Mathematical Logic

Lecture 6

Harbin, 2023

Graph colouring

Let's consider an application of the compactness theorem to prove a purely combinatorial result.

Recall that a graph $G = (V, E)$ (here V - vertices, E - edges) is $k-$colourable if there is a function $c : V \to \{1, \dots, k\}$ mapping the set of vertices to a set of k colours such that adjacent vertices do not have the same colour, i.e., $(u, v) \in E$ implies $c(u) \neq c(v)$.

Let us say that (V_1, E_1) is a subgraph of G if $V_1 \subseteq V$ and $E_1 \subseteq E$.

Proposition 1.

Let $G = (V, E)$ be a graph with set of vertices $V = \{v_i : i \in \mathbb{N}\}$. Suppose that every finite subgraph of G is $k-$colourable. Then G is $k-$colourable.

Proof. Recall how we reduced $k-$colouring to propositional satisfiability. Introduce propositional variables $P_{v,i}$ for each $v \in V$ and $1 \leq i \leq k$, interpreted as "vertex v has colour i ". We consider the following propositions:

- $F_v := \vee_{i=1}^{k} P_{v,i}$ (vertex v has some colour)
- $G_v := \wedge_{i=1}^{k} \wedge_{j=i+1}^{k} \neg P_{v,i} \vee \neg P_{v,j}$ (vertex v has at most one colour)
- $H_{u,v} := \wedge_{i=1}^{k} \neg P_{u,i} \vee \neg P_{v,i}$ (vertices u and v don't have the same colour)

Now define $\mathcal{S} = \{F_v, G_v : v \in V\} \cup \{H_{u,v} : (u, v) \in E\}$. We claim that $\mathcal{S}$ is satisfiable if and only if the graph G has a $k-$colouring. Indeed, given such a colouring c, define an assignment $\mathfrak{J}$ by $\mathfrak{J}(P_{v,i}) = 1$ if and only if $c(v) = i$. Then it is clear that $\mathfrak{J}$ satisfies $\mathcal{S}$. Conversely, given an assignment $\mathfrak{J}$ satisfying $\mathcal{S}$ we can define a $k-$colouring c by $c(v) = i$ if and only if $\mathfrak{J}(P_{v,i}) = 1$.

By assumption, every finite subgraph of G has a $k-$colouring. It follows that every finite subset of $\mathcal{S}$ is satisfiable. By the Compactness Theorem it must be that $\mathcal{S}$ is satisfiable, and thus G itself is $k-$colourable. ■

Applications

Theorem 2.

Let $(A, \prec)$ be a countable partial order. Then there exists a linear ordering $<$ of A which extends $\prec$.

Proof. We work with the propositional language which has sentence symbols $L_{a,b}$ for $a \neq b \in A$. Let Σ be the following set of well-formed formulas:

(a) $L_{a,b} \vee L_{b,a}$ for $a \neq b \in A$
(b) $\neg(L_{a,b} \wedge L_{b,a})$ for $a \neq b \in A$
(c) $((L_{a,b} \wedge L_{b,c}) \rightarrow L_{a,c})$ for distinct $a, b, c \in A$
(d) $L_{a,b}$ for distinct $a, b \in A$ with $a \prec b$

Claim. Suppose that v is a truth assignment which satisfies Σ. Define the binary relation $<$ on A by

$$a < b \text{ iff } v(L_{a,b}) = T$$

Then $<$ is a linear ordering of A which extends $\prec$.

Applications

proof of the claim: By (a), (b), (c), $<$ is a linear order. Finally, by (d), $<$ extends $\prec$.

Next we prove that Σ is finitely satisfiable. So let $\Sigma_0 \subseteq \Sigma$ be any finite subset. Let $A_0 \subseteq A$ be the finite set of elements that are mentioned in Σ_0 and consider the partial order $(A_0, \prec_0)$. Then there exists a partial ordering $<_0$ of A_0 extending $\prec_0$. Let v_0 be the truth assignment such that if $a \neq b \in A_0$, then

$$v_0(L_{a,b}) = T \text{ iff } a \leq_0 b$$

Clearly, v_0 satisfies Σ_0. By the compactness theorem, Σ is satisfiable. Hence there exists a linear ordering $<$ of A which extends $\prec$. ■

$\boxed{\textit{Definition.}}$ Suppose that S is a set and that $\langle S_i | i \in I \rangle$ is an indexed collection of (not necessarily distinct) subsets of S. A system of distinct representatives is a choice of elements $x_i \in S_i$ for $i \in I$ such that if $i \neq j \in I$, then $x_i \neq x_j$.

Example. Let $S = \mathbb{N}$ and let $\langle S_n | n \in \mathbb{N} \rangle$ be defined by

$$S_n = \{n, n+1\}$$

Then we can take $x_i = i \in S_i$.

Hall's Marriage Theorem

Let S be any set and let $n \in \mathbb{N}$. Let $\langle S_1, S_2, \ldots, S_n \rangle$ be an indexed collection of subsets of S. Then a necessary and sufficent condition for the existance of a system of distinct representatives is:
(H) For every $1 \leq k \leq n$ and choice of k distinct indices $1 \leq i_1, \ldots, i_k \leq n$, we have $|S_{i_1} \cup \ldots \cup S_{i_k}| \geq k$.

Example.

Suppose there are n women and n men, all of whom want to get married to someone of the opposite sex. Suppose further that the women each have a list of the men they would be happy to marry, and that every man would be happy to marry any woman who is happy to marry him, and that each person can only have one spouse.

In this case, Hall's marriage theorem says that the men and women can all be paired off in marriage so that everyone is happy, if and only if the marriage condition holds : if in any group of women, the total number of men who are acceptable to at least one of the women in the group is greater than or equal to the size of the group.

Again, it is clear that this condition is necessary. Hall's marriage theorem is that it is sufficient as well. To see why the theorem applies in this case, let S_i be the set of men that the ith woman would be happy to marry; then the marriage condition in the previous paragraph is the same as the marriage condition on the family of sets S_i. So there is a system of distinct representatives, which is a choice of an acceptable man for each woman.

Question. State and prove an infinite analogue of Hall's Marriage Theorem

First Attempt. Let S be any set and let $\langle S_n | n \in \mathbb{N} \rangle$ be an indexed collection of subsets of S. Then a necessary and sufficient condition for the existence of a system of distinct representatives is:
(H') For every $k \in \mathbb{N}$ and choice of k distinct indices $i_1, \ldots, i_k \in \mathbb{N}$, we have $|S_{i_1} \cup \ldots \cup S_{i_k}| \geq k$.

Counterexample. Take $S_1 = \mathbb{N}$, $S_2 = \{0\}$, $S_3 = \{1\}, \ldots, S_n = \{n-2\}, \ldots$
Clearly (H') is satisfied and yet there is no system of distinct representatives.

Infinite Hall's Theorem

Let S be any set and let $\langle S_n | n \in \mathbb{N} \rangle$ be an indexed collection of finite subsets of S. Then a necessary and sufficient condition for the existence of a system of distinct representatives is:
(H*) For every $k \in \mathbb{N}$ and choice of k distinct indices $i_1, \ldots, i_k \in \mathbb{N}$, we have $|S_{i_1} \cup \ldots \cup S_{i_k}| \geq k$.

Proof. We work with the propositional language with sentence symbols $C_{n,x}$, where $n \in \mathbb{N}, x \in S_n$. Let Σ be the following set of well-formed formulas:
(a) $\neg(C_{n,x} \wedge C_{m,x})$ for $n \neq m \in \mathbb{N}, x \in S_n \cap S_m$
(b) $\neg(C_{n,x} \wedge C_{n,y})$ for $n \in \mathbb{N}, x \neq y \in S_n \cap S_m$
(c) $\neg(C_{n,x_1} \vee \ldots \vee C_{n,x_k})$ for$n \in \mathbb{N}$, where $S_n = \{x_1, \ldots, x_k\}$

Claim. Suppose that v is a truth assignment which satisfies Σ. Then we can define a system of distinct representatives by

$$x \in S_n \text{ iff } v(C_{n,x}) = T$$

proof of the claim. By (b) and (c), each S_n gets assigned a unique representative. By (a), distinct sets $S_m \neq S_m$ get assigned distinct representatives.

Next we prove that Σ is finitely satisfiable. So let $\Sigma_0 \subseteq \Sigma$ be any finite subset. Let $\{i_1, \ldots, i_l\}$ be the indices that are mentioned in Σ_0. Then $\{S_{i_1}, \ldots, S_{i_l}\}$ satisfies condition (H*). By Hall's Theorem, there exists a set of distinct representatives for $\{S_{i_1}, \ldots, S_{i_l}\}$; say, $x_r \in S_{i_r}$. Let v_0 be the truth assignment such that for $1 \leq r \leq l$ and $x \in S_{i_r}$,

$$v(C_{i_r,x}) = T \text{ iff } x = x_r$$

Clearly v_0 satisfies Σ_0. By the Compactness Theorem, Σ is satisfiable. Hence there exists a system of distinct representatives. ■

Applications

Let's get more applications of the compactness theorem.

Definition 1. A theory of language $\mathcal{L}$ is a collection of sentences of $\mathcal{L}$.

Definition 2. A set of axioms for a theory is a set of sentences which has the same exact set of consequences in first-order logic as the theory itself.

Using this definition, we see that if we are given some theory Σ which has Δ as a set of axioms, then Δ, to some extent, characterizes Σ.

Example. Every one of the field axioms is expressible in first-order logic. Consequently, we consider every field to be an example of a theory which has the field axioms as a set of axioms. By adding the axioms for an ordering, which are also expressible in first-order logic, we can obtain a set of axioms for an ordered field.

Suppose that Δ is a set of axioms for two theories, Σ and Σ'. From our definition, we know that Σ and Σ' have the same exact set of consequences in first-order logic. Thus, if they differ, we know two things: first, the properties that they differ by are not expressible in first-order logic, and second, the properties that they differ by are not consequences of Δ in first-order logic.

Consider the Archimedean Property of the real numbers. This states: For all real $a, b > 0$, there exists a natural number n such that $na \geq b$.

We will show in the following example that it is possible to construct a theory which has the same consequences in first-order logic as the axioms for an ordered field, but does not have the Archimedean Property. This demonstrates that the Archimedean Property is not expressible in first-order logic and it is not a consequence of the field axioms.

Proposition 3.

There exists an ordered field $\Bbbk$ that is not Archimedean.

Proof. Let $\mathcal{L} = \{+, \cdot, 0, 1, \leq\}$ and let Γ be the set of all sentences which hold in the ordered field of real numbers. Now let x be a constant symbol which is not 0 or 1, and let

$$\Sigma = \Gamma \cup \{0 < x\} \cup \{1 \leq x\} \cup \{2 \leq x\} \cup \{3 \leq x\} \dots$$

This set of additional sentences is a way of stating in first-order logic that x is larger than every natural number. This is also an infinite collection of sentences, which is where the Compactness Theorem comes into play, by showing that Σ has a model.

Let Σ' be an arbitrary finite subset of Σ. Now, we must show that Σ' has a model. It is clear that $\Sigma' \cap \Gamma$ has a model because it is simply a subset of Γ, which is modeled by the axioms for the real numbers. Now for all sentences $\phi \in \Sigma' \setminus \Gamma$, we can expand the model of the real numbers to include ϕ, because the sentence ϕ does not have any interaction with any of the consequences of Γ, because it involves a constant symbol which is not in Γ, namely x.

Thus, every finite subset of Σ has a model, so by the Compactness Theorem, Σ has a model which clearly satisfies all of the properties of an ordered field. However, if we examine Σ, we see that while both 1 and x are positive, by construction there does not exist a natural number n such that $n \cdot 1 \geq x$. Therefore, in this model, we have an ordered field which does not have the Archimedean Property. ■

How to build such a field?

Hyperreal field $\mathcal{R}$

$\boxed{\textit{Definition } 3.}$ (i) A number δ in an ordered field is called infinitesimal if it satisfies $|\delta| < \frac{1}{m}$ for any natural number m.
(ii) Two hyperreal numbers x and y are said to be infinitely close, or differ by an infinitesimal, if $x - y$ is infinitesimal. In this case we write $x \approx y$.

Remark. 1.) This definition is intended to include 0 as an infinitesimal.
2.) So, our informal "approximately equal" notation "$\approx$" is replaced by this precise definition. An infinitesimal is a number that satisfies $\delta \approx 0$.
Archimedes Axiom is precisely the statement that the "classical" real numbers have no positive infinitesimals. Keisler's Algebra Axiom is the following:

Keisler's Algebra Axiom

The hyperreal numbers are an ordered field extension of the real numbers. In particular, there is a positive hyperreal infinitesimal, δ, satisfying $0 < \delta < \frac{1}{m}$ for any $m \in \mathbb{N}$.

It follows from the laws of ordered algebra that there are many different infinitesimals. For example, the law $a < b \Rightarrow a + c < b + c$ applied to $a = 0$ and $b = c = \delta$ says $\delta < 2\delta$. Similarly, all the integer multiples of δ are distinct infinitesimals.
If k is a natural number, $k\delta < \frac{1}{m}$, for any natural m, because $\delta < \frac{1}{km}$ when δ is infinitesimal.

$\boxed{\textit{Definition } 4.}$ A hyperreal number x is called limited if there is a natural number m so that $|x| < m$ (Denotation: $\mathcal{R}_{lim}$).
If there is no natural bound for a hyperreal number it is called unlimited (or infinite). (Denotation: $\mathcal{R}_{unlim}$).

Example. Infinitesimal numbers are limited, being bounded by 1.

Proposition 4.

Every limited hyperreal number x differs from some real number by an infinitesimal, that is, there is a real r so that $x \approx r$. This number is called the "standard part" of x (Notation: $r = st[x]$).

Proof. Define a Dedekind cut in the real numbers by $A = \{s : s \leq x\}$ and $B = \{s : x < s\}$. Then $st[x]$ is the real number defined by this cut. ■

Remark. The real numbers are Dedekind complete. Sometimes we think of this result as saying the real numbers are the points on a line with no gaps. The Theorem above says all the limited hyperreals are clustered around real numbers. When we take a line with no gaps and add lots of infinitesimals around each point, we create gaps! The cut in the hyperreals consisting of all numbers that are either negative or infinitesimal on one hand or positive and non-infinitesimal on the other has no number at the cut. There is no largest infinitesimal because twice that number would be infinitesimal and there is no smallest positive non-infinitesimal, because half of it would be infinitesimal, and then twice that also infinitesimal.

Proposition 5.

(a) If p and q are limited, so are $p + q$ and pq.
(b) If ϵ and δ are infinitesimal, so is $\epsilon + \delta$.
(c) If $\delta \approx 0$ and q is finite, then $q\delta \approx 0$.
(d) $\frac{1}{x}$ is unlimited only when $x \approx 0$.

Proof. Exercise!

Keisler's Function Extension Axiom

Roughly speaking, Keisler's Function Extension Axiom says that all real functions have extensions to the hyperreal numbers and these "natural" extensions obey the same identities and inequalities as the original function. Some familiar identities are $sin(x+y) = sin(x)cos(y) + cos(x)sin(y)$ or $log(xy) = log(x) + log(y)$.
The *log* identity only holds when x and y are positive. Keisler's Function Extension Axiom is formulated so that we can apply it to the Log identity in the form of the implication

$(x > 0 \text{ and } y > 0) \Rightarrow log(x) \text{ and } log(y) \text{ are defined and } log(xy) = log(x)+log$

Keisler's Function Extension Axiom

Every real function $f(x_1, x_2, \ldots, x_n)$ has a "natural" extension to the hyperreals such that every logical real statement that holds for all real numbers also holds for all hyperreal numbers when the real functions in the statement are replaced by their natural extensions.

There are two general uses of the Function Extension Axiom that underlie most of the theoretical problems in calculus. These involve extension of the discrete maximum and extension of finite summation. The proof of the Extreme Value Theorem below uses a hyperfinite maximum, while the proof of the Fundamental Theorem of Integral Calculus uses hyperfinite summation and a maximum.

Equivalence of infinitesimal conditions and the "epsilon - delta" real number conditions are usually proved by using an auxiliary real function as in the following theorem.

Theorem 6.

Let $f(x)$ be a real valued function defined for $0 < |x-a| < \Delta$ with Δ a fixed positive real number. Let b be a real number. Then the following are equivalent:
(a) Whenever the hyperreal number x satisfies $a \neq x \approx a$, the natural extension function satisfies $f(x) \approx b$
(b) For every real accuracy tolerance θ there is a sufficiently small positive real number γ such that if the real number x satisfies $0 < |x-a| < \gamma$, then $|f(x) - b| < \theta$

Proof. We show that $(a) \Rightarrow (b)$ by proving that not (b) implies not (a), the contrapositive. Assume (b) fails. Then there is a real $\theta > 0$ such that for every real $\gamma > 0$ there is a real x satisfying $0 < |x-a| < \gamma$ and $|f(x) - b| \geq \theta$. Let $X(\gamma) = x$ be a real function that chooses such an x for a particular γ. Then we have the equivalence

$$\gamma > 0 \Leftrightarrow (X(\gamma) \text{ is defined}, 0 < |X(\gamma) - a| < \gamma, |f(X(\gamma)) - b| \geq \theta)$$

By the Function Extension Axiom this equivalence holds for hyperreal numbers and the natural extensions of the real functions X and f. In particular, choose a positive infinitesimal γ and apply the equivalence. We have $0 < |X(\gamma) - a| < \gamma$ and $|f(X(\gamma)) - b| > \theta$ and θ is a positive real number. Hence, $f(X(\gamma))$ is not infinitely close to b, proving not (a) and completing the proof that (a) implies (b).

Conversely, suppose that (b) holds. Then for every positive real θ, there is a positive real γ such that $0 < |x - a| < \gamma$ implies $|f(x) - b| < \theta$. By the Function Extension Axiom, this implication holds for hyperreal numbers. If $\xi \approx a$, then $0 < |\xi - a| < \gamma$ for every real γ, so $|f(\xi) - b| < \theta$ for every real positive θ. In other words, $f(\xi) \approx b$ ■

Theorem 7.

Suppose $f(x)$ and $f'(x)$ are real functions defined on the open real interval (a, b). The following are equivalent definitions of, "The function $f(x)$ is smooth with continuous derivative $f'(x)$ on (a, b)." :

(a) Whenever a hyperreal x satisfies $a < x < b$ and x is not infinitely near a or b, then an infinitesimal increment of the extended dependent variable is approximately linear on a scale of the change, that is, whenever $\delta x \approx 0$

$$f(x + \delta x) - f(x) = f'(x)\delta x + \epsilon\delta x \text{ with } \epsilon \approx 0$$

(b) For every compact subinterval $[\alpha, \beta] \subset (a, b)$, the real limit

$$lim_{\Delta x \to 0} \frac{f(x + \Delta x) - f(x)}{\Delta x} = f'(x) \text{ uniformly for } \alpha \leq x \leq b$$

(c) For every pair of hyperreal $x_1 \approx x_2$ with $a < st(x_i) = c < b$, $\frac{f(x_2) - f(x_1)}{x_2 - x_1} \approx f'(c)$

Proof. Exercise!

The Inverse Function Theorem

If m is a nonzero real number and the real function $f(x)$ is defined for all $x \approx x_0$, a real x_0 with $y_0 = f(x_0)$ and $f(x)$ satisfies

$$\frac{f(x_2) - f(x_1)}{x_2 - x_1} \text{ whenever } x_1 \approx x_2 \approx x_0$$

then $f(x)$ has an inverse function in a small neighborhood of x_0 , that is, there is a real number $\Delta > 0$ and a smooth real function $g(y)$ defined when $|y - y_0| < \Delta$ with $f(g(y)) = y$ and there is a real $\epsilon > 0$ such that if $|x - x_0| < \epsilon$, then $|f(x) - y_0| < \Delta$ and $g(f(x)) = x$.

Proof. Elementary, but boring. ∎

We've seen the axiomatics of the fields $\mathcal{S}_{Fie}$. Let's add some more conditions.

- Characteristic p fields:

$$\Sigma_{Fields_p} = \mathcal{S}_{Fie} \cup \{\underbrace{1 + 1 \ldots 1}_{p} = 0\}$$

- Characteristic 0 fields:

$$\Sigma_{Fields_0} = \mathcal{S}_{Fie} \cup \{\underbrace{1 + 1 \ldots 1}_{p} \neq 0\}$$

- Algebraically closed fields:

$$\Sigma_{ACF} = \mathcal{S}_{Fie} \cup \{\forall a_0 \forall a_1 \ldots \forall a_n \exists r\ [a_n r^n + a_{n-1} r^{n-1} + \ldots + a_0 = 0]\ n \in \mathbb{N}\}$$

Lefschetz Principle.

Let $\mathcal{C} = \{\mathbb{C}, 0, 1, +, -, \cdot\}$ For a sentence ϕ the following are equivalent

1.) $\mathbb{C} \models \phi$.
2.) $\mathcal{K} \models \phi$, for some $\mathcal{K} \models \Sigma_{ACF_0}$.
3.) $\Sigma_{ACF_0} \models \phi$.
4.) For sufficiently large primes p, $\Sigma_{ACF_p} \models \phi$.
5.) For infinitely-many primes p, there is $\mathcal{K} \models \Sigma_{ACF_p}$ such that $\mathcal{K} \models \phi$

Proof. $1 \Leftrightarrow 2 \Leftrightarrow 3$ follows from the so-called Los-Vaught test (see also chapter X, Theorem 4.2 of Manin, "A course in Mathematical Logic for Mathematicians").
3) $\Rightarrow$ 4) By the Compactness theorem, there is a finite $T \subseteq \Sigma_{ACF_0}$ such that $T \models \phi$. But then, by the definitions of Σ_{ACF_0} and Σ_{ACF_p}, for sufficiently large prime p, $\Sigma_{ACF_p} \models T$, so $\Sigma_{ACF_p} \models \phi$.
4) $\Rightarrow$ 5) is trivial.
5) $\Rightarrow$ 3) We prove the contrapositive: assume (3) fails. But then $\Sigma_{ACF_0} \models \neg\phi$ and hence, by 3) $\Rightarrow$ 4) for sufficiently large primes p, $\Sigma_{ACF_p} \models \neg\phi$. Therefore 5) is false. ■

Ax's Theorem.

Let $f : \mathbb{C}^n \to \mathbb{C}^n$ be a polynomial map, i.e. $f = (f_1, \ldots, f_n)$, where each $f_i(z_1, \ldots, z_n)$ is a polynomial in $z_1, \ldots, z_n$ with coefficients in $\mathbb{C}$. If f is injective then it is surjective.

Proof. For fixed n and fixed degree $d := max_i deg(f_i)$, the statement is first-order expressible by a sentence $\phi_{n,d}$, and hence, instead of proving it for the field $\mathbb{C}$, by the Lefschetz principle, it is enough to prove $\phi_{n,d}$ for the algebraic closure $\bar{\mathbb{F}}_p = \cup_{k\in\mathbb{N}} F_k$ of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, for all primes p. So, fix a polynomial map $f : \bar{\mathbb{F}}_p^n \to \bar{\mathbb{F}}_p^n$ of degree d. Thus, letting $k_0 \geq 0$ be large enough so that all of the coefficients involved in the definition of f are in F_{k_0} , we can write: $\bar{\mathbb{F}}_p^n = \cup_{k\geq k_0} F_k^n$.

But then, because F_k is a field and the definition of f only uses field operations and elements of F_k, F_k^n is closed under f , i.e. $f(F_k^n) \subset F_k^n$, for all $k \geq k_0$. Because f is injective, the Pigeonhole Principle gives $f(F_k^n) = F_k^n$, so

$$f(\bar{\mathbb{F}}_p^n) = f(\cup_{k\geq k_0} F_k^n) = \cup_{k\geq k_0} f(F_k^n) = \cup_{k\geq k_0} F_k^n = \bar{\mathbb{F}}_p^n \qquad \blacksquare$$

Exercises

Exercise 1. (a) $\mathcal{R}_{lim}$ is a subring of $\mathcal{R}$.
(b) The set of infinitesimal hyperreals μ is an ideal in $\mathcal{R}_{lim}$.
(c) The map $st : \mathcal{R}_{lim} \to \mathbb{R}$ is a ring homomorphism.
(d) $\mathcal{R}_{lim}/\mu \cong \mathbb{R}$.

Exercise 2. For a sequence $(s_n)_{n\in\mathbb{N}}$ and $L \in \mathbb{R}$, $s_n \to L$ if and only if $s_N \approx L$ for all $N \in \mathcal{N} \setminus \mathbb{N}$.