Math Logic: Model Theory & Computability
Lecture 18

Consequences of the completeness of ACF_p.

The following was believed by algebraists, but was turned into a theorem by A. Robinson.

Lefschetz Principle. Let $\sigma_{ring} := (0, 1, +, -, \cdot)$ and $\underline{\mathbb{C}} := (\mathbb{C}, 0, 1, +, -, \cdot)$. Let φ be a σ_{ring}-sentence. Then TFAE (the following are equivalent):

(1) $\underline{\mathbb{C}} \models \varphi$.

(2) $\underline{F} \models \varphi$ for all $\underline{F} \models ACF_0$.

(3) $ACF_0 \models \varphi$.

(4) $ACF_p \models \varphi$ for all large enough primes $p \in \mathbb{N}$ ($\forall^\infty p := \exists N \, \forall p \geq N$).

(5) For infinitely-many primes $p \in \mathbb{N}$, there is $\underline{K_p} \models ACF_p$ such that $\underline{K_p} \models \varphi$.

Proof. (1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (3). Follows directly from the completeness of ACF_0 because $ACF_0 \models \varphi$ or $ACF_0 \models \neg\varphi$.

(3) $\Rightarrow$ (4). Proven in homework, follows from Compactness.

(4) $\Rightarrow$ (5). Trivial.

(5) $\Rightarrow$ (1). We prove $\neg(1) \Rightarrow \neg(5)$. $\neg(1)$ means $\underline{\mathbb{C}} \models \neg\varphi$, so by (1) $\Rightarrow$ (4) applied to $\neg\varphi$, we get $\forall^\infty p$ primes, $ACF_p \models \neg\varphi$, which implies $\neg(5)$. $\square$

Ax's Theorem. Let $f : \mathbb{C}^n \to \mathbb{C}^n$ be a polynomial function, i.e. $f := (f_1, f_2, \ldots, f_n)$, where each $f_i : \mathbb{C}^n \to \mathbb{C}$ is a polynomial in variables $x_1, x_2, \ldots, x_n$. If f is injective then it is surjective.

Remark. For $n = 1$, if f is injective then it is necessarily linear and nonconstant (HW), hence in particular surjective.

Proof (A. Robinson). The idea is to replace $\mathbb{C}$ with a finite field and use Pigeonhole Principle. For fixed n and $d := \max(f_1, f_2, \dots, f_n)$, we can write down a $\mathcal{L}_{ring}$-sentence $\varphi_{n,d}$ that says that for all polynomial functions $f := (f_1, f_2, \dots, f_n)$ on variables $\vec{x} := (x_1, x_2, \dots, x_n)$ of degree $\leq d$, if f is injective then f is surjective.
By the Lefschetz principle, to show $\mathbb{C} \models \varphi_{n,d}$, it is enough to show that for all primes p there is a field $K_p \models ACF_p$ such that $K_p \models \varphi_{n,d}$.
Fix a prime $p \in \mathbb{N}$. Let $\overline{\mathbb{F}_p}$ denote an algebraic closure of the field $\mathbb{F}_p$ of p elements. We will show that $\overline{\mathbb{F}_p} \models \varphi_{n,d}$.

Claim. $\overline{\mathbb{F}_p} = \biguplus_{m \in \mathbb{N}} F_m$, where each F_m is finite.

Proof. Let $F_0 := \mathbb{F}_p$, and supposing that F_n is define, we define F_{m+1} by adjoining to F_m one root for each polynomial of degree $\leq |F_m|$ with coefficients in F_m. Since there are only finitely many such polynomials, F_{m+1} is finite. Then the union $\biguplus_{m \in \mathbb{N}} F_m$ is algebraically closed since for each polynomial p with coefficients from this union, there $m \geq \deg(p)$ such that F_m contains all the coefficients of p, hence F_{m+1} contains a root of p. $\boxtimes$

Now to show $\overline{\mathbb{F}_p} \models \varphi_{n,d}$, let $f : \overline{\mathbb{F}_p}^n \to \overline{\mathbb{F}_p}^n$ be a polynomial function of max degree d. Suppose f is injective. Since all coefficients of f are from $\overline{\mathbb{F}_p}$, there is m_0 large enough so that F_m contains all the coefficients of f.
Note that $\overline{\mathbb{F}_p} = \bigcup_{m \geq m_0} F_m$ and $f(F_m^n) \subseteq F_m^n$ for all $m \geq m_0$ because $F_m \supseteq F_{m_0} \ni$ all coeffs of f and F_m is a field. But f is injective and F_m^n is finite, so by the Pigeonhole Principle, $f(F_m^n) = F_m^n$. Thus,

$$f(\overline{\mathbb{F}_p}) = \biguplus_{m \geq m_0} f(F_m) = \biguplus_{m \geq m_0} F_m = \overline{\mathbb{F}_p},$$

so f is surjective. $\square$

The syntactic aspect of first-order logic: proof theory.

For a σ-theory T and a σ-sentence φ, we have defined $T \models \varphi$, which means that φ holds in all models of T. We will now define a different relation "T proves φ", denoted $T \vdash \varphi$, which would mean that there is a (finite) proof of φ from T (a finite syntactic certificate). The Gödel's Completeness-of-first-order-logic theorem (call it syntactic-semantic duality) says that

$$T \models \varphi \quad \text{iff} \quad T \vdash \varphi,$$

equating a $\forall$-statement to a $\exists$-statement.

To define the notion of a proof, we need to fix a set $\mathrm{Axiom}(\sigma)$ of basic logical axioms (tautologies) to use in our formal proofs, as well as a rule of inference, call modus ponens.

Axioms(σ). Fix a signature σ.

Def. For σ-formula φ, we say that a σ-term t is okay to substitute for a variable x in φ if neither x nor any variable in t is quantified in φ. In this case, we denote by $\varphi(t/x)$ the formula obtained from φ by substituting every occurance of x in φ with t.

Convention. Below, whenever we write $\varphi(t/x)$ it is assumed that t is OK to substitute for x in φ.

Convention. The axioms in $\mathrm{Axioms}(\sigma)$ only use $\rightarrow, \neg, \forall$, so from now on we treat $\varphi \vee \psi$, $\varphi \wedge \psi$, $\exists v \varphi$ as abbreviations for

- $(\neg\varphi) \rightarrow \psi$.
- $\neg\big((\neg\neg\varphi) \rightarrow (\neg\psi)\big) \iff \neg\big(\varphi \rightarrow (\neg\psi)\big)$.
- $\neg \forall v \neg \varphi$.