Model Theory and Polynomials

Richard Rast

May 7, 2015

Why Logic?

Is there any interesting theorem which is *not* a logic theorem, but which has a *nice* logic proof?

Why Logic?

Is there any interesting theorem which is *not* a logic theorem, but which has a *nice* logic proof?

Theorem (Ax)

Let $f : \mathbb{C}^n \to \mathbb{C}^n$ be a polynomial. If f is injective, then f is surjective.

(converse is false)

First Order Logic

First order sentences have a *language*, like $L = \{0, 1, +, \cdot\}$.
Sentences are things like:

$$\forall x \exists y \ \ (x = 0 \vee x \cdot y = 1)$$
$$\forall x \forall y \forall z \ \ ((x \cdot y) \cdot z = x \cdot (y \cdot z))$$

We quantify over elements of the structure, but *not* sets, functions, etc.

First Order Logic

First order sentences have a *language*, like $L = \{0, 1, +, \cdot\}$.
Sentences are things like:

$$\forall x \exists y \ \ (x = 0 \vee x \cdot y = 1)$$
$$\forall x \forall y \forall z \ \ ((x \cdot y) \cdot z = x \cdot (y \cdot z))$$

We quantify over elements of the structure, but *not* sets, functions, etc.

So we can't say "for all polynomials f, ..."
What to do?

First Order Logic is Expressive

Example: every injective polynomial of degree 3 from F^2 to F^2 is surjective ($A_{2,3}$):

First Order Logic is Expressive

Example: every injective polynomial of degree 3 from F^2 to F^2 is surjective ($A_{2,3}$):

$$\forall c_{1,00} \forall c_{1,10} \cdots \forall c_{1,33}\ \forall c_{2,00} \forall c_{2,10} \cdots \forall c_{2,33}$$

$$\left(\forall x_1 \forall x_2 \forall y_1 \forall y_2 \left[x \neq y \rightarrow \bigvee_{i=1,2} \left(p(\overline{x}, \overline{c}_i) \neq p(\overline{y}, \overline{c}_2) \right) \right] \right)$$

$$\rightarrow \left(\forall y_1 \forall y_2 \exists x_1 \exists x_2 \left[p(\overline{x}, \overline{c}_1) = y_1 \wedge p(\overline{x}, \overline{c}_2) = y_2 \right] \right)$$

Here $p(\overline{x}, \overline{c}_i)$ is an abbreviation for:

$$c_{i,00} + c_{i,10} \cdot x_1 + c_{i,20} \cdot x_1 \cdot x_1 + \cdots + c_{i,33} \cdot x_1 \cdot x_1 \cdot x_1 \cdot x_2 \cdot x_2 \cdot x_2$$

First Order Logic is Expressive

Example: every injective polynomial of degree 3 from F^2 to F^2 is surjective ($A_{2,3}$):

$$\forall c_{1,00} \forall c_{1,10} \cdots \forall c_{1,33} \; \forall c_{2,00} \forall c_{2,10} \cdots \forall c_{2,33}$$
$$\left(\forall x_1 \forall x_2 \forall y_1 \forall y_2 \left[x \neq y \to \bigvee_{i=1,2} \left(p(\overline{x}, \overline{c}_i) \neq p(\overline{y}, \overline{c}_2) \right) \right] \right)$$
$$\to \left(\forall y_1 \forall y_2 \exists x_1 \exists x_2 \left[p(\overline{x}, \overline{c}_1) = y_1 \wedge p(\overline{x}, \overline{c}_2) = y_2 \right] \right)$$

Here $p(\overline{x}, \overline{c}_i)$ is an abbreviation for:

$$c_{i,00} + c_{i,10} \cdot x_1 + c_{i,20} \cdot x_1 \cdot x_1 + \cdots + c_{i,33} \cdot x_1 \cdot x_1 \cdot x_1 \cdot x_2 \cdot x_2 \cdot x_2$$

The point is that $A_{2,3}$ is first-order. We never actually use the precise sentences. But we can make $A_{n,k}$ for any n and k.

The Only Theorem You Need

Theorem (Gödel, Löwenheim, Skolem)

Let Σ be a set of first-order sentences in some fixed language L.
If every finite subset of Σ has an infinite model,
then Σ has a model of every infinite cardinality.

This is sometimes called the compactness theorem, combined with the upward and downward Löwenheim-Skolem theorems.

Fun with Compactness

Theorem

Let Σ be the axioms for "algebraically closed fields of characteristic p" (p is prime or zero). Then Σ is complete:

for every sentence σ, either $\Sigma \models \sigma$ or $\Sigma \models \neg\sigma$.

Fun with Compactness

Theorem

Let Σ be the axioms for "algebraically closed fields of characteristic p" (p is prime or zero). Then Σ is complete:

for every sentence σ, either $\Sigma \models \sigma$ or $\Sigma \models \neg\sigma$.

Proof:

- If not, both $\Sigma \cup \{\sigma\}$ and $\Sigma \cup \{\neg\sigma\}$ have a model of size continuum [compactness]

Fun with Compactness

Theorem

Let Σ be the axioms for "algebraically closed fields of characteristic p" (p is prime or zero). Then Σ is complete:

for every sentence σ, either $\Sigma \models \sigma$ or $\Sigma \models \neg\sigma$.

Proof:

- If not, both $\Sigma \cup \{\sigma\}$ and $\Sigma \cup \{\neg\sigma\}$ have a model of size continuum [compactness]
- There is only one algebraically closed field of characteristic p of that size [transcendence bases exist]

Fun with Compactness

Theorem

Let Σ be the axioms for "algebraically closed fields of characteristic p" (p is prime or zero). Then Σ is complete:

for every sentence σ, either $\Sigma \models \sigma$ or $\Sigma \models \neg\sigma$.

Proof:

- If not, both $\Sigma \cup \{\sigma\}$ and $\Sigma \cup \{\neg\sigma\}$ have a model of size continuum [compactness]
- There is only one algebraically closed field of characteristic p of that size [transcendence bases exist]
- The models from point 1 must be isomorphic, contradiction!

Proving Ax's Theorem - I

Lemma

If Ax's theorem is true for algebraically closed fields of positive characteristic, it's true for $\mathbb{C}$.

Proving Ax's Theorem - I

Lemma

If Ax's theorem is true for algebraically closed fields of positive characteristic, it's true for $\mathbb{C}$.

Proof:

- Enough to show $\mathrm{ACF} \cup \{n \neq 0 : n \in \mathbb{N}\} \cup \{A_{n,k} : n, k \in \mathbb{N}\}$ is consistent [completeness for ACF_0]

Proving Ax's Theorem - I

Lemma

If Ax's theorem is true for algebraically closed fields of positive characteristic, it's true for $\mathbb{C}$.

Proof:

- Enough to show $\mathrm{ACF} \cup \{n \neq 0 : n \in \mathbb{N}\} \cup \{A_{n,k} : n, k \in \mathbb{N}\}$ is consistent [completeness for ACF_0]
- Enough to show every finite subset is consistent [compactness]

Proving Ax's Theorem - I

Lemma

If Ax's theorem is true for algebraically closed fields of positive characteristic, it's true for $\mathbb{C}$.

Proof:

- Enough to show $\mathrm{ACF} \cup \{n \neq 0 : n \in \mathbb{N}\} \cup \{A_{n,k} : n, k \in \mathbb{N}\}$ is consistent [completeness for ACF_0]
- Enough to show every finite subset is consistent [compactness]
- The finite subset says (at most) the characteristic is at least p

Proving Ax's Theorem - I

Lemma

If Ax's theorem is true for algebraically closed fields of positive characteristic, it's true for $\mathbb{C}$.

Proof:

- Enough to show $\mathrm{ACF} \cup \{n \neq 0 : n \in \mathbb{N}\} \cup \{A_{n,k} : n, k \in \mathbb{N}\}$ is consistent [completeness for ACF_0]
- Enough to show every finite subset is consistent [compactness]
- The finite subset says (at most) the characteristic is at least p
- Any large positive characteristic ACF models the finite subset [Ax for ACF_p]

Proving Ax's Theorem - II

Lemma

If Ax's theorem is true for $\overline{\mathbb{F}_p}$, it's true for all algebraically closed fields of characteristic p.

Proving Ax's Theorem - II

Lemma

If Ax's theorem is true for $\overline{\mathbb{F}_p}$, it's true for all algebraically closed fields of characteristic p.

Proof:

- Say $A_{n,k}$ fails on some $F \models \mathrm{ACF}_p$

Proving Ax's Theorem - II

Lemma

If Ax's theorem is true for $\overline{\mathbb{F}_p}$, it's true for all algebraically closed fields of characteristic p.

Proof:

- Say $A_{n,k}$ fails on some $F \models \mathrm{ACF}_p$
- F and $\overline{\mathbb{F}_p}$ model the same sentences [completeness for ACF_p]

Proving Ax's Theorem - II

Lemma

If Ax's theorem is true for $\overline{\mathbb{F}_p}$, it's true for all algebraically closed fields of characteristic p.

Proof:

- Say $A_{n,k}$ fails on some $F \models \mathrm{ACF}_p$
- F and $\overline{\mathbb{F}_p}$ model the same sentences [completeness for ACF_p]
- So $A_{n,k}$ fails on $\overline{\mathbb{F}_p}$, contradiction!

Proving Ax's Theorem - III

This turns out to be our "technical lemma:"

Fact

Every injective function from a finite set to itself is surjective.

Proving Ax's Theorem - III

This turns out to be our "technical lemma:"

Fact

Every injective function from a finite set to itself is surjective.

Lemma

Ax's theorem holds for $\overline{\mathbb{F}_p}$.

Proving Ax's Theorem - III

This turns out to be our "technical lemma:"

Fact

Every injective function from a finite set to itself is surjective.

Lemma

Ax's theorem holds for $\overline{\mathbb{F}_p}$.

Proof:

- $\overline{\mathbb{F}_p}$ is the union of all the $\mathbb{F}_{p^m}$.

Proving Ax's Theorem - III

This turns out to be our "technical lemma:"

Fact

Every injective function from a finite set to itself is surjective.

Lemma

Ax's theorem holds for $\overline{\mathbb{F}_p}$.

Proof:

- $\overline{\mathbb{F}_p}$ is the union of all the $\mathbb{F}_{p^m}$.
- Pick an injective polynomial f from $\overline{\mathbb{F}_p}^n$ to $\overline{\mathbb{F}_p}^n$

Proving Ax's Theorem - III

This turns out to be our "technical lemma:"

Fact

Every injective function from a finite set to itself is surjective.

Lemma

Ax's theorem holds for $\overline{\mathbb{F}_p}$.

Proof:

- $\overline{\mathbb{F}_p}$ is the union of all the $\mathbb{F}_{p^m}$.
- Pick an injective polynomial f from $\overline{\mathbb{F}_p}^n$ to $\overline{\mathbb{F}_p}^n$
- Let $\overline{b}$ be from $\overline{\mathbb{F}_p}^n$

Proving Ax's Theorem - III

This turns out to be our "technical lemma:"

Fact

Every injective function from a finite set to itself is surjective.

Lemma

Ax's theorem holds for $\overline{\mathbb{F}_p}$.

Proof:

- $\overline{\mathbb{F}_p}$ is the union of all the $\mathbb{F}_{p^m}$.
- Pick an injective polynomial f from $\overline{\mathbb{F}_p}^n$ to $\overline{\mathbb{F}_p}^n$
- Let $\overline{b}$ be from $\overline{\mathbb{F}_p}^n$
- Let m be large enough that $\mathbb{F}_{p^m}$ contains $\overline{b}$ and the coefficients of f

Proving Ax's Theorem - III

This turns out to be our "technical lemma:"

Fact

Every injective function from a finite set to itself is surjective.

Lemma

Ax's theorem holds for $\overline{\mathbb{F}_p}$.

Proof:

- $\overline{\mathbb{F}_p}$ is the union of all the $\mathbb{F}_{p^m}$.
- Pick an injective polynomial f from $\overline{\mathbb{F}_p}^n$ to $\overline{\mathbb{F}_p}^n$
- Let $\overline{b}$ be from $\overline{\mathbb{F}_p}^n$
- Let m be large enough that $\mathbb{F}_{p^m}$ contains $\overline{b}$ and the coefficients of f
- $f : \mathbb{F}_{p^m}^n \to \mathbb{F}_{p^m}^n$ is injective, so surjective

Proving Ax's Theorem - III

This turns out to be our "technical lemma:"

Fact

Every injective function from a finite set to itself is surjective.

Lemma

Ax's theorem holds for $\overline{\mathbb{F}_p}$.

Proof:

- $\overline{\mathbb{F}_p}$ is the union of all the $\mathbb{F}_{p^m}$.
- Pick an injective polynomial f from $\overline{\mathbb{F}_p}^n$ to $\overline{\mathbb{F}_p}^n$
- Let $\overline{b}$ be from $\overline{\mathbb{F}_p}^n$
- Let m be large enough that $\mathbb{F}_{p^m}$ contains $\overline{b}$ and the coefficients of f
- $f : \mathbb{F}_{p^m}^n \to \mathbb{F}_{p^m}^n$ is injective, so surjective
- There is an $\overline{a} \in \mathbb{F}_{p^m}^n \subset \overline{\mathbb{F}_p}^n$ where $f(\overline{a}) = \overline{b}$

Bringing It All Together

So Ax's theorem is true for $\mathbb{C}$ essentially because injective functions on finite sets are surjective.

Bringing It All Together

So Ax's theorem is true for $\mathbb{C}$ essentially because injective functions on finite sets are surjective.

Exercise

Figure out why the proof doesn't also show the converse of Ax's theorem, which is false.

Bringing It All Together

So Ax's theorem is true for $\mathbb{C}$ essentially because injective functions on finite sets are surjective.

Exercise

Figure out why the proof doesn't also show the converse of Ax's theorem, which is false.

Exercise

Using the same proof, prove Ax's theorem for varieties over algebraically closed fields.