algebraically closed* if every non-constant polynomial $f \in K[x]$ has a zero in K. The fundamental theorem of algebra states that the field $\mathbb{C}$ of complex numbers is algebraically closed. The field of real numbers is not algebraically closed (e.g., the polynomial $x^2 + 1 \in \mathbb{R}[x]$ has no real zero). Note that the property of being algebraically closed and of having a given characteristic can be written as an infinite set of σ-sentences. We write $\boldsymbol{T}_{\mathrm{ACF}}$ for the theory of algebraically closed fields. For a given characteristic p (including $p = 0$) we write $\boldsymbol{T}_{\mathrm{ACF}_p}$ for the theory of algebraically closed fields of characteristic p.

Exercise 1. Write down axioms for theory $\boldsymbol{T}_{\mathrm{ACF}}$ and the theory $\boldsymbol{T}_{\mathrm{ACF}_p}$ for p prime and $p = 0$.

Exercise 2. Prove that every algebraically closed field is infinite.

2 Quantifier Elimination

2.1 Pseudo Division

Let K be a field. Recall that given polynomials $f, g \in K[x]$ with $\deg(f) \leq \deg(g)$, there exist unique polynomials $q, r \in K[x]$ such that $g = qf + r$ and $\deg(r) < \deg(f)$.[1] We say that dividing g by f gives *quotient* q and *remainder* r. Such a result no longer holds if we weaken the assumption that K be a field and merely ask that it be an *integral domain* (i.e., a ring, such as $\mathbb{Z}$, with no zero divisors but where elements need not have multiplicative inverses). We have instead the notion of *polynomial pseudo division*:

Proposition 3. Let R be an integral domain and let $f, g \in R[y]$ be such that $\deg(f) \leq \deg(g)$. Let a be the leading coefficient of f and let $d = \deg(g) - \deg(f) + 1$. Then there exist unique $q, r \in R[y]$ such that $a^d g = qf + r$ and $\deg(r) < \deg(f)$. (We call q the *pseudo quotient* and r the *pseudo remainder* of g divided by f.)

Proof. Intuitively, since we multiply g by a^d we can perform polynomial division without the need to divide in the ring R of coefficients. See the exercise sheet for details. □

Exercise 4. (i) Let $R = \mathbb{Z}$; compute the pseudo remainder when $g = y^3 + y + 1$ is divided by $f := 2y + 3$ in $R[y]$. (ii) Let $R = \mathbb{Z}[x]$; compute the pseudo remainder when $g := x^2y^3 - y$ is divided by $f = x^3y - 2$ in $R[y]$.

Exercise 5. Let $R = \mathbb{Z}[\boldsymbol{x}]$, where $\boldsymbol{x} = (x_1, \ldots, x_m)$. Given $f, g \in R[y]$, let r be the pseudo remainder when g is divided by f. Let K be a field and $\boldsymbol{\alpha} \in K^m$ be such that $c(\boldsymbol{\alpha}) \neq 0$ where $c(\boldsymbol{x})$ is the leading coefficient of f. Show that $f(\boldsymbol{\alpha}, y)$ divides $g(\boldsymbol{\alpha}, y)$ in $K[y]$ if and only if $r(\boldsymbol{\alpha}, y)$ is identically zero.

2.2 Elimination Without Parameters

Let K be an algebraically closed field. In this section, to build intuition, we consider how to determine the truth value in K of the following formula, where the f_i and g_j are polynomials in $K[y]$:

$$\exists y \left(\bigwedge_{i=1}^{m} f_i(y) = 0 \wedge \bigwedge_{j=1}^{n} g_j(y) \neq 0 \right). \tag{1}$$

Write $g = g_1 \cdots g_n$. Then (1) obviously has the same truth value as the formula

$$\exists y \left(\bigwedge_{i=1}^{m} f_i(y) = 0 \wedge g(y) \neq 0 \right). \tag{2}$$

We next simplify (2) to the case that $m = 1$. Suppose that $m \geq 2$ and, without loss of generality, that $\deg(f_1) \leq \deg(f_2)$. Let h_1 be the remainder on dividing f_2 by f_1 and let $h_i = f_i$ for $i \in$

[1] Where the zero polynomial has degree $-\infty$.

$\{2, \ldots, m\}$. Then $\{a \in K : f_1(a) = f_2(a) = 0\} = \{a \in K : h_1(a) = h_2(a) = 0\}$. Hence (2) has the same truth value in K as

$$\exists y \left(\bigwedge_{i=1}^{m} h_i(y) = 0 \wedge g(y) \neq 0 \right) \tag{3}$$

and $\sum_{i=1}^{m} \deg(h_i) < \sum_{i=1}^{m} \deg(f_i)$.

We repeat the previous simplification until we arrive at a formula

$$\exists y \ (f(y) = 0 \wedge g(y) \neq 0) \ . \tag{4}$$

We remark in passing that f, as constructed, is the gcd of $f_1, \ldots, f_m$ in $K[y]$, since $K[y]$ is a Euclidean domain and the above remainder step is exactly the Euclidean algorithm.

We claim that (4) is false in K iff f divides g^d in $K[y]$, where $d = \deg(f)$. Indeed, (4) is false in K iff every root of f in K is also a root of g. Since K is algebraically closed we can write $f = c \prod_{i=1}^{s} (y - \alpha_i)^{\nu_i}$ and $g = \prod_{i=1}^{s} (y - \alpha_i)^{\mu_i} h$ where $c \neq 0$, the α_i are distinct, $\nu_i \geq 1$, and $h(\alpha_i) \neq 0$ for all i. Then each α_i is a root of g iff $\mu_i \geq 1$, and in this case g^d has multiplicity $d\mu_i \geq \nu_i$. Thus $f \mid g^d$ exactly captures the condition that every root of f is also a root of g. This proves the claim.

Taking stock, we have presented a procedure to determine the truth of the sentence (1) in an algebraically closed field K by performing a sequence of polynomial divisions in $K[y]$.

2.3 Elimination with Parameters

In this section we describe the quantifier elimination procedure for the theory of algebraically closed fields. We follow the development in the previous section, but this time we work with formulas that contain free variables $\boldsymbol{x} = (x_1, \ldots, x_k)$ in addition to the quantified variable y. The key idea is to use pseudo division of polynomials in $\mathbb{Z}[\boldsymbol{x}][y]$, instead of division of polynomials in $K[y]$ as in the previous section.

The following proposition generalises the way that we determined the truth of (4) in the previous section.

Proposition 6. For all polynomials $f, g \in \mathbb{Z}[\boldsymbol{x}, y]$ the formula $\exists y \, (f(\boldsymbol{x}, y) = 0 \wedge g(\boldsymbol{x}, y) \neq 0)$ has an equivalent quantifier-free formula over algebraically closed fields.

Proof. Consider the polynomial ring $R := \mathbb{Z}[\boldsymbol{x}]$. We treat f and g as univariate polynomials in $R[y]$ and write $\deg(f)$ and $\deg(g)$ for the respective degrees of f and g in variable y. We prove the proposition by induction on $\deg(f)$.

The base case is that $\deg(f) = 0$, that is, f does not mention y. Write $g(\boldsymbol{x}, y) = \sum_{i=0}^{d} c_i(\boldsymbol{x}) y^i$, where $c_0, \ldots, c_d \in R$. Since every algebraically closed field K is infinite, for any non-zero polynomial $h \in K[y]$ there exists $a \in K$ with $h(a) \neq 0$. We deduce that

$$\boldsymbol{T}_{\mathrm{ACF}} \models \exists y \, (f(\boldsymbol{x}) = 0 \wedge g(\boldsymbol{x}, y) \neq 0) \leftrightarrow \left(f(\boldsymbol{x}) = 0 \wedge \bigvee_{i=0}^{d} c_i(\boldsymbol{x}) \neq 0 \right) .$$

Here we use that $g(\boldsymbol{\alpha}, \cdot)$ is the zero polynomial in $K[y]$ iff all coefficients $c_i(\boldsymbol{\alpha})$ vanish.

The induction step is as follows. Write $f(\boldsymbol{x}, y) = a(\boldsymbol{x}) y^d + f_1(\boldsymbol{x}, y)$ where $\deg(f_1) \leq d - 1$. Let $r(\boldsymbol{x}, y) = \sum_{i=0}^{d-1} b_i(\boldsymbol{x}) y^i$ be the pseudo remainder of g^d divided by f in $R[y]$ (note that $\deg(g^d) \geq \deg(f)$, so pseudo division is allowed). It follows from Exercise 5 that for any assignment $\boldsymbol{\alpha} \in K^k$

to the variables $\boldsymbol{x}$ such that $a(\boldsymbol{\alpha}) \neq 0$, it holds that polynomial $r(\boldsymbol{\alpha}, y)$ is identically zero if and only if the remainder when dividing $(g(\boldsymbol{\alpha}, y))^d$ by $f(\boldsymbol{\alpha}, y)$ in $K[y]$ is zero. It follows (by the claim in the last paragraph of Section 2.2) that $r(\boldsymbol{\alpha}, y)$ is identically zero iff $\exists y(f(\boldsymbol{\alpha}, y) = 0 \wedge g(\boldsymbol{\alpha}, y) \neq 0)$ is false in K. Thus we have

$$\boldsymbol{T}_{\mathrm{ACF}} \models \exists y\,(f = 0 \wedge g \neq 0) \leftrightarrow [a = 0 \wedge \exists y\,(f_1 = 0 \wedge g \neq 0)] \vee \left[a \neq 0 \wedge \bigvee_{i=0}^{d-1} b_i \neq 0\right]$$

Since $\deg(f_1) < \deg(f)$ we can apply the induction hypothesis to eliminate the right-hand existential quantifier above. □

The next proposition generalises the reduction of (1) to (4) in the previous section.

Theorem 7. The theory of algebraically closed fields has quantifier elimination.

Proof. To start, observe that a conjunction of disequalities $\bigwedge_{i=1}^m g_i \neq 0$ can be equivalently written as a single disequality $g_1 \cdots g_m \neq 0$. Hence it suffices to eliminate the quantifier $\exists y$ in formulas of the following type:

$$\exists y \left(\bigwedge_{i=1}^m f_i(\boldsymbol{x}, y) = 0 \wedge g(\boldsymbol{x}, y) \neq 0 \right). \tag{5}$$

As in the proof of Proposition 6, we treat f_i and g as elements of the univariate polynomial ring $R[y]$ where $R := \mathbb{Z}[\boldsymbol{x}]$. Recall that for $f \in R[y]$, $\deg(f)$ denotes the degree of f in the variable y.

We reduce the problem of eliminating the quantifier $\exists y$ in (5) to the special case in which $m = 1$, which is the case treated in Proposition 6. This reduction is by induction on $\sum_{i=1}^m \deg(f_i)$. We show that whenever $m \geq 2$ this quantity can be strictly reduced.

Suppose that $m \geq 2$ and that $0 < \deg(f_1) \leq \cdots \leq \deg(f_m)$. Write

$$f_1(\boldsymbol{x}, y) = a_d(\boldsymbol{x})y^d + \cdots + a_1(\boldsymbol{x})y + a_0(\boldsymbol{x}), \quad \text{and let} \quad \widetilde{f_1}(\boldsymbol{x}, y) := a_{d-1}(\boldsymbol{x})y^{d-1} + \cdots + a_1(\boldsymbol{x})y + a_0(\boldsymbol{x})$$

be obtained by dropping the leading term of f_1. Note that under the side condition $a_d(\boldsymbol{x}) = 0$ we have $f_1(\boldsymbol{x}, y) = \widetilde{f_1}(\boldsymbol{x}, y)$.

Pseudo dividing f_2 by f_1 in $R[y]$ gives $a_d^e f_2 = q f_1 + r$ where $e = \deg(f_2) - \deg(f_1) + 1$ and $\deg(r) < \deg(f_1)$. Now we have that formula (5) is equivalent over algebraically closed fields to the formula

$$\left[a_d = 0 \wedge \exists y \left(\widetilde{f_1} = 0 \wedge \bigwedge_{i=2}^m f_i = 0 \wedge g \neq 0 \right)\right] \vee \left[a_d \neq 0 \wedge \exists y \left(r = 0 \wedge \bigwedge_{i=2}^m f_i = 0 \wedge g \neq 0 \right)\right]$$

Notice that the above formula is Boolean combination of formulas that either don't mention y or that have same form as the original formula (5), but in which the induction parameter is strictly smaller. This completes the announced reduction.

□