Ax's Theorem with Model Theory

Cornell DRP Spring 2021

Felix Roz
fr247@cornell.edu

Mentor: Yibo Ji

May 28, 2021

When are injective polynomial maps surjective?

Simple cases

Simple cases

Finite fields

Any injective map from a finite set to itself is surjective.

Simple cases

Finite fields

Any injective map from a finite set to itself is surjective.

Algebraic closure of finite fields

Suppose $f : (\mathbb{F}_p^{alg})^n \to (\mathbb{F}_p^{alg})^n$ is an injective polynomial function with coefficients a and let $b \in (\mathbb{F}_p^{alg})^n$ be outside its range.

Simple cases

Finite fields
Any injective map from a finite set to itself is surjective.

Algebraic closure of finite fields
Suppose $f : (\mathbb{F}_p^{alg})^n \to (\mathbb{F}_p^{alg})^n$ is an injective polynomial function with coefficients a and let $b \in (\mathbb{F}_p^{alg})^n$ be outside its range. Since $(\mathbb{F}_p^{alg})$ is locally finite, the subfield k generated by a, b is finite and $f|_{k^n}$ is surjective.

Simple cases

Finite fields

Any injective map from a finite set to itself is surjective.

Algebraic closure of finite fields

Suppose $f : (\mathbb{F}_p^{alg})^n \to (\mathbb{F}_p^{alg})^n$ is an injective polynomial function with coefficients a and let $b \in (\mathbb{F}_p^{alg})^n$ be outside its range.
Since $(\mathbb{F}_p^{alg})$ is locally finite, the subfield k generated by a, b is finite and $f|_{k^n}$ is surjective.
This contradicts the assumption on b so f must be surjective as well.

Simple cases

Finite fields

Any injective map from a finite set to itself is surjective.

Algebraic closure of finite fields

Suppose $f : (\mathbb{F}_p^{alg})^n \to (\mathbb{F}_p^{alg})^n$ is an injective polynomial function with coefficients a and let $b \in (\mathbb{F}_p^{alg})^n$ be outside its range.
Since $(\mathbb{F}_p^{alg})$ is locally finite, the subfield k generated by a, b is finite and $f|_{k^n}$ is surjective.
This contradicts the assumption on b so f must be surjective as well.

What about polynomial maps $f : \mathbb{C}^n \to \mathbb{C}^n$?

Syntax

Syntax

Definition (Language $\mathcal{L}$)

A set of function symbols, relation symbols, and constant symbols each with a specified 'arity' (number of arguments)

Syntax

Definition (Language $\mathcal{L}$)

A set of function symbols, relation symbols, and constant symbols each with a specified ‘arity’ (number of arguments)

Definition ($\mathcal{L}$-formula)

Well-formed string of symbols from the language along with $=, \neg, \vee, \wedge, \exists, \forall$ and variable symbols. If all variables are bound, it is an $\mathcal{L}$-sentence.

Syntax

Definition (Language $\mathcal{L}$)

A set of function symbols, relation symbols, and constant symbols each with a specified 'arity' (number of arguments)

Definition ($\mathcal{L}$-formula)

Well-formed string of symbols from the language along with $=, \neg, \vee, \wedge, \exists, \forall$ and variable symbols. If all variables are bound, it is an $\mathcal{L}$-sentence.

Definition ($T \vdash \phi$)

A set T of $\mathcal{L}$-sentences proves an $\mathcal{L}$-sentence ϕ if there are a sequence of statements connected by a proof system. Usually Modus Ponens

Semantics

Semantics

Definition ($\mathcal{L}$-Structure $\mathcal{M}$)

An underlying set M, a function $f^{\mathcal{M}} : M^n \to M$ for each n-ary function symbol f, a relation $R^{\mathcal{M}} \subset M^n$ for each n-ary relation symbol R, and an element $c^{\mathcal{M}}$ for each constant symbol c.

Semantics

Definition ($\mathcal{L}$-Structure $\mathcal{M}$)

An underlying set M, a function $f^{\mathcal{M}} : M^n \to M$ for each n-ary function symbol f, a relation $R^{\mathcal{M}} \subset M^n$ for each n-ary relation symbol R, and an element $c^{\mathcal{M}}$ for each constant symbol c.

Definition ($\mathcal{M} \models T$)

An $\mathcal{L}$-structure, $\mathcal{M}$ models a set T of $\mathcal{L}$-sentences if the $\mathcal{M}$ interpretation of each sentence is true in the structure.

Semantics

Definition ($\mathcal{L}$-Structure $\mathcal{M}$)

An underlying set M, a function $f^{\mathcal{M}} : M^n \to M$ for each n-ary function symbol f, a relation $R^{\mathcal{M}} \subset M^n$ for each n-ary relation symbol R, and an element $c^{\mathcal{M}}$ for each constant symbol c.

Definition ($\mathcal{M} \models T$)

An $\mathcal{L}$-structure, $\mathcal{M}$ models a set T of $\mathcal{L}$-sentences if the $\mathcal{M}$ interpretation of each sentence is true in the structure.

Definition ($T \models \phi$)

ϕ is true in every model of T

Example

Example

$\mathcal{L}_r = \{+, -, \cdot, 0, 1\}$ is the language of rings (no relation symbols)
$Z = (\mathbb{Z}, +, -, \cdot, 0, 1)$ is an $\mathcal{L}_r$-structure.
The ring axioms are a set of $\mathcal{L}_r$-sentences
Z is a model of the ring axioms

Two Big Theorems of Model Theory

Two Big Theorems of Model Theory

Theorem (Completeness Theorem)

$T \vdash \phi$ *if and only if* $T \models \phi$

Two Big Theorems of Model Theory

Theorem (Completeness Theorem)

$T \vdash \phi$ if and only if $T \models \phi$

Theorem (Compactness Theorem)

If $T \models \phi$ then there is a finite subset $\Delta \subset T$ such that $\Delta \models \phi$.

Application to Algebraically Closed Fields

Application to Algebraically Closed Fields

ACF_p is the set of axioms for Algebraically Closed Fields with characteristic p as $\mathcal{L}_r$-sentences.

Application to Algebraically Closed Fields

ACF_p is the set of axioms for Algebraically Closed Fields with characteristic p as $\mathcal{L}_r$-sentences.

ACF_p is **complete** for $p = 0$ or prime p: $ACF_p \models \phi$ or $ACF_p \models \neg\phi$ for all $\mathcal{L}_r$-sentences ϕ. Can be proved using Vaught's test or Quantifier Elimination.

Back to Injective Polynomials

Back to Injective Polynomials

There is an $\mathcal{L}_r$ sentence $\Phi_{n,d}$ such that $K \models \Phi_{n,d}$ iff every injective degree d polynomial map from $K^n \to K^n$ is surjective.

Back to Injective Polynomials

There is an $\mathcal{L}_r$ sentence $\Phi_{n,d}$ such that $K \models \Phi_{n,d}$ iff every injective degree d polynomial map from $K^n \to K^n$ is surjective.

Suppose there is a counterexample in $\mathbb{C}$ ($ACF_0 \not\models \Phi_{n,d}$). By completeness $ACF_0 \models \neg\Phi_{n,d}$.

Back to Injective Polynomials

There is an $\mathcal{L}_r$ sentence $\Phi_{n,d}$ such that $K \models \Phi_{n,d}$ iff every injective degree d polynomial map from $K^n \to K^n$ is surjective.

Suppose there is a counterexample in $\mathbb{C}$ ($ACF_0 \not\models \Phi_{n,d}$). By completeness $ACF_0 \models \neg\Phi_{n,d}$.

By the compactness theorem there is a finite subset $\Delta \subset ACF_0$ such that $\Delta \vdash \neg\Phi_{n,d}$.

Back to Injective Polynomials

There is an $\mathcal{L}_r$ sentence $\Phi_{n,d}$ such that $K \models \Phi_{n,d}$ iff every injective degree d polynomial map from $K^n \to K^n$ is surjective.

Suppose there is a counterexample in $\mathbb{C}$ ($ACF_0 \not\models \Phi_{n,d}$). By completeness $ACF_0 \models \neg\Phi_{n,d}$.

By the compactness theorem there is a finite subset $\Delta \subset ACF_0$ such that $\Delta \vdash \neg\Phi_{n,d}$.

Δ will contain some of the axioms for an algebraically closed field and some of the axioms for characteristic 0, so for large enough p, $ACF_p \models \Delta$.

Back to Injective Polynomials

There is an $\mathcal{L}_r$ sentence $\Phi_{n,d}$ such that $K \models \Phi_{n,d}$ iff every injective degree d polynomial map from $K^n \to K^n$ is surjective.

Suppose there is a counterexample in $\mathbb{C}$ ($ACF_0 \not\models \Phi_{n,d}$). By completeness $ACF_0 \models \neg\Phi_{n,d}$.

By the compactness theorem there is a finite subset $\Delta \subset ACF_0$ such that $\Delta \vdash \neg\Phi_{n,d}$.

Δ will contain some of the axioms for an algebraically closed field and some of the axioms for characteristic 0, so for large enough p, $ACF_p \models \Delta$.

In particular, $ACF_p \models \neg\Phi_{n,d}$ which is a contradiction since we've already shown that $\mathbb{F}_p^{alg} \models \Phi_{n,d}$.

Main Result

Theorem (Ax's Theorem)

All injective polynomial maps $f : \mathbb{C}^n \to \mathbb{C}^n$ *are surjective*