Final Project

Yumin Shen

Definition For $S \subset K[x_1, ..., x_n]$, let $V(S) = \{\overline{a} \in K^n | \forall f \in S, f(\overline{a}) = 0\}$ denotes the vanishing set of S. Likewise, for $X \subset K^n$, let $I(X) = \{f \in K[x_1, ..., x_n] | \forall \overline{a} \in X, f(\overline{a}) = 0\}$ be the ideal of polynomials which vanish on X. A set is called algebraic if it is of the form $V(S)$ for some collection of polynomials S. Algebraic sets are also called Zariski closed because they constitute the closed sets in the Zariski topology. A set is called constructible if it is a boolean combination of algebraic sets.

Theorem (Tarski-Chevalley) In an algebraically closed field, the images of constructible sets under polynomial maps are constructible.

Let R be a ring and let Spec$R$ denote the collection of all prime ideals of R. We can equip Spec$R$ with a topology by defining the collection of closed sets to be $\{V_I | I$ is an ideal of $R\}$ where V_I denotes the set of all prime ideals extending I. This is called the Zariski topology.

Hilbert's basis theorem If R is a Noetherian ring, then $R[X]$ is an Noetherian ring.

Corollary $K[x_1, ..., x_n]$ is a Noetherian ring for an algebraic closed field K.

Problem 1 Describe ACF$^{\forall}$. Prove that ACF has quantifier elimination.

Proposition T is an $\mathcal{L}$-theory, then the following are equivalent:

1. T has quantifier elimination;
2. M_1, M_2 are two models of T, A is a common substructure of M_1, M_2 then for all quantifier free $L_{\mathcal{A}}$-formula, we have
$$M_1 \models \exists x\phi(x) \iff M_2 \models \exists x\phi(x)$$

Proof: In the language of $\mathcal{L} = \{0, 1, +, -, \cdot\}$, we can write ACF as:

1. $\forall x\forall y\forall z[x + (y + z) = (x + y) + z]$
2. $\forall x\forall y(x + y = y + x)$
3. $\forall x(x + 0 = x)$
4. $\forall x\exists y(x + y = 0)$
5. $\forall x\forall y\forall z(x \cdot (y \cdot z) = (x \cdot y) \cdot z)$
6. $\forall x\forall y(x \cdot y = y \cdot x)$
7. $\forall x(x \cdot 1 = x)$
8. $\forall x\forall y\forall z(x \cdot (y + z) = x \cdot y + x \cdot z)$
9. $\forall x(x \neq 0 \to \exists y(x \cdot y = 1))$
10. $\forall a\forall b(a \cdot b = 0 \to a = 0 \vee b = 0)$
11. $\forall x_0 ... \forall x_{n-1}\exists y(y^n + x_0 y^{n-1} + ... + x_{n-1} = 0)$, $n \in \mathbb{N}$ (Not universal)

Let $\mathcal{M} \models$ ACF, $\mathcal{N} \models$ ACF, $\mathcal{A}$ is a substructure of both $\mathcal{M}$ and $\mathcal{N}$. A substructure must satisfies all universal sentence, therefore satisfies $\forall a\forall b(a \cdot b = 0 \implies a = 0 \vee b = 0)$. So, $\mathcal{A}$ must be an integral domain. Take $\overline{\mathcal{F}_{\mathcal{A}}}$, the algebraic closure of field of fractions of $\mathcal{A}$. $\overline{\mathcal{F}_{\mathcal{A}}}$ must be a substructure of $\mathcal{M}$ and $\mathcal{N}$ by ACF.

By the above proposition, we only need to prove for all quantifier-free $\mathcal{L}_{\mathcal{A}}$-formula $\phi(x)$, $\mathcal{M} \models \exists x\phi(x)$ iff $\mathcal{N} \models \exists x\phi(x)$. However, since all $\mathcal{L}_{\mathcal{A}}$-atomic formula are in the form of $f(x) = 0$, where $f \in \mathcal{A}[x] \subset \overline{\mathcal{F}_{\mathcal{A}}}[x]$. Therefore, for all quantifier-free $\mathcal{L}$-formula $f(x) = 0$, there exists finitely many polynomials $f_1, ..., f_n \in A[x] \subset \overline{\mathcal{F}_{\mathcal{A}}}[x]$ such that every $\phi_i(x)$ is in the form of $f_1(x)\Box 0 \wedge ... \wedge f_m(x)\Box 0$, where $\Box$ is $=$ or $\neq$. We assume $\phi(x)$ to be:

$$f_0(x) = 0 \wedge ... \wedge f_{n-1}(x) = 0 \wedge g_0(x) \neq 0 \wedge ... \wedge g_{n-1} \neq 0$$

Case 1 Exists $0 \leq i_0 < n$ such that f_{i_0} is not constant, and $M \models \exists x\phi(x)$, that is, exists $a \in M$ such that $M \models \phi(a)$. Since f_{i_0} is not constant, a is algebraic on $\overline{\mathcal{F}_{\mathcal{A}}}$. Let $m_a(x) \in A[x]$ be the minimal polynomial of a on field $\overline{\mathcal{F}_{\mathcal{A}}}$. Since M is an algebraic closed field, there is a $b \in N$ such that $m_a(b) = 0$. Therefore, $N \models \phi(b)$. That is, $\mathcal{N} \models \exists x\phi(x)$.

Case 2 Suppose f_i are constant for all i. Then, $f_i(x) \equiv 0$. g_i can have at most finitely many roots, therefore there must have $b \in N$ such that $\mathcal{N} \models g_0(b) \neq 0 \wedge ... \wedge g_{n-1}(b) \neq 0$. Therefore $N \models \exists x\phi(x)$.

We're done.

Problem 2 Prove the following corollaries to quantifier elimination: ACF is model complete, ACF is decidable, the Tarski-Chevalley Theorem, ACF is strongly minimal, ACF is the model companion of the theory of fields.

Proof (Model Completeness)

Let $\mathcal{M}, \mathcal{N} \models T$. $\mathcal{M}$ is a substructure of $\mathcal{N}$. Let $\phi(\overline{v})$ be an $\mathcal{L}$-formula and let $\overline{a} \in M^n$. By quantifier elimination, there should be a quantifier-free formula $\psi(\overline{v})$ such that $T \models \forall \overline{v}(\phi(\overline{v}) \leftrightarrow \psi(\overline{v}))$. Since $\mathcal{M} \models T$, $\mathcal{M} \models \forall \overline{v}(\phi(\overline{v}) \leftrightarrow \psi(\overline{v}))$. For the same reason, $\mathcal{N} \models \forall \overline{v}(\phi(\overline{v}) \leftrightarrow \psi(\overline{v}))$.
Therefore, $\mathcal{M} \models \phi(\overline{a}) \Leftrightarrow \mathcal{M} \models \psi(\overline{a}) \Leftrightarrow \mathcal{N} \models \psi(\overline{a}) \Leftrightarrow \mathcal{N} \models \phi(\overline{a})$

Proof: (Tarski-Chevalley)

All definable sets are quantifier-free definable, by QE of ACF.

However, all constructible sets exactly quantifier-free definable sets. Indeed, for an atomic $\mathcal{L}$-formula $\phi(\overline{x}, \overline{y})$, there is a formula $q(\overline{x}, \overline{y}) = 0$ that is equivalent to $\phi(\overline{x}, \overline{y})$. If X is defined by $\phi(\overline{x}, \overline{a})$, then $X = V(q(\overline{x}, \overline{a}))$. If $p \in K[\overline{x}]$, then $V(p)$ is QF definable by QE.

Let $X \subset K^n$ be constructible, and p be a polynomial map. Then the image of X is definable, hence constructible.

Proof: (Strongly minimal)

By QE, if $X \subset K$ is definable then it is a finite boolean combination of sets of the form $V(p)$, where $p \in K[x]$. $V(p)$ is either finite or all of K.

Proof: (Model companion)

ACF is model complete. Every model of ACF is a model of theory of field. Every model of theory of field can be extended to a model of ACF by taking its algebraic closure. So, by definition, ACF is a model companion of theory of field.

Proposition: ACF$_p$ is κ-categorical for all uncountable cardinals κ.
Proof: Two algebraically closed fields are isomorphic if and only if they have same characteristic and transcendence degree. An algebraically closed field of transcendence degree λ has cardinality $\lambda + \alpha_0$. If $\kappa > \aleph_0$, then an algebraically closed field of cardinality κ also has transcendence degree κ. Thus, any two algebraically closed fields of the same characteristic and same uncountable cardinality are isomorphic.

Corollary ACF$_p$ is complete. This is by Łos-Vaught's test.

Recall that we say an $\mathcal{L}$-theory T is decidable if there is an algorithm that when given an $\mathcal{L}$-sentence ϕ as input decides whether $T \models \phi$.

Proof: (Decidable)

To decide if ACF$_p \models \phi$ search for a proof of ϕ or $\neg\phi$. By completeness, there is a finite step proof.
To decide if ACF$\models \phi$ search for either a proof of ϕ from ACF or a prime p and a proof of $\neg\phi$ from ACF_p.
By saying searching for a proof, we are actually listing all sentence and see whether it is a valid proof.

Problem 3 Use model theory to prove Hilbert's Nullstellensatz:
If $K \models \text{ACF}$ and $P \subset K[x_1, ..., x_n]$ is prime ideal, then $V(P) \neq \varnothing$.

$$V(P) = \{\overline{a} \in K^n | \forall f \in P, f(\overline{a}) = 0\}$$

Proof $K[x_1, ..., x_n]$ is Noetherian, hence P is generated by finitely many element in $K[x_1, ..., x_n]$. Let $P = (f_1, ..., f_k)$. Let M be the maximal ideal containing P, then we have $F = K[x_1, ..., x_n]/M$ is a field.

Let $\overline{F}$ be the algebraic closure of F. Then, $K \subset F \subset \overline{F}$, where $K \models \text{ACF}$, $L \models \text{ACF}$.

Let $\overline{a} = (x_1 + M, ..., x_n + M)$ be an element of F^n such that $f_1(\overline{a}) = ... = f_k(\overline{a}) = 0$. Then, we have

$$\overline{F} \models \exists \overline{a}((f_1(\overline{a}) = 0) \wedge ... \wedge (f_k(\overline{a}) = 0))$$

by model completeness,

$$K \models \exists \overline{a}((f_1(\overline{a}) = 0) \wedge ... \wedge (f_k(\overline{a}) = 0))$$

Therefore we have $f_1(\overline{a}) = ... = f_k(\overline{a}) = 0$.

Problem 4 Let $k \models$ ACF and let $k \prec \mathbb{K}$. Construct a continuous bijection from $S_n^{\mathbb{K}}(k) \to$Spec$(k[x_1, ..., x_n])$. Prove that the theories ACF$_0$ and ACF$_p$ for p prime are κ-stable for all infinite cardinals κ.

Proof First, we list out all elements in $S_n^{\mathbb{K}}(k)$. The set all complete n-types are the ultrafilters of boolean algebra generated by all n-variables polynomial equations, and their negation.

Let $(\phi) := \{p \in S_n^{\mathbb{K}}(k) | \phi \in p\}$.

Clearly

We construct a mapping

$$\iota : S_n^{\mathbb{K}}(k) \to \text{Spec}(k[x_1, ..., x_n])$$
$$p \to \iota(p) = \{f \in k[x_1, ..., x_n] : \{f(\overline{x}) = 0\} \in p\}$$

Apparently, P is an ideal.

To prove it is prime, notice that if $fg \in \iota(p)$, then $\mathbb{K} \models \forall \overline{x}(fg(\overline{x})) = 0$

Since $k[x_1, ..., x_n]$ is integral domain, either $f = 0$ or $g = 0$. So, $\iota(p)$ is prime.

Injectivity: Let $p \neq q \in S_n^{\mathbb{K}}(k)$. Therefore, exists $\phi \in p, \phi \notin q$. However, by completeness, $\neg\phi \in q$.

We can write by QE,

$$\phi = \bigvee_{i=1}^{m} \left[\bigwedge_{j=1}^{n} f_j^i(\overline{x}) = 0 \wedge \bigwedge_{l=1}^{k} g_l^i(\overline{x}) \neq 0 \right]$$

If $\iota(p) = \iota(q)$, then $f_j^i(\overline{x}) = 0 \in p$ iff $f_j^i(\overline{x}) = 0 \in q$, $g_l^i(\overline{x}) = 0 \in p$ iff $g_l^i(\overline{x}) = 0 \in q$. So, we cannot have $\phi \in p$ and $\neg\phi \in q$.

Surjectivity: Suppose $P \subset k[x_1, ..., x_n]$ is a prime ideal. Then, there is a prime ideal $Q \subset \mathbb{K}[x_1, ..., x_n]$ generated by P. We take the algebraic closure of $\mathcal{F}_{\mathbb{K}[x_1,...,x_n]/Q} = \mathbb{F}$, and then $k \prec F$ by model completeness.

For $f \in \mathbb{K}[\overline{x}]$, $f(x_1 + Q, ..., x_n + Q) = 0$ iff $f \in Q$. Let $p =$tp$^F(\overline{x}/k)$, then $\iota(p) = P$, since $(P) \cap k[\overline{x}] = P$.

Continuity: For a prime ideal $P = (f_1, ..., f_m)$, we have $\iota^{-1}(P) = \{p | \bigwedge_{i=1}^{m} f_i(\overline{x}) = 0 \in p\}$, which is an open set. Hence this is continuous.

κ-Stability: We already have a bijection between $S_n^{\mathbb{K}}(k)$ and Spec$(k[x_1, ..., x_n])$. $|\text{Spec}(k[x_1, ..., x_n])| = \kappa + \aleph_0$ since all the prime ideals are finitely generated. Since κ is an infinite cardinal, $\kappa = \kappa + \aleph_0$, hence $|S_n^{\mathbb{K}}(k)| = \kappa$.

If $A \subset k$ be a set of cardinal κ, then we take the field generated by A, which is no bigger than κ by Löwenheim-Skolem. So, we conclude that

$$\kappa \leq |S_n^{\mathbb{K}}(A)| \leq |S_n^{\mathbb{K}}(k)| \leq \kappa$$

Problem 5 Let $\mathcal{K} \models$ ACF be uncountable and let $k \prec \mathcal{K}$ be a proper subfield. If you like you can assume $|k| < |\mathcal{K}|$, although this shouldn't be necessary. For $\overline{a}, \overline{b} \in \mathcal{K}^n$, prove that $\text{tp}^{\mathcal{K}}(\overline{a}/k) = \text{tp}^{\mathcal{K}}(\overline{b}/k)$ if and only if there is an automorphism $\sigma \in \text{Aut}_k(\mathcal{K})$ fixing k pointwise such that $\sigma(\overline{a}) = \overline{b}$. Prove that $\mathcal{K}$ realizes every type in $S_n^{\mathcal{K}}(k)$ for all $n \in \mathbb{N}$.

Proof: The first part is a corollary of problem 2 of homework 3. Every type of $\overline{a}$ is like

$$\text{tp}^{\mathcal{K}}(\overline{a}/A) = \{\phi(v_1, ..., v_n) \text{ an quantifier free } \mathcal{L}_k\text{-formula } |\mathcal{K} \models \phi(\overline{a})\}$$

If there is an automorphism $\sigma \in \text{Aut}_k(\mathcal{K})$ fixing k pointwise such that $\sigma(\overline{a}) = \overline{b}$

Then,

$$\text{tp}^{\mathcal{K}}(\overline{b}/A) = \{\phi(v_1, ..., v_n) \text{ an quantifier free } \mathcal{L}_k\text{-formula } |\mathcal{K} \models \phi(\overline{b})\}$$

$$\sigma_* : \text{tp}^{\mathcal{K}}(\overline{a}/A) \to \text{tp}^{\mathcal{K}}(\sigma(\overline{a})/A)$$

$$\text{tp}^{\mathcal{K}}(\sigma(\overline{a})/A) = \{\sigma_*\phi(v_1, ..., v_n) \text{ an quantifier free } \mathcal{L}_k\text{-formula } |\mathcal{K} \models \phi(\sigma(\overline{a}))\}$$

$$= \text{tp}^{\mathcal{K}}(\overline{b}/A) = \{\phi(v_1, ..., v_n) \text{ an quantifier free } \mathcal{L}_k\text{-formula } |\mathcal{K} \models \sigma \circ \phi(\overline{a})\}$$

$$= \text{tp}^{\mathcal{K}}(\overline{b}/A) = \{\phi(v_1, ..., v_n) \text{ an quantifier free } \mathcal{L}_k\text{-formula } |\mathcal{K} \models \phi(\overline{a})\}$$

Therefore they are same.

Conversely, since all the formulas are polynomial equations, then if $\overline{a}$ and $\overline{b}$ shares the same roots over all polynomial equation, they must be conjugate. Therefore, we know there is an field automorphism that sends $\overline{a}$ to $\overline{b}$, and fix k pointwise.

Every type in $S_n^{\mathcal{K}}(k)$ defines a prime ideal. By Hilbert's Nullstellensatz, this is realizable.

Problem 6 (Ax-Grothendieck) Use model theory to prove the following: Every injective polynomial map from $\mathbb{C}^n$ to $\mathbb{C}^n$ is surjective.

Proof: For finite field, this is trivial, since $\mathbb{F}^n$ is finite, injectivity implies surjectivity.

For infinite case, we shall first state the theorem in the language of ACF.

Injectivity of f can be defined as follows:

$$\forall \overline{x} \forall \overline{y} (f(\overline{x}) = f(\overline{y}) \rightarrow \overline{x} = \overline{y})$$

Similarly, the surjectivity of f is defined as follows:

$$\forall \overline{y} \exists \overline{x} (y = f(\overline{x}))$$

We shall also define what does it mean for f to be a polynomial, which can be defined by specifying coefficients.

Let $\overline{a} = (a_0, ..., a_n)$ be the coefficients of a degree n polynomial f. Then, we can denote the polynomial $f = \sum_{i=0}^{n} a_i x^i$ by $f_{\overline{a}}(x)$.

Finally, we can state it in ACF.

$\phi : \forall a_0 \forall a_1 .... \forall a_n (\forall \overline{x} \forall \overline{y} (f_{\overline{a}}(\overline{x}) = f_{\overline{a}}(\overline{y}) \rightarrow \overline{x} = \overline{y}) \rightarrow \forall \overline{y} \exists \overline{x} (y = f_{\overline{a}}(\overline{x})))$

Recall the Lefschetz Principle, the following are equivalent:

1. $\mathrm{ACF}_0 \models \phi$
2. ϕ is true in some algebraically closed field of characteristic 0
3. There are arbitrarily large primes p such that ϕ is true in some algebraically closed field of characteristic p.
4. There is $N \in \mathbb{N}$ such that for all $p > N$, ϕ is true in every algebraically closed field of characteristic p.

We now pass from a finite field $\mathbb{F}_p$ to its algebraic closure $\overline{\mathbb{F}}_p$. Suppose $f : \overline{\mathbb{F}}_p^n \rightarrow \overline{\mathbb{F}}_p^n$ is injective. Choose $\overline{a} \in \overline{\mathbb{F}}_p^n$. We want to find $\bar{b}$ such that $f(\bar{b}) = \overline{a}$. Let L be the field generated by K and all the coordinates of b and the coefficients of f. Then, f is an injective map from $L^n \rightarrow L^n$. However, L is a finite extension, therefore finite. So we must have the surjectivity of f, and $\overline{a}$ is in the image of f. Hence we're done by applying Lefschtez Principle.