Ultraproducts, asymptotics, and model theory

Frank O. Wagner
Institut Camille Jordan
Université Claude Bernard Lyon 1
France

27 August 2014

Plan

Limits

Recall that given a sequence $(r_n : n \in \mathbb{N})$ of real numbers, a real number r is the *limit* of the sequence if for all $\epsilon > 0$ there is n_ϵ such that $|r - r_n| < \epsilon$ for all $n \geq n_\epsilon$.

Similarly, for any sequence $(\bar{r}_n : n \in \mathbb{N})$ in $\mathbb{R}^n$, a vector $\bar{r}$ is the *limit* of the sequence if for all $\epsilon > 0$ there is n_ϵ such that $\|\bar{r} - \bar{r}_n\| < \epsilon$ for all $n \geq n_\epsilon$.

This can be generalized to any metric space, and in fact to any topological space $\mathfrak{X}$: A point $P \in \mathfrak{X}$ is a *limit* of the sequence $(P_n : n \in \mathbb{N})$ if for any neighbourhood $\mathfrak{O}$ of P there is $n_{\mathfrak{O}} \in \mathbb{N}$ such that $P_i \in \mathfrak{O}$ for all $n \geq n_{\mathfrak{O}}$.

Existence

However, not all sequences have a limit. For instance, the sequence $(\frac{1}{n} : n \in \mathbb{N})$ in $(0, 1]$ does not have a limit in $(0, 1]$. Similarly, a sequence of rational numbers approaching π does not have a limit in $\mathbb{Q}$.

In the above examples it is easy just to add the limit point to the ambient space. This is slightly more difficult for the sequence $(n : n \in \mathbb{N})$ in $\mathbb{N}$ (or $\mathbb{R}$): One has to add a suitable point at infinity. However, some sequences such as $((-1)^n : n \in \mathbb{N})$ just do not have a limit.

To some extent this may be remedied via the notion of an *accumulation point: P* is an accumulation point of the sequence $(P_n : n \in \mathbb{N})$ if any neighbourhood $\mathfrak{O}$ of P contains infinitely many points of the sequence.

However, we would like to have a method to somehow choose a particular limit point.

Ultrafilters

Let I be a set (of indices), for instance $I = \mathbb{N}$. A non-empty collection $\mathfrak{F}$ of subsets of I is called a *filter* if it satisfies:

- If $X \in \mathfrak{F}$ and $X \subseteq Y \subseteq I$, then $Y \in \mathfrak{F}$.
- If $X \in \mathfrak{F}$ and $Y \in \mathfrak{F}$, then $X \cap Y \in \mathfrak{F}$.
- $\emptyset \notin \mathfrak{F}$.

It is an *ultrafilter* if in addition

- For any $X \subseteq I$, either $X \in \mathfrak{F}$ or $I \setminus X \in \mathfrak{F}$.

For instance, for any $x \in I$ the collection

$$\{X \subseteq I : x \in X\}$$

forms an ultrafilter, the *principal ultrafilter generated by x*.
If I is infinite, then the collection of *co-finite* subsets of I forms a filter, the *Frechet filter* on I.
It follows from the axiom of choice that every filter can be completed to an ultrafilter. In fact, this condition is slightly weaker than the axiom of choice.

Limits along an ultrafilter

Now let X be a closed an bounded subset of $\mathbb{R}^n$ (or more generally a compact Hausdorff topological space). Consider a sequence $(P_i : i \in I)$. Then any non-principal ultrafilter $\mathfrak{U}$ on I determines a unique point $P_{\mathfrak{U}} \in X$ such that for any neighbourhood $\mathfrak{O}$ of $P_{\mathfrak{U}}$ the set

$$\{i \in I : P_i \in \mathfrak{O}\}$$

is in $\mathfrak{U}$. This point is the limit of the sequence along $\mathfrak{U}$.

We now want to do such a limit construction not only for points in a compact space, but for arbitrary mathematical structures.

Structures

A *structure* $\mathfrak{M}$ is just a set M, its *domain*, together with some functions $\{f_i^{\mathfrak{M}} : i \in I_1\}$ and some relations $\{R_i^{\mathfrak{M}} : i \in I_2\}$ of arbitrary finite arity.
The relations are supposed to include equality, although this will not be mentioned explicitly.
We can also name some particular constants $\{c_i^{\mathfrak{M}} : i \in I_0\}$, although we shall be allowed to use any element of M as parameter.
The set

$$\mathcal{L} = \{c_i : i \in I_0\} \cup \{f_i : i \in I_1\} \cup \{R_i : i \in I_2\}$$

of (symbols for the) functions, relations and constants forms the *language* of the structure $\mathfrak{M}$.

Structures

Examples

- A graph $\langle V, E\rangle$.
- A partial order $\langle X, \leq\rangle$.
- A group $\langle G, 1, \cdot, ^{-1}\rangle$
- An ordered field $\langle K, 0, 1, +, -, \cdot, \leq\rangle$.

Formulas

Using parameters, variables, the functions and relations, logical connectives $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$ (negation, conjunction, disjunction, implication, equivalence) and quantifiers $\forall$, $\exists$ (universal, existential), we can build meaningful statements called *formulas*.

A formula without free variables is a *sentence*.

These formulas are interpreted in $\mathfrak{M}$ in the natural way.

If $\varphi(\bar{x})$ is a formula with free variables $\bar{x}$ and $\bar{m}$ a tuple of elements of $\mathfrak{M}$ of the same length, then $\varphi(\bar{m})$ is a sentence, canonically interpreted in $\mathfrak{M}$ (and hence either true or false).

Note that we can only quantify over the elements of M.

Examples

1. An equivalence relation.
   - $\forall x \;\; E(x,x)$.
   - $\forall x \forall y \;\; (E(x,y) \to E(y,x))$.
   - $\forall x \forall y \forall z \;\; ((E(x,y) \wedge E(y,z)) \to E(x,z))$.
2. A partial order.
   - $\forall x \;\; (x \leq x)$.
   - $\forall x \forall y \;\; ((x \leq y \wedge y \leq x) \to x = y)$.
   - $\forall x \forall y \forall z \;\; ((x \leq y \wedge y \leq z) \to x \leq z)$.
3. A group.
   - $\forall x \forall y \forall z \;\; (x \cdot y) \cdot z = x \cdot (y \cdot z)$.
   - $\forall x \;\; (x \cdot x^{-1} = 1 \wedge x^{-1} \cdot x = 1)$
   - $\forall x \;\; (x \cdot 1 = x \wedge 1 \cdot x = x)$

Examples

1. The sentence

$$\forall x \forall y \exists z_0 \ldots \exists z_n \; (x = z_1 \wedge y = z_n \wedge \bigwedge_{i<n} E(z_i, z_{i+1}))$$

says that the graph is connected of diameter at most n.

2. The sentence

$$\neg \exists x_0 \ldots \exists x_n \; \bigwedge_{i<n} x_i < x_{i+1}$$

signifies that the partial order has height n, i.e. there are no chains of length $n+1$.

3. The sentence

$$\forall x \; \underbrace{x \cdot x \cdots x}_{n \text{ times}} = 1$$

tells us that the group has exponent dividing n.

However, in the previous sentences

$$\forall x \forall y \exists z_0 \ldots \exists z_n \ \left(x = z_1 \wedge y = z_n \wedge \bigwedge_{i<n} E(z_i, z_{i+1})\right)$$

$$\neg \exists x_0 \ldots \exists x_n \ \bigwedge_{i<n} x_i < x_{i+1}$$

$$\forall x \ \underbrace{x \cdot x \cdots x}_{n \text{ times}} = 1$$

we cannot quantify over *n*. In particular, we cannot easily express that a graph is connected, that a partial order has finite height, or that a group has finite exponent.
In fact, this is outright impossible, due to the so-called *compactness theorem*.

Finite products

Given two groups G_1 and G_2, we can form the direct product

$$G_1 \times G_2 = \{(g, h) : g_1 \in G_1, g_2 \in G_2\}$$

with group multiplication

$$(g_1, g_2) \cdot (g_1', g_2') = (g_1 \cdot g_1', g_2 \cdot g_2').$$

It is again a group.
Similarly, for two rings R_1 and R_2, we can from the direct product $R_1 \times R_2$ where addition and multiplication is componentwise. It is again a ring.
If R_1 and R_2 are fields, the direct product is not a field, but only a ring.
We can divide out by a maximal ideal I and obtain a field $(R_1 \times R_2)/I$. If G_1 and G_2 are simple groups, we can divide out by a maximal normal subgroup N and obtain a simple group $(G_1 \times G_2)/N$. However, the resulting object will be isomorphic to one of the coordinates.

Infinite products

This is different if we consider an infinite product

$$\prod_{i \in I} G_i = \{(g_i : i \in I) : g_i \in G_i \text{ for all } i \in I\}$$

or

$$\prod_{i \in I} R_i = \{(r_i : i \in I) : r_i \in R_i \text{ for all } i \in I\}$$

with componentwise additon and/or multiplication. We may again divide out by a normal subgroup/maximal ideal, but the properties of the resulting group/ring quotient will depend heavily on the normal subgroup/ideal chosen, and it is not onvious which one to choose to obtain a particular property.
Moreover, we should like to form a product of arbitrary structures, not just algebraic ones.

Ultraproducts

Let $\{\mathfrak{M}_i : i \in I\}$ be a family of structures in the same language $\mathcal{L}$, and $\mathfrak{U}$ an ultrafilter on I.
The *ultraproduct* $\prod_I \mathfrak{M}_i/\mathfrak{U}$ will be the following structure:

- The domain of $\mathfrak{M}$ is the product $\prod_{i\in I} M_i$ modulo the equivalence relation $\sim$ given by:

  $$(a_i : i \in I) \sim (b_i : i \in I) \text{ if and only if } \{i \in I : a_i = b_i\} \in \mathfrak{U}.$$

The class of a tuple $(a_i : i \in I)$ modulo $\sim$ is denoted by $[a_i]_I$.

- For a constant symbol $c \in \mathcal{L}$ we interpret c in $\mathfrak{M}$ by

  $$c^{\mathfrak{M}} = [c^{\mathfrak{M}_i}]_I.$$

- For an n-ary function symbol $f \in \mathcal{L}$ we put

  $$f^{\mathfrak{M}} : ([a_i^1]_I, \ldots, [a_i^n]_I) \mapsto [f^{\mathfrak{M}_i}(a_i^1, \ldots, a_i^n)]_I.$$

- For an n-ary relation symbol $R \in \mathcal{L}$ we define $R^{\mathfrak{M}}$ as

  $$\{([a_i^1]_I, \ldots, [a_i^n]_I) \in M^n : \{i \in I : (a_i^1, \ldots, a_i^n) \in R^{\mathfrak{M}_i}\} \in \mathfrak{U}\}.$$

Of course, one has to check that $\sim$ is indeed an equivalence relation, and that the functions $f^{\mathfrak{M}}$ and relations $R^{\mathfrak{M}}$ are well-defined and do not depend on the representative chosen for its argument. This follows easily from the filter properties of $\mathfrak{U}$.

If $\mathfrak{U}$ is the principal ultrafilter generated by i_0, then $\prod_I \mathfrak{M}_i/\mathfrak{U}$ is canonically isomorphic to $\mathfrak{M}_{i_0}$.

If all $\mathfrak{M}_i$ are equal, the diagonal map $m \mapsto [m]_I$ gives a canonical embedding of $\mathfrak{M}_0$ into $\mathfrak{M}$.

Łos' Theorem

Let $\mathfrak{M} = \prod_I \mathfrak{M}_i/\mathfrak{U}$ be the ultraproduct of a family $(\mathfrak{M}_i : i \in I)$ of $\mathcal{L}$-structures modulo the ultrafilter $\mathfrak{U}$ on I.
Consider a formula $\varphi(x_1, \ldots, x_n)$ with free variables $x_1, \ldots, x_n$, and an n-tuple $([m_i^1]_I, \ldots, [m_i^n]_I)$ of elements of $\mathfrak{M}$.

Theorem (Łos)

The sentence $\varphi([m_i^1]_I, \ldots, [m_i^n]_I)$ is true in $\mathfrak{M}$ if and only if

$$\{i \in I : \varphi(m_i^1, \ldots, m_i^n) \text{ is true in } \mathfrak{M}_i\} \in \mathfrak{U}.$$

Corollaries

It follows that if (almost) all structures $\mathfrak{M}_i$ have a property expressible in the language $\mathcal{L}$ by a sentence or a collection of sentences, then any ultraproduct $\prod_I \mathfrak{M}_i/\mathfrak{U}$ again has this property.
In particular, an ultraproduct of algebraically closed fields is again an algebraically closed field, and an ultraproduct of real closed fields is again real closed.
If m_i and n_i have distance i in the graph $\mathfrak{M}_i$, then $[m_i]_I$ and $[n_i]_I$ have infinite distance in the graph $\prod_I \mathfrak{M}_i/\mathfrak{U}$;
if g_i has order i in the group G_i, then $[h_i]_I$ has infinite order in the group $\prod_I G_i/\mathfrak{U}$ (unless $\mathfrak{U}$ is principal).
This shows that connectivity or finite exponent is not expressible by a formula or a set of formulas (unless the diameter or the exponent is bounded).

The Compactness Theorem

The compactness theorem is the most fundamental theorem in model theory and is used practically everywhere.

Let Φ be a collection of sentences.
We shall say that a structure $\mathfrak{M}$ is a *model* of Φ if every sentence of Φ is true in $\mathfrak{M}$.

Theorem (Compactness)

A collection Φ of sentences has a model if and only if every finite subcollection has a model.

The direction from left to right is obvious.

The Completeness Theorem

The semantic notion of model is related to the syntactic notion of consistency via Gödel's Completeness Theorem:

Theorem (Completeness)

Φ has a model if and only if Φ is consistent.

The Compactness Theorem is an easy consequence of the Completeness Theorem:
If Φ has no model, then it is inconsistent and there is a proof of inconsistency from Φ. This proof uses only finitely many hypotheses $\Phi_0 \subseteq \Phi$, so Φ_0 is inconsistent and does not have a model.
Conversely, the Completeness Theorem can be deduced from the Compactness Theorem.

Proof of the Compactness Theorem

Let I be the collection of finite subsets of Φ. By hypothesis, for every $i \in I$ there is a model $\mathfrak{M}_i$ of i. Let $\mathfrak{F}$ be the filter generated by the sets

$$I_i = \{j \in I : i \subseteq j\}$$

for $i \in I$. Note that $I_i \cap I_j = I_{i \cup j}$, so this generates indeed a filter. Let $\mathfrak{U}$ be an ultrafilter extending $\mathfrak{F}$, and $\mathfrak{M} = \prod_I \mathfrak{M}_i / \mathfrak{U}$.

If $\varphi \in \Phi$, then φ is true in $\mathfrak{M}_i$ for all $i \in I_{\{\varphi\}}$. Since $I_{\{\varphi\}} \in \mathfrak{F} \subseteq \mathfrak{U}$, by Łos' Theorem φ is true in $\mathfrak{M}$.

Examples

Let $\mathfrak{U}$ be a non-principal ultrafilter on $\mathbb{N}$. Put

$$\mathbb{N}^* = \prod_{\mathbb{N}} \mathbb{N}/\mathfrak{U}.$$

This is a non-standard model of the natural numbers; an element $n^* \in \mathbb{N}^* \setminus \mathbb{N}$ is called a *non-standard integer*. For instance, the element $[n!]_{\mathbb{N}}$ is greater than every (standard) integer, and divisible by all (standard) prime numbers.

Examples

Put $\mathbb{R}^* = \prod_{\mathbb{N}} \mathbb{R}/\mathfrak{U}$.
This is a non-standard model of the real numbers; an element $r^* \in \mathbb{R}^* \setminus \mathbb{R}$ is called a *non-standard real*.
For instance, the element $\epsilon = [\frac{1}{n}]_{\mathbb{N}}$ is strictly positive but smaller than $\frac{1}{k}$ for all (standard) $k > 0$, a so-called *infinitesimal* element.
An element of $\mathbb{R}^*$ is *bounded* if there is $r \in \mathbb{R}$ with $|r^*| \leq r$; since $\mathbb{R}$ is complete, for every bounded non-standard real r^* there is a unique standard real $\mathrm{st}(r^*) \in \mathbb{R}$ infinitesimally close to r^*. The map st is the *standard part map*.
A function $f : \mathbb{R} \to \mathbb{R}$ gives rise to a function $f^* : \mathbb{R}^* \to \mathbb{R}^*$.
Then f is derivable at x if and only if

$$\mathrm{st}\left(\frac{f^*(x+\epsilon) - f^*(x)}{\epsilon}\right) = f'(x)$$

does not depend on the infinitesimal ϵ.

Examples

Let K_p be an algebraically closed field of characteristic p, for instance the algebraic closure of $\mathbb{Z}/p\mathbb{Z}$. If $\mathfrak{U}$ is a non-principal ultrafilter on the set $\mathfrak{P}$ of primes, put

$$K = \prod_{\mathfrak{P}} K_p/\mathfrak{U}.$$

This is an algebraically closed field of characteristic zero. If all K_p are countable, K is of size continuum, and hence isomorphic to the complex numbers $\mathbb{C}$.
It follows that a sentence is true in $\mathbb{C}$ if and only if it is true in all but finitely many K_p (transfer principle).

Pseudo-finite structures

An $\mathcal{L}$-structure $\mathfrak{M}$ is *pseudo-finite* if it is infinite and satisfies all sentences true in all finite $\mathcal{L}$-structures.

Examples of such sentences:

- An injective function from a set to itself is surjective.
- A partially ordered set has minimal and maximal elements.
- A totally ordered set has a maximum and a minimum.

Theorem

A stucture is pseudo-finite if and only if it satisfies the same sentences as some ultraproduct of finite structures.

Pseudo-finite fields

The first use of pseudo-finiteness was in Ax' characterization of the asymptotic theory of finite fields.

A field K of characteristic p is *perfect* if every element has a (unique) p-th root.
K is *pseudo-algebraically closed* if every variety which is irreducible over the algebraic closure $\widetilde{K}$ has a K-rational point.

Theorem (Ax)

A field K is pseudofinite if and only if it is perfect, pseudo-algebraically closed, and has exactly one extension of degree n for every $n > 0$.

Internal sets

Given an ultraproduct $\mathfrak{M} = \prod_I \mathfrak{M}_i/\mathfrak{U}$, a subset A of $\mathfrak{M}$ is *internal* if it is of the form $\prod_I A_i/\mathfrak{U}$ for some sequence of subsets $A_i \subseteq M_i$.

Internal sets of $\mathbb{R}^*$ and $\mathbb{N}^*$ are one of the main tools of non-standard analysis.

Counting

If A is a pseudo-finite internal subset in an ultraproduct $\mathfrak{M} = \prod_I \mathfrak{M}_i/\mathfrak{U}$, then the cardinality $n(A_i)$ is finite for almost all i. We define the non-standard cardinality of A to be the non-standard integer

$$n^*(A) = [n(A_i)]_I \in \mathbb{N}^* = \prod_I \mathbb{N}/\mathfrak{U}.$$

It quantifies the growth rate of $(n(A_i) : i \in I)$.

The non-standard cardinality is invariant under internal bijections: If $\sigma_i : A_i \to B_i$ is a bijection in $\mathfrak{M}_i$ for all $i \in I$, then $\sigma = \prod_I \sigma_i/\mathfrak{U} : A \to B$ is a bijection in $\mathfrak{M}$ preserving cardinality.

Measure

If M is an ultraproduct, an *internal measure* on M is a finitely additive map from the collection of all internal subsets of M to $\mathbb{R}^{\geq 0} \cup \{\infty\}$, i.e. for all disjoint internal subsets A, B of M

$$\mu(A \cup B) = \mu(A) + \mu(B).$$

The union of a countable family of internal sets is in general not internal, so we cannot ask for countable additivity.
Clearly for any pseudo-finite A, the map

$$\mu(B) = \mathrm{st}\left(\frac{n^*(B)}{n^*(A)}\right)$$

is an internal measure on A with $\mu(A) = 1$.
In particular, a pseudo-finite group is *internally amenable*.

Approximate subgroups

Let G be a group. A subset A of G is *symmetric* if $1 \in A$ and $a \in A$ implies $a^{-1} \in A$. A symmetric subset A is a *k-approximate subgroup* of G if

$$A^2 = \{a \cdot a' : a, a' \in A\}$$

is covered by k-left translates of A.

A subset is a 1-approximate subgroup if and only if it is a real subgroup.

A d-dimensional symmetric arithmetic progession

$$\{k_1 b_1 + \cdots + k_d b_d : -n_i \leq k_i \leq n_i \text{ for } 1 \leq i \leq d\}$$

is a 2^d-approximate subgroup. This can be generalized to the nilpotent case, the so-called *nilprogressions*.

Breuillard, Green and Tao have recently classified finite approximate subgroups. They show that they are essentially an extension of a nilprogression by a real subgroup.

Approximate subgroups

The classification theorem implies Gromov's theorem on groups of polynomial growth.

In fact, the proofs of either theorem proceed by first constructing a homomorphism into a finite-dimensional real Lie group. This homomorphism can be obtained via an ultraproduct construction.

One first considers a sequence $(G_i, A_i : i \in \mathbb{N})$ of k-approximate subgroups with $n(A_i) \to \infty$.

If $\mathfrak{U}$ is a non-principal ultrafilter on $\mathbb{N}$, the ultraproduct $A = \prod_I A_i/\mathfrak{U}$ is a pseudo-finite k-approximate subgroup of $G = \prod_I G_i/\mathfrak{U}$.

One then constructs of sequence $(X_j : j \in \mathbb{N})$ of internal symmetric subsets of A^4 such that

$$(X_{j+1}^2)^A \subseteq X_j$$

and $\mu(X_j) > 0$ for all $j \in \mathbb{N}$, where μ is the internal measure normalized at A. Then $N = \bigcap_{j\in\mathbb{N}} X_j$ is an actual normal subgroup of $\langle A \rangle$.

We can define a topology on $\langle A\rangle/N$ whose closed sets are those whose pre-image in $\langle A\rangle$ are the whole set, or intersections of internal sets.

The condition that $\mu(X_j) > 0$ for all $j \in \mathbb{N}$ yields that the topology is locally compact. The characterization of locally compact groups allows us to modify A and N slightly, so that the locally compact quotient becomes a finite-dimensional real Lie group.

Now pseudo-finiteness is used (in a highly non-trivial way) to show that the Lie group is nilpotent, and A/N is a non-standard nilprogression. Pulling back to the A_i yields the result.

Thank You