

G22.3033-003 Logic and Verification

Spring 2004

Lecture 10

1

Outline

- Algebraically Closed Fields

Sources:

Harrison, John. *Introduction to Logic and Automated Theorem Proving*.
Unpublished manuscript. Used by permission.

Gallian, Joseph A. *Contemporary Abstract Algebra, Second Edition*.
Heath and Company, 1990.

3

Review

- Quantifier Elimination
- Presburger Arithmetic

2

Groups, Rings, and Fields

In abstract algebra, the notions of groups, rings and fields are described in terms of sets with operations that obey certain laws. This leads to a nice characterization of these objects as models of a particular set of axioms.

Group Axioms

- $\forall x y z. x + (y + z) = (x + y) + z$
- $\forall x. 0 + x = x$
- $\forall x. (-x) + x = 0$

An *Abelian* group is commutative: $\forall x y. x + y = y + x$.

A *ring* is an Abelian group under the $+$ operator, but includes an additional operator \times with the following additional axioms.

Ring Axioms

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

A *commutative* ring has the additional axiom: $\forall x y. x \times y = y \times x$.

4

Groups, Rings, and Fields

A commutative ring is a *field* if it satisfies the following additional axioms:

Field Axioms

- $\forall x. 1 \times x = x$
- $\forall x. (x \neq 0) \rightarrow (x^{-1} \times x) = 1$

Notice that the signature of a field includes the constants **0** and **1**, unary functions $-$ and $()^{-1}$, and binary functions $+$ and \times .

We have chosen these symbols to match our intuition for common arithmetic fields such as the rational numbers, the real numbers, and the complex numbers. There are, however, many other possible models for these axioms.

If p is the smallest positive integer such that the sum of p 1's is **0**, then the field is said to have *characteristic* p , and to have *characteristic* **0** if there is no such p .

From now on, we will use standard mathematical convention and write xy to mean $x \times y$, a numeral n to mean the sum of n 1's, and x^n to represent the product of n x 's.

5

Algebraically Closed Fields

Canonical Forms

As with Presburger arithmetic, it will be useful to have a canonical form for terms. Given a total order \prec on variables, the canonical form for a term will be:

$$c_0 + x(c_1 + x(c_2 + x(\dots))),$$

where each c_i is a canonical term not containing x and $x \prec y$ for every variable y appearing in any of the c_i 's.

Each c_i must also be in canonical form with respect to the other variables.

Example

$$\begin{aligned}
& 3xy^2 + 2x^2yz + xz + 3yz \\
= & [2yz]x^2 + [3y^2 + z]x + [3yz] \\
= & [3yz] + x([3y^2 + z] + x[2yz]) \\
= & [0 + y(3z)] + x([z + y(0 + y(3))] + x[0 + y(2z)]) \\
= & [0 + y(0 + z(3))] + x([(0 + z(1)) + y(0 + y(3))] + x[0 + y(0 + z(2))])
\end{aligned}$$

7-d

Algebraically Closed Fields

If a field has the property that every polynomial other than nonzero constants has a zero, it is said to be *algebraically closed*. This can be characterized by an infinite set of additional axioms, one for each $n \geq 1$:

$$\forall a_0 \dots a_n. a_n \neq 0 \rightarrow \exists x. a_n x^n + \dots + a_1 x + a_0 = 0.$$

The theory of algebraically closed fields is the one axiomatized by all the axioms just described. This theory admits quantifier elimination.

However, as we will see, this is a case where quantifier elimination does not automatically guarantee decidability.

The best-known example of an algebraically closed field is the field of complex numbers.

The field of real numbers is *not* algebraically closed. For example, the following instance of the algebraically closed axiom (for $n = 2$) fails:

$$\exists x. x^2 + 1 = 0.$$

6

Algebraically Closed Fields

Recall that in order to show that a theory T admits quantifier elimination, it is sufficient to show that for every formula ϕ of the form $\exists x (\alpha_0 \wedge \dots \wedge \alpha_n)$, where each α_i is a literal, there is a quantifier-free formula ψ such that $T \models (\phi \leftrightarrow \psi)$.

For the case of algebraically closed fields, a literal is either an equation or a disequation. Thus, we must consider formulas of the form:

$$\exists x. p_1(x) = 0 \wedge \dots \wedge p_n(x) = 0 \wedge q_1(x) \neq 0 \wedge \dots \wedge q_m(x) \neq 0.$$

Note first that we can get rid of all but a single disequation by using the following equivalence:

$$q_i(x) \neq 0 \wedge q_{i+1}(x) \neq 0 \leftrightarrow q_i(x)q_{i+1}(x) \neq 0.$$

Why?

Our next goal is to get rid of all but a single equation.

8-a

Algebraically Closed Fields

Pseudo-division

To reduce a conjunction of equations to a single equation, we will use *pseudo-division* of polynomials.

This is a process by which, given terms $s(x)$ and $p(x)$, we find c , $q(x)$, and $r(x)$ such that

$$cs(x) = p(x)q(x) + r(x),$$

where c is a term not containing x and $r(x)$ is a term whose degree (with respect to x) is less than that of p .

9

Algebraically Closed Fields

From the previous slide, we have $as_1(x) = bx^{m-n}p(x) + s_2(x)$

Because $s_2(x)$ has a lower degree than $s_1(x)$, we can recursively apply the factoring step to $s_2(x)$ until we have:

$$\begin{aligned} as_{k-1}(x) &= b_{k-1}x^{m_{k-1}-n}p(x) + s_k(x), \text{ and} \\ as_k(x) &= b_k(x)x^{m_k-n}p(x) + s_{k+1}(x) \\ &= q_k(x)p(x) + r(x), \end{aligned}$$

where the degree of $r(x)$ is less than that of $p(x)$. Then,

$$\begin{aligned} a^2s_{k-1}(x) &= a(b_{k-1}x^{m_{k-1}-n}p(x) + s_k(x)) \\ &= ab_{k-1}x^{m_{k-1}-n}p(x) + as_k(x) \\ &= ab_{k-1}x^{m_{k-1}-n}p(x) + q_k(x)p(x) + r(x) \\ &= (ab_{k-1}x^{m_{k-1}-n} + q_k(x))p(x) + r(x) \\ &= q_{k-1}(x)p(x) + r(x) \end{aligned}$$

Thus, we end up with $a^k s_1(x) = q_1(x)p(x) + r(x)$ for some $q_1(x)$ found as above, where a is the leading coefficient of $p(x)$ and k is the number of applications of the basic separation procedure.

11-d

Algebraically Closed Fields

We wish to pseudo-divide $s(x)$ by $p(x)$ to obtain $cs(x) = p(x)q(x) + r(x)$. Suppose we separate out the leading terms:

$$\begin{aligned} s(x) &= bx^m + s'(x), \text{ and} \\ p(x) &= ax^n + p'(x). \end{aligned}$$

If $m < n$, then the conditions for pseudo-division are trivially satisfied with $c = 1$, $q(x) = 0$ and $r(x) = s(x)$.

Otherwise, we can write:

$$as(x) = bx^{m-n}p(x) + (as'(x) - bx^{m-n}p'(x)).$$

Letting $s_1(x) = s(x)$ and $s_2(x) = as'(x) - bx^{m-n}p'(x)$, we get

$$as_1(x) = bx^{m-n}p(x) + s_2(x),$$

where $s_2(x)$ has a lower degree than $s_1(x)$.

10

Algebraically Closed Fields

We can now see how to use pseudo-division to eliminate all but one equation:

Suppose we have $p(x) = 0 \wedge s(x) = 0$ and the degree of $p(x)$ is less than the degree of $s(x)$.

We can pseudo-divide to get $a^k s(x) = q(x)p(x) + r(x)$.

Thus, if $a \neq 0$, we have:

$$p(x) = 0 \wedge s(x) = 0 \leftrightarrow p(x) = 0 \wedge r(x) = 0.$$

The same approach works for more than two equations:

$$p(x) = 0 \wedge \bigwedge_i s_i(x) = 0 \leftrightarrow p(x) = 0 \wedge \bigwedge_i r_i(x) = 0.$$

Thus, we can repeat the process, pseudo-dividing by the equation with the lowest degree, until at most one equation contains x .

12

Algebraically Closed Fields

Sign Determination

Notice that the step to eliminate all but one equation assumes that the leading coefficient a is nonzero.

In general, a may be an arbitrary term not containing x , which may or may not be equal to zero.

Thus, in general, we need to perform a case split. Suppose we have

$$p(x) = 0 \wedge \bigwedge_i s_i(x) = 0,$$

and we want to pseudo-divide by $p(x)$ with leading coefficient a . We first form a case-split as follows:

$$a = 0 \wedge p(x) = 0 \wedge \bigwedge_i s_i(x) = 0 \vee a \neq 0 \wedge p(x) = 0 \wedge \bigwedge_i s_i(x) = 0.$$

This is implemented by maintaining a database of terms which are assumed to be zero or nonzero.

13

Algebraically Closed Fields

The final case is one equation and one disequation:

$$\exists x. p(x) = 0 \wedge q(x) \neq 0.$$

It will be convenient to rewrite this as $\neg(\forall x. p(x) = 0 \rightarrow q(x) = 0)$.

Now, a fundamental property of algebraically closed fields is that polynomials can be factored into linear factors, so we have:

$$\exists a_0 a_1 \dots a_n. p(x) = a_0(x - a_1)(x - a_2) \dots (x - a_n), \text{ and}$$

$$\exists b_0 b_1 \dots b_m. q(x) = b_0(x - b_1)(x - b_2) \dots (x - b_m),$$

where n is the degree of $p(x)$. This assumes that a_0 , the leading coefficient of $p(x)$, is nonzero. Instead of assuming that the leading coefficient of $q(x)$ is nonzero, we can instead wave our hands a bit and assume that m is less than or equal to the degree of $q(x)$.

With this insight, let's look again at the formula $\forall x. p(x) = 0 \rightarrow q(x) = 0$.

This can only be true if $q(x) = 0$ or if each of the a_i 's appear among the b_i 's.

Thus, we can rewrite this condition as $p(x) | a_0 q(x)^n$. Note that this is true regardless of the value of m .

15

Algebraically Closed Fields

Main Quantifier Elimination Algorithm

Consider again the problem of eliminating the quantifier in

$$\exists x. p_1(x) = 0 \wedge \dots \wedge p_n(x) = 0 \wedge q_1(x) \neq 0 \wedge \dots \wedge q_m(x) \neq 0.$$

As shown above, we can eliminate all but one of the equations and disequations.

Suppose there are no disequations. Then we simply have $\exists x. p(x) = 0$, which is true, by algebraic closure, unless $p(x)$ is a nonzero constant with respect to x , so we can replace $\exists x. a_n x^n + \dots + a_1 x + c = 0$ with $\bigvee_i a_i \neq 0 \vee c = 0$.

Suppose there are no equations. Then we have $\exists x. q(x) \neq 0$. This is true unless $q(x)$ is zero or the field is trivial (containing only 0, in which case $1 = 0$). We can easily see this by noting that for nonconstant $q(x)$, the equation $q(x) = 1$ must have a root by algebraic closure.

Thus we can replace $\exists x. a_n x^n + \dots + a_1 x + c \neq 0$ with $(\bigvee_i a_i \neq 0 \vee c \neq 0) \wedge (1 \neq 0)$.

14

Algebraically Closed Fields

Thus we have:

$$\begin{aligned} \exists x. p(x) = 0 \wedge q(x) \neq 0 & \text{ iff } \neg(\forall x. p(x) = 0 \rightarrow q(x) = 0) \\ & \text{ iff } \neg(p(x) | a_0 q(x)^n) \\ & \text{ iff } p(x) \not\propto a_0 q(x)^n. \end{aligned}$$

Now, we can use pseudo-division on $a_0 q(x)^n$ to get:

$$a_0^{k+1} q(x)^n = p(x) q'(x) + r(x),$$

where the degree of $r(x)$ is less than that of $p(x)$. Then, since $a_0 \neq 0$, we have:

$$\begin{aligned} p(x) \not\propto a_0 q(x)^n & \text{ iff } p(x) \not\propto (a_0 q(x)^n - (a_0^{-k} q'(x) p(x))) \\ & \text{ iff } p(x) \not\propto a_0^{-k} r(x) \\ & \text{ iff } a_0^{-k} r(x) \neq 0 \\ & \text{ iff } r(x) \neq 0 \end{aligned}$$

Thus, we are left with $\exists x. r(x) \neq 0$ which is a single disequation, a case already covered.

16

Algebraically Closed Fields

After quantifier elimination, we are left with some quantifier-free formula whose atomic formulas are equations or disequations between terms which are built up from 0 and 1 .

At this point, the question of the characteristic of the field comes in. If the characteristic is unknown, then these formulas cannot be evaluated.

If the characteristic is known, then every formula reduces to true or false.

Harrison's implementation assumes a characteristic of 0 , which is true for the most important case, the complex numbers.

The implementation is in [complex.ml](#).